

ID 2912 - Gara a procedura aperta, suddivisa in due Lotti, per l'acquisizione dei servizi di conduzione, manutenzione e supporto specialistico per la gestione e l'evoluzione dell'infrastruttura ICT di INAIL

**Appendice 1 al Capitolato tecnico
Contesto tecnologico ed infrastrutturale**

CLASSIFICAZIONE CONSIP: AMBITO PUBBLICO

INDICE

1. PREMESSA	6
2. SISTEMI	9
2.1. Sistemi centrali	10
2.1.1. Sistemi IBM System P E980 Power	10
2.1.2. Sistemi IBM System P 10 Power	12
2.1.3. Sistemi Intel x86 e Farm VMware	12
2.1.4. Ambiente CLOUD	18
2.2. Sistemi periferici	20
2.3. Sistemi Centro Protesi INAIL	21
2.4. Postazioni di lavoro	21
2.5. Cooperazione Applicativa	21
2.5.1. Porta di Dominio	22
2.6. Posta Elettronica PEL e PEC	26
2.7. Infrastruttura Active Directory	27
2.8. Sistema Documentale Centralizzato	28
2.9. Data Lake	28
3. SERVICE ORIENTED ARCHITECTURE (SOA)	29
4. SOASEC	30
Descrizione architettura di riferimento	30
4.1.1. Architettura fisica	32
5. API REST GATEWAY	33
5.1. Architettura di riferimento	35
5.2. Piattaforma Digital Nazionale Dati	36
5.3. Nuovo modello interoperabilità (MoDI)	36
5.4. I profili di sicurezza INAIL	37
5.5. Azure API Manager	38

5.5.1.	Architettura di riferimento	41
5.6.	IBM Aspera	41
6.	OCP	43
7.	SISTEMI DI MESSAGING	45
8.	DATABASES SQL E NOSQL	46
9.	APPLICATION SERVER	47
10.	ARCHITETTURA TECNOLOGICA E INFORMATIVA DI PORTALE	48
10.1.	Il portale pubblico	48
10.1.1.	Adobe Experience Manager (cloud)	48
10.2.	Sistemi integrati nel portale	51
10.3.	Gestione accessi e profilazione	52
10.4.	Il post login utenti esterni: da PLAP a MyInail.....	52
10.4.1.	Il post login evoluto: la MyInail.....	53
10.4.2.	La chatbot di assistenza	54
10.5.	Il post login utenti interni: il Digital Workplace	55
10.6.	Architetture Ancillari	56
10.6.1.	Ambienti di staging	56
10.6.2.	Consultazione Amministrazione Trasparente (CAT)	57
10.6.3.	Campagne e survey.....	58
10.6.4.	Analytics.....	58
10.6.5.	Multimedia.....	59
10.6.6.	Esercizio applicativo del portale	60
11.	STRUMENTI DI NOTIFICA APPLICATIVA E CAMPAGNE	61
11.1.	Gestione Posta Multicanale (GPM)	61
11.2.	Gestore eventi	63
11.3.	Notification Gateway (NGW)	65
11.4.	Adobe Journey Optimizer (AJO)	65
11.5.	Microsoft Dynamics / Customer Voices	66

12. INFRASTRUTTURE DI RETE	68
12.1. Architettura generale di Rete	68
12.2. Connettività verso Infranet	69
12.3. Reti Locali	69
12.4. Connettività verso Internet	69
12.5. Architettura Sedi, Direzioni Regionali e Direzione Generale.....	70
12.6. Architettura Agenzie	70
12.7. Collegamento ADSL Telelavoratori.....	70
12.8. Wireless (Mobile e WI-FI).....	70
13. PUNTO DI ACCESSO POLISWEB	72
13.1. Servizio PDA PolisWeb	72
13.1.1. Architettura del PDA PolisWeb.....	72
13.1.2. Autenticazione e Autorizzazione	73
14. SICUREZZA	77
14.1. Identity Management	77
14.2. Tracciatura	77
14.3. Single Sign On INAIL	80
14.4. Sistema unico di profilazione	84
14.5. Servizi del Security Operations Center (SOC)	87
14.5.1. SOC – Log Management e Correlazione	90
14.5.2. SOC – Vulnerability Assessment	90
14.5.3. SOC – Network Forensics	90
14.6. Web Application Firewall (WAF)	90
14.7. System Center Configuration Management.....	90
14.8. Security Patch Management	91
14.9. Sicurezza delle connessioni	92
14.10. CERT	93
14.11. Firma Digitale Centralizzata	98

14.12.	Privacy e sicurezza delle informazioni.....	98
15.	PROGETTAZIONE E SVILUPPO DELLE APPLICAZIONI	102
15.1.	Servizi internet	103
15.2.	Servizi internet con funzionalità intranet.....	103
15.3.	I servizi intranet.....	104

1. PREMESSA

L'INAIL - Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro - persegue una pluralità di obiettivi tra cui ridurre, attraverso una intensa attività dedicata alla salute e sicurezza sul lavoro, il fenomeno infortunistico e tecnopatico, assicurare i lavoratori che svolgono attività a rischio, garantire il reinserimento nella vita lavorativa degli infortunati sul lavoro.

La tutela nei confronti dei lavoratori ha assunto sempre più le caratteristiche di un "sistema integrato" che va dagli interventi di prevenzione nei luoghi di lavoro, alle prestazioni sanitarie ed economiche, alle cure, alla riabilitazione e al reinserimento nella vita sociale e lavorativa.

L'Istituto ha, inoltre, assunto anche le competenze e le risorse degli enti disciolti ISPESL ed IPSEMA; ciò, da un punto di vista del business, ha comportato un incremento dei compiti istituzionali dell'INAIL.

In particolare, con l'incorporazione dell'ISPESL si sono aggiunte due nuove linee di business, quella della "Ricerca", in precedenza perseguita in maniera limitata e circoscritta ad alcuni settori ben definiti (es. Riabilitazione Motoria) e quella della "Verifica e certificazione", che estende l'azione di prevenzione, già assolta dall'INAIL, includendo l'attività di ispezione e di attestazione di conformità.

In sintesi, gli obiettivi dell'Istituto si realizzano in sei linee di business distinte, ciascuna con le proprie peculiarità per tipologia di clienti, stakeholder e modalità di servizio:

- Prevenzione;
- Rischi (Rapporto Assicurativo - Entrate);
- Prestazioni (Rapporto Assicurativo - Uscite);
- Riabilitazione e Prime cure;
- Ricerca;
- Verifica e Certificazione.

Tali linee di business costituiscono la cosiddetta "attività istituzionale" dell'INAIL e sono gestite da strutture organizzative dell'Istituto sia centrali che territoriali.

L'Istituto ha un modello funzionale che prevede strutture centrali e strutture decentrate su tutto il territorio nazionale. L'insieme delle strutture centrali (Direzioni Centrali, Servizi, Dipartimenti di Ricerca, Sovrintendenza Sanitaria Centrale, Avvocatura Generale, Consulenze professionali Centrali), costituisce la Direzione Generale, avente funzioni di direzione, coordinamento, indirizzo, programmazione e controllo.

A livello regionale operano le Direzioni Regionali con compiti di governo del territorio di competenza, supporto delle attività produttive, indirizzo e controllo a garanzia dell'omogeneità e della correttezza di funzionamento delle Direzioni Territoriali.

A livello sub-regionale operano le Direzioni Territoriali, articolate in Sedi Locali, che garantiscono la gestione dell'attività assicurativa e la tutela nei confronti dei lavoratori, attraverso un "sistema integrato" di interventi di prevenzione nei luoghi di lavoro, di prestazioni sanitarie ed economiche e di reinserimento sociale e

lavorativo e, pertanto, tutte le attività di gestione degli utenti esterni, con particolare riferimento agli assistiti, sono svolte a livello di Sedi periferiche.

Il Centro Protesi di Vigorso di Budrio e sue Filiali ed il Centro di Riabilitazione Motoria di Volterra operano nel contesto dei servizi di erogazione di protesi e ortesi ed offrono servizi riabilitativi finalizzati alla completa reintegrazione nel mondo del lavoro, nella famiglia, e più ampiamente nella società.

Ai Sistemi Informativi è demandata la complessa automazione di tutte le attività operative necessarie all'erogazione dei servizi e, pertanto, sotto la denominazione "sistemi istituzionali" sono raggruppati tutti i sistemi che automatizzano le attività delle singole linee di business. Ai sistemi istituzionali si affiancano i "sistemi gestionali" che automatizzano le funzioni aziendali di supporto.

Il sistema informatico dell'Istituto è, attualmente, costituito da più sistemi di elaborazione siti presso due Data Center della Direzione Centrale Organizzazione Digitale e da sistemi elaborativi siti presso le Direzioni Regionali e le Sedi Locali. Ai sistemi di elaborazione on premise si aggiungono sistemi in private e public cloud di tipo PaaS e SaaS che verranno meglio descritti nel seguito.

I sistemi sono interconnessi mediante la rete geografica SPC (Sistema Pubblico di Connettività). L'INAIL ha da tempo investito nelle architetture open coerentemente con le indicazioni tecnologiche del mercato e dell'Agenzia per l'Italia Digitale (ex DigitPA). Sono presenti sistemi operativi Linux e Windows su piattaforma x86, nonché LPAR IBM AIX su HW power, P8, p9 e p10 e RDBMS standard di mercato quali DB2, Oracle, SQLServer, MySQL, MongoDB e PostgreSQL.

Le procedure applicative in esercizio supportano tutte le attività istituzionali e gran parte delle esigenze strumentali, di controllo e informative dell'Istituto.

In sintesi, il sistema informativo e informatico dell'Istituto è, attualmente, costituito da:

- sistemi di elaborazione ospitati presso i Data Center della DCOD;
- sistemi di elaborazione periferici ospitati presso le Direzioni Regionali e le Sedi Locali;
- postazioni di lavoro (PC e stampanti) ad uso del personale, postazioni di servizio, personal computer portatili;
- Web Server Farm presso il Data Center della DCOD per la gestione dei servizi di interoperabilità, dei servizi web e di cooperazione applicativa costituito da sistemi in alta affidabilità ridondati per gli ambienti di collaudo, certificazione e produzione;
- rete geografica di interconnessione all'interno delle sedi INAIL (contesto Intranet), con le altre Pubbliche Amministrazioni (contesto Infranet) e verso la rete pubblica (contesto Internet);
- reti locali (LAN) presso le Sedi Locali, le Direzioni Regionali e le Direzioni Centrali (ivi compresi il Centro Protesi di Vigorso di Budrio e il CRM di Volterra);
- rete fonia VoIP (Voice over IP), apparecchi di telefonia mobile assegnati al personale;
- diverse tipologie di software di base;

- patrimonio applicativo e informativo che supporta tutte le attività istituzionali e gestionali dell'Istituto incrementato, come sopra detto, dopo l'incorporamento di ISPESL e IPSEMA.

L'Istituto ospita altre PA, in modalità housing e hosting. In particolare:

Housing: ISTAT, CONSAP, AGID, MEF/DAG;

Hosting:

- evoluto (INAIL fornisce anche servizi PaaS e servizi per il rilascio del SW): MdS;
- base (INAIL fornisce servizi di tipo IaaS): INMP.

Le attività di hosting e housing richiedono punti di raccordo specifici con le PA, ospitate attualmente su infrastrutture dedicate e, laddove previsto, su architetture diverse (housing).

2. SISTEMI

L'INAIL ha recentemente concluso un progetto "Data Center Transformation", al termine di un percorso di trasformazione e rinnovamento complessivo dal punto di vista tecnologico, impiantistico, gestionale e organizzativo. Il progetto, che ha avuto durata pluriennale, alla sua conclusione, ha portato alla costruzione di una infrastruttura tecnologica su due Data Center di Tier 3+ come definito da TEIA-942 e Uptime Institute. Tale progetto ha consentito all'INAIL di dotarsi di un'infrastruttura moderna ed efficiente tale da potersi candidare al ruolo di uno dei poli all'interno dei quali la Pubblica Amministrazione consoliderà le proprie dotazioni tecnologiche. Il programma ha inoltre portato al rinnovo tecnologico di oltre l'80% dell'hardware e la sostanziale rivoluzione dell'infrastruttura fisica che coinvolge tutte le sue componenti e i suoi livelli operativi.

Uno dei pilastri fondamentali del progetto è stata la virtualizzazione dei server che ha consentito di diminuire il numero dei server fisici riducendo in tempo reale consumi e costi di gestione, aumentando efficienza, affidabilità e disponibilità della potenza di calcolo.

Grazie a ciò, è stato possibile inoltre consolidare l'infrastruttura di Storage e Backup, riducendo allo stesso tempo il footprint del Data Center dell'Istituto, passando da oltre 1.000 metri quadrati a circa 300, incidendo sulla potenza elettrica necessaria e il relativo raffreddamento per circa il 75%. In questo modo, le infrastrutture necessarie a garantire la continuità di tutti i servizi INAIL presenti e futuri sono state dapprima ospitate nel Data Center che in precedenza era il sito Secondario e che in questa fase è diventato il sito Primario.

Il vecchio sito Primario (DCOD Santuario Regina Degli Apostoli) ha subito una radicale ristrutturazione della durata di più un anno, al termine del quale è stato "rieletto" a sito Primario e da cui sono, in condizioni normali, erogati i servizi della DCOD.

Dal punto di vista tecnologico i passi fatti sono tanti e sostanziali. Sono stati unificati SAN e LAN, semplificando la connettività e riducendo del 90% i cavi, con un utilizzo pressoché totale di fibre in sostituzione delle connessioni più vecchie e meno funzionali in rame. I server sono stati raggruppati in "pod" omogenei composti da più rack, che sono stati soggetti a una lineare standardizzazione e si configurano come la struttura atomica da replicare in caso di espansione. I server stessi sono stati tutti aggiornati, portati allo stadio tecnologico di ultima generazione e, in futuro, saranno gestiti e sostituiti, come il resto dell'infrastruttura, secondo i cicli di vita previsti dai produttori, in modo da evitare i pericoli dell'obsolescenza che inducono oneri di gestione e limitano le possibilità evolutive e l'efficienza dell'organizzazione.

Attualmente, quindi, il sistema informatico dell'Istituto è costituito da più sistemi di elaborazione siti presso il DC Primario e Secondario e da sistemi elaborativi al servizio del territorio siti presso le Direzioni Regionali e le Sedi Locali, interconnessi mediante la rete geografica SPC (Sistema Pubblico di Connettività).

Il DC Secondario coopera all'erogazione dei servizi con il DC primario. Tra i due DC è attiva una soluzione di Business Continuity, per la maggior parte dei servizi in modalità active-active, per alcuni in modalità active-passive.

È inoltre presente una soluzione di DR, presso il DC esterno di Casamassima, al momento attiva soltanto per i servizi in hosting (Ministero della Salute).

È prevista la realizzazione di un terzo sito, per il DR per INAIL e per le altre PA che lo richiedano.

Di seguito è descritto sinteticamente lo stato dell'arte delle infrastrutture tecnologiche e del patrimonio informativo e applicativo dell'INAIL.

2.1. Sistemi centrali

L'ambiente centrale è costituito da sistemi open su piattaforme Linux e Windows. L'ambiente distribuito AIX (Unix) funge anche da data server, tramite il DB2, per gli ambienti collegati.

Sulle piattaforme Linux, Windows e AIX sono presenti le basi dati DB2, ORACLE, SQLServer, MySQL, MongoDB e Postgresql relative ai servizi online interni esterni, del portale INAIL, del sistema di autenticazione e del MdS.

Nell'ambiente Windows e Linux sono installate le applicazioni in architettura web su piattaforma ESX/VMware che forniscono:

- i servizi online interni ed esterni all'istituto quali le applicazioni istituzionali, DURC, CCI, Denuncia infortuni online, ISI, SSI, Open data, Autoliquidazione, Contabilità Finanziaria, Gestione Risorse Umane, Data Warehouse (Cloudera), Controllo di Gestione e l'Avvocatura.
- I servizi online interni ed esterni del MdS e INMP.

2.1.1. Sistemi IBM System P E980 Power

L'infrastruttura comprende due elaboratori IBM 9080-M9S System P E980 in tecnologia Power9, e due IBM P10-9080-HEX uno presso il Sito Primario ed uno presso il sito Secondario, comprensivi di Sistema Operativo AIX 7.x Piattaforma di Virtualizzazione PowerVM, Rack Standard e console di gestione IBM HMC; ogni macchina è composta di 100 CPU attive con capacità di gestire 8 Threat contemporaneamente per ogni core, 5 TB attive per macchina di memoria, e sono collegate alla SAN Dell-EMC.

Questi sistemi sono posizionati in due Datacenter diversi, distanti circa 30 KM e fanno recovery delle funzionalità e degli ambienti l'uno sull'altro, qualora si presentino problemi ad un Datacenter o il cliente ne consideri la necessità per proprie motivazioni.

- Sistema Server Power E980 Model 9080-M9S (Santuario)
- Sistema Server Power E980 Model 9080-M9S 8 (Acilia)

La tipologia di HW e distribuzione è la seguente:

- N. 2 IBM Power 9 E980 Series (1 Santuario - 1 Acilia)
- N. 2 IBM P10-9080-HEX (1 Santuario – 1 Acilia)

Su questi sistemi sono installati, su LPAR (partizioni virtuali), i seguenti ambienti di, Sviluppo, Collaudo e Certificazione con architetture in alta affidabilità in Disaster recovery:

- BPM IBM (Business Process Management) dove girano le applicazioni critiche come flussi monetari, fatturazione elettronica e POM massivo (posta multicanale);
- IBM Sterling B2B Integrator per l'invio e ricezione dati in maniera automatica ed affidabile di posta massiva, flussi finanziari con monitoraggio dei flussi di dati;
- Infosphere Information Server per esigenze di governance, data quality, modellazione ed integrazione dati;
- Infosphere Federation Server utilizzato per applicazioni contabili che dialogano con database DB2 e Oracle;

IBM Power 9: la quasi totalità delle installazioni su questi apparati sono LPAR con sistema IBM AIX ed ospitano i seguenti servizi:

- Servizio di Schedulazione (AIX + IBM IWS);
- Gestione Flussi (IBM AIX + IBM Sterling);
- Applicazione flussi monetari - BPM (IBM AIX + IBM Websphere) Active – Active;
- Applicazioni Fatture PA, Contenzioso, Lotta Evasione (Suse Linux + IBM Websphere) Active – Active;
- Applicazione Glossario (IBM AIX + IBM Infosphere);

Servizio	Distribuzione dei LPAR
Schedulazione	Active su sito primario + DR
Gestione Flussi	Active su sito primario + DR
Glossario	Active su sito primario + DR
Applicazione flussi monetari – BPM	50% Active su Sito primario + 50% Active su Sito secondario
Applicazioni Fatture PA, Contenzioso, Lotta Evasione	50% Active su Sito primario + 50% Active su Sito secondario

L'infrastruttura comprende un elaboratore IBM 9080-MHE System P E880 in tecnologia Power8 comprensivo di Sistema Operativo AIX 7.X Piattaforma di Virtualizzazione PowerVM, Rack Standard e console di gestione IBM HMC, è composto di 114 CPU attive con capacità di gestire 8 Threat contemporaneamente per ogni core, 4068 TB di memoria, e collegato alla SAN Dell-EMC.

il Power 8 potrebbe svolgere prevalentemente funzioni di DR svolgerebbe dunque, prevalentemente ruolo di DBMS Server e Microfocus Server .

2.1.2. Sistemi IBM System P 10 Power

Nel corso del 2024, l'Inail ha inoltre acquisito n.2 Server IBM Enterprise Power 10, configurati con le seguenti caratteristiche:

Sistemi P10 E1080
120 core Power10@ 3.7 GHz di cui 120 attivati
6 TB di RAM DDR4 di cui 6 TB attivati
8 PCIe3 2-Port 16Gb FC Adapter
14 PCIe3 LP 2-Port 25/10Gb NIC&ROCE SR/Cu Adapter
2 PCIe4 2-port 100GbE RoCE Adapter x16

Su questi sistemi sono installati, su LPAR (partizioni virtuali), gli ambienti di , produzione con architetture in alta affidabilità in Disaster recovery:

- BPM IBM (Business Process Management) dove girano le applicazioni critiche come flussi monetari, fatturazione elettronica e POM massivo (posta multicanale);
- IBM Sterling B2B Integrator per l'invio e ricezione dati in maniera automatica ed affidabile di posta massiva, flussi finanziari con monitoraggio dei flussi di dati;
- Infosphere Information Server per esigenze di governance, data quality, modellazione ed integrazione dati;
- Infosphere Federation Server utilizzato per applicazioni contabili che dialogano con database DB2 e Oracle;

2.1.3. Sistemi Intel x86 e Farm VMware

I sistemi fisici x86 tradizionali sono principalmente di tecnologia DELL Vxblock 1000 e HPE synergy e Proliant DL rack mounted a cui si aggiungono, in particolare, server DELL Poweredge R730xd e R740xd per ospitare l'infrastruttura Cloudera.

L'utilizzo di questi server fisici è prevalentemente destinato ad ospitare:

Installazioni Microsoft Windows SQL Server in configurazione cluster geografico, esteso sui due siti, mediante tecnologia storage DELL-Powermax;

Installazioni Microsoft Windows Server per servizi infrastrutturali Active Directory e DNS Server;

Oracle DBMS su Red Hat Linux (ad esclusione dei servizi su EXACC) in configurazione cluster e modalità Active – Data Guard sui due DC;

Cloudera Software su Centos Server su singolo sito (per produzione);

Server applicativi per piattaforma Openshift;

Server ed appliance per servizi di sicurezza;

Server ed appliance per servizi di backup e restore;

Server applicativi per la vecchia contabilità finanziaria (Oracle E-Business Suite);

Hypervisor VMWare meglio dettagliati di seguito.

I sistemi sono distribuiti uniformemente su entrambi i Data Center (siti) e con soluzioni sia hardware che software al fine di garantire l'affidabilità in caso di un fault parziale o totale di un sito.

Ruolo / Servizio offerto	Distribuzione dei server
Cluster Microsoft SQL Server (Produzione)	100% in cluster distribuito al 50%+50% su due DC (SA / AC)
Cluster Microsoft SQL Server (Certificazione)	100% in cluster distribuito al 50%+50% su due DC (SA / AC)
Cluster Microsoft SQL Server (Collaudo)	100% in cluster sul singolo DC (SA)
Windows Active Directory + DNS	Distribuzione dei server al 50% + 50 % sue due DC
Oracle DBMS (Produzione)	Distribuzione dei server al 50% (Active) + 50%(Data Guard) sui due DC
Oracle DBMS (Certificazione)	Distribuzione dei server al 50% (Active) + 50%(Data Guard) sui due DC
Oracle DBMS (Collaudo)	Distribuzione dei server al 50% + 50% sui due DC
Cloudera (Produzione)	Servizio disponibile su sito Primario
Server Applicativi a servizio della infrastruttura Openshift Container Platform (Certificazione e Produzione)	Distribuzione dei server al 50% sui due siti
Server / Appliance servizi di sicurezza	Distribuzione dei server al 50% + 50 % sue due DC
Server / Appliance per servizi di Backup / Restore	Distribuzione dei server al 50% + 50 % sue due DC
Vecchia Contabilità finanziaria (EBS) - Produzione	Distribuzione dei server al 50% + 50 % sue due DC

L'infrastruttura VMware, distribuita nei due DC di INAIL, è servita da HW HPE synergy suddivisa in farm, di cui 2 locali e 3 estese, tra i due DC, mediante tecnologia storage primera (senza witness).

In particolare, sulle farm locali insistono principalmente Virtual Machine che erogano esclusivamente servizi bilanciati (Virtual Machine ridondate per servizio).

A questa si aggiunge una ulteriore farm, servita da tecnologia Nutanix e destinata ad ospitare servizi per la VDI INAIL.

Farm Name	Tecnologia	Servizi erogati	DC	% Nodi (hypervisor)	% Virtual Machine
“Multi sito PSN”	HPE synergy su storage + primera	Servizi per il Polo Strategico Nazionale	Multi sito (SA / AC)	7%	10%
“Multi sito Cloud Privato”	Vxbloc storage powermax	Private / Hybrid Cloud	Multi sito (SA / AC)	97%	90%

La Server Farm VMware è costituita da sistemi in alta affidabilità ridondati su entrambi i datacenter dell'Istituto. Una parte dei sistemi opera in business continuity con bilanciamento sui due siti. Per le componenti non bilanciate invece è adottata una soluzione VFarm estesa “multisito” e virtualizzazione storage su tecnologia EMC Powermax in grado di garantire tempi di ripristino immediati di componenti infrastrutturali in caso di indisponibilità parziale o totale del singolo sito.

Le infrastrutture appena descritte ospitano per lo più server applicativi e web server virtuali Linux e Microsoft e forniscono prevalentemente i servizi web. L'uptime e le prestazioni (fault tolerance e load balancing) delle applicazioni è garantito dal bilanciatore di carico applicativo NetScaler. L'estensione della farm su entrambi i siti è a garanzia di continuità operativa, e si integra con la rete dell'Istituto utilizzando tecnologie che limitino eventuali perdite di dati al minimo (no data loss). Garantisce inoltre la flessibilità operativa per assicurare tempi estremamente rapidi e processi semplici per l'attivazione del centro di backup o il fail back sul sito primario, preservando l'integrità e la coerenza delle basi informative e un alto grado di indipendenza, ovvero la capacità di offrire servizi su Internet anche in assenza dei back end centrali dell'Istituto.

L'architettura prevede i seguenti elementi:

- Connettività di rete & Sistemi di Load Balancing
- Sistemi Server Wintel & Linux
- Web Server & Application Server
- Microservizi
- Database

Questi elementi contribuiscono a coadiuvare l'installazione e la gestione dei siti e delle applicazioni Web dell'Istituto.

L'elemento della connettività di rete e dei sistemi di Load Balancing dal NOC di Inail. La componente di rete è alla base del servizio. Con l'obiettivo di erogare servizi in alta affidabilità si utilizzano le tecnologie Citrix NetScaler che garantiscono un meccanismo efficiente e stabile di alta affidabilità dei servizi.

Affiancati ai sistemi “Multi Tier” tradizionali, sono presenti alcuni sistemi convergenti finalizzati non solo ad aumentare la capacità elaborativa dei DC ma anche per raggruppare componenti tradizionali in un’unica entità e semplificarne la gestione.

La scelta comprende:

- Infrastrutture convergenti basate su sistemi DELL-EMC Vxblock;
- Infrastrutture convergenti basate su sistemi HPE Synergy.

Di seguito, in sintesi, l’installato DCOD Inail alla data di stesura del presente documento, delle piattaforme convergenti.

Si tratta di una soluzione convergente DELL VxBlock 1000 che comprende:

- Due rack per sito in cui sono stati installati e configurati, di fabbrica, apparati computazionali e network che abilitano la convergenza;
- Due apparati storage DELL Powermax (uno per ciascun sito), a complemento, per la componente storage.

Il dettaglio, di ciascun blocco (un blocco per ciascun sito), si compone di:

- 6 frame Cisco UCS 5108;
- 42 Blade UCS B200 M5;
- 1 storage DELL EMC Unity XT Hybrid New Solution (6 x 600GB 10K SAS drive);
- 4 server di tipo “rack mounted” destinati alla gestione della soluzione di convergenza;

Lo storage DELL Unity XT fornisce le LUN di boot alle lame Blade UCS.

L’accoppiamento al Powermax è diretto, attraverso porte dedicate L’allineamento storage tra i siti è realizzato tramite il protocollo sincrono SDRF. La soluzione comprende due rack, per ciascun sito, così composto:

Rack 1

- n° 2 HPE Synergy Frame 12000;
- n° 20 lame HPE Synergy blade SY480 (10 per frame)
- 1 storage HPE Nimble

Rack 2

- 1 apparato storage HPE Primera 650
- La replica storage “intra site” è garantita nel modo seguente:
- Via rete, per lo storage Nimble, mediante due ToR Switch direttamente connessi al DWDM;
- Via SAN, per lo storage Primera, attraverso la SAN (già esistente) di INAIL.

I moduli computazionali Synergy possono usufruire di entrambi gli storage via SAN.

2.2. Storage

L'infrastruttura storage INAIL si sviluppa su due poli principali, Santuario e Acilia, configurati secondo un modello di ridondanza geografica e basati su apparati SAN e NAS di classe enterprise. A tali poli si affianca un terzo sito, Bari, dedicato alle funzioni di Disaster Recovery nell'ambito dell'architettura HPE.

L'infrastruttura complessiva integra componenti Dell EMC (PowerMax, Unity, Isilon, VxBlock) e HPE (Primera, Nimble), collegati tramite apparati di rete Cisco MDS su fabric ridondati con trasporto DWDM.

L'adozione di tecnologie all-flash, meccanismi di replica sincrona e asincrona e sistemi di gestione automatica del failover permette di garantire la continuità dei servizi, la coerenza dei dati e la resilienza dell'intero sistema.

2.2.1. Architettura Dell EMC – Poli di Santuario e Acilia

2.2.1.1. Storage a Blocchi (SAN)

L'infrastruttura SAN dei due poli principali si basa sui sistemi:

- Dell EMC PowerMax: piattaforma all-flash ad alte prestazioni, con replica sincrona tramite SRDF Metro.
 - Dell EMC Unity e Unity XT: utilizzati principalmente nella soluzioni SAN per videosorveglianza, mentre lo Unity XT è integrato nei sistemi convergenti VxBlock.
 - Dell EMC VxBlock 1000: infrastruttura convergente utilizzata per workload virtualizzati e mission-critical.
- Queste piattaforme costituiscono il cuore dei servizi applicativi critici dell'Ente, gestendo carichi di lavoro eterogenei con requisiti di alta disponibilità.

Gli apparati Dell PowerMax sono in replica mediante la tecnologia SRDF Metro assicurando la coerenza ed allineamento dei dati tra Santuario e Acilia

2.2.1.2. Storage a File (NAS)

La componente NAS è affidata ai sistemi:

Dell EMC Isilon H500: piattaforma scalabile per dati non strutturati.

La replica dei dati tra i due poli avviene in modalità asincrona tramite protocolli IP

2.2.1.3. Rete SAN

La connettività inter-data center è realizzata con:

- Switch Cisco MDS 9148S / 9148T / 9710-V2,
- Fabric multipli con ridondanza completa,
- Trasporto DWDM per la replica sincrona tra siti.
- Il backbone di rete SAN è realizzato tramite gli switch Cisco MDS 9710-V2 collegati tra loro mediante collegamenti DWDM, garantendo un'elevata disponibilità e tolleranza ai guasti.

2.2.2. Architettura HPE – Modello 3DC Peer Persistence

Per i servizi erogati al Ministero della Salute, INAIL ha implementato un'architettura dedicata basata sui sistemi HPE Primera con modello 3DC PP (Three Data Center Peer Persistence).

Gli HPE Primera, sono configurati in 3DC Peer Persistence. In questo modello, i siti di Santuario e Acilia operano in replica sincrona, mentre verso il sito di Bari (polo di Disaster Recovery) la replica avviene attraverso collegamenti asincroni.

Gli storage HPE Nimble sono presenti solo sui siti di produzione (Santuario ed Acilia) ed in replica Network.

2.2.3. Backup

L'infrastruttura di backup INAIL nasce originariamente come piattaforma completamente basata su tecnologie Dell EMC (Networker, Avamar e Data Domain). A fronte delle nuove esigenze istituzionali, questa soluzione è stata estesa con l'introduzione della piattaforma Commvault integrata con storage PureStorage FlashBlade.

L'architettura è distribuita sui tre CED dell'Istituto:

- Santuario
- Acilia
- Casamassima (Bari) – Polo di Disaster Recovery

La coesistenza dei due tecnologie (Dell EMC e Commvault/PureStorage) garantisce un'architettura moderna ad alta efficienza, basata su deduplica e replica multisito.

Infrastruttura di Backup Dell EMC, è costituita da:

- EMC Networker
- Storage Node Networker
- EMC Avamar
- Avamar Accelerator.
- PPDm

Storage Data Domain DD9900/DD9400 per la memorizzazione dei dati presenti sui 3 Siti

La piattaforma garantisce la protezione di:

- ambienti VMware,
- database (Oracle, Oracle Exadata, SQL, DB2, Exchange),
- file system (AIX, Linux, Windows)
- protezione dei dati NAS (ISILON).

È inoltre presente un Data Domain DD9900 dedicato al Cyber Security Vault (CRS), sul quale vengono replicate copie dei dati ai fini di analisi post-evento.

Infrastruttura di Backup Commvault

L'infrastruttura Commvault, basata su tecnologia PureStorage FlashBlade, è distribuita nei tre Data Center dell'Istituto (Santuario, Acilia, Casamassima).

L'infrastruttura Commvault si articola come segue:

- 1 CommServe attivo presso Santuario
- 1 CommServe in LiveSync presso Acilia (standby con replica continua)
- Il LiveSync assicura l'alta disponibilità tramite sincronizzazione costante del database di orchestrazione.
- Media Agent
- Virtual Server Agent (VSA)
- FREL Linux

La piattaforma Pure/Commvault protegge i seguenti sistemi:

- Cluster Nutanix
- Cluster OpenShift (OCP)
- Office 365
- SharePoint
- OCI Cloud

Tutti i backup vengono effettuati via rete.

2.3. Ambiente CLOUD

Le aree di cloud computing presenti nell'istituto sono:

- Cloud pubblico
- Cloud ibrido

nell'ambito delle tipologie di cloud universalmente riconosciute - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), DaaS (Desktop as a Service) - vengono erogati i servizi inclusi nelle seguenti categorie:

- Compute Services
- Databases Services
- Development Services
- Identity Services
- Security Services
- Integration Services
- Migration Services
- Networking Services

- Storage Services

L'Istituto dispone di un'infrastruttura distribuita come servizio (IaaS) ospitata su cloud pubblico Microsoft Azure Windows. L'infrastruttura ospita server Windows e cloni Linux, a supporto di infrastrutture dedicate ai servizi Documentale, Sharepoint, Mobility, Big Data. Una VLAN dedicata collega direttamente le macchine in cloud con l'infrastruttura on-premise di INAIL per consentirne l'integrazione.

Sono utilizzati anche dei servizi IAAS su Cloud IBM dove girano macchine Windows e macchine VMWare della suite di Vcloud Foundation.

Su cloud pubblico Microsoft Azure l'Istituto dispone già di applicazioni che utilizzano anche soluzioni basate su servizi PaaS. Al momento l'Istituto utilizza i principali servizi (Azure Active Directory, App Service, Function, Logic App, SQL Database, Cosmos DB, AKS, B2C, MFA, Blob Storage, Media Services, Azure Front Door, Windows Application Firewall, Azure Security Center, Azure Monitoring, APIM, CLU), ma la previsione è di utilizzare l'intera gamma dei servizi PaaS.

Oltre ai servizi PaaS Azure, l'Istituto fa uso di quelli sulla piattaforma IBM BlueMix impiegati soprattutto per lo sviluppo di applicazione in ambito intelligenza artificiale.

Sul fronte dei servizi cloud SaaS, l'Istituto utilizza:

- l'intera offerta dei servizi Office 365 (Office, Teams, OneDrive, SharePoint, Exchange online, ATP, CASB, WDATP, MIP), ivi incluso Dynamics 365.
- Service Now per l'automazione di processi;
- Adobe per servizi di Content Management System, gestione di adaptive forms, elaborazione e conversione di Pdf, gestione di campagne multicanale, analisi multicanale delle sessioni di navigazione utente (analytics);
- Sailfor per la formazione a distanza e strumenti di learning management system;
- Altre piattaforme specifiche quali:
 - PagoPA per i pagamenti verso la PA;
 - Piattaforma Digitale Nazionale Dati (PDND);
 - Piattaforma Notifiche Digitali (PND -> Send).

Nel corso del 2023, è stata implementata un'infrastruttura dedicata per i servizi Oracle Identity Governance (OIG) ospitata sulla piattaforma cloud Oracle OCI. Al fine di garantire la corretta connettività e integrazione tra la piattaforma OIG nel cloud e l'infrastruttura on-premise dell'INAIL, è stata istituita una VLAN appositamente dedicata. L'infrastruttura OCI ospita servizi server come Oracle Linux, Windows e Database Oracle (DBAAS) mediante l'approccio Infrastructure as a Service (IaaS), necessari per supportare tutti i software e i servizi della piattaforma OIG. I principali componenti includono:

- OCI IaaS:
 - Oracle Access Manager (OAM)

- Oracle Identity Governance (OIG)
- Oracle HTTP Server (OHS)
- Oracle Internet Directory (OID)
- Connector Server (ICF)
- OCI OKE (Oracle Kubernetes Engine):
 - Oracle Identity Role Intelligence (OIRI)
- PAAS (Platform as a Service):
 - Oracle Identity Cloud Service (IDCS) / OCI Identity and Access Management (IAM)
- OCI DBAAS:
 - Database Applicativi
 - Database di Audit

Inoltre, l'INAIL ha intrapreso un'altra importante scelta nella strategia cloud rappresentata dall'adozione delle soluzioni Oracle SaaS e PaaS per le aree ERP (Enterprise Resource Planning) ed EPM (Enterprise Performance Management):

- Oracle ERP Cloud: offre una suite di applicazioni integrate che supportano le funzioni aziendali chiave come contabilità, gestione finanziaria, gestione delle risorse umane, gestione della supply chain e altro ancora;
- Oracle EPM Cloud: fornisce strumenti per la pianificazione finanziaria, il budgeting, la modellazione dei costi e la creazione di report.

Nel corso del 2022 e del 2023 su piattaforma Adobe sono stati pubblicati i nuovi siti di Superabile, della sezione dedicata ai Centri di Eccellenza di Vigorso e Volterra e del Casellario Centrale Infortuni e nel 2024 è stato pubblicato il nuovo portale Inail.

Nel 2023 è stata resa disponibile la nuova intranet basata su Sharepoint 365 (Digital Workplace).

L'integrazione delle soluzioni cloud nel sistema di SSO è garantita da soluzioni specifiche a livello di backend che garantiscono elevate prestazioni (Express Route) e sicurezza (antivirus e IP Inspection).

2.4. Sistemi periferici

Su 200 Sedi sono stati posizionati i 200 distribution point della piattaforma di gestione centralizzata delle postazioni di lavoro System Center Configuration Manager.

2.5. Sistemi Centro Protesi INAIL

Le applicazioni del Centro Protesi INAIL, precedentemente ospitate direttamente nel DC di Vigorso di Budrio, sono migrate nella infrastruttura centrale dell'Istituto a servizio di circa 200 utenti distribuiti in diverse unità territoriali:

- il Centro di Riabilitazione Motoria di Volterra;
- la Filiale di Roma e la Filiale di Lamezia;
- i Punti Assistenza del Centro Protesi di Roma, Milano, Cagliari, Ancona, Palermo, Torino, Venezia, Napoli, Bari e Lamezia

L'intero sistema comprende sistemi software di "produzione" per la gestione delle attività direttamente connesse alla "mission" del Centro Protesi, sistemi software "gestionali" come le Oracle Applications utilizzati dalle aree acquisti e controllo di gestione e software "clinici" destinati al supporto delle aree sanitarie.

La rete del Centro Protesi è inserita nell'infrastruttura di Active Directory dell'INAIL e gli utenti utilizzano gli stessi servizi di Posta elettronica e di accesso ad internet erogati a livello centrale.

Le applicazioni che costituiscono l'intero sistema sono state sviluppate utilizzando il tool RAD Instant Developer – Programma v.21 configurato per lo sviluppo su tecnologia Microsoft (.NET) e database Oracle v12.

Il sistema **GIMAP**, in corso di progettazione, è una applicazione custom a microservizi per la gestione delle forniture di dispositivi personalizzati, dei cicli di produzione, delle scorte di magazzino delle politiche di riordino. GIMAP, oltre al colloquio con le procedure istituzionali, dovrà garantire la completa integrazione con CCR per la realizzazione del progetto protesico riabilitativo.

2.6. Postazioni di lavoro

Il personale dell'Inail dispone di postazioni di lavoro agili, delle soluzioni Microsoft Office 365 (Teams, Exchange online, One Drive, Dynamics 365 e altro) e svolge la propria attività in presenza o da remoto.

2.7. Cooperazione Applicativa

In esecuzione degli accordi relativi allo sviluppo del sistema di cooperazione applicativa nell'ambito del SPC, l'Agenzia per l'Italia Digitale (già DigitPA) ha definito un set di documenti che costituisce il riferimento tecnico per lo sviluppo dei servizi infrastrutturali generali e della porta di dominio (PDD). Unitamente alle specifiche della busta di e-Government questi documenti delineano compiutamente il quadro tecnico-implementativo del Sistema Pubblico di Cooperazione (SPCoop).

Il Sistema Pubblico di Connettività e Cooperazione permette agli utenti di avere una visione integrata di tutti i servizi di ogni amministrazione pubblica sia centrale che locale ed indipendente dal canale di erogazione.

Il modello di cooperazione applicativa del SPCoop si basa sui seguenti principi:

- Cooperazione tra amministrazioni - Le amministrazioni cooperano attraverso l'erogazione e la fruizione di servizi applicativi offerti dalla singola amministrazione attraverso un unico elemento (logico) del proprio sistema informativo denominato Porta di Dominio (PDD). Questo principio

garantisce la completa autonomia, da parte dell'amministrazione, nella progettazione, realizzazione e gestione dei servizi applicativi, in quanto essi possono essere basati su qualsiasi piattaforma applicativa, preesistente o di nuova acquisizione, purché vengano poi erogati attraverso la Porta di Dominio. La fruizione dei servizi applicativi avviene attraverso lo scambio di messaggi applicativi, secondo il formato definito nel documento di specifica della busta di e-Gov.

- Ambito di responsabilità - Ciascuna amministrazione cooperante mantiene la responsabilità dei servizi da essa erogati e dei dati forniti attraverso tali servizi, dando luogo ad un singolo Dominio di servizi applicativi (brevemente Dominio). Ciò consente il disaccoppiamento tra i vari soggetti cooperanti, mantenendo nel loro ambito di responsabilità gli elementi di propria competenza.
- Accordi - Un servizio applicativo opera sulla base di accordi tra almeno due soggetti (erogatore e fruitore), accordi che hanno un fondamento normativo/istituzionale oltre che tecnico.
- Tutti i servizi applicativi (offerta da un Dominio o da un Dominio di Cooperazione per il tramite del soggetto coordinatore responsabile) sono offerti attraverso un unico elemento (logico) denominato

2.7.1. Porta di Dominio

Di fatto essa è la piattaforma presso cui sono disponibili le interfacce applicative dei servizi; non necessariamente i componenti software che realizzano tali servizi sono poi ospitati sulla stessa piattaforma della PDD, anzi molto frequentemente ed opportunamente essa svolgerà le funzioni di semplice proxy e dispatcher verso altre piattaforme di back-end presso cui sono effettivamente dispiestate le realizzazioni dei servizi.

Il protocollo applicativo con cui i servizi applicativi sono invocabili remotamente è una estensione dello standard SOAP, necessaria al fine di supportare sicurezza point-to-point, affidabilità della trasmissione e tracciatura di tutte le comunicazioni (aspetti avanzati non ancora standardizzati).

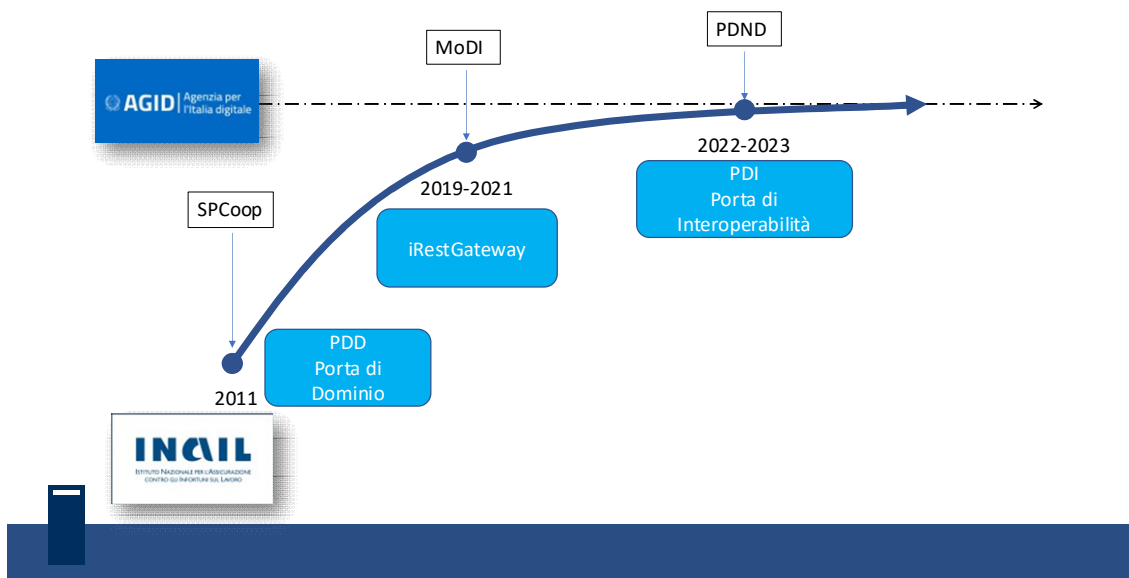
Questa estensione di SOAP, specificatamente progettata per SPCoop, viene chiamata Busta e-Gov e prevede l'utilizzo di un header appositamente predisposto, elaborato dalle Porte di Dominio, in grado di veicolare tutte le informazioni necessarie per implementare le suddette funzionalità; tutto questo in maniera "trasparente" alle applicazioni che fanno uso delle Porte.

La PDD realizzata in INAIL risponde ai requisiti di una porta di dominio di fascia avanzata. La PDD INAIL è riconosciuta come "Porta di Dominio Qualificata", in quanto ha superato il processo di qualificazione previsto da ex DigitPA (19 marzo 2009) ed è utilizzata per tutti i servizi che l'Amministrazione eroga/fruisce con i soggetti pubblici e privati che sono, a loro volta, dotati di una PDD qualificata su SPCoop.

2.7.1.1. Architettura Tecnica PDD

La porta di dominio INAIL è set di componenti applicative che realizzano le funzionalità di una porta di dominio avanzata basata sullo standard di busta eGov 1.1 e delle linee guida 2008. È basata sulla piattaforma Java EE7, sull'application server open source Wildfly 15 ed il JDK 1.8. I componenti di rilievo che realizzano le funzionalità core sono:

Dalla PDD alla PDI – Breve Storia Interoperabilità



- Apache CXF (JAX-WS, JAX-RS)
- Apache WSS4J (WS-Security, SAML 1.1/2.0)
- ActiveMQ (messaggistica JMS)
- Infinispan (clustering)

La PDD si è evoluta per includere anche i pattern di sicurezza MODI e PDND.

Il nuovo layer informatico INAIL che implementa la soluzione di Interoperabilità è denominato “PDI - Porta di Interoperabilità” ed include implementa tutti gli standard ancora in essere:

- PDD - Porta di Dominio, nell'ambito della struttura SPC (Servizi di Pubblica Connettività);
- MoDI - Modello di Interoperabilità;
- PDND - Piattaforma Digitale Nazionale Dati.

2.7.1.2. Architettura logica

- Porta Applicativa: ruolo assunto da una porta di dominio SPCoop nell'ambito di un episodio di collaborazione applicativa. Assume tale ruolo la porta di dominio che, a seguito della ricezione di un messaggio di richiesta proveniente da un'altra porta di dominio (porta delegata) invia al mittente un messaggio di risposta

- Porta Delegata: ruolo assunto da una porta di dominio SPCoop nell'ambito di un episodio di collaborazione applicativa. Assume tale ruolo la porta di dominio che origina un messaggio di richiesta (di servizio) destinato ad un'altra porta di dominio (porta applicativa).
- Modulo applicativo: (da Allegato 2b del Capitolato Tecnico SPC Lotto 2) modulo, parte di un servizio applicativo, composto a sua volta da uno o più componenti applicativi, che implementa una funzionalità amministrativa completa e che espone tale funzionalità attraverso una interfaccia in modalità Web Services.
- Componente applicativo: (da Allegato 2b del Capitolato Tecnico SPC Lotto 2) un componente software, parte di un modulo applicativo, che realizza una funzionalità elementare di dimensioni non superiori a 5 Function Points. Un componente applicativo consente l'accesso a tale funzionalità attraverso un'interfaccia specifica accessibile con modalità standard. A tale fine sono considerate standard le modalità di accesso previste da interfacce di tipo:
 - Web Services sviluppate con tecnologie J2EE o .NET
 - CORBA, RMI, COM/DCOM
 - API scritte in linguaggi multiplatforma quali Java o C/C++ e basate su code o librerie standard quali JMS.

La PDD INAIL in modalità erogatore, oltre ad integrarsi con i moduli applicativi tramite protocollo SOAP, è anche in grado di integrarsi direttamente con i singoli componenti applicativi a patto che questi siano invocabili tramite il protocollo nativo Java EJB. In questa modalità la PDD opera una trasformazione dei messaggi SPCoop in chiamate a metodi di oggetti Java remoti residenti su altre piattaforme, rendendo assolutamente trasparente la presenza o meno della PDD e svincolando i componenti dalla conoscenza del formato dei singoli messaggi conformi al relativo Accordo di servizio.

È importante sottolineare che il protocollo EJB è attualmente in uso per il servizio di "Comunicazione unica".

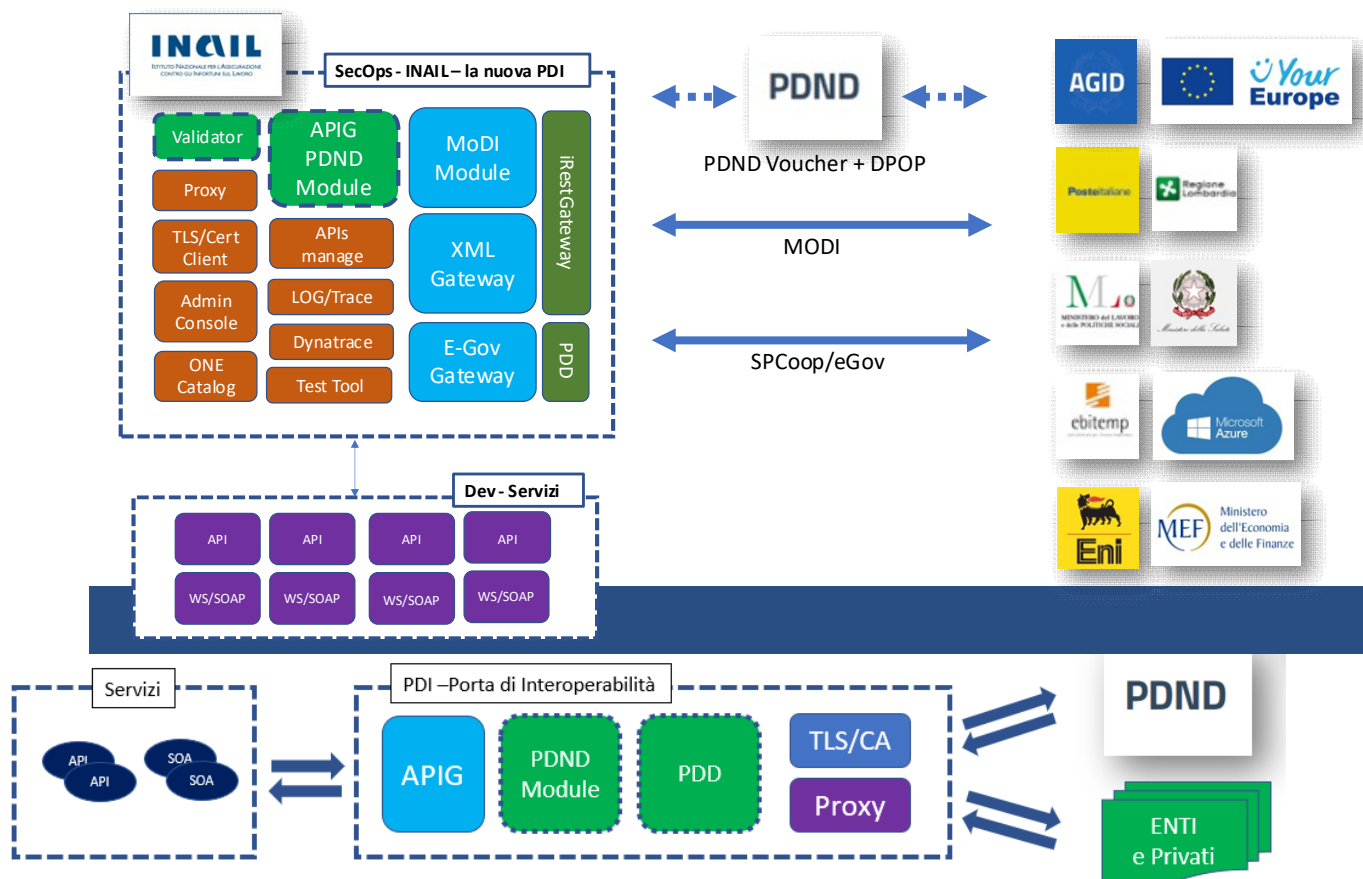
In modalità fruitore (quindi PDeI) l'integrazione con i moduli applicativi avviene esclusivamente mediante protocollo SOAP.

La PDD è logicamente suddivisa in due elementi logici:

- Componente di cooperazione, che gestisce le comunicazioni in entrata ed in uscita con le altre PDD, sbusta/imbusta i messaggi SPCoop, gestisce i profili di collaborazione, gestisce la sicurezza tra PDD, gestisce la tracciatura dei messaggi. Disaccoppia completamente le funzioni tipiche di una PDD dalla logica di business dei moduli applicativi.
- Completamente di integrazione, che si occupa di smistare i messaggi non imbustati ai moduli applicativi dedicati esclusivamente alla logica di business. Il presente documento descrive il funzionamento di tale componente.

Il Disegno più ampio della PDI include anche altri componenti che sono così rappresentati:

La Nuova PDI – Porta di Interoperabilità INAIL



2.7.1.3. Architettura fisica

In linea con le strategie adottate dall'istituto per proteggersi da possibili situazioni di emergenza, la Porta di Dominio eroga il proprio servizio con infrastrutture ICT installate nei due siti di Santuario e Acilia.

In particolare, l'infrastruttura è composta da 6 macchine virtuali (4 a Santuario e 2 a Acilia) che lavorano in Business Continuity in modalità active-active, ovvero il carico di lavoro viene distribuito equamente da un bilanciatore a tutti i server, garantendo quindi la continuità in caso di problematiche su uno dei due siti. Anche tutti i moduli applicativi (BE) lavorano in Business Continuity, mentre le macchine con il database della PDD, gestiti dal Team DBA Oracle, sono configurati con Oracle Data Guard e non sono in modalità "Active", ovvero i database risultano montati e replicati su entrambi i siti di Santuario e Acilia, ma non sono contemporaneamente aperti - il failover viene quindi gestito manualmente dal Team.

La PDD prevede comunque una stringa di connessione che gestisce in automatico lo switchover, e nei periodi di mancata connessione al database (indisponibilità/manutenzione), è in grado, in piena autonomia, di memorizzare

ID 2912 - Gara a procedura aperta, suddivisa in due lotti, per l'affidamento dei servizi di conduzione, manutenzione e supporto specialistico per la gestione e l'evoluzione dell'infrastruttura ICT di INAIL

Appendice 1 al Capitolato tecnico – Contesto tecnologico ed infrastrutturale

Classificazione Consip: Distribuzione Ristretta

le informazioni su un sistema di recovery alternativo e sempre disponibile, per ripristinarle in un secondo momento sul DB a situazione ripristinata.

I server della PDD sono installati in una DMZ, dove il traffico è strettamente regolato da entrambi i lati, in modo da rendere fruibili i servizi verso l'esterno minimizzando i rischi per la rete interna. Per un maggior livello di sicurezza viene, inoltre, mascherato l'indirizzo IP privato a cui risponde la PDD con un indirizzo IP esterno (NAT).

2.8. Posta Elettronica PEL e PEC

L'attuale soluzione di posta elettronica (PEL) è basata sul servizio cloud denominato Microsoft Exchange Online che offre le funzionalità di Microsoft Exchange Server.

Il servizio è accessibile da parte degli utenti con un'ampia gamma di dispositivi dall'interno della rete dell'Istituto o da Internet, prevede funzionalità avanzate di messaggistica e di collaborazione e delle componenti integrate di sicurezza tra le quali Microsoft Exchange Online Protection (EOP) servizio di filtro della posta elettronica per spam e malware e Microsoft Office 365 Advanced Threat Protection (ATP) servizio di filtro di protezione zero-day. La dimensione delle caselle è pari a 100 GB. Attualmente sono presenti circa 13000 caselle PEL.

La soluzione è pienamente integrata con il servizio di Active Directory dell'Istituto garantendo sia il Single sign-on che l'utilizzo degli strumenti di amministrazione, per gestire le funzionalità di Exchange Online.

Alla soluzione basata su cloud si affianca un'infrastruttura di posta elettronica ospitata on-premise presso i due data center dell'Istituto basata su tecnologia Microsoft Exchange Server per l'esercizio delle funzionalità di posta elettronica applicativa e massiva.

Di seguito sono elencate le principali componenti software e le tecnologie impiegate per il "core" della soluzione.

- Ambienti virtuali VMware con S.O. Windows Server 2012
- Microsoft Exchange Server 2013 configurato in modalità DAG
- Trellix
- NetWorker

Attualmente sono presenti on-premise circa 2000 caselle.

Per quanto riguarda le caselle PEC, sono previsti i seguenti profili:

1. PEC Base. Attualmente non utilizzate, con le seguenti caratteristiche:

- Numero massimo di invii giornalieri: 500;
- Numero massimo di invii al minuto: 50;
- Dimensione della mailbox: 2Gb;
- Dimensione massima dei messaggi: 100MB;
- Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi.

2. Caselle PEC Strutturate. Attualmente ve ne sono in esercizio 886, con le seguenti caratteristiche:

- Numero massimo di invii giornalieri: 500;
- Numero massimo di invii al minuto: 50;
- Dimensione della mailbox: 4Gb;

- Dimensione massima dei messaggi: 100MB;
 - Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi;
 - Conservazione Sostitutiva dei messaggi inviati e ricevuti per l'intera durata del contratto.
3. Caselle PEC Massiva Small. Attualmente ve ne sono in esercizio 59, con le seguenti caratteristiche:
- Numero massimo di invii giornalieri: 2000;
 - Numero massimo di invii al minuto: 200;
 - Dimensione della mailbox: 4Gb;
 - Dimensione media dei messaggi 200 kbyte;
 - Dimensione massima dei messaggi: 100MB;
 - Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi.
4. Caselle PEC Massiva Medium. Attualmente ve ne sono in esercizio 80, con le seguenti caratteristiche:
- Numero massimo di invii giornalieri: 6000;
 - Numero massimo di invii al minuto: 600;
 - Dimensione della mailbox: 12Gb;
 - Dimensione media dei messaggi 200 kbyte;
 - Dimensione massima dei messaggi: 100MB;
 - Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi.
- Caselle PEC Massiva Large. Attualmente ve ne sono in esercizio 29, con le seguenti caratteristiche:
- Numero massimo di invii giornalieri: 12000;
 - Numero massimo di invii al minuto: 1200;
 - Dimensione della mailbox: 24Gb;
 - Dimensione media dei messaggi 200 kbyte;
 - Dimensione massima dei messaggi: 100MB;
 - Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi.

2.9. Infrastruttura Active Directory

L'attuale architettura INAIL di Directory Services è costituita da molteplici foreste di Active Directory.

Nello specifico la foresta principale Active Directory di Netlogon basata su Microsoft Windows 2019 si compone di un dominio di root denominato inail.pri e da due domini child denominati rispettivamente inailutenti.inail.pri e inailservizi.inail.pri.

Il dominio inailutenti.inail.pri è il contesto di sicurezza nel quale si trovano le risorse INAIL (utenti, personal computers, etc.) mentre il dominio child inailservizi.inail.pri è il contesto di sicurezza nel quale sono definite le risorse server e le risorse applicative.

Alla foresta principale si affianca una foresta Active Directory di tipo Risorse basata su Microsoft Windows 2019 denominata tiucc.local necessaria per la gestione degli attributi della posta elettronica.

Per entrambe le foreste (inail.pri e tiucc.local) è attiva la sync verso Azure Active Directory (Entra) per gli oggetti di tipo Utenti e Computers.

Ulteriori foreste Active Directory presenti sono la foresta denominata inailrh.local funzionale ai servizi di re-hosting, le tre foreste EESSI funzionale alla cooperazione con altri enti europei e inailadmin.local per la gestione.

Tutte le foreste sono in alta disponibilità e distribuite sui due siti di erogazione (Santuario / Acilia) e per esigenze specifiche sono stati implementati alcuni Domain Controller di inailutenti e inailservizi anche sullo IAAS Azure.

2.10. Sistema Documentale Centralizzato

La piattaforma del sistema documentale centralizzato “DocInail” per le Unità Centrali e periferiche è realizzata con architettura applicativa a microservizi e gira su piattaforma cloud on-premise OCP4.

I dati sono memorizzati su un PDB Oracle18 su soluzione Oracle EXACC e per la parte di Document Management viene utilizzato Oracle Web Center Content.

La soluzione consta di tre interfacce web per utenti finali e un app mobile per la firma in mobilità.

Inoltre, DocInail espone tre servizi REST (Documento, Lavorazione e Archivio) attraverso i quali possono integrarsi con il protocollo informatico le altre applicazioni del dominio INAIL.

2.11. Data Lake

Il Data Warehouse di INAIL è stato migrato da Oracle DWH ad Enterprise Data HUB (denominato IANUA). IANUA si basa sul prodotto Cloudera Data Platform e si compone di Data Lake, Data Hub e Data Lab. L’infrastruttura IANUA è on-prem ed è composta da nodi master e worker con storage HDFS locale ai worker come definito nelle best practice Hadoop e reference architecture di Cloudera.

Di recente l’infrastruttura è stata estesa con ulteriori 15 nodi per soddisfare l’esigenza delle componenti Kafka-NiFi con le quali è in corso di realizzazione lo streaming near real time dei dati dai DB operazionali a IANUA.

Ad oggi l’infrastruttura consiste di 38 macchine fisiche e 22 macchine virtuali di cui 18 ospitati da nodi fisici dedicati all’infrastruttura IANUA.

3. SERVICE ORIENTED ARCHITECTURE (SOA)

L'obiettivo della SOA è quello di creare valore dalla "conoscenza" che è già all'interno dell'Istituto. L'INAIL ha pianificato una strategia globale di evoluzione del proprio Environment organizzativo e tecnologico, in modo da garantire il raggiungimento della "business flexibility" attraverso la creazione, l'orchestrazione, il riuso ed il governo di servizi ingegnerizzati nell'ottica dell'efficienza operativa, la sicurezza e le performance.

Nella SOA i Web Services possono essere visti come i "building block" per l'implementazione dei processi di business. Un processo può essere "mappato" graficamente all'interno del sistema, migliorandone il controllo e la gestione e rendendo l'IT più pronto alle costanti evoluzioni. Attualmente migrata nell'api gateway

4. ISOASEC

L'architettura SOASEC è una soluzione abilitante alla securizzazione dell'infrastruttura SOA. La soluzione coniuga l'introduzione del protocollo HTTPS per il canale di comunicazione tra i client e l'infrastruttura SOA presente in Inail con la transizione tecnologia per la componente ORACLE ESB SOA, e inoltre permetterà l'estensione dell'architettura SOASEC all'interno dei nuovi contesti tecnologici ibridi.

Con il termine SOA si indica una specifica architettura software che supporta l'uso di Web Services al fine di garantire l'interoperabilità tra diversi sistemi in modo da consentire l'utilizzo delle singole applicazioni come componenti del processo di business e soddisfare le richieste degli utenti in modo integrato e trasparente. Le tecnologie che contribuiscono all'architettura SOA sono:

- i Web Services che permettono di definire le modalità di comunicazione dei vari applicativi;
- l'Enterprise Service Bus (ESB) che ha la funzionalità di coordinare e orchestrare i vari applicativi per svolgere le funzioni di business.

Il linguaggio formale utilizzato per la creazione dei "documenti" per la descrizione di Web Service è il Web Services Description Language (WSDL) in formato XML. Il linguaggio di comunicazione della SOA è il SOAP su HTTP in cui è incapsulato il relativo messaggio. SOAP si basa sul metalinguaggio XML e la sua struttura segue la configurazione head-body, analogamente ad HTML.

Descrizione architettura di riferimento

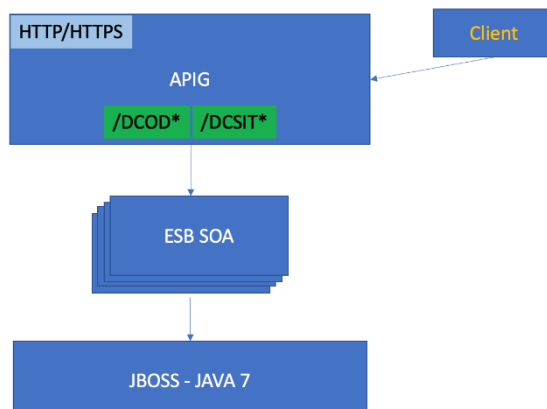


Figura 2 Architettura Logica SOASEC

In Istituto l'attuale architettura di riferimento è la seguente:

Le componenti tecnologiche dell'architettura SOASEC sono:

- **Client:** applicazioni client dei servizi SOA non censiti per definizione architetturale

- **API Gateway SOASEC:** è la componente di Front End che si occupa di ricevere le richieste da parte delle applicazioni client ed instradarle verso il servizio SOA di Back End corretto; tale componente si comporta come proxy/orchestratore dei servizi SOA
- **Oracle ESB SOA:** è la componente di Front End non securizzata che si occupa di ricevere le richieste da parte delle applicazioni client ed instradarle verso il servizio SOA di Back End corretto; tale componente si comporta come proxy/orchestratore dei servizi SOA.
- **Red Hat JBoss 7/11:** è l'application server di Back End utilizzato per erogare e gestire i servizi SOA; tale componente si appoggia su Java 7/11 e i Web Services sono sviluppati secondo lo standard SOAP/XML.

Le principali funzionalità di APIG SOASEC sono:

1. **Gestione delle Richieste:**

L'API Gateway SOASEC riceve e inoltra le richieste dai client alle risorse appropriate all'interno del sistema distribuito.

All'interno di API Gateway i servizi SOA sono pubblicati utilizzando la tipologia di servizio SOAP Web Service. I servizi così pubblicati sono:

- Servizi in modalità "solo routing": i servizi inoltrano le richieste all' Oracle ESB SOA;
- Servizi in modalità "puntuale": i servizi richiamando direttamente i web services, la logica applicativa by-passa la componente Oracle ESB.

In aggiunta a questi servizi, sono presenti Servizi CoreSOA, utilizzati per effettuare specifiche operazioni necessarie per la corretta operatività della piattaforma SOASec; tali servizi sono divisi in tre tipologie:

- config: sono i servizi deputati alla gestione centralizzata della configurazione di alcuni parametri dell'infrastruttura SOASec;
- log: sono i servizi deputati alla gestione dell'invio dei log alle piattaforme di "log collection" esterne;
- wsdl: sono i servizi deputati alla gestione delle richieste per ottenere i file descrittori di uno specifico servizio

2. **Sicurezza:**

- Protezione del canale di comunicazione:** la comunicazione avviene su protocollo HTTPS;
- Protezione di messaggio:** la comunicazione avviene solo tramite parsing del protocollo SOAP/XML;
- Monitoraggio:** il monitoraggio delle prestazioni di SOASEC avviene tramite i sistemi di monitoraggio nativi della piattaforma Dynatrace;

- d. **Analisi e Audit:** l'analisi del traffico a fini di troubleshooting e audit avviene tramite la piattaforma ONEAudit con cui APIG SOASEC è integrato.

4.1.1. Architettura fisica

L'architettura fisica nei vari ambienti e si composta:

- Collaudo: OVA v11 in singola istanza;
- Certificazione: OVA v11 in cluster multi-node nel numero di 2;
- Produzione: OVA v11 in cluster multi-node nel numero di 2.

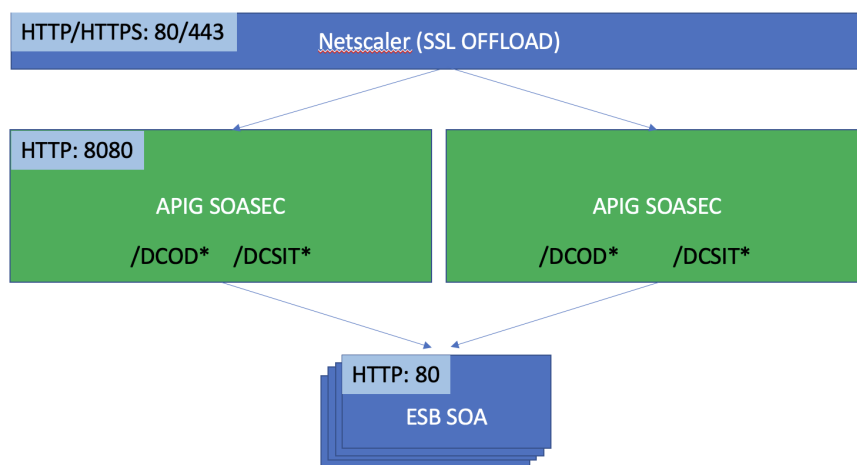


Figura 3 Architettura Fisica SOASEC

5. API REST GATEWAY

Nell'architettura applicativa generale INAIL, nell'ambito della gestione dei servizi, è presente una infrastruttura di API Gateway che protegge l'accesso ai servizi INAIL (API REST/ SOAP).

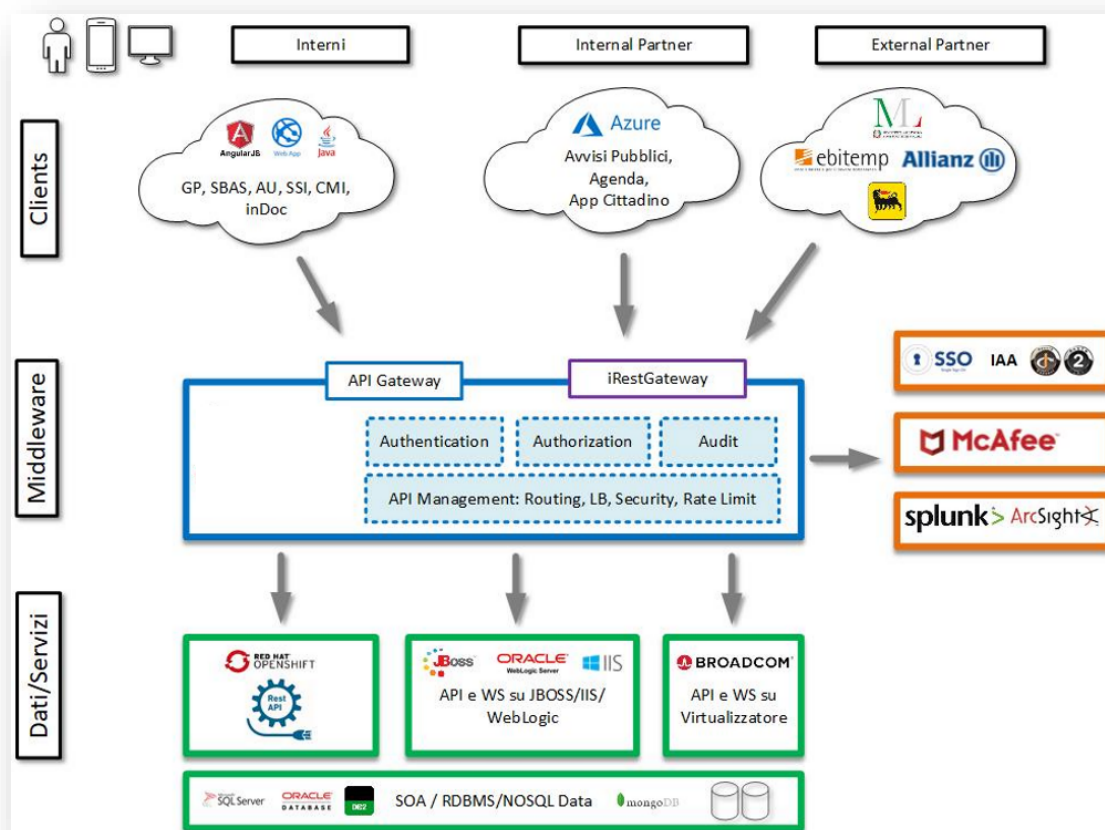
Tale infrastruttura comprende API Gateway di diverse tecnologie con vari ruoli a protezione di:

- Servizi on premise
- Servizi cloud istituzionali
- Servizi in interoperabilità

Questo layer infrastrutturale permette di orientarsi verso un'architettura API-Based che ha una valenza abilitante sia per l'esposizione di servizi verso client Web Intelligenti, sia per servizi da erogare in mobilità ad App istituzionali, estendendo il paradigma SOA alla Mobility.

Altresì, l'API Gateway è l'oggetto abilitante per l'applicazione del modello architetturale a Microservizi, consentendo la realizzazione di applicazioni software più moderne e per tutti i casi di decomposizione di applicazioni "monolitiche" tramite l'applicazione di "Pattern di Trasformazione".

L'architettura base di riferimento dell'API Gateway è rappresentata nell'immagine seguente.



In tale scenario, l'API Gateway è l'elemento centrale necessario a rendere la suddetta architettura sostenibile, sicura e scalabile e rappresenta il componente per governare tutte le comunicazioni tra client e servizi API erogati dall'Istituto, ma anche per la fruizione di servizi erogati da soggetti esterni all'Istituto.

Pertanto, è il componente verso il quale dovranno convergere tutte le chiamate a API, siano esse in ingresso o in uscita.

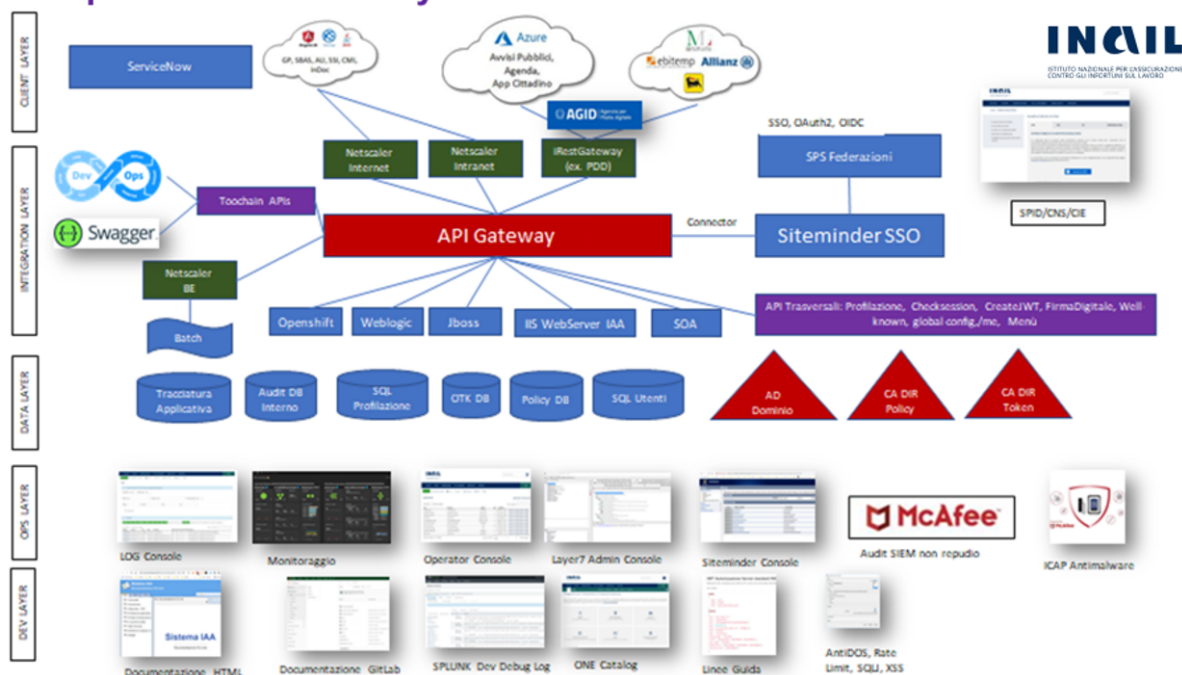
L'API Gateway è integrato con il Sistema di Controllo degli Accessi, interagendo con il sistema di Single Sign ON e con il sistema di strong authentication di Microsoft (MFA) che svolge i ruoli di:

- Autenticazione
- Autorizzazione
- Verifica del token
- Protezione delle API (in aggiunta ai sistemi di protezione perimetrali del SOC)

In aggiunta a questi ruoli principali l'API Gateway interagisce con vari componenti applicativi e infrastrutturali dell'Istituto per altre finalità quali

- Interazione con il servizio DevOps per la pubblicazione di policy ed API
- Federazione con altri sistemi di autenticazione e autorizzazione
- Integrazione con Service Now
- Integrazione One Catalog (catalogo unico dei servizi INAIL)
- Integrazione con l'audit centralizzato
- Integrazione con console e dashboard di monitoraggio

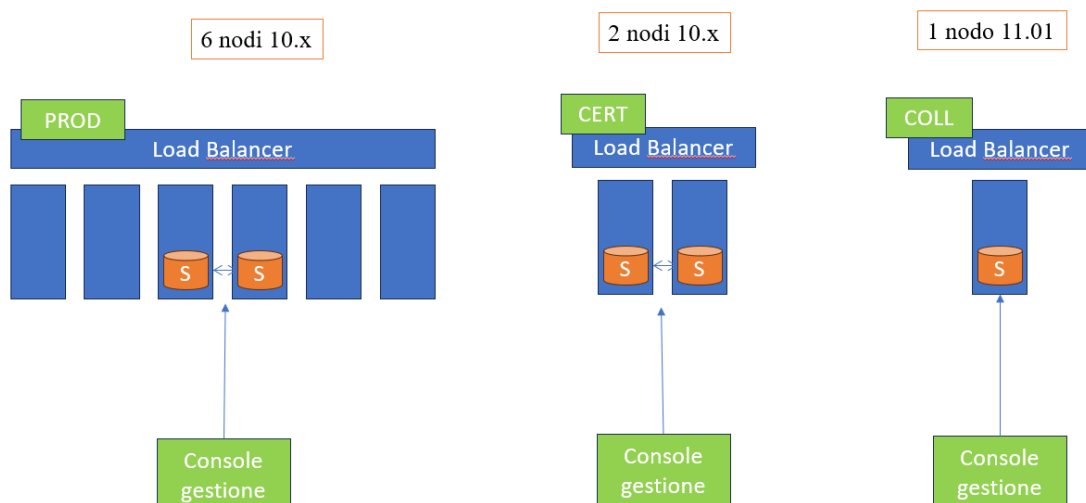
Componenti API Gateway



5.1. Architettura di riferimento

Attualmente l'APIG è rilasciato nella 3 infrastrutture INAIL di riferimento: Collaudo, Certificazione e Produzione.

La quantità di nodi e l'architettura di riferimento è rappresentata nel disegno:



5.2. Piattaforma Digital Nazionale Dati

La PDND è gestita dalla PCM (presidenza Consiglio dei Ministri) ed è costituita da un'infrastruttura tecnologica che rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici [...], mediante l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa, nonché la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite.

La condivisione di dati e informazioni avviene attraverso la messa a disposizione e l'utilizzo, da parte dei soggetti accreditati, di interfacce di programmazione delle applicazioni (API). Le interfacce, sviluppate dai soggetti abilitati con il supporto della PCM e in conformità alle Linee guida AgID in materia interoperabilità, sono raccolte nel "catalogo API" reso disponibile dalla Piattaforma ai soggetti accreditati.

In fase di prima applicazione, la Piattaforma assicura prioritariamente l'interoperabilità con le basi di dati di interesse nazionale [...] e con le banche dati dell'Agenzia delle entrate individuate dal Direttore della stessa Agenzia.

La nuova modalità di integrazione denominata "Interoperabilità" andrà pian piano a sostituire l'attuale integrazione fra enti denominata realizzata con la PDD (SPC): "Porta di Dominio". I concetti fondamentali non cambiano, ma la piattaforma tecnologica a supporto è stata evoluta per adeguarsi alle nuove Linee Guida AGID.

Le Nuove Linee Guida AGID indirizzano questi concetti fondanti:

- **pattern di interoperabilità**, ovvero la definizione di una soluzione a una esigenza di scambio di messaggi e informazioni, declinata in una specifica tecnologia. Si suddividono in:
- **pattern di interazione**, puntualizzano le modalità tecniche per implementare i modelli di scambio dei messaggi (anche detti message exchange patterns), necessari all'interazione tra i sistemi informatici di erogatori e fruitori;
- **pattern di sicurezza**, individuano le modalità tecniche per assicurare che i pattern di interazione rispettino specifiche esigenze di sicurezza (autenticazione e autorizzazione delle parti, confidenzialità delle comunicazioni, integrità dei messaggi scambiati, . . .) negli scambi realizzati;
- **profili di interoperabilità**, la combinazione di più pattern per descrivere le esigenze di specifici domini di interoperabilità, quale ad esempio il non ripudio delle comunicazioni e/o dei messaggi scambiati.

Nel presente documento si descrive quindi la declinazione INAIL del "Pattern di Interoperabilità" e del "Profilo di Interoperabilità": <https://www.inail.it/api/docs/home>.

5.3. Nuovo modello interoperabilità (MoDI)

Il Modello di Interoperabilità delle PA (MoDI) rende possibile la collaborazione tra PA e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l'interazione e lo scambio di informazioni senza vincoli sulle implementazioni.

Nell'ambito del MoDI si utilizza il termine generico API per indicare indifferentemente le WebAPI, i webservice e le APIREST. In tal senso assorbe ed estende SPCoop. Mantiene lo scambio di servizi basati su XML/SOAP ma elimina la busta eGov.

Il MoDI è definito dalle Linee Guida (LG) adottate da AgID ai sensi dell'articolo 71 del CAD e nello specifico Determinazione AgID n.547 Ottobre e n.627 Dicembre 2021.

INAIL ha adottato il MoDI dal 2019 ed è attualmente lo standard in essere per le comunicazioni in Outbound e Inbound da e verso INAIL. Sono stati integrati queste tipologie di cooperanti: ENTI, PRIVATI, HYBRID CLOUD.

5.4. I profili di sicurezza INAIL

Gli scenari implementati seguono le LG emesse da AGID. In particolare: "LG AGID" (https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilitadocs/it/bozza/doc/istruzioni_consultazione.html).

Gli scenari disponibili per le connessioni interoperabili sono classificati come:

- Sicurezza Canale: gestione della sicurezza inerente il canale di comunicazione tra i domini fruitore ed erogatore. La specifica prevede i seguenti due pattern:
 - ID_AUTH_CHANNEL_01 - Direct Trust Transport-Level Security: comunicazione basata sul canale TLS dopo aver effettuato il trust del certificato X509 fornito dal dominio erogatore.
 - ID_AUTH_CHANNEL_02 - Direct Trust mutual Transport-Level Security: comunicazione basata sul canale TLS dopo aver effettuato il trust dei certificati X509, del fruitore e dell'erogatore, nella modalità di mutua autenticazione.
- Sicurezza Messaggio: gestione della sicurezza inerente lo scambio di informazioni tra le applicazioni agli estremi del flusso di comunicazione. I pattern di sicurezza previsti si distinguono per il caso SOAP e per quello REST:
 - ID_AUTH_SOAP_01 o ID_AUTH_REST_01 - Direct Trust con certificato X.509 su SOAP o REST: Tramite la validazione del certificato X509, inserito dall'applicazione mittente nel token di sicurezza della richiesta, l'applicativo destinatario verifica la corrispondenza delle identità e la validità del messaggio, prima di procedere con la produzione della risposta attraverso un trust tra fruitore e erogatore basato su certificati x509.
 - ID_AUTH_REST_01 tramite la Piattaforma Digitale Nazionale Dati (PDND): con l'aggiornamento delle linee guida nella "Determinazione n. 128 del 23 maggio 2023", viene indicato di utilizzare la PDND per ottenere un token conforme al pattern ID_AUTH_REST_01; la costituzione del trust avviene attraverso il materiale crittografico depositato sulla PDND applicando i profili di emissione dei voucher previsti.
 - ID_AUTH_SOAP_02 o ID_AUTH_REST_02 - Direct Trust con certificato X.509 su SOAP o REST con unicità del messaggio/token: estensione dei pattern precedenti con l'aggiunta di un meccanismo di filtro che impedisce il processamento di un messaggio duplicato.

- INTEGRITY_SOAP_01 o INTEGRITY_REST_01 - Integrità del payload del messaggio SOAP o REST: pattern che estende i precedenti aggiungendo la gestione della firma del payload come verifica di integrità del messaggio ricevuto.
- INTEGRITY_REST_02 - Integrità del payload delle request REST in PDND: simile al precedente pattern INTEGRITY_REST_01, assume che il trust avvenga tramite il materiale crittografico depositato sulla PDND applicando i profili di emissione dei voucher previsti. All'interno del token viene indicato l'identificativo della chiave pubblica (kid) associata alla chiave privata utilizzata dal client per firmare il token di integrità; identificativo kid generato dalla PDND e recuperabile dall'erogatore tramite le API messe a disposizione dalla PDND stessa.
- PROFILE_NON_REPUDIATION_01 - Profilo per la non ripudiabilità della trasmissione: estende i pattern di integrità allo scopo di fornire una conferma al fruitore da parte dell'erogatore della ricezione del contenuto della richiesta. Descrive inoltre la necessità di definire un arco temporale di persistenza dei messaggi utile per soddisfare l'opponibilità ai terzi.

INAIL ha scelto di utilizzare per tutti i servizi esposti in Interoperabilità tramite PDI: ID_AUTH_CHANNEL_02 + ID_AUTH_REST_02.

Il layer informatico che implementa la soluzione di Interoperabilità è denominato PDI.

5.5. Azure API Manager

All'interno dell'infrastruttura API Gateway adottata dall'Istituto, è presente la componente cloud Azure API Management (APIM). Questo particolare API Gateway è un componente essenziale che funge da punto di accesso unificato per le applicazioni client che intendono accedere a servizi distribuiti tra l'infrastruttura Azure cloud e quella On-Premises.

Le principali funzionalità di APIM sono:

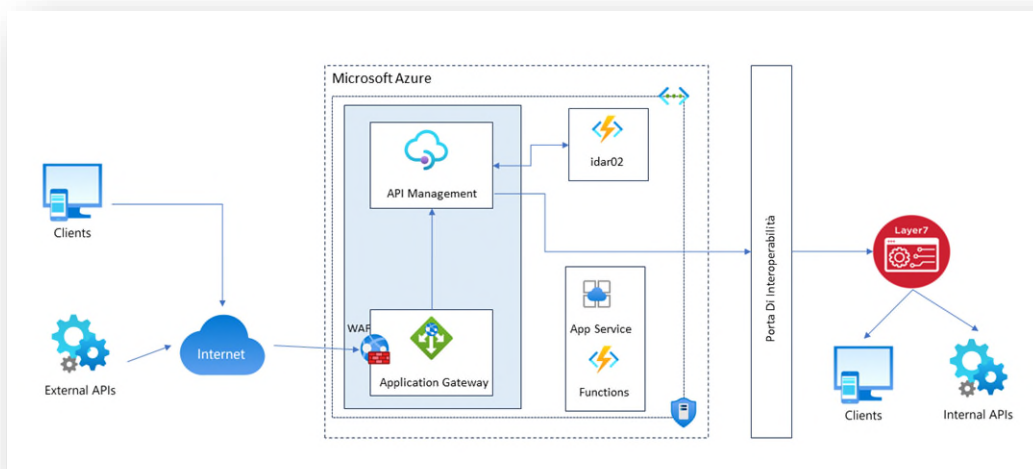
1. **Gestione delle Richieste:** L'API Gateway riceve e instrada le richieste dai client alle risorse appropriate all'interno del sistema distribuito.
2. **Sicurezza:** APIM offre le seguenti funzionalità di sicurezza fondamentali per proteggere le API esposte e garantire la protezione dei dati:
 - **validazione del JWT:** per poter consumare un'API esposta tramite APIM, il client deve presentare un JWT valido rilasciato tramite Azure Active Directory (AAD) o tramite Azure B2C; tale JWT, a seconda della tipologia di flusso, deve contenere specifici claim autorizzativi.
 - **protezione del canale di comunicazione:** la comunicazione avviene su protocollo HTTPS
 - **protezione del canale di comunicazione con il mondo On-Premises:** al fine di garantire l'interazione tra le componenti On-Premises e quelle ospitate in Cloud, l'Istituto ha abilitato una connessione

sicura tra l'ApiGateway On-Prem e l'ApiGateway in Cloud utilizzando la componente "iRestGateway"; tale connessione garantisce:

1. Riservatezza: la comunicazione avviene su protocollo https;
 2. Immutabilità delle due componenti: la connessione viene stabilita previa mutua autenticazione;
 3. Utilizzo di subset di Token JWT firmati, approvati e codificati dall'istituto specifici per ogni scenario coinvolto.
3. Monitoraggio e Analisi: il monitoraggio delle prestazioni di APIM avviene tramite i sistemi di monitoraggio nativi della piattaforma Azure, mentre l'analisi del traffico a fini di Audit avviene tramite la piattaforma ONEAudit con cui APIM è integrato.
4. Scalabilità: APIM è configurato in modalità "auto-scale" per permettere di gestire carichi di lavoro variabili e di scalare orizzontalmente per soddisfare le esigenze di traffico in costante evoluzione.

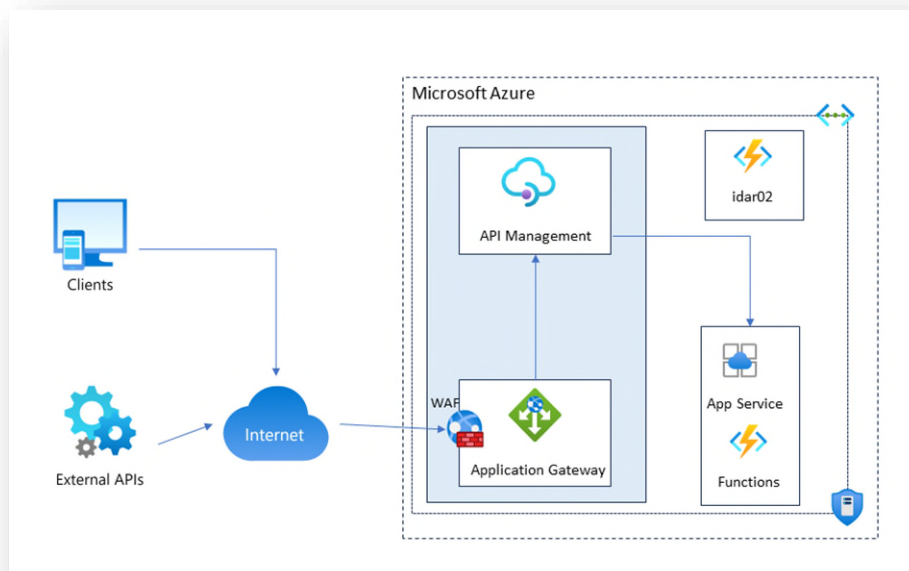
I flussi di comunicazione attualmente implementati presso l'istituto sono:

1. **Flow Azure to On-Premises:** in questo caso il client può essere una Mobile App su Internet o un'applicazione pubblicata sul Cloud Azure, mentre il servizio è pubblicato sui sistemi On-Premises. In questo caso i servizi esposti da APIM hanno la funzione di Proxy di API On-Premises.



In questo scenario la generazione dell'access_token è in carico alle componenti AAD/B2C (a seconda della tipologia di utente). La componente APIM si occupa della verifica dell'access_token presentato dal client e della generazione di un JWT riconosciuto da APIGateway On-Premises.

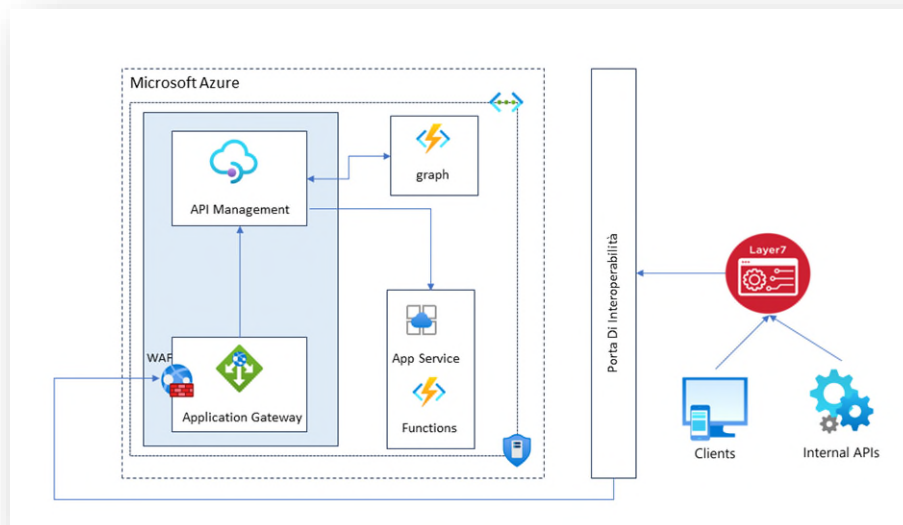
2. **Flow Azure to Azure:** in questo caso il client può essere o una Mobile App su Internet o un'applicazione pubblicata sul Cloud Azure, mentre il servizio è una Azure Function o un Azure App Service pubblicato sul Cloud Azure.



In questo scenario la generazione dell'`access_token` è in carico alle componenti AAD/B2C (a seconda della tipologia di utente). La componente APIM si occupa della verifica dell'`access_token` presentato dal client e dell'instradamento della richiesta verso la componente di BackEnd presente in Cloud.

3. **Flow On-Premises to Azure:** in questo caso il client può essere un'applicazione pubblicata sui sistemi On-Premises, mentre il servizio richiamato è una Azure Function o un Azure App Service pubblicato sul Cloud Azure. Anche in questo caso l'interazione avviene tra componenti ospitate in Cloud e componenti ospitate On-Premises, ma il flusso viene seguito in verso contrario. La generazione dell'`access_token` è in carico alla componente On-

Premises SiteMinder; la componente APIG si occupa della verifica dell'access_token presentato dal client e della generazione di un JWT riconosciuto dalla componente di BackEnd presente in Cloud.



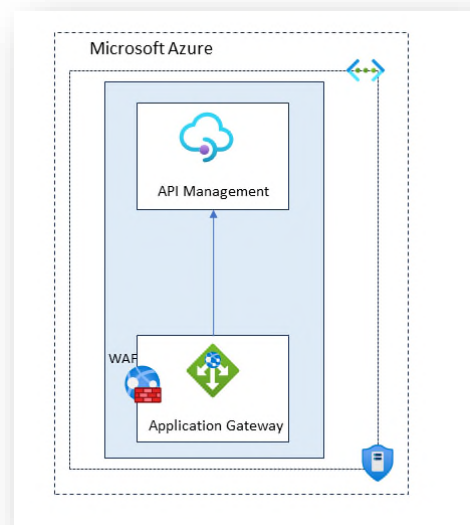
5.5.1. Architettura di riferimento

Attualmente APIM è rilasciato nei 3 ambienti INAIL di riferimento: Collaudo, Certificazione e Produzione. L'architettura di riferimento è rappresentata nel disegno accanto.

APIM risiede all'interno di una specifica Virtual Network ed è posizionato a valle di un'Application Gateway che ne garantisce la segregazione.

Di seguito si riporta la numerosità delle istanze di APIM in base all'ambiente:

- collaudo: 1 singola istanza;
- certificazione: da 6 a 12 istanze con configurazione "auto-scale";
- produzione: da 6 a 12 istanze con configurazione "auto-scale".



5.6. IBM Aspera

IBM Aspera è lo standard adottato in INAIL per upload/download di file. Si tratta di una soluzione avanzata per il trasferimento rapido e sicuro di file di grandi dimensioni attraverso reti IP. Aspera utilizza un protocollo di

trasferimento chiamato FASP (Fast, Adaptive, and Secure Protocol) per ottimizzare la velocità di trasferimento, riducendo la dipendenza dalle limitazioni di larghezza di banda e garantendo la sicurezza dei dati durante il trasferimento. IBM Aspera offre diverse API che consentono agli sviluppatori di integrare le funzionalità di trasferimento rapido e sicuro di file nei propri progetti e applicazioni. Queste API sono integrate con l'API Gateway che agisce come punto di ingresso centralizzato per la gestione, il monitoraggio e la sicurezza delle API.

6. OCP

La piattaforma OCP è dedicata all'erogazione delle applicazioni a micro-servizi.

La piattaforma è stata realizzata su un cluster VMware ospitato dalla piattaforma hardware VXBLOCK e storage DELL

Nello schema sottostante viene riportato il numero delle VM che realizzano la piattaforma distribuite per ruolo.

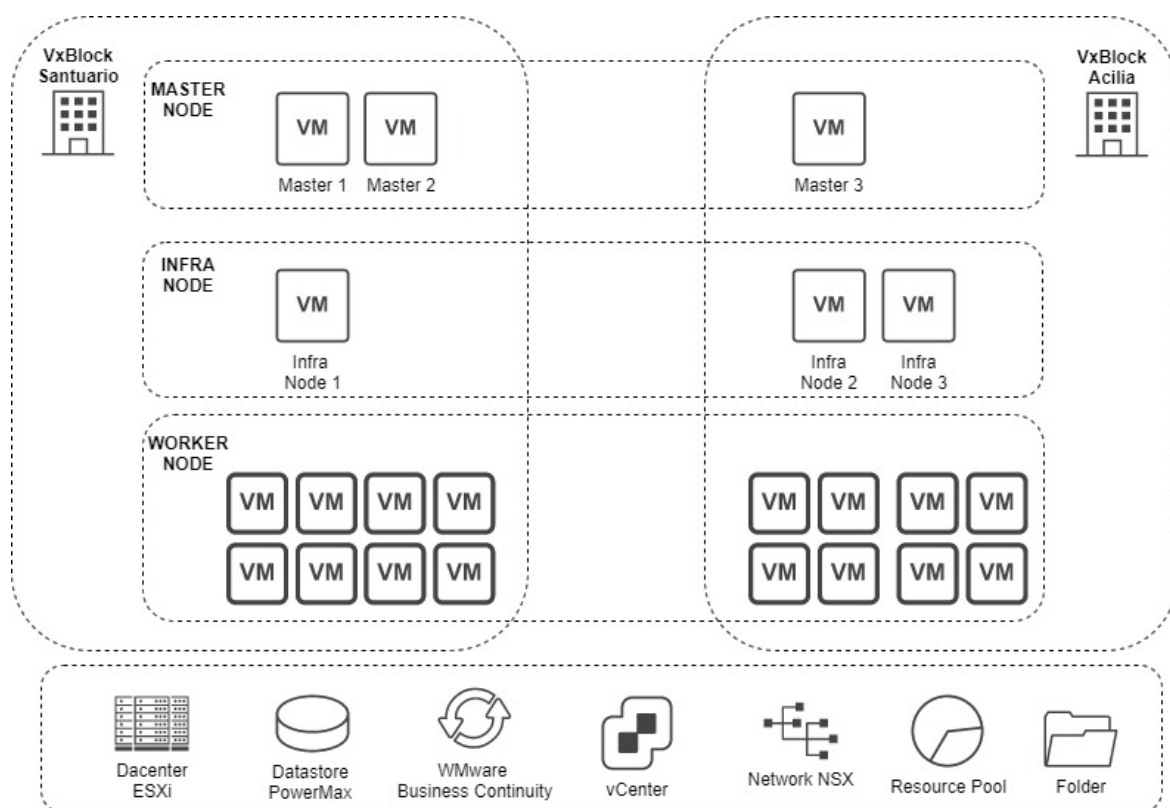


Figura 4 – Schema architetturale HL di OCP

La versione di riferimento per la piattaforma di OCP è la versione 4.18 ed è dislocata presso i Data Center Santuario, Acilia e Bari Casamassima (DR)

Openshift ospita come servizi base:

- AMQ Stream (Kafka) per la gestione delle code;
- Service mesh per l'interoperabilità dei servizi;
- ODF per la gestione della persistenza dello storage e non;
- Agent Splunk per collezione i log e inviarli al sistema log management;
- Agent Dynatrace per monitorare il sistema;
- Oadp strumento per schedulare i backup.

Di seguito i dati di riepilogo relativi alle versioni dei prodotti

software	modulo	versione
OCP	Red Hat OCP	4.18
Sistema operativo	RHCOS	4.x
AMQ	ation AMQ Stream	2.2.0
ODF	Foundation	4.x

7. SISTEMI DI MESSAGING

Per quanto riguarda i servizi di Event/Message Broker, la soluzione implementata in INAIL utilizza la tecnologia Red Hat AMQ basata su community open source come Apache ActiveMQ e Apache Kafka eseguiti all'interno di un cluster OpenShift consentendo così ai micro-servizi e ad altre applicazioni di condividere dati con un throughput estremamente elevato ed una latenza estremamente bassa.

Le versioni attualmente in uso sono:

- Queue: Red Hat AMQ Broker 7.8;
- Red Hat Integration AMQ Stream 2.2.0.

8. DATABASES SQL E NOSQL

Le Basi Dati DB2, ORACLE, SqlServer, Mongo e Postgresql sono presenti sia sull'ambiente distribuito AIX (Unix) che sulle piattaforme Linux, Windows e sono relative ai servizi online interni esterni, del portale INAIL, del sistema di autenticazione e del MdS.

Oracle DBMS su Red Hat Linux (ad esclusione dei servizi su EXACC) è in configurazione cluster e modalità Active – Data Guard sui due DC; Le versioni di riferimento sono la 18 , 19c e 26ai su Oracle EXXACC e dalla 11 alla 19c per Oracle On Prem x86.

- Installazioni Microsoft Windows SQL Server sono in configurazione cluster geografico, esteso sui due siti, mediante tecnologia storage DELL-power max; DB2 LUW;

Il DB2 luw è ospitato su piattaforma aix installato in modalità Purescale

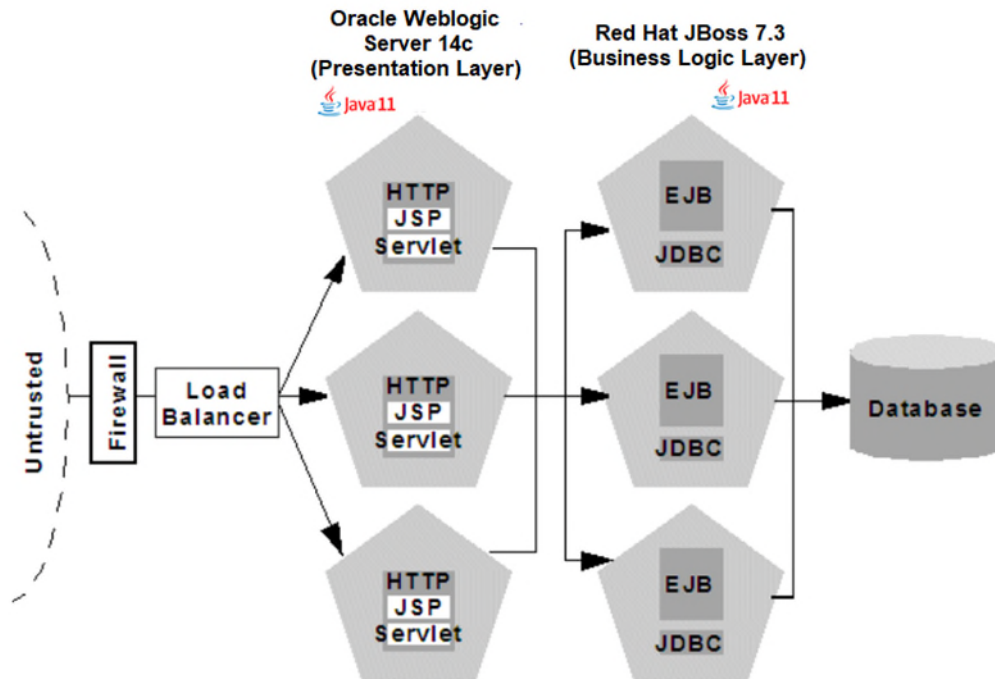
ospita la base dati per le principali applicazioni istituzionali

Altri DBMS di riferimento sono:

- PostgreSQL ;
- MySQL
- MongoDB.

9. APPLICATION SERVER

Lo scenario di deploy principale dei progetti di sviluppo software basati sul modello Three-Tier è realizzato su un'infrastruttura on-premise ed è costituito da un cluster per il Presentation Layer e da un cluster per il Business Logic Layer con le componenti tecnologiche rappresentate nello schema:



Le componenti tecnologiche, framework e software di base sono le seguenti:

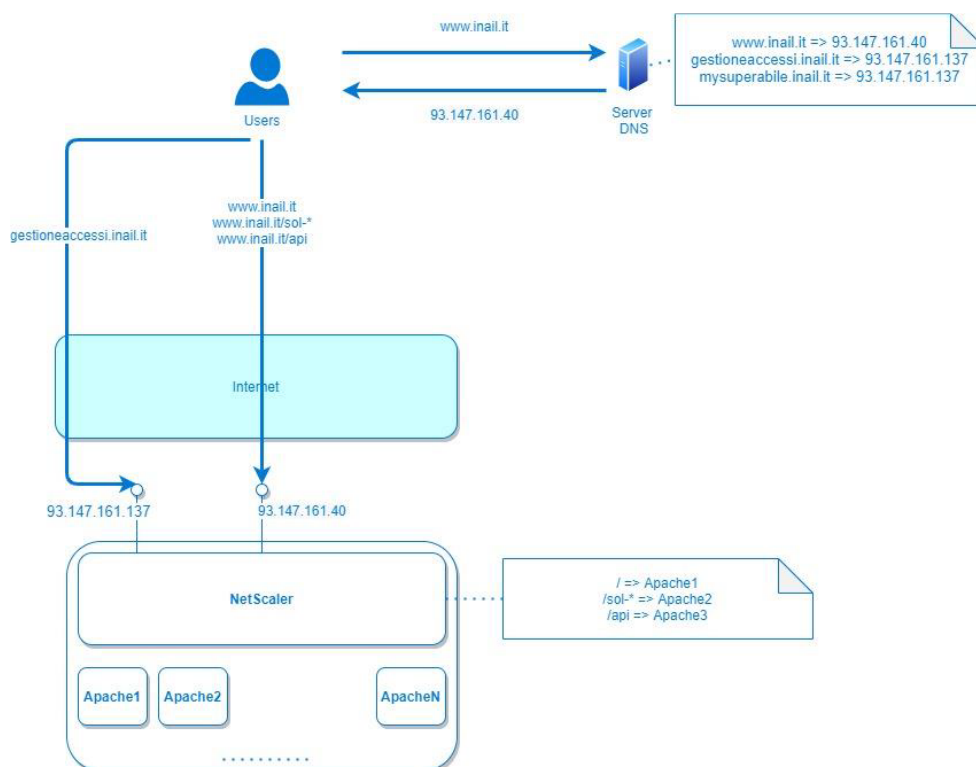
- Presentation Layer: Oracle Weblogic Server 14c + Oracle JDK 11;
- Business Logic Layer: Red Hat JBoss 7.4 + Oracle JDK 11.

Per garantire un miglior supporto ed agevolare le attività di gestione, si consiglia l'utilizzo del sistema operativo Red Hat Enterprise Linux 8.

10. ARCHITETTURA TECNOLOGICA E INFORMATIVA DI PORTALE

10.1. Il portale pubblico

10.1.1. Adobe Experience Manager (cloud)



La nuova architettura scelta per il portale, dopo Oracle Wcs, d'accordo con la politica Dcod di adesione al cloud del 2020, è Adobe Experience Manager, suite di prodotti per la gestione dei contenuti (Sites), delle risorse multimediali (Asset), delle campagne multicanale (Ajo), dei moduli adattivi nonché la realizzazione applicativa di Pdf (Forms) e della raccolta e l'analisi dei dati di navigazione utente (Analytics). La suite integra e consente la più flessibile gestione di tutti i prodotti acquisiti. L'integrazione della piattaforma in ecosistema Inail ha previsto nel 2021 una intensa attività organizzativa nonché infrastrutturale per armonizzare il cambiamento tecnologico.

La suite contiene anche altri prodotti come:

- **Target** A/B testing e personalizzazione multicanale per migliorare l'esperienza utente,
- **App Builder** che estende le capacità e la logica di business di Adobe Experience Manager a tutte le soluzioni Adobe e al resto dello stack IT, in modo da costruire facilmente microservizi personalizzati e applicazioni a pagina singola
- **Places** servizio di geolocalizzazione che consente alle app mobili dotate di awareness della posizione di contestualizzare quest'ultima mediante l'uso di interfacce SDK avanzate e facili da usare, associate a un database flessibile di punti di interesse (POI).

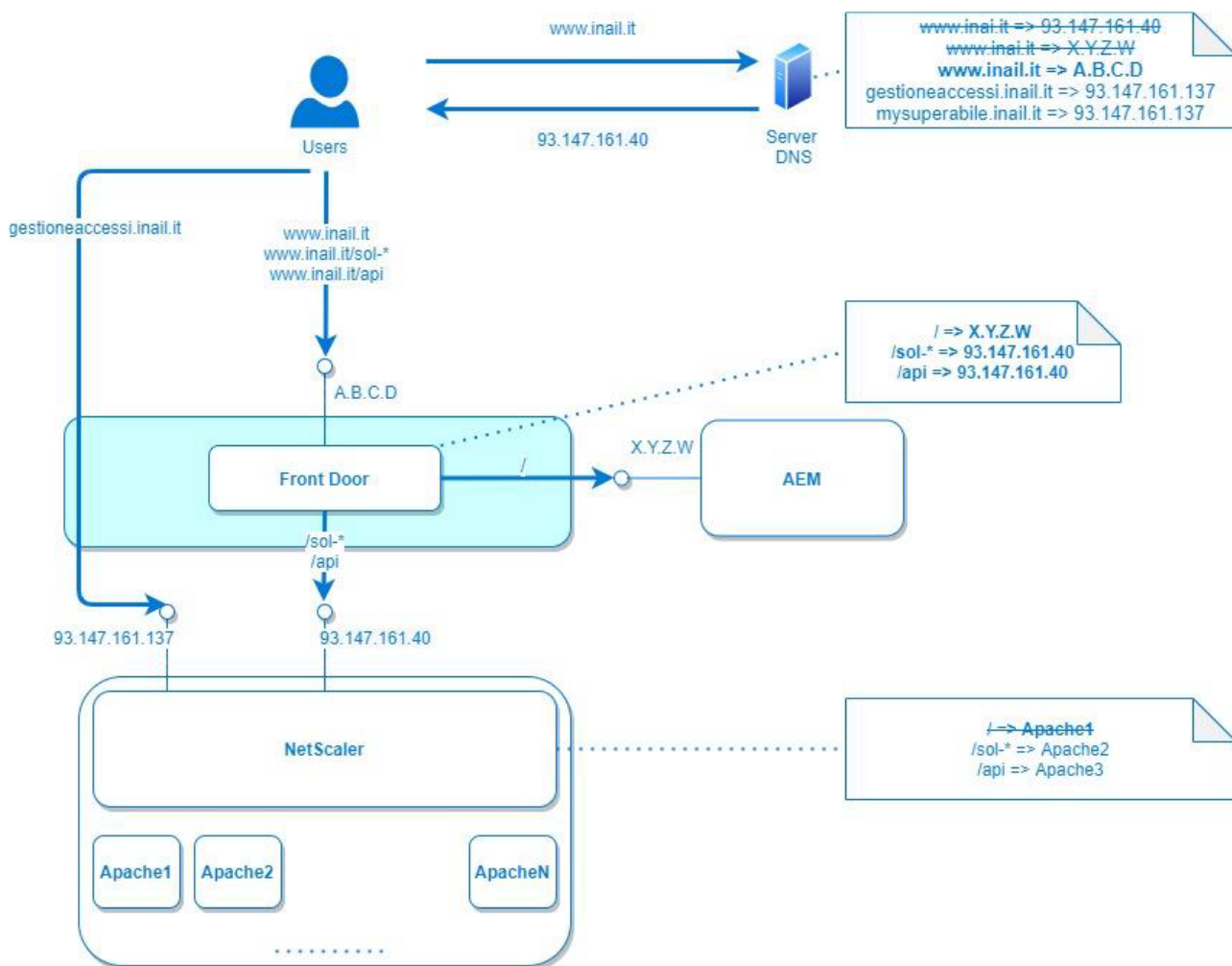
utilizzabili per vari scopi e necessità.

10.1.1.1. Integrazione in ecosistema INAIL

Per mantenere il dominio `www.inail.it` su piattaforma Adobe e gestire anche le richieste alle API e ai servizi online allo stesso indirizzo è stato necessario introdurre un elemento di tipo application gateway, la scelta architetturale è ricaduta sull'esistente Microsoft Front Door, che applica le regole di livello applicativo (Level 7) e sulla base del context path smistano il traffico 1) verso il portale Adobe, 2) verso le risorse pubbliche di Inail. È stato previsto e ben gestito un impatto sul routing del traffico che coinvolge API e servizi online.

Per il Portale Adobe, il NetScaler effettua l'operazione di forward verso Front Door allo stesso modo di come avviene verso gli Apache on premises. Le API indicate sui flussi in rosso verranno chiamate tramite Internet su `www.inail.it`. Occorre assicurare l'host name preservation al fine di evitare la serie di inconvenienti descritti nella documentazione di Front Door circa cookie, URL, etc.

Per consentire la comunicazione tra job che girano su AEM (es. Convenzioni) e le relative API on premises anche in ambienti di preproduzione, si è scelto utilizzare una VPN Site to Site che, pur introducendo un elemento architetturale aggiuntivo, impatta una funzionalità circoscritta e di fatto lascia l'architettura identica tra gli ambienti di Collaudo e Produzione per tutte le altre funzionalità.



10.1.1.2. Architettura Adobe

La piattaforma Adobe supera il concetto di content management system verso un più completo ed evoluto digital experience manager¹, e si pone come middleware per low code integration di esperienze digitali. In particolare, AEM Sites è composto da:

- Un'istanza di publishing, area di pubblicazione isolata fisicamente dal motore di gestione di contenuti e servizi;
- L'istanza di authoring, che permette la gestione dei flussi redazionali, l'acquisizione e conservazione ordinata e catalogata delle risorse digitali, la configurazione delle integrazioni con i servizi di backend; presente inoltre una interfaccia classica, WCM, per personale con taglio tecnico contenente funzioni per amministratori, in particolare la gestione dei Replication Agent cui sono veicolati i flussi di pubblicazione;
- Un'interfaccia (CRXDE Lite) che fornisce agli utenti di backend una vista sul repository documentale (modulo Asset), l'engine del prodotto basato su JackRabbit OAK, e consente oltre all'esplorazione ed il monitoraggio degli oggetti in repository l'estensione o la modifica dei componenti predefiniti e dei bundle Java;
- Una interfaccia Web Console Configuration, dedicata alla gestione di configurazione e monitoraggio del sistema;
- una Cloud Console Manager, per la centralizzazione ed il governo degli strumenti di sviluppo e customizzazione basati su tecnologie open source (Git) e altamente configurabili (YAML).

Grazie all'impiego del framework Sling qualsiasi elemento della piattaforma, incluse configurazione, monitoraggio ed amministrazione, vengano esposte tramite verbi http ad endpoint ReST, per l'invocazione da altri software in modalità headless.

L'engine è costituito da un repository conforme allo standard JCR, implementazione custom di Apache Jackrabbit OAK, e sul concetto di asset: tutto ciò che risiede in una istanza di authoring, componenti interni dell'istanza (workflow, connettori, componenti) come pure contenuti documentali, templates, articoli pubblicati, commenti degli utenti, immagini, ecc., è gestito come un oggetto del repository, ossia un oggetto corredato di metadati archiviato in un file system logico organizzato gerarchicamente come un tree simile a quello di un sistema operativo linux.

Questa caratteristica fa sì che ci sia la massima flessibilità nella definizione di gerarchie e attributi: un repository flat, dove ogni oggetto è istanza della stessa classe astratta (asset) senza rigide gerarchie, permette di declinarvi sopra qualsiasi modello organizzativo di mappa mentale e concettuale per la gestione di qualsiasi aspetto (redazioni, profilazione, architettura dell'informazione, tassonomie e gerarchie, ecc.ecc.).

¹ Gartner definisce DXP – Digital Experience Platform, “come un pezzo di tecnologia integrato e coeso progettato per consentire la composizione, la gestione, la consegna e l'ottimizzazione di esperienze digitali contestualizzate attraverso percorsi multicanale dell'esperienza utente”.

La piattaforma è dotata di un motore di ricerca basato su tecnologia open Solr (Apache Lucene) e permette sia di navigare le classificazioni realizzate nell'Architettura dell'Informazione con prestazioni quasi in tempo reale, che interagire col repository e con l'engine con grande semplicità e rapidità (Omni Search Bar).

L'intera filiera delle funzioni viene erogata attraverso il motore di workflow (interno e proprietario) di AEM, senza sviluppo di codice.

La profilatura in ambito di console editoriale è estremamente semplice ed efficace, permette di calare modelli organizzativi complessi tramite la distribuzione di ACL molto granulari (7 elementi: Lettura, Modifica, Creazione, Cancellazione, Lettura ACL, Scrittura ACL, Replica= Pubblicazione) agli utenti così come a gruppi.

La ricchezza delle funzioni offerta dall'interfaccia AEM-WCC fa sì che l'oggetto possa essere esercitato, in termini sistemistici, con pochissimo sforzo: grazie all'impiego di una java virtual machine basata sugli standard OSGi (Felix) è possibile la modifica 'a caldo' dei componenti direttamente da interfacce web o invocazioni ReST.

10.2. Sistemi integrati nel portale

10.2.1.1. Inail Risponde (Service Now)

La sezione Supporto del portale è in gran parte ospitata sul prodotto SaaS Service Now, che mette a disposizione strumenti per l'apertura di ticket utente, knowledge base e FAQ. L'integrazione nel portale, pur essendone parte integrante, è effettuata attraverso meccanismi di sincronizzazione custom, volti a indicizzare le risorse informative di Service Now e metterle a disposizione degli utenti che effettuano una ricerca sul portale.

L'integrazione con il portale viene effettuata tramite API.

10.2.1.2. Applicazioni e funzionalità ospitate nel portale

Non possono esistere applicazioni autenticate integrate nelle pagine pubbliche del portale; tuttavia, è possibile estendere le funzionalità del portale tramite Adobe App Builder, feature disponibile nella suite AEM. Nei casi di riuso è possibile l'integrazione di servlet o tecnologie simili es. API pubbliche esterne. Occorre sempre assicurare l'integrazione nel sistema di raccolta dei dati di navigazione utente (Analytics).

L'applicazione "cerca patronati" è una servlet integrata nella relativa pagina del portale Adobe.

Le mappe per la geolocalizzazione sono integrate nel portale attraverso il consumo di API.

10.2.1.3. Assistenti virtuali

Il portale pubblico dal 2017 al 2020 disponeva di un unico assistente virtuale, addestrato per rispondere in linguaggio naturale a domande sul tema della registrazione utente al portale con credenziali proprietarie, argomento molto complesso sul quale venivano aperti moltissimi ticket sul Contact Center. L'assistente virtuale è stato dismesso poco dopo l'integrazione del portale nei sistemi SPID, CIE e CNS.

Dalle analisi effettuate sull'utilizzo dello strumento, per il portale pubblico non si sente il bisogno di un assistente virtuale.

10.3. Gestione accessi e profilazione

Come tutte le Pubbliche Amministrazioni, l'INAIL nell'erogare i servizi digitali è conforme alle indicazioni normative del CAD e implementa il protocollo SAML per l'autenticazione così come disciplinato dalle norme tecniche del Sistema Pubblico di Identità Digitale (SPID).

L'Identity Provider dell'Istituto si basa da numerosi anni su una personalizzazione spinta della piattaforma di mercato, CA Siteminder, oggi Broadcom CA Single Sign On; Profilazione

Una volta autenticato, all'utente va associato un profilo che descriva il suo livello di sicurezza di accesso alle informazioni e le funzionalità che può utilizzare con quale ruolo.

Il sistema IdM Custom mette a disposizione degli utenti strumenti web utili ad effettuare diverse operazioni.

Il contesto di utilizzo tipico di questi strumenti segue questo processo

- Tramite la Console di gestione delle configurazioni viene registrato un nuovo ruolo e i suoi attributi e vengono definite le regole di richiesta abilitazione. Viene quindi pubblicata la possibilità di richiederlo sul Portale di Richiesta Abilitazioni;
- Tramite il Portale di Richiesta Abilitazioni gli utenti inviano i moduli necessari alle sedi;
- Tramite la Console di Gestione delle Abilitazioni Esterne il personale dell'Istituto provvede a rilasciare l'abilitazione al soggetto richiedente;
- Tramite la Console di Gestione dei Delegati il soggetto definisce i suoi delegati in base all'organizzazione prevista dai ruoli e descritta nei capitoli precedenti;
- Tramite le Console di Utility gli operatori Inail e gli specialisti dell'Ufficio Esercizio danno assistenza agli utenti e monitorano eventuali anomalie.

10.4. Il post login utenti esterni: da PLAP a MyInail

L'attuale post login utente (PLAP) è basato su una semplice interfaccia che elenca e consente l'accesso alle applicazioni disponibili per il suo profilo.

L'applicazione PLAP è una web application cui viene reindirizzato ciascun utente autenticato e che in base alle autorizzazioni restituite dall'Access Manager a servizio costruisce dinamicamente il pacchetto di servizi a disposizione dell'utente autenticato.

PLAP conosce i seguenti gruppi di utenza/profili:

- Utente Generico
- Medico

- Patronato
- Consulente
- Lavoratore
- Azienda

Le voci di menu associate all'utente vengono recuperate automaticamente tramite il servizio Infoprofilazione e renderizzate nelle aree dei menu del layout di pagina, l'albero di menu sulla sinistra e i due top menu; la profilazione funzionale per il backend redazionale risiede invece correttamente nello strumento di Content Management come vedremo nel paragrafo seguente.

La componente è una web application J2EE modulare, composta di una serie di progetti/moduli:

- Componenti web a riuso (authenticated pages template: header + footer + left menu + 2 top menu + iframe)
- Dashboard (home page arricchite) dedicati ai diversi profili/personas (utente generico, lavoratore, consulente, medico, patronati, azienda)
- Componente per la gestione del ticket di single sign on
- Utilities varie (messaggi, pratiche, agenda)
- Componente API ReST

Il layout viene costruito estraendo, attraverso il modulo dei web server WebLogic Server Templates, il template impiegato dal CMS, con in più l'integrazione, via ReST API, delle componenti a riuso indicate al primo punto della lista di cui sopra.

La parte più ricca di logica di business, che si concretizza nella costruzione di user home differenziate a seconda del profilo dell'utente, si basa sull'integrazione con una libreria jar che parla via SOAP con il servizio di Infoprofilazione SOA di cui al paragrafo precedente.

Alcune delle componenti sopra indicate costituiscono anche la piattaforma per l'integrazione di alcuni tipi di applicazione in ecosistema Inail, nel layout attraverso l'iframe e nel sistema di autenticazione grazie alle componenti ancillari.

La PLAP come piattaforma di integrazione offre funzionalità di gestione del multilingua solo dalla v2 in poi, disponibile da dicembre 2023 per le attività in ambito SDG – Single Digital Gateway (Your Europe).

10.4.1. Il post login evoluto: la MyInail

Ad aprile del 2024 la Plap viene sostituita da una applicazione snella e moderna, realizzata secondo i seguenti principi:

- anticipare i bisogni degli utenti e offrire un'assistenza proattiva

- valorizzare gli operatori di assistenza
- spingere verso soluzioni automatizzate anche con l'utilizzo di strumenti di IA per aumentare la produttività e migliorare l'esperienza degli utenti
- rilevare e prevenire i potenziali problemi
- collaborazione anche con altre PPAA, innovazione e implementazione rapida
- aumentare la fiducia nei servizi pubblici

Il nuovo ambiente di post login My Inail offre caratteristiche user oriented moderne ed un layout accattivante, mettendo in pratica i principi sopra citati. In questa area personale l'utente può accedere alle proprie informazioni e, coerentemente con il profilo di accesso, può visualizzare contenuti personalizzati e usufruire dei servizi online messi a disposizione dall'Istituto.

Tecnologia impiegata per la MyInail:

- SPA in Angular 12;
- microService OpenJDK 11;
- microService Red Hat Spring Boot 2.5.12;
- database Oracle 19c Multimodel – JDBC driver 19

Il layout della MyInail è simile a quello del nuovo portale.

- La MyInail offre varie funzionalità a disposizione degli utenti profilati sul portale Inail, tra le quali:
- area personale con varie dashboard specializzate (es. Pratiche, Pagamenti, Mio Profilo, ecc.);
- catalogazione, esposizione, lancio e preferitizzazione dei servizi online;
- accesso alle informazioni disponibili per il profilo di accesso;
- chatbot di assistenza, che risponde in linguaggio naturale alle domande degli utenti e li indirizza verso la risoluzione di problemi applicativi o di interpretazione normativa.

La MyInail è integrata nel sistema di analytics per la raccolta e l'analisi dei dati di esperienza utente.

10.4.2. La chatbot di assistenza

Il portale attuale offre molti strumenti di supporto, ma è l'utente a dover decidere a quale rivolgersi per avere l'assistenza che chiede, in quanto la proposta consiste di vari touchpoint presentati con egual valenza (FAQ; Inail Risponde; Sportello Digitale; Guide e manuali, ecc.). L'utente sceglie, senza alcuna guida, lo strumento che preferisce, ma che non sempre si rivela quello più idoneo alla risoluzione della problematica riscontrata, allungando i tempi di risoluzione e appesantendo il lavoro degli operatori di contatto.

Per quanto detto è stato realizzato la chatbot, lo strumento di supporto sempre disponibile nella home page della MyInail e nei servizi online, che offre supporto contestuale e proattivo sui servizi online:

- in base della richiesta digitata dall'utente, propone i touchpoint più idonei alla risoluzione della problematica (FAQ; Manuali; Inail Risponde; Sportello Digitale, ecc.)
- l'ordine di priorità dei touchpoint proposti è definito dalla «Matrice di correlazione utente/servizio/canale», configurabile per ciascun servizio.

Tecnologia impiegata: Microsoft Azure.

La chatbot è impiegata anche per offrire assistenza in lingua agli utenti transfrontalieri che adoperano i servizi applicativi Inail che fanno parte del network SDG – Single Digital Gateway (Your Europe).

La chatbot va considerato come una applicazione estensibile sia nei contenuti, attraverso l'integrazione di ulteriori domini di conoscenza per le conversazioni in linguaggio naturale, che nella funzionalità di indirizzamento utente al canale di assistenza più idoneo.

10.5. Il post login utenti interni: il Digital Workplace

Da dicembre 2023 la intranet si è evoluta in un moderno concetto di digital workplace. L'applicazione, basata su Sharepoint, offre moltissime funzionalità per il benessere lavorativo di dipendenti e fornitori Inail attraverso widget configurabili. Il digital workplace Inail è composto dai moduli:

- **Scrivania digitale:** offre vari widget configurabili che offrono funzionalità di accesso e gestione dei propri file, lancio di applicazioni, consultazione di informazioni e documentazione
- **Contenuti personali:** offre funzionalità per la gestione della posizione lavorativa del dipendente e l'accesso a strumenti applicativi specifici;
- **Formazione:** consente l'accesso ai corsi per i dipendenti, al curriculum formativo e altre risorse per la formazione;
- **Assistenza:** strumenti e canali per risolvere in autonomia problemi di ogni natura, sugli applicativi come alla dotazione personale.

Dalla stessa interfaccia è possibile lanciare ulteriori funzionalità, tra le quali:

- **Rubrica:** consultazione del directory dipendenti attraverso Rest con Anagrafica Unica (Active Directory, Persone, Strutture);
- **Notifiche:** centro di consultazione delle notifiche applicative; è integrato attraverso la piattaforma Notification Gateway;
- **Feedback:** breve questionario di soddisfazione utente;
- **Assistente virtuale:** risponde a domande in linguaggio naturale sull'utilizzo del digital workplace (tecnologia Microsoft CLU);

Dalla home page della scrivania è possibile accedere alla piattaforma informativa del Mondo Inail, realizzata tramite funzionalità e layout nativi Sharepoint, che consente l'organizzazione, la pubblicazione, l'accesso e la ricerca, anche basata sugli strumenti di intelligenza artificiale di Viva Topics, di informazioni e documenti di carattere istituzionale. Il Mondo Inail contiene i minisiti, contenitori di informazioni e documenti realizzati e mantenuti dalle direzioni competenti.

Ulteriori servizi a disposizione del dipendente basati su Sharepoint 365:

- **Stream** per la raccolta e condivisione di materiale video;
- **Collaboration** ambiente Sharepoint 365 per la condivisione di informazioni e documenti a diversi livelli di riservatezza.

10.6. Architetture Ancillari

10.6.1. Ambienti di staging

Il portale **internet** si basa su tecnologie di Content Management System (CMS), attraverso la quale utenti Inail profilati come redattori possono contribuire informazioni in forma di testi, elementi multimediali e allegati es. Pdf nei rami del portale.

Il CMS del portale pubblico (OWCS -> AEM Sites) consente di aggiungere, modificare e togliere:

- voci nei menu ad albero
- pagine dall'alberatura
- contenuti nelle pagine, basate su attraverso l'uso di template standardizzati. Solitamente non è consentito l'utilizzo di Html non previsto nel template, questo per evitare che redazionalmente si inseriscano errori di accessibilità.

Le attività redazionali vengono svolte in gran parte dalla redazione centrale in Dcpc, solo alcune sezioni del portale pubblico sono contribute da redattori delocati secondo flussi approvativi stringenti. La sezione Amministrazione Trasparente viene contribuita in parte da redattori centrali e delocati e in parte dalle funzionalità dell'applicativo CAT (vedi di seguito).

Il CMS del portale **intranet** (Dwp – Mondo Inail) è basato su Sharepoint 365. Il Mondo Inail dal 20 dicembre 2023 ha preso il posto della sezione Informazioni della vecchia intranet, eliminando le complessità operative del doppio ambiente OWcs/Sharepoint 2013.

Su Mondo Inail possono contribuire solo redattori centrali, tutti i contenuti di Mondo Inail sono pubblici per dipendenti e fornitori Inail. L'architettura dell'informazione di Mondo Inail è fissa e standardizzata.

Il nuovo ambiente di collaboration basato su Sharepoint 365, collegato a Mondo Inail da link, ha invece una gestione capillare dei permessi di scrittura e lettura, tale da consentire la creazione di aree riservate. L'architettura dell'informazione del nuovo collaboration è flessibile e a discrezione del singolo utente.

Sharepoint 365 consente ricerche intelligenti sui contenuti pubblicati attraverso la tecnologia Microsoft Viva Topics, che va istruito e aggiornato da operatori abilitati responsabili della certificazione dei contenuti.

I contenuti multimediali sulla nuova intranet e Mondo Inail vanno inseriti e pubblicati attraverso le funzionalità di Microsoft Stream, disponibile nella suite Microsoft 365. Il nuovo Stream ha un sistema capillare di autorizzazione all'accesso ai singoli video, permettendo quindi anche la segregazione di materiale non destinato a tutto il personale che si autentica alla intranet Digital Workplace.

La suite Microsoft 365 in combinazione con le funzionalità offerte da Sharepoint 365 offre svariati strumenti per la rapida automazione di processi, tra i quali la Power Suite che comprende Assistant, Automate, Business Intelligence e Apps.

10.6.2. Consultazione Amministrazione Trasparente (CAT)

Nella Sezione amministrazione trasparente sono pubblicati i dati e le informazioni previste dal Decreto legislativo 14 marzo 2013, n. 33 “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni” ed è quindi un repository complesso e articolato difficile da gestire redazionalmente, secondo gli obblighi di pubblicazione previsti per norma. Per questa ragione, anni fa, è stata realizzata una applicazione configurabile che automaticamente preleva dati e documenti da fonti certificate e compone pagine di portale consultabili dall'utente.

La piattaforma CAT è composta dai seguenti moduli:

- **Applicazione CAT** integrata nel portale INAIL, offre agli utenti internet funzioni di visualizzazione, ricerca, stampa ed esportazione in vari formati dei dati
- **Console CAT** strumento di amministrazione e gestione, consente ad utenti interni (intranet) di pubblicare i contenuti della sezione “Amministrazione Trasparente” gestiti automaticamente. Inoltre consente la certificazione del dato in base alle metriche configurate
- **Connettori CAT** componenti di accesso ai dati che acquisiscono automaticamente i dati dalle fonti alimentanti (data source) e li rendono disponibili ai processi di pubblicazione.

Il processo redazionale automatico è composto delle seguenti fasi:

- **Connettore:** attua l'integrazione di una fonte dati e configura rispetto al formato di pubblicazione il documento target
- **Certificazione:** controllo che i dati siano completi, coerenti e conformi applicando opportune metriche di qualità
- **Validazione:** verifica che i dati siano corrispondenti con il formato dell'informazione target definita
- **Pubblicazione:** invio dei dati online sul canale richiesto e nella sezione prevista

La piattaforma viene adoperata, tra gli altri, negli ambiti:

- ISI
- Sovvenzioni
- Bandi di gara – appalti
- Tassi di assenza
- Aste e trattative riservate
- Patrimonio immobiliare

10.6.3. Campagne e survey

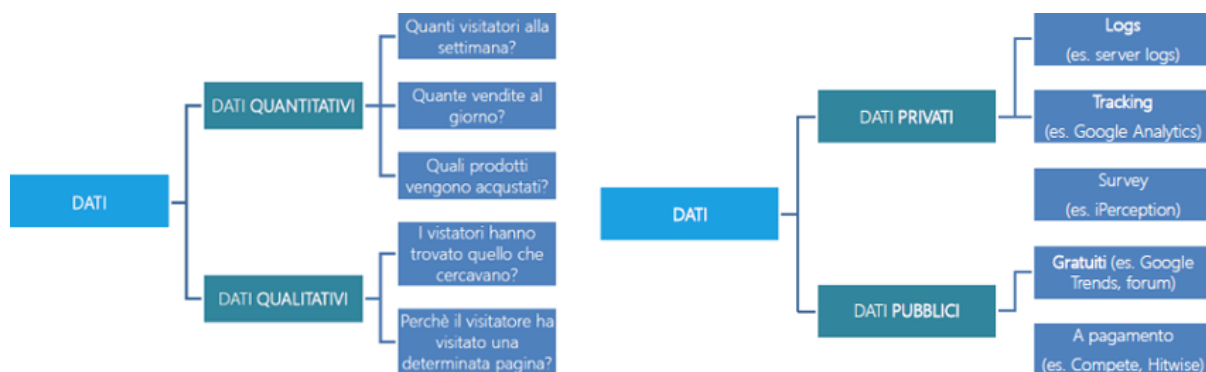
Soprattutto nell'ambito della analisi della *customer experience* è necessario realizzare campagne per la raccolta di dati, solitamente anonimi, tramite questionari. Un questionario ben costruito consente rapidamente di raccogliere dati su interessi e abitudini utente, che una volta analizzati potrebbero condurre ad esempio all'avvio di attività di miglioramento dell'esperienza utente, o alla raccolta di adesioni per una certa attività, alla scelta di un dispositivo, ecc.

Le campagne solitamente si compongono di due fasi: individuazione del target e invio della email ai soli destinatari con il link al questionario. Gli strumenti per realizzare campagne sono Gestore Eventi e Ajo (Adobe Journey Optimizer), adoperato per la customer satisfaction.

Per la realizzazione dei questionari si può utilizzare lo strumento **Microsoft Form**, disponibile tra gli strumenti di Microsoft 365.

10.6.4. Analytics

Negli ultimi contratti Adobe è stato acquisito il prodotto Adobe Analytics, *best in class* sul tema della raccolta e analisi del traffico utente. I dati che possono essere raccolti sono informazioni anonime di carattere comportamentale (es. le pagine visitate da un utente, le conversioni effettuate ovvero i *goal* raggiunti, le azioni compiute dall'utente per raggiungere il sito tramite motori di ricerca, etc), mentre non possono essere raccolte tutte le informazioni personali e sensibili degli utenti, soggette a restrittive leggi per la tutela della privacy.



Il prodotto **Adobe Analytics** dispone di una piattaforma SaaS di reportistica avanzata, attraverso la quale è possibile interpretare statisticamente le attività degli utenti sui canali istituzionali, digitali e analogici. Tutte le applicazioni devono essere integrate nel sistema di analytics, in modo che possano venire analizzati i flussi utente e avviate azioni di miglioramento della customer experience.

Nella suite è disponibile il prodotto Report Builder, add-on per Excel che consente la creazione e personalizzazione di dashboard sui dati di analytics.

Il Dwp – Digital Workplace è nativamente integrato in **Microsoft Application Insight**, potente strumento di APM - Application Performance Management che offre anche funzionalità di raccolta e analisi dell'esperienza utente, tra le quali:

- **Users, sessions, and events:** quando, dove e come gli utenti interagiscono con le applicazioni;
- **Funnels:** analizza il comportamento nei *funnel* per capire dove l'utente procede o interrompe la navigazione;
- **Flows:** visualizza i percorsi utente per identificare aree di *high engagement* come anche gli *exit points*;
- **Cohorts:** raggruppa gli utenti in base a caratteristiche condivise per semplificare l'identificazione di tendenze, la segmentazione e la risoluzione di problemi prestazionali.

10.6.5. Multimedia

10.6.5.1. Video e video tutorial

I file multimediali sul portale pubblico vengono erogati dal servizio Microsoft Media Services che consiste di due funzionalità:

- **Encoding:** il file mp4 viene predisposto in più versioni per essere fruito dagli utenti attraverso il sistema di streaming;
- **Streaming:** il servizio eroga il contenuto multimediale nella modalità più adatta al dispositivo e alla disponibilità di rete.

Microsoft Media Services è in dismissione a giugno 2024, in sua sostituzione si sta scegliendo tra Mediakind e Harmonic, come suggerito da Microsoft stessa.

10.6.5.2. Tutorial e pubblicazioni multimediali interattive

È possibile fare un uso limitato del prodotto Microsoft Sway per la realizzazione di sezioni web internet o intranet dinamiche, interattive e multimediali.

10.6.6. Esercizio applicativo del portale

Il team di esercizio del portale si occupa sia dell'assistenza applicativa su problematiche redazionali e tecniche che della gestione degli utenti redattori.

Oltre a ciò, dato che lo scenario di portale Inail viene indicizzato dai motori di ricerca, a volte il team interviene sulle console di Google o di Bing per escludere o eliminare contenuti dai sistemi di indicizzazione.

11. STRUMENTI DI NOTIFICA APPLICATIVA E CAMPAGNE

11.1. Gestione Posta Multicanale (GPM)

Lo scopo principale della piattaforma è la generazione e l'invio di comunicazioni ad uno o più destinatari, tramite servizi o tramite il Front End dedicato «Gestione Posta».

L'applicazione garantisce da anni la trasmissione di milioni di comunicazioni dell'istituto, verso persone, aziende, enti pubblici ed altre sedi INAIL.

La piattaforma GPM, evoluzione architetturale di POM, fornisce un insieme di servizi REST o UI adibiti all'emissione, renderizzazione, trasmissione e tracking di comunicazioni e libera i fruitori del servizio dai dettagli implementativi dei protocolli di comunicazione, grazie all'astrazione del concetto di CANALE/PROVIDER.

I canali di trasmissione delle comunicazioni, attualmente gestiti da GPM, sono:

- Posta Elettronica Certificata (PEC, in futuro REM);
- Email;
- Posta ordinaria centralizzata o territoriale;
- Posta raccomandata centralizzata o territoriale;
- Posta raccomandata A/R centralizzata o territoriale;
- Atti giudiziari;
- Stampa semplice;
- Consegna a sportello.

L'emissione delle comunicazioni può essere effettuata in modalità on-demand o tramite campagne massive.

Il tracking normalizzato consente agli utenti e alle applicazioni di ottenere una tracciatura sempre coerente a prescindere dal canale utilizzato, agevolando i processi di gestione degli eventi.

Il tracking tramite servizi, ove previsto, consente ad un utente di richiedere l'aggiornamento on-demand.

La piattaforma GPM è usata da vari attori all'interno dell'istituto. Possono essere processi automatici (c.d. Procedure Conferenti) oppure soggetti che a vario titolo hanno necessità di inviare comunicazioni o consultarne contenuto ed esito di trasmissione. Le comunicazioni sono caratterizzate da una sede mittente ed una competente, in modo da consentire la consultazione per competenza territoriale e/o funzionale. Tutti gli operatori abilitati sul territorio nazionale, per struttura, regione o sede, possono operare, secondo competenza, su tutte le comunicazioni emesse tramite GPM, utilizzando l'applicazione «Gestione Posta». Altre classi di utenti sono abilitate ad accedere, in sola lettura, alle comunicazioni emesse, per attività connesse con il supporto o il controllo dei contratti di postalizzazione (SLA, fatturazione passiva, ecc.).

Componente fondamentale di GPM è la *Document Factory*, insieme di servizi che consente di sviluppare e mantenere documenti efficaci, coerenti e di qualità per l'istituto, redatti secondo i requisiti delle specifiche tecniche di postalizzazione e degli standard INAIL. La Document Factory si realizza attraverso il processo di gestione dei template, il know how tecnico e le sinergie tra i vari attori che partecipano alla realizzazione del documento finale.

L'applicazione fornisce vari modi per gestire le campagne di comunicazione.

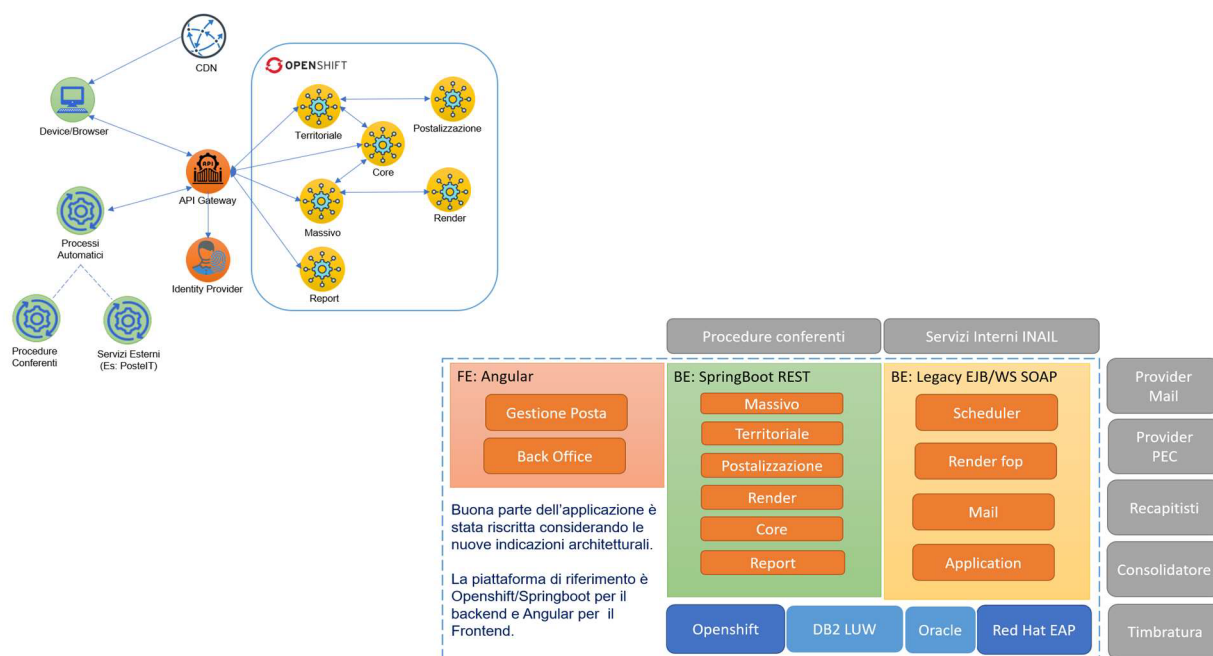
- POM Massivo (es. Casalinghe, 20SM, 10SM);
- Import da file CSV parametrici, per qualsiasi canale (es. Carta Blu Trenitalia);
- Campagne massive tramite Posta Centrale Giornaliera (es. Avvisi Bonari);
- Campagne massive tramite Posta Centrale Massiva (es. FISCO).

Tutte le comunicazioni emesse tramite queste modalità sono consultabili attraverso l'applicazione «Gestione Posta». Ogni anno si eseguono campagne massive nell'ordine dei milioni di comunicazioni, come nel caso dei 10SM e dei 20SM.

La piattaforma GPM è dotata di un Back Office di amministrazione, dal quale è possibile gestire i parametri ed i processi, tra cui:

- Mail/PEC (Indirizzi, soglie, inoltri);
- Canali e provider;
- Modelli (template, trasformazioni).
- Invii tramite import da CSV;
- Richieste asincrone massive;
- Invii con il POM Massivo;
- Scheduleri dei processi;
- File ricevuti da enti esterni;
- Log degli errori;
- Codici di prenotazione distinta;
- CAP recapitista.

L'architettura dell'applicazione è in standard Inail.



È in corso l'analisi e lo sviluppo degli indicatori di qualità dei servizi di recapito. Essi permetteranno di valutare sia la qualità del servizio del fornitore, sia la qualità dei dati utilizzati per la spedizione. Si andranno ad esaminare le varie casistiche dei mancati esiti, le anomalie derivanti dalla normalizzazione degli indirizzi, l'uso di CAP impropri,

ecc. Le informazioni estratte dal sistema potranno essere utilizzate dagli utenti o dalle procedure conferenti per migliorare le informazioni anagrafiche.

È in corso l'attività di sviluppo per l'integrazione sia con i nuovi protocolli della REM (Registered Electronic Mail) che con la piattaforma Send (ex PND), e grazie al meccanismo di astrazione del canale/provider e del tracking la transizione sarà trasparente per le procedure conferenti.

La Registered Electronic Mail è un sistema di comunicazione elettronica affidabile, legalmente valida e altamente sicura utilizzata per scopi commerciali, legali e amministrativi. Analogamente alla PEC, che andrà a sostituire a partire dal 2024, fornirà prove di consegna e garantirà l'autenticità del mittente.

SEND è la piattaforma standard realizzata da PagoPA che consente l'invio e la ricezione sicuri e veloci di notifiche a valore legale.

Per la redazione dei template ed il rendering dei PDF viene utilizzato in parte il prodotto AEM Forms 6.5 e in parte il sistema nativo custom basato su XSL-FO.

11.2. Gestore eventi

Lo scopo principale della piattaforma è quello di offrire servizi di comunicazione attraverso i canali mail, pec, SMS sia per gli applicativi che per gli uffici.

La natura delle comunicazioni varia:

- Comunicazioni istituzionali: campagne informative interne ed esterne
- Comunicazioni di servizio: avvisi interni e segnalazioni applicative di servizio (pubblicazione atti, valutazioni, determine)
- Invio ufficiale verso utenti esterni e/o interni di comunicazioni ufficiali legate alle funzionalità dell'ente, (pratiche, completamento procedure login, validazione recapiti inseriti, etc.)

Inoltre, il Gestore Eventi offre tutta una serie di servizi per la verifica della spedizione nonché per la lettura dell'account di posta certificata, l'analisi della stessa e il reinoltro alle procedure interessate.

Recentemente il Gestore Eventi si è integrato con il middleware Notification Gateway nell'ottica di fornire un unico punto di accesso ad entrambi i servizi di comunicazione.

È realizzata su una architettura a 3 livelli (Java e Oracle 19 Exadata): mette a disposizione servizi Rest e SOAP attraverso sia l'APIGATEWAY sia la Porta di Dominio.

La piattaforma Gestore Eventi si compone di due componenti principali: la Console ed il Motore. Le comunicazioni che si intendono inviare vengono descritte in "eventi", che riportano l'oggetto, la motivazione ed i destinatari della comunicazione. Gli eventi sono suddivisi in due tipologie:

- eventi manuali, in cui le comunicazioni vengono descritte, composte ed inviate tramite console web. Gli eventi di questo tipo prevedono un invio delle comunicazioni definite dalla console e si "declinano" in più sottotipi:
 - Redazionali
 - Help Desk

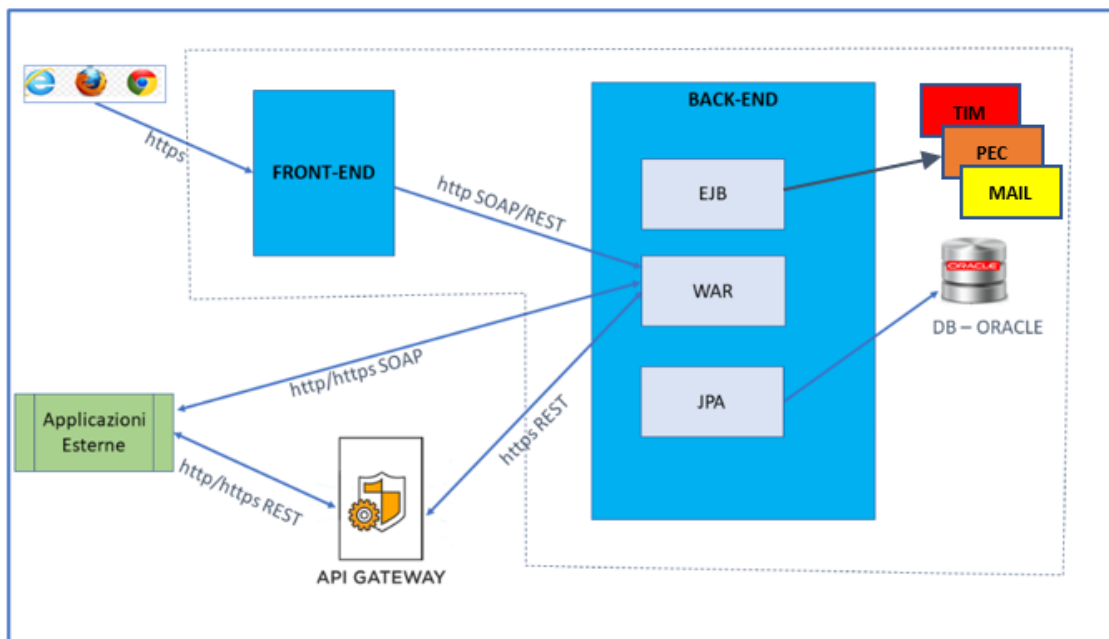
- Comunicazione Plus
- Comunicazioni custom.
- eventi procedurali, in cui le comunicazioni vengono descritte tramite console web, e l'invio viene effettuato tramite apposito web service da una applicazione.

I canali supportati per le comunicazioni sono: SMS, e-mail, Posta Elettronica Certificata (PEC) e Notification Gateway per Scrivania Digitale.

Tra le caratteristiche salienti della piattaforma troviamo:

- servizi / comunicazioni
 - Interfaccia grafica per gli invii costruita su consolidata *user experience*
 - Disponibilità dei servizi sia Rest che SOAP per rispondere alle nuove e vecchie esigenze
 - Possibilità di spedire direttamente MAIL, PEC e SMS
 - Possibilità di spedire tramite NGW notifiche sui relativi canali
 - Gestione completa delle caselle di posta certificata (ricezione delle PEC e svuotamento INBOX)
 - Realizzazione di invii multipli tramite la CC e la CCN
- Gestione della comunicazione
 - Monitoraggio dell'esito spedizione sia tramite servizi esposti che da console
 - Gestione dei consumi e costi con segnalazione di alert per l'acquisto di pacchetti di SMS
 - Supporto all'editing delle comunicazioni (editor HTML) con possibilità di creare un template per personalizzare le comunicazioni
 - Gestione delle spedizioni massive (più di 100.000 destinatari) con l'utilizzo di varie tecniche (chiamate asincrone, invio a blocchi).

L'architettura della piattaforma è così strutturata:



11.3. Notification Gateway (NGW)

Il Notification Gateway è un middleware applicativo con architettura a microservizi che consente di raccogliere le richieste di notifica da parte delle applicazioni intranet ed internet Inail, gestire la composizione e formattazione del messaggio, impostare delle politiche di consegna e visualizzare lo status delle notifiche tramite dashboard dedicata. Attualmente gestisce gli invii sui canali App IO, App Firma, Scrivania Digitale, MyInail ed altri.

La piattaforma offre una gestione facilitata di notifiche multicanale attraverso la configurazione di eventi associati a uno o più canali in pochi semplici step.

Il campo di applicazione del NGW è quello delle notifiche di cortesia, ovvero messaggi che possano ricordare all'utente di una scadenza immediata o di una azione da intraprendere (caratteristiche dei due canali intranet più importanti App Firma e Scrivania Digitale) evitando che questo tipo di comunicazioni transitino per il canale mail, secondo una politica volta alla limitazione degli invii sulla posta elettronica.

Le comunicazioni che l'Istituto effettua verso il cittadino attraverso il canale App IO possono essere corredate anche del relativo evento di pagamento: attraverso la notifica arriva anche l'identificativo univoco del pagamento che permette al cittadino di adempiere direttamente da App IO.

Il NGW inoltre permette alle applicazioni chiamanti di utilizzare una serie di funzionalità avanzate che facilitano la gestione delle notifiche direttamente da dashboard, senza dover procedere ad alcun aggiornamento software della propria applicazione, tra le quali:

- **Sospensione applicazioni e canali:** le notifiche inviate dalle applicazioni non vengono perse ma poste in sospenso per essere poi inviate al momento della riattivazione;
- Gestione e **formattazione del testo del messaggio** in tre diversi linguaggi: text, html e markdown (specifico per App IO).
- **Dashboard dedicata al monitoraggio** e alle statistiche delle notifiche inviate;
- Possibilità di ricevere un **report** relativo all'andamento delle notifiche direttamente sulla mail.

La struttura a microservizi di NGW consente una grande flessibilità e facilità nell'implementazione di nuove features, che siano esse rivolte all'ampliamento delle funzionalità per l'esperienza utente, quindi da dashboard, oppure avere un respiro più ampio di integrazione con altri canali e, soprattutto, altri strumenti di notifica.

Per l'integrazione di nuovi canali in Ngw è stato realizzato il middleware Notification Layer, che si occupa di distribuire i messaggi secondo le specifiche degli applicativi trasmittenti.

11.4. Adobe Journey Optimizer (AJO)

Adobe Journey Optimizer è uno strumento SaaS di mercato, pensato principalmente per le attività di marketing delle grandi aziende, che permette di creare delle campagne informative personalizzate su vari canali come e-mail PEL e PEC, SMS e *push notification* su app.

La peculiarità più importante di AJO è quella di poter configurare delle campagne con le seguenti caratteristiche:

- Campagne pianificate, consentono comunicazioni batch semplici ad hoc per casi d'uso di marketing come offerte promozionali, campagne di coinvolgimento, annunci, avvisi legali o aggiornamenti dei criteri.
- Campagne attivate dall'API, consentono l'invio di semplici messaggi operativi/transazionali con API REST; è possibile personalizzare il messaggio utilizzando gli attributi del profilo e i dati contestuali del payload.

In entrambi i casi è necessario aver predisposto la classe di destinatari. I segmenti di destinatari devono essere disponibili prima di creare la campagna.

Il campo di applicazione di AJO è più che altro quello delle campagne di *customer satisfaction*, attività che prevede l'invio massivo di inviti a compilare un questionario di gradimento ad una classe di destinatari rappresentata da utenti dei servizi Inail. Ogni campagna può prevedere l'invio su canali diversi tra il primo invito e i solleciti successivi. Le caratteristiche per gli invii sono configurate direttamente su Ajo, e la campagna si svolge senza intervento manuale. Sono disponibili *dashboard* per il monitoraggio dell'andamento della campagna.

11.5. Microsoft Dynamics / Customer Voices

Microsoft Dynamics 365 è una piattaforma basata su cloud che combina diversi prodotti per fornire funzionalità complete di gestione delle attività aziendali e relazioni con i clienti. La suite è costituita da applicazioni i cui dati sono archiviati e gestiti attraverso un servizio Dataverse che ne consente l'interconnessione e la condivisione tra le diverse applicazioni.

Customer Voice è la soluzione di gestione del feedback dei clienti appartenente alla suite Dynamics 365 che consente di raccogliere, analizzare ed agire in base alle opinioni espresse in tempo reale dagli utenti al fine di comprenderne le esigenze, misurarne la soddisfazione e migliorare l'esperienza complessiva.

La soluzione consente di creare e distribuire sondaggi per raccogliere feedback dai clienti su più canali come posta elettronica, Web, dispositivi mobile ed include modelli di indagine e questionari predefiniti che possono essere personalizzati per soddisfare le specifiche esigenze di ricerca.

La rilevazione può arricchirsi di metriche che consentono la misurazione della soddisfazione e con l'analisi del sentiment sulle risposte alle domande a testo aperto sfruttando un modello di apprendimento automatico ed elaborazione del testo gestito da Microsoft.

Una volta raccolto il feedback, lo strumento si compone di dashboard e report in tempo reale che consentono una sintesi visiva delle risposte utile all'identificazione delle tendenze, modelli ed aree di miglioramento.

La soluzione, pensata ed utilizzata per finalità di gestione di campagne o comunicazioni in uscita, è integrata con altre applicazioni Dynamics 365, consentendo di connettere i dati di feedback con i profili dei clienti, monitorandone ovvero la soddisfazione nel tempo. Questa integrazione fornisce una visione a tutto tondo del cliente e consente la creazione di esperienze personalizzate e proattive verso i clienti basate sui dati.

Il feedback ottenuto dalle rilevazioni è riconducibile all'esperienza pregressa di un utente censito in Inail, ovvero all'interno di una "scheda" contenente dati anagrafici, transazionali e d'interazione che si riferiscono all'esperienza dell'utente con l'Istituto. L'integrazione tra Dynamics 365 Customer Voice e Dynamics 365 Customer Insights consente

infatti di raccogliere e analizzare le informazioni provenienti dai clienti al fine di ottenere una comprensione più completa ed approfondita di esigenze, preferenze e feedback registrata su tutti i canali di contatto tra utente ed Istituto. Complessivamente, l'integrazione tra i due prodotti della suite Dynamics 365 è strategica al miglioramento dei servizi e dei processi d'interazione che avvengono tra l'utente ed Inail.

12. INFRASTRUTTURE DI RETE

12.1. Architettura generale di Rete

L'infrastruttura della rete INAIL collega tutte le Sedi (di tipo A, B e C), le Direzioni Regionali, la Direzione Generale, le Agenzie e le postazioni di Telelavoro alla DCSIT DCOD tramite una WAN a larga banda, secondo quanto predisposto dal Sistema Pubblico di Connettività per il trasporto, con una banda di accesso al CED in fibra ridondata. L'accesso al CED centrale è completamente ridonato sia sul sito Primario che su quello Secondario.

Il collegamento delle Sedi sul territorio nazionale viene effettuato con link rispettivamente da 10 Mbit/s a 100 Mbit/s secondo la quantità di traffico effettuato.

Il Centro Protesi di Vigorso di Budrio ha una connettività di 300 Mbit/s.

Le strutture della Direzione Generale hanno tutte collegamenti in fibra a 200 Mbit/s e la Sede Centrale di Piazzale Pastore in Roma ha una connettività di 600 Mbit/s. Le linee e gli apparati di rete sono duplicati per avere massima affidabilità in caso di guasto e di backup.

Le Agenzie sono connesse al DC del sito Primario sempre tramite la rete SPC (su una diversa VPN MPLS rispetto alle Sedi) mediante una linea principale FTTC o BTS a 8 Mbit/s non ridondata.

Alcune postazioni mobili sono parimenti collegate all'Istituto tramite un collegamento alla rete GPRS/UMTS di Telecom Italia Mobile secondo il contratto CONSIP.

I due data center principali sono situati a Roma Via Santuario Regina degli Apostoli e ad Acilia - Via Macchia Palocco a una distanza di circa 30 km, sono collegati sia a livello 2 che a livello 3 tramite collegamenti DWDM ridondata su dark fiber.

La rete Lan del data center è costituita principalmente da collegamenti in fibra a 10,25,40 Gb in tecnologia Unified fabric (LAN e SAN unificate), pur esistendo residui collegamenti a 1Gb sia fibra che rame, per alcuni server, e fiber channel per quanto riguarda il collegamento delle control unit dei dischi SAN.

Gli apparati attivi del CED sono switch Cisco della serie Nexus 9000, 7000, 5000, 2000, 1000, Catalyst 6509 in configurazione VSS, Catalyst 9000

I firewall dell'Istituto sono attivi su tecnologia Checkpoint su cui sono stati configurati vari VSX in linea con la suddivisione degli ambienti (produzione, certificazione, servizi Interni, Exadata, ecc per i servizi bilanciati vengono utilizzati apparati Netscaler SDX e per alcuni servizi specifici (ad esempio captive portal) sono utilizzati firewall Fortinet

Per quanto riguarda l'ambiente Cloud privato, questo viene gestito tramite NSX-T. A protezione dell'ambiente Cloud Azure, Cloud OCI sono attivi NVA della Checkpoint.

Attualmente il CED fornisce servizi ad altre Pubbliche Amministrazioni, quali l'hosting evoluto del Ministero della Salute, comprendente il sito di Disaster Recovery di Casamassima (BA), con attivi apparati Firewall CheckPoint e Fortinet, switch Cisco Nexus 9000, Catalyst 3850 e Catalyst 9200, e bilanciatore Netscaler.

12.2. Connettività verso Infranet

Così come previsto dall'architettura generale del Sistema Pubblico di Connettività, l'Istituto comunica con le altre Amministrazioni Pubbliche, che aderiscono al Sistema Pubblico di Connettività (SPC), tramite una rete dedicata ad elevato livello di sicurezza denominata "Infranet".

Nella nuova architettura di Business Continuity è possibile effettuare sia la navigazione verso Infranet che l'esposizione dei siti Web dell'Istituto indifferentemente dal collegamento di via Santuario che da Acilia. Anche se considerata una rete "sicura", viene comunque protetta da firewall ed IDS/IPS.

12.3. Reti Locali

La LAN della DCOD è realizzata con cablaggi certificati in categoria 5E e 6 fino a 1Gbit/s con dorsali a 10 Gigabit Ethernet e con Switch di piano layer 2 e Centri Stella Layer 3, direttamente collegati a Switch di core che servono la Server Farm e l'elaboratore centrale.

Le LAN delle strutture della Direzione Generale sono realizzate anch'esse con cablaggi certificati in categoria 5E e 6 fino a 1Gbit/s con dorsali a 10 Gigabit Ethernet e con Switch di piano Layer 2 e Centri Stella Layer 3.

Nelle Sedi periferiche è stato effettuato il cambio degli apparati passivi (cablaggio) ed attivi (switch) in convenzione CONSIP.

Nella maggior parte delle strutture periferiche i cablaggi sono certificati in categoria 6 per la parte in rame ed OM3/OM4 per la fibra, le LAN sono dotate di Switch di accesso Layer 2 10/100/1000 Mbit/s e Centri Stella Layer 3.

L'indirizzamento IP di ogni singolo device viene effettuato automaticamente tramite DHCP centralizzato presso la DCOD, l'infrastruttura LAN eroga il servizio VOIP per quanto riguarda la fonia su piattaforma Teams. Le LAN sono tutte secondo lo standard Ethernet 10/100/1000 Mbit/s. Per i livelli di network e transport dello standard ISO:OSI la rete utilizza esclusivamente il protocollo TCP/IP.

12.4. Connettività verso Internet

La connettività verso internet è fornita da Vodafone S.p.A. (adesso Fastweb + Vodafone) attraverso due Link fisici per ogni Datacenter attestati sul Contesto SPC Internet; viene eletto come sito Primario Santuario e come Backup il sito di Acilia, la banda è la stessa per entrambi i datacenter, a 10Gbps.

È possibile usufruire del servizio di accesso ad internet (per i dipendenti) e offrire i servizi web dell'Istituto (all'utenza esterna e ai dipendenti) sia dal sito Primario, sia da quello Secondario.

12.5. Architettura Sedi, Direzioni Regionali e Direzione Generale

Per il collegamento delle Sedi (di tipo A, B e C) e delle Direzioni Regionali sul territorio nazionale vengono utilizzati link da 10 a 40 Mbit/s. I collegamenti sono ridondati verso il sito Primario, così come pure gli apparati di Accesso (tramite l'utilizzo di 2 Router), per i flussi sono attestati per ridondanza su PoP differenti. Tutte le Sedi Locali hanno una LAN a 10/100/1000 Mbit/s.

Le connessioni della MAN, che riguarda sei siti sul territorio metropolitano, sono realizzate con collegamenti ridondati in fibra da 200 Mbps fino a 600Mbps

12.6. Architettura Agenzie

Le Agenzie sono connesse al sito Primario sempre tramite la rete SPC su una VPN MPLS separata per il collegamento delle sedi mediante una linea principale xDSL a 10 Mbit/s.

12.7. Collegamento ADSL Telelavoratori

I Telelavoratori sono connessi al sito Primario via rete SPC, su una VPN MPLS diversa dalla VPN per il collegamento delle sedi attraverso un collegamento di tipo xDSL.

Anche le connessioni dei telelavoratori saranno interessate ad un aumento della banda disponibile.

12.8. Wireless (Mobile e WI-FI)

È stato realizzato ed attivato il servizio di Captive Portal (Portale mobile) per le Wi-Fi Area.

Relativamente al Wi-Fi sono stati installati access-point interni per consentire il collegamento wireless a copertura totale dello stabile per consentire la piena mobilità e roaming dei dispositivi ad essa connessa, mantenendo comunque un elevato grado di sicurezza e con gestione centralizzata.

Gli utenti interni possono accedere alla rete Wi-Fi tramite le proprie credenziali di dominio.

È stato realizzato un hot-spot "pubblico" per consentire il collegamento internet agli utenti guest, utilizzando un sistema di autenticazione centralizzato (Captive Portal).

Per mezzo di questo meccanismo, gli utenti che si collegano alla rete wireless, al primo tentativo di accedere a Internet con il proprio browser, saranno dirottati su una pagina di autenticazione, dove sarà richiesta un'autoregistrazione e l'accettazione delle clausole di utilizzo del servizio. Terminato il form di autoregistrazione le credenziali saranno inviate via SMS al numero di cellulare inserito nel form e una volta che l'utente fornirà le credenziali corrette e accetterà le clausole indicate, il sistema permetterà da quel momento la navigazione a internet.

Il servizio attualmente è stato esteso a tutti gli ospiti (utenti esterni) delle Sedi, delle Direzioni Regionali e delle Direzioni Centrali nelle quali sono stati installati gli access-point.

Tutti gli utenti mobili dell'Istituto sono dotati, tra l'altro, sui propri portatili di scheda Wi-Fi e, quindi, possono collegarsi agli hot-spot pubblici.

13. PUNTO DI ACCESSO POLISWEB

13.1. Servizio PDA PolisWeb

Il servizio PolisWeb consente agli avvocati dipendenti dell'INAIL l'accesso in consultazione ai dati dei processi civili degli uffici giudiziari, purché costituiti come parte in un procedimento civile. L'Istituto ha realizzato i sistemi per la gestione degli strumenti hardware e software, delle interfacce e dei protocolli necessari affinché i legali dell'Istituto possano usufruire dei servizi offerti dal Punto di Accesso PolisWeb, tramite la Intranet con autenticazione al dominio INAILUTENTI.

Tutti i sistemi di PDA PolisWeb sono attestati nella DMZ Front-End. Il servizio è gestito direttamente dall'INAIL, in particolare dall'Ufficio "Centro per i Servizi Web e la Cooperazione Applicativa" di DCSIT. In qualità di gestore del Punto di Accesso, INAIL ha provveduto ad adottare particolari misure di sicurezza per l'erogazione del servizio, per garantire che l'accesso a PolisWeb sia conforme con gli standard di sicurezza stabiliti dal Ministero della Giustizia.

Per garantire la riservatezza e l'integrità dei dati trasmessi, per usufruire dei servizi PolisWeb occorre stabilire una comunicazione sicura tra il client, il browser web dell'avvocato e il server web del PDA utilizzando il protocollo SSL v.3.

L'accesso è consentito con meccanismi di autenticazione forte: gli utenti sono provvisti di un dispositivo 'Business Key', su cui è memorizzato un certificato digitale di autenticazione, rilasciato da un certificatore accreditato dal CNIPA, e per far richiesta del servizio devono utilizzare la Business Key e digitare un codice di attivazione (PIN) per consentire l'abilitazione delle funzionalità del proprio certificato di autenticazione digitale presente sul dispositivo e proseguire la procedura di autenticazione.

Per il controllo della Business Key, è stata sviluppata una soluzione client-side ad hoc; durante la navigazione dell'utente sul portale PolisWeb un applet client-side verifica che il certificato sia inserito nel dispositivo e qualora non sia presente, l'utente è rediretto verso una pagina di errore dove viene richiesto nuovamente l'inserimento del dispositivo.

È stato inoltre attivato un sistema di registrazione di tutti gli accessi degli utenti al PDA, delle transazioni verso il server PolisWeb in un sistema di archiviazione sicuro che contenga informazioni sufficienti per identificare l'utente, le operazioni effettuate e i riferimenti temporali di inizio e fine delle connessioni.

13.1.1. Architettura del PDA PolisWeb

Implementazione del PDA

Per l'implementazione del PDA è stato utilizzato il linguaggio Java (J2EE JDK1.5). Per ognuna delle tre tipologie di richieste previste da PolisWeb:

- attivazione sessione utente,
- consultazione,

- chiusura sessione utente, è implementata una servlet con funzione di proxy verso PolisWeb. La servlet prende in carico le richieste HTTP, aggiunge all'Header le informazioni sul tipo di richiesta, apre una nuova connessione con PolisWeb ed inoltra la richiesta HTTP.

Architettura

Di seguito sono descritti i componenti dell'architettura di autenticazione INAIL e le loro interazioni all'interno dei processi autorizzativi.

Application server

Il PDA è pubblicato su un application server JBoss 5.1 installato su un server Linux Red Hat. I servizi HTTP sono protetti da WebAgent Siteminder che effettuano l'autenticazione e autorizzazione degli utenti all'utilizzo delle risorse.

Policy Server SiteMinder

La procedura di autenticazione con certificato digitale è affidata al prodotto CA Siteminder, versione 6 service pack 12.8. L'elemento centrale dell'architettura del prodotto è rappresentato da un Policy Server che svolge le principali funzionalità di sicurezza fornite da SiteMinder, in particolare:

- l'autenticazione, per fornire alla soluzione PolisWeb i metodi di verifica del certificato e di estrazione del codice fiscale dell'utente dal certificato;
- l'autorizzazione in base alle politiche di controllo degli accessi definite per le risorse da proteggere. Nella soluzione adottata da INAIL, SiteMinder è stato customizzato in modo da integrarsi con il sistema di "profilazione applicativa" dell'istituto per autenticare ed autorizzare gli utenti che possono usufruire del servizio PDA.

I sistemi di profilazione applicativa

I sistemi di profilazione applicativa consentono la gestione centralizzata dei livelli di accesso alle procedure. Sono costituiti da:

- Una Console web per la creazione degli utenti. Attualmente sono definite tre tipologie di gruppi contenenti le categorie di utenti: avvocati, amministrativi e segreterie
- I Web services di interrogazione che veicola le informazioni alla procedura
- Un database SQL 2016 contenente tutte le informazioni di profilazione.
- La console Web e i web services sono entrambi sviluppati in linguaggio C#, framework 3.5.
- Siteminder contatta direttamente la basi dati di profilazione.

13.1.2. Autenticazione e Autorizzazione

Autenticazione

Di seguito è descritto il processo di autenticazione e validazione delle credenziali.

- L'utente richiede di accedere ai servizi Web forniti dal PDA collegandosi al sito <https://pda.processotelematico.giustizia.it>
- Il PDA presenta il proprio certificato digitale per poter essere correttamente riconosciuto dal client ed assicurare l'integrità dei dati.
- Il Webagent Siteminder installato sul server web intercetta la richiesta di accesso alla risorsa.
- La richiesta è inoltrata al policy server che verifica la tipologia di credenziali richieste dal servizio.
- Per l'accesso all'Area Servizi del PDA all'utente è richiesto il certificato di autenticazione. Si richiede l'inserimento di un dispositivo
- L'utente utilizza la Business Key, per fornire il proprio certificato di autenticazione
- Il certificato digitale contenuto nella carta è reso leggibile tramite l'inserimento del codice di attivazione della stessa da parte dell'utente.
- Siteminder recupera il common name della CA emittente e verifica che sia contenuto nella lista delle CA configurate come attendibili.
- Verifica che il certificato di autenticazione non sia stato revocato o sospeso, controllando le liste dei certificati revocati (CRL) e sospesi (CSL) dell'Ente Emittitore dello stesso. Se il certificato di autenticazione non è stato revocato o sospeso o non è scaduto, si effettua la validazione del certificato; altrimenti, qualora risulti irregolare, l'accesso al servizio è temporaneamente disabilitato e l'evento è notificato all'utente con un messaggio di errore. La disattivazione del servizio permane fino alla presentazione di un certificato regolare.
- Siteminder estrae il Codice Fiscale dal certificato di autenticazione per i controlli e la comunicazione con PolisWeb

Autorizzazione

Dopo aver effettuato con successo l'autenticazione degli utenti, Siteminder si collega ai sistemi di profilazione standard dell'istituto per l'autorizzazione degli utenti al PDA. Siteminder è stato configurato in modo tale da poter interrogare direttamente la base dati di profilazione, attraverso l'esecuzione di apposite Stored Procedures.

La fase di autorizzazione di un utente si articola nelle seguenti fasi.

Il Siteminder esegue una Stored Procedure sulle basi dati di profilazione, per richiedere il profilo dell'utente autenticato. La stored procedure contiene come parametro il codice fiscale estratto dal certificato nella fase di autenticazione.

- La stored procedure restituisce in output la lista dei gruppi cui l'utente appartiene.
- Siteminder verifica l'appartenenza dell'utente ad almeno uno dei gruppi autorizzati alla risorsa PolisWeb. Attualmente l'unico gruppo autorizzato è il gruppo Avvocati).
- La sessione è autorizzata e sono inserite nell'header le informazioni richieste dal PDA.

Tracciatura dei dati e archiviazione dei file di log

Al fine di prevenire e rilevare tempestivamente usi illeciti o abusi, e in conformità con le indicazioni fornite dal Ministero di Giustizia per l'attivazione del servizio PolisWeb, è stato attivato un sistema di registrazione di tutti gli accessi al PDA e conseguentemente all'area privata di PolisWeb da parte degli utenti. Le registrazioni devono contenere informazioni sufficienti per identificare l'utente che ha aperto la sessione, per esempio indirizzo IP del client, le operazioni effettuate e i riferimenti temporali di inizio e fine delle connessioni. Sono registrate e conservate tutte le transazioni fra l'utente e il PDA e tutte le richieste di consultazione a PolisWeb.

Negli archivi gestiti dal gestore tecnico del servizio di accesso a PolisWeb sono conservati e mantenuti i dati relativi a:

- dati di registrazione degli utenti;
- associazione tra identificativo dell'utente e certificato di autorizzazione di cui è questi Titolare;
- associazione tra identificativo dell'utente e password assegnatagli da PolisWeb;
- dati di sessione al sistema e ai servizi e altri dati necessari a tracciare le operazioni rilevanti ai fini della sicurezza.

Inoltre, il gestore dell'accesso al servizio PolisWeb deve conservare le registrazioni per il periodo di tempo determinato da norme e leggi applicabili. Al termine del periodo di conservazione previsto, in conformità con il Provvedimento del Garante del 1 marzo 2007, è prevista la cancellazione periodica ed automatica dei file di log (per esempio mediante meccanismi di sovrascrittura come la rotazione dei file di log) contenenti dati personali relativi agli accessi. L'eliminazione dei dati allo scadere del periodo di conservazione deve essere effettuata con particolare attenzione assicurandosi di cancellarli o renderli anonimi, eliminandoli anche dalle copie di back-up create per il salvataggio dei dati, in modo da rendere i dati irrecuperabili anche successivamente.

UC (Unified Communication)

Mediante il Servizio di Unified Communication (UC) si intende integrare i servizi di comunicazione in tempo reale (Instant Messaging, Telefonia IP, Video Conferenza) con quelli non in tempo reale (Voice Mail, SMS, FAX) ad oggi in essere presso l'Istituto. In questo modo è possibile coadiuvare i processi di business, tramite l'utilizzo di un'unica interfaccia utente, che consente di accedere ai servizi integrati a prescindere dalla posizione fisica dell'utilizzatore, riducendo drasticamente sia i costi infrastrutturali che di movimentazione.

Il Servizio si pone come interfaccia unica fra l'utilizzatore ed i servizi di business e di comunicazione, erogati dalle infrastrutture dell'Istituto, di modo che si possa incrementare la produttività degli utilizzatori facilitando il controllo, la gestione, l'integrazione e l'uso di più metodi di comunicazione aziendale. Il Servizio, ad oggi in fase di transizione sia per ciò che concerne l'architettura che i servizi erogati, prevedrà a regime la fruizione di quest'ultimi sia all'interno della Intranet d'Istituto che attraverso il canale pubblico mediante delle sessioni autenticate e crittografate.

L'architettura, realizzata mediante tecnologia Microsoft, sarà integrata nel servizio di Directory d'Istituto e prevedrà l'utilizzo di politiche, ad oggi in fase di definizione, per l'utilizzo dei Servizi in base al ruolo assegnato all'utilizzatore.

Poiché il Servizio si rivolge ad una Utenza Standard, la sua applicabilità è demandata essenzialmente alle politiche definite per il Servizio di Directory d'Istituto ed è attiva esclusivamente per i Servizi di Instant Messaging, Video Conferenza, Live Meeting e Net Presence. Per i Servizi che saranno attivati a regime, saranno definite delle politiche ad hoc in base al ruolo assegnato all'utilizzatore.

Questa soluzione adottata è completamente software e si può integrare con soluzioni di telefonia legacy, sia TDM che VoIP, senza richiedere la sostituzione dei telefoni o i sistemi di videoconferenza esistenti, aggiungendo i servizi elencati successivamente ai servizi di telefonia tradizionali, realizzando così una unificazione completa di tutti i canali di comunicazione, sia real time che non real time.

Le informazioni di presenza sono automaticamente basate sul contenuto del calendario Exchange e sono comunque fortemente integrate con la piattaforma Office. Il servizio di presenza consente di visualizzare in tempo reale lo stato dei dipendenti (in base alle informazioni del calendario, lo stato di accesso/attività e le preferenze dell'utente), permettendo agli utenti di contattare subito la persona giusta utilizzando il metodo di comunicazione più appropriato. In un ambiente di lavoro questa funzionalità si rivela fondamentale per garantire la collaborazione.

14. SICUREZZA

Di seguito sono approfonditi alcune politiche attuate nell'ambito della sicurezza ICT dell'Istituto.

14.1. Identity Management

La piattaforma WEB sostiene molteplici canali tramite i quali utenti dell'organizzazione INAIL ed utenti singoli o di altre organizzazioni accedono ad applicazioni e dati.

La necessità di realizzare un punto di vista unico dell'utente rispetto ai servizi INAIL trova risposta nell'applicazione delle tecnologie di Portale e negli strumenti di cooperazione che si aggiungono alle applicazioni WEB attualmente esistenti. Il processo di "portalizzazione" delle applicazioni è in corso, ma gli elementi tecnologici e le metodiche utilizzate per creare una "vista unica" dei servizi, se da un lato astraggono l'utente dalle particolarità di ciascun ambiente applicativo, fornendo un'interfaccia comune, dall'altro impongono una revisione di elementi dei processi e delle applicazioni al fine di realizzare la condivisione su una infrastruttura comune.

È in questo contesto che è impostata l'evoluzione del Portale al fine di unificare anche, per le applicazioni istituzionali in fase di reingegnerizzazione verso il WEB, le modalità di identificazione e di profilazione degli utenti.

L'utilizzo del sistema di Identity Management (IM) consente l'effettiva realizzazione del singolo punto di vista utente, dal momento che tale sistema consente di associare l'identità della persona fisica con i servizi utilizzabili.

Il sistema IM fa da "collante" verso i servizi applicativi, in quanto procede all'identificazione ed all'abilitazione, in base alle caratteristiche di profilazione ed alle credenziali gestite per ciascun utente e per ciascun servizio disponibile sul Portale INAIL, sia per l'ambiente WEB/Intranet, prevalentemente basato sui domini di rete, sia per il più variegato ambiente Internet, con credenziali universali (SPID, CNS, CIE, etc.) superando le credenziali proprietarie (ES: matricola, codice ditta, etc.).

Oltre a concretizzare il concetto di "punto di vista unico dell'utente", i servizi infrastrutturali consentono di orientare l'accesso a funzioni ed informazioni con un'ottica per processi. Qualsiasi problematica di gestione in ottica Service Oriented, con concetti EAI (Enterprise Application Integration) e BPM (Business Process Management) *impone che ai dati accedano componenti e non persone ovvero che le persone possano accedere ai dati esclusivamente tramite processi.*

14.2. Tracciatura

Come è noto, in tema di sicurezza e privacy si distinguono aspetti di **Confidenzialità** (trattamento e cessione dati in transito conosciuti e gestiti soltanto da ruoli ed individui in possesso dei requisiti necessari), **Accesso** (raggiungimento di funzionalità ed informazioni per chi è in possesso delle necessarie credenziali) ed **Integrità** (l'informazione custodita e gestita non subisca manomissioni non autorizzate, perdite o danneggiamenti).

Il sistema di accoglienza INAIL, parte integrante del sistema Portale che racchiude funzionalità di autenticazione ed autorizzazione all'accesso ai servizi, consente di **"tracciare"** le unità di lavoro dell'utente, nell'ambito della singola sessione logica soggetta ad un unico passo di "login".

Tutte le applicazioni WEB del portale trovano nel Modulo Tracciatura le interfacce per registrare gli eventi di business secondo il paradigma del "CHI" ha fatto, "COSA", secondo un modello di dizionario univoco di dominio, "QUANDO".

Attualmente il servizio TRACCIA tutti gli accessi al sistema di accoglienza INAIL, parte integrante del sistema Portale che racchiude funzionalità di autenticazione ed autorizzazione all'accesso ai servizi. In questo contesto è già attivo dai primi mesi del 2006 il servizio di "tracciatura" che verrà esteso progressivamente a tutti gli altri eventi di business mediante l'integrazione di tutte le applicazioni (interne ed esterne) che vanno ad affacciarsi sul Portale secondo la logica del "punto di vista unico dell'utente".

Ogni utilizzo di informazioni destinate a "tracciatura" alimenta il Provider Eventi. In generale occorre distinguere tra:

- Eventi di business, generati da utenti che utilizzano servizi dal Portale INAIL o altri canali come la porta di dominio o la multicanalità (ad esempio tracciatura di dati sensibili oppure log di processi).
- Eventi tecnici, affidati al Provider, sia dalle applicazioni, sia da agenti di sistema allo scopo di rilevare informazioni relative a particolari stati oggetto di monitoraggio (condizioni dei sistemi, monitoraggi di flussi applicativi, etc.).

TRACCIATURA APPLICATIVA

L'Istituto, sempre nell'ottica di proteggere l'accesso ai dati attraverso le applicazioni, ha deciso di integrare il sistema di accoglienza INAIL con componenti che permettano di **"tracciare"** le attività svolte dall'utente (tracciatura applicativa).

È stato, quindi, realizzato il Servizio Tracciatura Applicativa, che si propone come strumento a supporto delle applicazioni, fornendo alle stesse dei servizi utili a tracciare eventi:

- Eventi di sicurezza: eventi di login, logout, accesso a risorse;
- Eventi applicativi: operazioni di consultazione o modifica dati.

Inoltre, i Web Service che lo compongono possono essere forniti alle applicazioni attraverso l'infrastruttura SOA, consentendone la massima diffusione all'interno dell'Istituto ed eventualmente l'orchestrazione in processi complessi.

Il servizio si colloca idealmente a valle di un processo di Assessment delle applicazioni dell'Istituto avente lo scopo di determinare il valore del portafoglio applicazioni dell'Istituto attraverso la valutazione della complessità delle regole di business implementate, dell'importanza per il business dell'azienda, dell'importanza dei dati elaborati e della loro rilevanza ai fini di una corretta gestione della privacy.

Le risultanze di questo Assessment (che potrebbero essere memorizzate in un database per poter poi essere consultate da un apposito cruscotto) consentono di definire in maniera oggettiva, in funzione appunto del

valore dell'applicazione e dei dati trattati, quali informazioni devono essere tracciate e con che livello di tracciatura deve essere implementato dall'applicazione (ovvero di definire quali Eventi devono essere tracciati e quali Termini devono essere oggetto della tracciatura).

Le informazioni identificate (Eventi e Termini) vengono inviate dalle applicazioni al servizio tracciatura che le utilizza per alimentare un database consultabile, come detto, tramite strumenti applicativi di reportistica, consultazione e ricerca.

Architettura di sistema

Il sistema si basa su tre gruppi di servizi: Servizi di Tracciatura, Servizi di Reportistica e Servizi di Amministrazione. Le informazioni identificate che devono essere tracciate (Eventi e Termini) vengono inviate dalle applicazioni ai servizi di tracciatura che le utilizza per alimentare un database consultabile tramite i servizi di reportistica, consultazione e ricerca.

In particolare, i **servizi di tracciatura** si occuperanno:

- della raccolta dei dati ed il controllo degli stessi dall'interno delle applicazioni monitorate;
- dell'instradamento degli stessi verso il servizio di raccolta dei dati;
- della mappatura dei dati rispetto al Repository dei metadati di tracciatura.

Il servizio di raccolta informazioni si compone di una fase sincrona (verifica informazioni ed accodamento dei dati da elaborare) e di una fase asincrona (smistamento dei dati accodati, scrittura su DB, eventuale memorizzazione dei dati su altri sistemi di archiviazione e tracciatura).

Il servizio di raccolta informazioni si occupa quindi, in prima istanza, di gestire i dati inviati dai componenti applicativi, controllandone la validità a livello formale.

Ogni applicazione che deve tracciare le informazioni accede al servizio tramite i web Services esposti fornendo una serie di parametri necessari al tracciamento dell'evento scelto.

I dati necessari alla tracciatura dell'evento sono:

- l'identificativo dell'applicazione che sta utilizzando il servizio;
- evento che l'applicazione vuole tracciare tra quelli previsti per quella applicazione;
- dati utili a tracciare l'evento

Il **servizio di raccolta**:

- riceve le richieste dai servizi di tracciatura;
- verifica la correttezza formale dei dati forniti;
- verifica la consistenza dei dati forniti; in particolare,
- verifica che l'evento sia tra quelli previsti nel Repository dei metadati;
- verifica che i dati forniti siano tutti quelli previsti nel Repository dei metadati per quell'evento;
- scrive una coda con le richieste ricevute (una per gli eventi relativi alla sicurezza ed un'altra per gli eventi applicativi);

- elaborare le richieste accodate in maniera asincrona rispetto alle richieste. In particolare, il servizio si occupa, in modo sincrono, di:
- verificare che l'applicazione che richiede la tracciatura sia censita all'interno del sistema;
- verificare che i dati inviati siano formalmente corretti; i dati, a seconda delle esigenze della tracciatura dello specifico evento, potranno essere strutturati in maniera semplice (stringa XML) o complessa (i parametri vengono passati sotto forma di Oggetto Evento);
- crittografare i dati e scriverli sulla coda JMS relativa agli eventi di sicurezza;
- informare il componente applicativo chiamante dell'esito dell'operazione. Nella fase asincrona il servizio si occupa di:
- prelevare le richieste dalla coda JMS, decriptare i dati;
- inserire i dati nel database di tracciatura degli eventi;
- inviare i dati ad eventuali altri sistemi di tracciatura e log (se richiesto).

I **servizi di reportistica** renderanno disponibili:

- la produzione di reportistica relativa all'utilizzo delle risorse monitorate;
- la consultazione dei dati alle applicazioni proprietarie.

I **servizi amministrativi**, attualmente in fase di definizione, si occuperanno di definire i parametri funzionali del sistema; in particolare di definire quali applicazioni potranno utilizzare i servizi, quali eventi potranno essere tracciati e quali dati dovranno essere forniti per ogni evento.

14.3. Single Sign On INAIL

L'obiettivo del sistema SSO è creare un'architettura unitaria fortemente integrata, idonea a sostenere l'evoluzione dei servizi e di minimizzare allo stesso tempo gli impatti dei continui cambiamenti del business e delle tecnologie. Il sistema di Single Sign On (SSO) dell'INAIL offre un unico punto di accesso per i servizi verticali web dell'Istituto e si fa carico della fase di autenticazione e autorizzazione dell'utente Internet e Intranet.

La presenza di diverse applicazioni eterogenee e di diverse tipologie di utenze ha reso necessario implementare una infrastruttura di SSO per offrire l'autenticazione e la profilazione degli utenti finali come servizi infrastrutturali e non come parti integranti delle singole applicazioni, in quanto SSO e profilazione sono entità logiche separate dalle applicazioni.

Il sistema consente, una volta superata la fase di verifica delle credenziali, di navigare fra i servizi senza richiedere ogni volta di autenticare nuovamente l'utente, anche se questo ultimo "salta" da un dominio applicativo ad un altro.

Tale processo è trasparente alla logica applicativa, ovvero ai pacchetti applicativi che incapsulano la logica di business dei servizi. L'applicazione non partecipa alla fase di autenticazione ed autorizzazione

all'accesso alle risorse, anche se gestisce una lista di ruoli che permettono di determinare le tipologie di utenti con i privilegi necessari ad accedere al servizio.

Il servizio comprende anche di una libreria, in distribuzione alle applicazioni, che consente di accedere al servizio di profilazione applicativa, che effettua l'associazione di un profilo all'utente che si è autenticato.

L'infrastruttura di Single Sign On è costituita da più domini logici:

- un Principal domain in cui è posizionata la pagina di login dell'area riservata agli utenti registrati ((<http://gestioneaccessi.inail.it>)), nel portale INAIL (<http://www.inail.it/>), realizzata in tecnologia J2EE;

Possiamo suddividere la parte operativa in tre livelli:

- autenticazione utente alle applicazioni,
- autorizzazione utente alle applicazioni,
- propagazione della sicurezza e profilazione applicativa.
- Componenti del Servizio di Single Sign On

Siteminder

Le procedure di autenticazione ed autorizzazione ai servizi web sono affidate al prodotto SiteMinder di Computer Associates, versione 12.8. L'architettura del prodotto ruota intorno ad un Policy Server che provvede le funzionalità di:

- Autenticazione; attraverso tutti i metodi più diffusi di autenticazione, quali, per esempio User-Name/Password, Two factor tokens, X.509 certificates, Passwords over SSL, smart cards, SPID, Method Chaining, Authentication Levels, Forms-based, Custom Method, Full CRL support.
- Autorizzazione; in base alle regole di controllo degli accessi stabilite dall'amministratore.

Nella soluzione adottata in INAIL la fase autorizzativa degli utenti è basata sui sistemi di "profilazione applicativa" dell'istituto.

Di seguito sono descritte in dettaglio le principali componenti di SiteMinder.

WEB Agent

Il Web Agent è un modulo installato come filtro aggiuntivo dell'HTTP Server del Reverse Proxy o direttamente sul Web Server dell'applicazione. Effettua il processo di autorizzazione e, intercettando tutte le richieste di pagine web fatte dagli Utenti, verifica l'autenticazione rispetto all'Utente che ha effettuato la richiesta. Il Web Agent riceve ed invia all'applicazione attributi specifici dell'utente, sotto forma di "Response" (descritte nel paragrafo "Autorizzazione"), per permettere eventuali personalizzazioni e gestione della sessione all'applicativo. Nel caso di applicazioni su BEA Web Logic il WA crea il "token" di autenticazione perimetrale necessario all'ASA (Application Server Agent) per la fase di Identity Assertion.

Application Agent

L'application server BEA Web Logic gestisce la sicurezza secondo lo standard JAAS (Java Authentication e Authorization Services) che prevede l'uso di un'autenticazione perimetrale seguita dalle fasi di Identity Assertion, Authentication ed Authorization ciascuna fornita da uno o più security provider.

La propagazione dell'Identity dal WA all'ASA avviene tramite un cookie SiteMinder che rappresenta il token dell'autenticazione perimetrale.

Policy/Key Store su ADAM

Repository per le regole e per le chiavi di crittografia che governano il controllo degli accessi e la comunicazione tra i vari componenti. Nel progetto è stato scelto l'uso di CA Directory come repository per le Policy e le Key.

User Store

Lo User Store è progettato per essere funzionale ai tre processi principali:

- Autenticazione (AUTH);
- Autorizzazione (AUTZ);
- Provisioning.

Profilazione Applicativa

Il "profilo" di un utente è rappresentato dalle sue informazioni anagrafiche e dall'insieme dei gruppi cui appartiene. Tali informazioni risiedono in parte nelle basi dati istituzionali (HR per gli utenti interni e DB2 per le aziende ed i patronati) ed in parte in quelle infrastrutturali (database intranet per i consulenti informatici e database degli utenti Internet per i consulenti del lavoro, i delegati, ecc.) dell'istituto. Il servizio di profilazione utente garantisce un sistema centralizzato per il recupero di tali informazioni, disponibile per tutte le piattaforme informative tramite l'esposizione di interfacce di interrogazione standard, basate su web-services richiamabili da client SOAP (Simple Object Access Protocol).

Il "profilo" di un utente rimane concettualmente invariato in tutti i sistemi anche se le sue mansioni possono variare.

Il profilo applicativo di una procedura è l'insieme di ruoli/competenze/funzioni che un gruppo di utenti può ricoprire all'interno della stessa. Tali possibili "ruoli applicativi" sono identificati dai responsabili delle singole applicazioni garantendo in questo modo la possibilità di stabilire regole di accesso diverse per lo stesso gruppo all'interno di ognuna delle procedure. Un utente è considerato autorizzato ad una procedura se ad almeno uno dei gruppi cui appartiene è stato assegnato un ruolo applicativo valido nella stessa.

La componente di profilazione applicativa si compone di una base dati SQL 2016, di console web e di web-services ed API di interrogazione, entrambi sviluppati in linguaggio C#, framework 10.

La console web fornisce gli strumenti che consentono ad utenti autorizzati di popolare i gruppi di sicurezza definiti dall'istituto e i web-services/API veicolano tali informazioni alle procedure.

Come descritto in seguito, SiteMinder è in grado di interrogare direttamente le basi dati di profilazione e di ricavare un set di dati necessari all'autorizzazione.

ARCHITETTURA DEL SERVIZIO DI SINGLE SIGN ON

La rete di servizi INAIL è divisa in due aree logiche e fisiche: l'area Intranet nella DMZ cui accedono solo utenti INAIL registrati nel dominio Active Directory e l'area Internet separata dalla DMZ cui accedono utenti Internet ed utenti Intranet, provenienti da Internet.

I Meccanismi di accesso supportati sono

Per i dipendenti dell'Istituto:

- Microsoft MFA

Per Aziende, Intermediari, Cittadini ed in generale tutti i Clienti esterni che accedono ai Servizi On-Line dell'Istituto:

- SPID;
- CNS;
- CIE;
- Eidas.

Il policy server di SiteMinder diventa il fulcro del nuovo sistema di SSO e di controllo degli accessi. In tale soluzione sugli HTTP ed Application server coinvolti nei servizi e sottoposti a SSO sono installati i Web Agent (per i server Http) e gli Application Agent (per gli application server) che agiscono da filtro per tutti gli accessi alle applicazioni dialogando con il Policy Server. Il Policy Server si interfaccia con i Database SQL Server 2016 e con i Domain Controller del Dominio di Active Directory, per gestire le operazioni di autenticazione/autorizzazione ed implementare le policy di accesso richieste dalle applicazioni.

Autenticazione

La fase di autenticazione prevede che al momento in cui un utente non ancora autenticato tenta l'accesso ad una risorsa protetta (sia essa una pagina html o un'intera applicazione web) possano verificarsi due casistiche

- gli agent installati verificano la presenza di una sessione autenticata ed eventualmente reindirizzano l'utente al Principal domain l'autenticazione dell'utente.
- L'applicazione, secondo il modello OAuth 2.0, verifica l'esistenza e la validità di una sessione utente tramite l'access token

Autorizzazione

Per tutti gli utenti INAIL sia esterni che interni l'autorizzazione dipende da due fattori rappresentati nelle strutture dati del DB:

- ID dell'applicazione (o della applicazione che contiene la risorsa protetta);
- Il profilo applicativo dell'utente.

L'ID dell'applicazione è un codice che identifica univocamente una procedura Web all'interno del Database di profilazione. La profilazione applicativa (si veda il paragrafo 6.3) restituisce il profilo dell'utente per la

specifica applicazione ossia l'elenco delle proprietà e dei ruoli che l'utente ha e che determina se l'utente può accedere e con quali diritti.

Il profilo applicativo è veicolato alle procedure tramite web services o API (protocollo SOAP\REST) che restituiscono un documento XML con i dati di profilazione dell'utente.

La fase autorizzativa non richiede l'intero profilo applicativo, ma solo le parti che contengono i ruoli di sicurezza. Siteminder è quindi in grado di interrogare i servizi di profilazione senza passare tramite le interfacce rappresentate dai web services e di restituire alle procedure i soli ruoli di sicurezza tramite il meccanismo della "Active Response" o inserendoli all'interno di JWT.

Una "Active Response" è costituita da coppie di attributi nome/valore che sono aggiunte dal Web Agent all'Header http (o anche come cookie) nella sessione dell'utente. Il servizio SSO inserisce nelle variabili header i "ruoli" di sicurezza dell'utente per la specifica applicazione. Per tutte le applicazioni basate su JAAS tali ruoli saranno inseriti dall'application server agent nel "principal" dell'utente come da standard.

Superata le fasi di autenticazione e autorizzazione, le applicazioni che avranno bisogno dell'intero profilo dell'utente continueranno ad invocare web services o API di profilazione.

Il profilo completo dell'utente contiene i gruppi di appartenenza e loro proprietà come le sedi di competenza dell'utente. Al momento dell'accesso ad un servizio web di un utente, che avviene solo una volta superate le fasi di autenticazione ed autorizzazione, le procedure potranno richiederne il profilo completo.

14.4. Sistema unico di profilazione

La nuova architettura dei servizi di profilazione nasce dall'esigenza di garantire una sempre maggiore distribuzione delle competenze per quanto riguarda la gestione della sicurezza applicativa. Il responsabile centrale di un servizio applicativo non provvede più ad abilitare gli utenti alle procedure, tale compito è ora completamente demandato ai responsabili delle strutture territoriali o anche a vicari da essi a loro volta autorizzati, generando gerarchie di gestione degli accessi anche molto complesse.

Questa crescente responsabilizzazione degli uffici territoriali nell'ambito dei processi applicativi istituzionali ha richiesto la creazione di console di profilazione sempre più flessibili e distribuibili nonché di servizi in grado di veicolare informazioni molto più complesse che in passato. In altre parole la creazione di un "profilo" di un utente e la sua assegnazione ad un "ruolo applicativo" (la creazione della sua "profilazione applicativa") sono stati resi più flessibili per venire incontro alle nuove esigenze dell'istituto. La nuova profilazione degli utenti garantisce inoltre la creazione di gruppi riutilizzabili da tutte le procedure e strumenti di interrogazione centralizzata verso le basi dati di Human Resource che ricopre in maniera ancora più decisa un ruolo centrale ed ufficiale per quanto riguarda le informazioni anagrafiche degli utenti e delle strutture nonché per l'identificazione di figure istituzionali dell'istituto quali ad esempio i direttori di sede.

Il nuovo Sistema Unico di profilazione rappresenta in tutte le sue componenti un'architettura comune a tutta l'infrastruttura compresi i servizi esterni in internet. In questo caso i concetti di gerarchia e delega

vengono estesi alla gestione delle utenze dei grandi utenti abbinata, per quanto riguarda le credenziali di accesso, ad una piena compatibilità con la CNS e SPID.

IL “PROFILO UTENTE”

Il “profilo” di un utente è rappresentato dalle sue informazioni anagrafiche e dall’insieme dei gruppi a cui appartiene. Tali informazioni risiedono in parte nelle base dati istituzionali (HR per le utenti interni e DB2 per le aziende ed i patronati) ed in parte in quelle infrastrutturali (Cercapersone per i consulenti informatici e database degli utenti Internet per i consulenti del lavoro, i delegati) dell’istituto. Il servizio di profilazione utente garantisce un sistema centralizzato per il recupero di tali informazioni, disponibile per tutte le piattaforme informative tramite l’esposizione di interfacce di interrogazione standard (basate su web-services richiamabili da client SOAP, Simple Object Access Protocol, o REST).

Il “profilo” di un utente rimane concettualmente invariato in tutti i sistemi anche se le sue mansioni potrebbero variare.

PROFILI MULTIPLI

L’incremento e la diversificazione delle attività e competenze lavorative pone, come diretta conseguenza, l’esigenza che uno stesso utente possa ricoprire più ruoli funzionali.

L’evoluzione del sistema informativo, relativamente alle credenziali per l’accesso ai servizi web dell’Amministrazione, verso una architettura la quale preveda che le credenziali digitali siano riconducibili ad un’unica persona fisica, decreta che l’autorizzazione circa le condotte attuate sui portali web sia discriminata, non più a livello di credenziali bensì a livello di profili.

Il valore aggiunto dall’attività risiede nella trasparenza, lato utente finale, circa il sistema di autorizzazione, ovvero, i servizi applicativi sono in grado di discriminare autonomamente il profilo autorizzato, fra i possibili condivisi da una stessa utenza.

Qualora più profili, associati ad una stessa utenza, siano idonei all’accesso ad un servizio, l’applicazione individuerà quello più adeguato in funzione dell’azione eseguita.

I GRUPPI

L’associazione di un utente ad uno o più ruoli applicativi è piuttosto intuitiva ma quando ad un ruolo è associato un gruppo è fondamentale comprendere cosa esso rappresenta, quali utenti ne possono far parte e in base a quali processi viene alimentato.

Per **gruppo** si intende un insieme logico di utenti aventi una serie di proprietà che ne descrivono il comportamento sia in fase di interrogazione che in quella di amministrazione. Nei paragrafi successivi saranno descritte le principali proprietà dei gruppi e le loro finalità.

DOMINIO

Ogni gruppo fa riferimento ad un insieme di utenti che “potenzialmente” possono farne parte. Tale insieme di utenti viene definito “dominio del gruppo”.

Es.: il gruppo “Amministratori Intranet” ha come dominio tutti gli utenti Intranet e solo un’utente Intranet può farne parte, mentre il gruppo “Consulenti del lavoro” ha come dominio tutti gli utenti Internet.

Tipologia (gruppo standard o applicativo)

- **standard:** sono gruppi visibili a tutte le procedure. I membri di questa tipologia di gruppo quasi sempre sono ricavati da informazioni presenti sulle basi dati istituzionali.
Es.: i “direttori di sede”, gli “ispettori” ed i “medici” sono gruppi ricavati dalla base dati di Human Resources dell’istituto in base ad informazioni di incarico, qualifica e processo. Tali utenti non possono essere gestiti tramite la console dei gruppi.
- **applicativo:** sono gruppi specifici per una o più procedure. I membri di tali gruppi sono amministrati direttamente tramite la console generalizzata di amministrazione dei gruppi.
L’assegnazione degli utenti a tali gruppi avviene tramite la console di gestione centralizzata.

ATTRIBUTI DI APPARTENENZA (O DISCRIMINANTI)

Ogni gruppo può avere uno o più attributi di appartenenza che definiscono proprietà dei propri membri. In tal senso gli “Attributi di appartenenza” sono le proprietà che è necessario specificare ad un utente per inserirlo in un dato gruppo e contribuiscono a discriminare i vari membri l’uno dall’altro. I valori possibili di queste proprietà possono essere definiti, quindi limitati ad uno specifico set, o inseriti tramite una digitazione libera e pertanto validati solo “formalmente”.

Es.: il gruppo “direttori di sede” ha come attributo di appartenenza il “codice sede” (i valori possibili di questo attributo sono i codici delle unità presenti nelle basi dati istituzionali). Tale attributo definisce una proprietà che tutti i membri del gruppo dovranno implementare e che contribuirà a distinguerli l’uno dall’altro: il direttore della sede 11000 può essere distinto da direttore della sede 14000 anche se entrambi appartengono allo stesso gruppo.

Per ogni utente si può avere più di un valore dell’attributo di appartenenza per ogni gruppo. Tale situazione genera quelle che vengono definite “istanze” di appartenenza.

Es.: un utente può appartenere al gruppo “direttori di sede” con due valori di “codice sede” essendo così direttore di due sedi e generando due istanze.

MODALITÀ DI AMMINISTRAZIONE

- **statica:** il gruppo è popolato attraverso la console di gestione dei gruppi dagli amministratori definiti in fase di implementazione. Tutte le informazioni sui membri di gruppi ad amministrazione statica sono contenute nelle basi dati della profilazione utente.
- **dinamica:** il gruppo è popolato attraverso plug-in a basi dati esterne e la sua amministrazione è definita “dinamica”. I membri di tali gruppi non sono gestibili da console (sono tuttavia visualizzabili). *Es.: i gruppi standard sono quasi sempre dinamici perché popolati dalle basi dati di HR e come già evidenziato non sono direttamente gestibili dalla console.*

FUNZIONI AMMINISTRATIVE E CRITERI DI COMPETENZA

I gruppi possono essere amministrati da singoli utenti o da altri gruppi tramite la creazione di funzioni amministrative.

Es: “gestisci i validatori pratiche” e “gestisci gli amministratori del cercapersone” sono due funzioni amministrative definite rispettivamente per i gruppi “validatori pratiche” e “amministratori cercapersone”.

La gestione di un gruppo può essere ulteriormente limitata e distribuita tramite la definizione di diversi “criteri di competenza” per ogni utente (o gruppo) avente una funzione amministrativa. I criteri di competenza per una funzione amministrativa specificano quali utenti di un gruppo si possono vedere, quali amministrare, quali modificare e quali aggiungere.

Es: “gestisci i validatori pratiche” e “gestisci gli amministratori del cercapersone” possono essere ulteriormente specializzati definendo quali “validatori pratiche” e quali “amministratori del cercapersone” un utente può amministrare.

LA CONSOLE DI GESTIONE DEI GRUPPI

Mentre per il servizio di profilazione applicativa le modifiche e gli adeguamenti si riferiscono per lo più alla struttura di Back-end, per facilitare la definizione e l'alimentazione dei gruppi è stata implementata una nuova console di gestione più flessibile e completamente distribuibile, sviluppata in linguaggio C#, framework .net 3.5. Basata interamente sul sistema delle “funzioni di amministrazione” e dei “criteri di competenza” sopra descritti, permette di demandare la gestione di ogni gruppo a più utenti o gruppi, ognuno con il proprio ambito di amministrazione. Come evidenziato nei capitoli precedenti, i gruppi possono essere di varia natura e non sempre sono riconosciuti da tutti i mondi applicativi. Per questo motivo la console è collegata ai servizi di profilazione applicativa ed è in grado di fornire agli amministratori la sensazione dell'impatto che le modifiche da lui apportate avranno sui sistemi, visualizzando quali procedure utilizzeranno i gruppi da lui gestiti.

RIUSO DEI GRUPPI E RAPPRESENTAZIONE APPLICATIVA

Come già descritto in precedenza lo stesso gruppo può avere ruoli o competenze diverse nelle varie procedure. Questo garantisce la possibilità di riutilizzare i gruppi già presenti nelle architetture di profilazione, semplificando notevolmente le procedure di gestione a carico degli amministratori.

Assegnando un'utente ad un gruppo “funzionale” se ne garantisce l'autorizzazione all'accesso in varie applicazioni in ognuna delle quali potrebbe svolgere mansioni differenti. Oltre ad avere ruoli diversi i gruppi possono anche essere rappresentati diversamente alle varie procedure. Questa “rappresentazione applicativa” consente di definire lo stesso gruppo con nomi diversi o anche più gruppi con lo stesso nome se ne esiste la necessità.

Es.: il gruppo “responsabili di processo” è amministrato dai direttori di sede. Tale gruppo accede, seppur con mansioni diverse, a tutte le procedure istituzionali tramite i servizi di profilazione. Questo permette al direttore di sede di definire una sola volta gli utenti che fanno parte di questo gruppo garantendone al contempo l'accesso a tutte le applicazioni interessate.

Il servizio e la console della “Profilazione Utente” forniscono rispettivamente gli strumenti necessari all'assegnazione degli utenti ai gruppi e le interfacce di interrogazione alle relative basi dati.

14.5. Servizi del Security Operations Center (SOC)

Nell'infrastruttura dell'Istituto sono installate e attive diverse soluzioni di sicurezza a protezione sia dei server sia dei client. È quindi stata istituita la funzione del SOC, con mansioni di monitoraggio e operatività

sugli eventi legati alla sicurezza informatica. Per sua stessa natura, un SOC è necessariamente composto, tra l'altro, da personale che opera in regime di presidio, verificando, controllando e reagendo alle eventuali minacce di sicurezza presentatesi mediante l'utilizzo di varie soluzioni tecnologiche.

I sistemi gestiti dal SOC sono i seguenti:

- Sistemi Proxy Trellix Web Gateway per la navigazione internet bilanciati da Citrix NetScaler per il controllo della navigazione Internet. Attraverso dei motori di scansione antivirus, antispyware, url filtering etc. che analizzano il traffico HTTP(S) impedisce il download di virus, malware e spyware. Con gli MWG il SOC controlla la navigazione sia cablata che tramite il wireless dell'Istituto (Captive Portal);
- Domain Controller costituito da Writable Domain Controller, disposti sulla rete interna, e da Read Only Domain Controller disposti sulle reti dmz.
- Trellix che serve per la gestione centralizzata e relativo deploy ed aggiornamenti dei seguenti prodotti di sicurezza distribuiti sulle PDL e sui Server dell'Istituto;
- SQL Server che viene utilizzato come BackEnd per ePO.
- Network Intrusion Prevention System (NIPS) gestito utilizzando tecnologia Trellix. Il NIPS è un sistema di rilevamento delle intrusioni che fornisce il monitoraggio e la sorveglianza continua della rete, analizzando il flusso di dati ed il traffico dell'infrastruttura a livello di contenuto dei pacchetti. Essi analizzano i contenuti del traffico, alla ricerca di attività non autorizzate e attacchi informatici, consentendo al SOC di contrastare immediatamente le azioni malevoli che vengono eseguiti verso i sistemi.
- DXL – Framework per la comunicazione tra prodotti McAfee;
- TIE – Database che raccoglie la categorizzazione della reputazione dei file e attraverso il framework di comunicazione Trellix permette a tutti agli altri prodotti della suite di agire secondo policy;
- ATD – Servizio di analisi statica e dinamica di file sospetti attraverso l'uso di sandbox, sottomessi automaticamente allo stesso dagli altri prodotti Trellix attraverso il framework di comunicazione DXL;
- Citrix NetScaler – Reverse proxy degli ambienti di collaudo, certificazione e produzione, gestisce la pubblicazione di siti e applicazioni INAIL sulla Intranet, Infranet e Internet; permette di eseguire bridging oppure terminare le connessioni SSL e bilanciare in chiaro verso i front-end, inoltre ottimizza il processo di caching e, soprattutto, intercetta request e response operando sugli header: questo permette di aumentare la sicurezza delle applicazioni esposte e di ovviare a problemi di sviluppo e/o applicativi che non permetterebbero la buona riuscita dei test prestazionali e/o di sicurezza;
- Horus – È una piattaforma di sandboxing basata su un progetto open source; tramite questo servizio è possibile inviare ad una specifica casella di posta elettronica un allegato sospetto per un'analisi automatica e più approfondita rispetto ai sistemi basati su firme; la soluzione restituisce poi un report dettagliato con uno "score" che esprime se e quanto il file sottomesso è malevolo;

- Maya – È una piattaforma di sandboxing basata su un progetto open source; questo servizio è stato messo a disposizione del CERT-PA integrandolo nella piattaforma infosec. Maya è utilizzato dalle altre PA come analisi comportamentale dei Malware e per inviare Indicatori di Compromissione verso sistemi di Infosharing.
- Misp – È una piattaforma di Threat Intelligence che aiuta il SOC ad aggregare, correlare e analizzare i dati delle minacce da più fonti in tempo reale per supportare azioni difensive.
- TheHive – Stumento utilizzato in unione con il MISP per effettuare indagini di Threat Intelligence in caso di Incidenti e analisi più approfondite.
- DNS Firewall – Firewall DNS che intercetta le query DNS applica sicurezza;
- WSUS – Servizio di Windows Update centralizzato per i server del SOC.
- Cassaforte Elettronica – Sistema di gestione delle credenziali amministrative; il prodotto permette la connessione ai vari sistemi tramite vari protocolli garantendo un controllo mediante registrazione della sessione amministrativa sul sistema target; la sua funzione principale è quella della gestione delle password, in quanto in base alle policy dell'istituto, può riconciliare e quindi cambiare le credenziali amministrative a seguito di ogni sessione;
- Trellix – È la componente antivirus in grado di bloccare e rimuovere proattivamente il software malevolo ed estende la copertura contro i nuovi rischi per la sicurezza; comprende anche una parte di Host Intrusion Prevention, componente che aiuta a proteggere i desktop e server dalle minacce esterne, controllando e bloccando le attività potenzialmente pericolose;
- File and Removable Media Protection – È la componente che permette di criptare e proteggere file in maniera tale che solo determinati utenti possano accedervi;
- Certificati Digitali – Emissione, revoca e rinnovo di certificati digitali di vario tipo (Client authentication, Server authentication, Code Signing, etc.) tramite Certification Authority locale e gestione dei rapporti con le Certification Authority pubbliche;
- AIP – Prodotto Microsoft che permette la classificazione e la protezione dei documenti Office; sono implementate policy di sicurezza che permettono di taggare e condividere i documenti (Word, Excel, PowerPoint, etc.) applicando delle restrizioni per l'accesso con varie granularità (utente, azienda, dominio, etc.); inoltre, è possibile applicare criteri di protezioni diversi in base alla classificazione, come il blocco dell'inoltro, della stampa, del copia-incolla, etc.;
- ATP – Prodotto Microsoft che effettua scansione di allegati e link malevoli; le policy applicate permettono l'analisi in real-time degli allegati in base al tipo di file e all'estensione; inoltre, i link all'interno delle email vengono modificati in automatico per permettere l'analisi immediata al click dell'utente;
- DKIM – Configurazione basata su coppia di chiavi pubblica/privata per prevenire lo spoofing di email; in questo modo un attaccante esterno non può impersonificare un indirizzo email appartenente all'istituto;
- BitSight – Prodotto esterno che monitora i servizi esposti su Internet dell'istituto; il SOC controlla i report e applica misure di sicurezza aggiuntive oppure contatta direttamente (o tramite apertura di ticket al CERT) il referente del servizio impattato;

14.5.1. SOC – Log Management e Correlazione

Il servizio INAIL di Log Management & Correlazione (LM & CO) si compone di una piattaforma di sicurezza, composta da ESM Trellix in prem e Sentinel in cloud, per:

- collezionare, aggregare, conservare, ricercare ed analizzare centralmente i log provenienti da tutti i sistemi, database, applicazioni, apparati e dispositivi dell'Istituto;
- correlare, mettendo in relazione gli eventi di diversa origine raccolti centralmente allo scopo di evidenziare e segnalare sequenze di attività potenzialmente ostili e/o non autorizzate.

La piattaforma stessa si articola sulla raccolta delle seguenti due macro-tipologie di eventi:

Privacy

Al fine di garantire principalmente la conformità alle misure obbligatorie previste dal Provvedimento del Garante Privacy sugli Amministratori di Sistema;

Rete

Per aderire alle regole previste dall'SPC per la conservazione dei log dei firewall, degli altri apparati di sicurezza e di rete.

14.5.2. SOC – Vulnerability Assessment

Il servizio di VA consente il monitoraggio periodico dei livelli di rischio, delle minacce e delle vulnerabilità, permettendo l'adeguamento, in tempi ragionevoli, del livello di sicurezza dei sistemi informatici e telematici dell'Istituto in conformità alle normative vigenti, agli standard ed alle best practices.

14.5.3. SOC – Network Forensics

La piattaforma di Network Forensics è stata concepita per mettere a disposizione degli operatori gli strumenti necessari per acquisire ed analizzare il traffico di rete entrante ed uscente dai link Internet.

14.6. Web Application Firewall (WAF)

Il WAF, servizio per il controllo, filtraggio, ed eventuale blocco del traffico HTTP(S), si basa sulla piattaforma Imperva SecureSphere.

14.7. System Center Configuration Management

Per la gestione delle PdL si utilizza una soluzione di System Center Configuration Manager Sp1 R2 (SCCM). L'architettura SCCM è composta da un Server centrale o Central Site (inailsrvscm01), su cui risiedono il Database e le componenti core del sistema ed un server con funzionalità di distribution point che rende disponibili alle PdL i contenuti supportati da SCCM (Software, Patch, Applicazioni virtuali e sistemi operativi). Attualmente SCCM ha funzionalità di:

- Hardware, Software and Asset Inventory – un agent installato sulle PdL invia periodicamente al Central Site informazioni sulla configurazione hardware e software della PdL. Le informazioni sono archiviate nel Database centralizzato di SCCM, per l’elaborazione o la generazione di report.
- Software Distribution – è possibile installare il software e gli aggiornamenti, creare politiche per diversi profili di client mediante l’identificazione di parametri relativi alla configurazione hardware o software.
- Patch Management – SCCM si integra con WSUS, rileva il livello di patch presenti sulle PdL e permette di controllare lo stato della distribuzione e lo stato delle PdL e, se necessario, notifica la necessità di provvedere alla distribuzione delle ultime patch rilasciate.
- Virtual Application Distribution – SCCM integra gli strumenti per supportare l’utilizzo da parte delle PdL delle Applicazioni virtuali. Al momento, l’applicazione SIPERT è stata pacchettizzata e distribuita con successo su alcuni client in un ambiente di test.
- Operating System Deployment – SCCM installa ed aggiorna i sistemi operativi delle PdL. Sono possibili diverse modalità di installazione, per esempio mediante una periferica di Boot su PdL con o senza sistema operativo, o con la software distribution di SCCM su PdL con sistema operativo già installato o effettuando il boot da rete tramite i server PXE dell’infrastruttura SCCM. In caso di migrazione ad un nuovo sistema operativo, si possono salvare e ripristinare i dati e le impostazioni degli utenti della PdL. Per la distribuzione di Windows XP è necessario creare una immagine su sistema di riferimento per catturarne l’immagine da distribuire successivamente, per Windows Vista e Windows7 si può utilizzare l’immagine in Formato WIM fornita dal produttore sul DVD di installazione e personalizzabile sfruttando i tool integrati in SCCM.

14.8. Security Patch Management

L’infrastruttura di security patch management basata su Microsoft Windows Server Update Services service pack 1 (WSUS) permette la gestione degli aggiornamenti critici dei sistemi operativi e delle principali applicazioni Microsoft per le PdL ed i Server distribuiti sul territorio.

L’architettura WSUS è costituita da:

- un server principale con il ruolo di “master server”, di interfaccia tra l’infrastruttura interna dell’INAIL ed il portale del servizio di Windows Update di Microsoft, che gestisce gli aggiornamenti;
- da un sistema in configurazione cluster in “load balancing” di 4 server WSUS che opera come replica del server principale ed ha funzioni di server di riferimento per l’aggiornamento delle PdL;
- Un database server Microsoft SQL 2005 centralizzato condiviso da tutti i nodi del cluster del sistema di replica. Il database server è configurato in modalità failover cluster a due nodi. Il cluster gestisce anche il servizio di file server necessario per fornire un supporto di memorizzazione (storage) dei pacchetti di update utilizzati da WSUS.

- La configurazione in load balancing del sistema di replica garantisce la disponibilità del servizio di Patch Management e minimizza l'occorrenza di soluzioni di continuità nell'erogazione del servizio, anche nel caso in cui sia necessario inserire e/o rimuovere risorse server dal cluster.
- Dalla console di gestione di WSUS è possibile selezionare gli update da scaricare e rendere disponibili per le PdL e i server della propria infrastruttura, effettuare il monitoraggio dello stato di distribuzione degli aggiornamenti sui sistemi gestiti da WSUS e generare una reportistica dettagliata sulla distribuzione delle singole patch, nonché sullo stato di aggiornamento delle singole PdL e server gestite da WSUS.

14.9. Sicurezza delle connessioni

SICUREZZA PERIMETRALE

Sono stati individuati gli obiettivi di sicurezza (politiche di sicurezza) al fine di proteggere mediante servizi di firewalling tutto il traffico da Internet/Infranet e da altre tipologie di connessioni esterne, quali accessi in commutata, agenzie, ispettori, 'mobile user', connessioni remote in ADSL, telelavoratori. Quindi tale traffico è controllato effettuando filtri dei pacchetti in transito e facendo passare solo quelli che rispondono ai requisiti definiti dalle politiche di sicurezza.

La corretta configurazione e gestione degli apparati in questione e la corretta implementazione dei diritti di privilegio sono stati sempre effettuati in maniera tale da prevedere un controllo continuo delle misure di sicurezza e l'evoluzione del sistema dell'Istituto.

A tal fine viene anche effettuato un monitoraggio costituito dalla raccolta dei file di "log" degli apparati coinvolti, in cui vengono scritte tutte le principali operazioni svolte dagli utenti attraverso applicazioni. Tali file vengono attualmente memorizzati in maniera da avere uno storico di quanto catturato per una eventuale successiva analisi.

Vista l'importanza di tali apparati (firewall) è stato realizzato anche il controllo dell'accesso agli stessi mediante un protocollo di cifratura sicuro (SSH).

VPN

Il meccanismo attualmente utilizzato per garantire la sicurezza delle connessioni e del conseguente traffico di rete è costituito dall'implementazione di una o più VPN (Virtual private network). Si tratta di un meccanismo che consente la cifratura del traffico tra due punti di una rete in modo trasparente rispetto all'utente.

Requisito fondamentale per realizzare una VPN è che le due entità coinvolte siano tra loro compatibili nello svolgimento della suddetta funzione. Una volta predisposta una VPN tra due punti della rete tutti i pacchetti di informazione tra questi punti vengono cifrati/decifrati dai due dispositivi in questione automaticamente garantendo la riservatezza delle informazioni trasmesse, il riconoscimento reciproco dei due nodi e l'integrità delle informazioni trasportate.

L'architettura di connessione per garantire adeguatamente la sicurezza è integrata con componenti in grado di realizzare VPN dal PC (tipicamente di mobile user, di utenti aventi connessioni remote in ADSL e di postazioni dislocate in altre Amministrazioni) fino all'interno della Intranet INAIL.

A tale scopo vengono utilizzati apparati specializzati a tale funzione e server di autenticazione.

14.10.CERT

Per garantire che il personale ed i partner siano a conoscenza delle procedure di rilevazione e notifica degli incidenti di sicurezza, nonché delle vulnerabilità dei sistemi, delle minacce alla sicurezza IT e dei malfunzionamenti software, INAIL ha implementato alcuni processi volti alla gestione delle sopraindicate occorrenze. A tale proposito, è stata costituita un'apposita unità denominata CERT-INAIL cui è demandato il coordinamento nella gestione degli incidenti di tipo informatico e l'avvio di un'accurata campagna di sensibilizzazione degli utenti finali ad un corretto utilizzo delle infrastrutture, hardware e software, dell'Istituto fungendo da punto di riferimento all'interno del panorama di sicurezza IT di INAIL.

L'obiettivo è fornire all'Istituto servizi allineati con le best practices di sicurezza e con quanto definito dal CSIRT/ACN in materia di gestione della sicurezza delle informazioni. Nei compiti del CERT rientrano le attività di:

- Early Warning, per la divulgazione di informazioni sulle principali minacce di sicurezza informatica, acquisiti attraverso canali di sicurezza IT autorevoli, corredate da raccomandazioni per limitare possibili esposizioni;
- Incident Management, per la rilevazione e il contrasto in tempo reale di incidenti di sicurezza o in genere di situazione di emergenza di tipo informatico;
- Vulnerability Assessment, per l'analisi periodica e la notifica delle nuove vulnerabilità hardware e software e l'identificazione delle contromisure da adottare;
- Security Topic Disclosure, per la divulgazione delle principali e migliori pratiche di sicurezza per un utilizzo sicuro e corretto delle infrastrutture IT di INAIL.

Sono stati definiti ed approvati i processi per le diverse attività e si è provveduto all'adozione di SERVICE NOW

EARLY WARNING

Tra gli obiettivi dell'Early Warning, vi è la pubblicazione di advisories che descrivono:

- un nuovo attacco di tipo intrusivo,
- una nuova vulnerabilità,
- un nuovo codice maligno,
- attività di educational/prevenzione rivolta all'utenza, corredate da raccomandazioni, volte alla comprensione dei problemi risultanti, e da consigli sugli atteggiamenti da adottare al fine di limitare possibili esposizioni.

Il processo è articolato come un processo continuo, al fine di assicurare un costante aggiornamento sulle nuove minacce di sicurezza presenti sulla rete ed è costituito da tre fasi:

- **Collezionamento:** in questa fase vi è la rilevazione e l'analisi delle notifiche di sicurezza IT rilasciate dalle più autorevoli fonti di settore più recenti;
- **Analisi:** in questa fase si procede con la valutazione e classificazione dell'impatto che la potenziale minaccia potrebbe avere sulle risorse IT di INAIL sulla base di parametri ad esse correlati. Per la classificazione degli impatti si è utilizzato un modello di classificazione a tre livelli (Alto, Medio e Basso);
- **Distribuzione:** Una volta identificato e classificato l'impatto potenziale delle minacce, le contromisure volte a mitigarle sono pubblicate su un sito web accessibile da Intranet, o sono comunicate mediante l'invio di email.

INCIDENT MANAGEMENT

Il processo di Incident Management è strutturato in sottoprocessi:

- **Identificazione:** rappresenta la fase in cui viene individuato e circoscritto l'attacco o la presunta violazione delle politiche di sicurezza;
- **Classificazione:** in questa fase si stabilisce l'impatto del potenziale incidente, in base alla tipologia e/o categoria di attacco, per esempio DoS, Malicious Code, Misuse, alla valutazione delle criticità dei sistemi target coinvolti;
- **Notifica:** in questa fase si notifica lo stato di allarme e si attiva il processo vero e proprio di Incident Response;
- **Response:** costituisce la fase fondamentale del processo. In relazione alla tipologia di incidente, il CERT-INAIL, con la collaborazione del responsabile della Sicurezza e dei responsabili delle Aree coinvolte, definisce le strategie di contenimento più appropriate da attivare. In questa fase sono conservate le evidenze documentali dell'avvenuta violazione (digital evidence);
- **Recovery:** in questa fase sono adottate le procedure organizzative e tecniche per il ripristino della piena funzionalità dei sistemi compromessi e per riportare i sistemi al livello di sicurezza iniziale. Tutte le attività di ripristino devono essere condotte senza compromettere l'integrità di eventuali prove (digital evidence), per poter perseguire legalmente le violazioni;
- **Post-mortem:** rappresenta la fase di analisi della dinamica dell'incidente, per stabilirne le cause, le modalità e le conseguenze, al fine di migliorare il processo di gestione degli incidenti, con l'identificazione delle eventuali lacune od errori, la definizione delle strategie di comunicazione nelle diverse fasi del processo e delle eventuali azioni legali da intraprendere.

Rilevazione e Classificazione degli incidenti

All'interno della struttura organizzativa di INAIL, il compito di rilevare le eventuali anomalie, violazioni e/o incidenti di sicurezza IT è affidato:

- al Security Operation Center (SOC), , mediante l'analisi degli eventi ed allarmi provenienti dai dispositivi di sicurezza monitorati;

- alle Strutture operative delle Aree Interne alla DCOD , preposte alla gestione dei sistemi e delle infrastrutture dell'Istituto;
- ai Referenti di Sede, a livello provinciale, con i canali di comunicazione resi disponibile (per esempio e- mail, help desk, piattaforma di trouble ticket);
- agli utenti interni autorizzati dall'Istituto, con i canali di comunicazione resi disponibile (per esempio e- mail, help desk, piattaforma di trouble ticket);
- al CERT durante l'attività di monitoraggio delle infrastrutture e dei sistemi.

L'evidenza di un incidente o evento anomalo di sicurezza può essere rilevata in modo automatizzato, dal sistema di allarmi degli strumenti di rilevazione adottati (SIM) o in modo non automatizzato da fonti esterne all'ambito di competenza dei sistemi di monitoraggio, per esempio segnalazioni di malfunzionamenti e/o anomalie comunicate in forma verbale o scritta.

A fronte della rilevazione di una anomalia o di un incidente di sicurezza, il CERT-INAIL prende in carico la segnalazione, classifica l'evento e determina il livello di allarme, per stabilire le priorità di intervento e le modalità di escalation.

Per la determinazione del livello di allarme si è scelto un approccio di tipo qualitativo, in funzione della categoria o livello di gravità dell'attacco, della criticità delle risorse IT coinvolte, sorgente dell'attacco e priorità di attacco. In base al livello di allarme è possibile stabilire le modalità di intervento adottate dal CERT-INAIL e dalle strutture interne all'Istituto coinvolte nei processi di risposta e contenimento e le priorità di intervento. Si è adottato un modello di classificazione a 3 livelli (Alto, Medio e Basso), in base all'impatto e alla probabilità di occorrenza di compromissione dei sistemi, alla criticità delle risorse coinvolte o in generale dell'operatività dell'Istituto.

Notifica e Contenimento degli incidenti

Il CERT-INAIL ha il compito di aprire una segnalazione verso le funzioni interne all'INAIL competenti, per il coordinamento delle attività di risposta, recovery ed eventualmente delle attività di indagine Post Mortem. In base al livello di allarme si determina la modalità di escalation per la gestione dell'incidente.

Sono possibili tre diverse modalità di escalation:

- First Level Technical Escalation (1TE), che prevede la gestione dell'incidente da parte dei responsabili dell'esercizio e della manutenzione dei sistemi e delle infrastrutture IT;
- Second Level Technical Escalation (2TE), che prevede l'escalation nei confronti del responsabile della Sicurezza o di un suo delegato,.
- Management Escalation (ME), che comporta l'escalation nei confronti della Direzione dei singoli uffici coinvolti nel caso di un incidente in corso o già accaduto con conseguenze particolarmente gravi sull'operatività dei sistemi e delle infrastrutture IT. In questo caso, se necessario, saranno coinvolte anche altre Strutture dell'istituto, esterne a DCOD per esempio Relazioni Esterne, Ufficio Legale.

La notificazione dell'incidente alle funzioni interne all'INAIL competenti deve essere effettuata sempre in forma scritta, fatto salvo le circostanze per le quali la gravità è tale (nella fattispecie Alto), in cui è consentita la comunicazione verbale per ottimizzare i tempi di intervento e poter attivare la fase di Recovery. In tal caso, alla comunicazione verbale deve seguire una comunicazione scritta.

L'obiettivo principale di questa fase è contenere il più velocemente possibile gli incidenti per minimizzare l'impatto su sistemi e servizi. Il CERT-INAIL ha il compito di individuare la migliore strategia di contenimento, di suggerire le opportune azioni da intraprendere, anche in riferimento al livello di criticità, alle aree operative interne alla DCSIT coinvolte nell'attività di contenimento dell'incidente.

Ripristino del servizio

In questa fase, identificata nel processo di Incident Management dallo stadio Response, si adottano le procedure tecniche ed organizzative volte a riportare i target degli attacchi ai livelli originari di funzionalità e sicurezza. Questa fase non è obbligatoria nel processo di Incident Management, ma è prevista nel caso di necessità effettiva di attuare o meno azioni di ripristino a fronte di un incidente di sicurezza.

L'individuazione e la condivisione delle azioni di recovery è uno dei compiti del CERT-INAIL che deve suggerire le azioni da prevedere in riferimento alla tipologia di attacco alle aree operative interne alla DCOD coinvolte nella gestione dell'incidente.

Indagini retroattive

A fronte dell'occorrenza di un incidente e su esplicita richiesta del Responsabile della Sicurezza dell'UQS, il CERT-INAIL ha il compito di effettuare l'analisi retroattiva (identificata nel processo di Incident Management dallo stadio Post Mortem). Tale analisi comporta l'esame delle informazioni fornite dalle parti coinvolte nell'incidente, la scomposizione del processo di gestione dell'incidente in tutte le sue fasi, rivisitandone ogni dettaglio per identificare eventuali migliorie da apportare al processo, eventuali modifiche nelle politiche, per ottimizzare le comunicazioni e le procedure da affinare. L'analisi ha l'obiettivo di:

- ricostruire la dinamica degli eventi;
- determinare la capacità dello staff coinvolto a gestire gli eventi, rilevando eventuali carenze nella formazione o errori umani o inadeguatezza delle procedure operative;
- valutare se le azioni di contrasto o contenimento hanno determinato un rallentamento nelle operazioni di recovery dei sistemi e se occorrono delle migliorie;
- identificare le contromisure da implementare per minimizzare la probabilità di occorrenza dell'incidente stesso;
- documentare formalmente le valutazioni effettuate, producendo una relazione dettagliata dell'incidente, in cui deve essere riportata la cronologia esatta degli eventi, eventualmente supportata dalle informazioni di timestamp dei dati di log dei sistemi per esempio per la conferma della validità delle evidenze documentali raccolte, per stime monetarie per ricorsi assicurativi.

Al fine di poter supportare eventuali azioni legali da intraprendere a fronte dell'occorrenza di incidenti e/o eventi di sicurezza che abbiano comportato perdite significative anche temporanee dei requisiti di Riservatezza, Integrità e Disponibilità di risorse critiche, devono essere raccolte le evidenze documentali (Digital Evidence) e deve essere possibile dimostrare la conformità agli standard dei sistemi informativi che hanno prodotto tali evidenze. Il CERT-INAIL deve identificare le informazioni importanti e rilevanti relative all'incidente da raccogliere e conservare, fornendo indicazioni sui metodi e sulle modalità per la raccolta delle evidenze per le varie categorie di attacco e sulle modalità di conservazione e di trasferimento dalla loro origine alle aree di custodia (Chain of Custody).

VULNERABILITY MANAGEMENT

Per garantire una gestione efficace delle più recenti vulnerabilità hardware o software, il processo è idealmente articolato come un processo continuo a sei stadi:

- **Asset Inventory:** in questa fase si effettua il censimento delle risorse IT aziendali, necessarie per l'operatività e la mission dell'Istituto. Questa attività richiede il coinvolgimento dei responsabili delle aree operative e organizzative dell'Istituto.
- **Collection:** in questa fase si individuano le vulnerabilità più recenti e le contromisure pubblicate dalle più autorevoli fonti di settore, per esempio mediante l'iscrizione a newsgroup di fonti affidabili di analisi e reporting, l'analisi dei siti web o l'adozione di altri strumenti di analisi delle vulnerabilità. Sono state selezionate come fonti di rilevamento Organizzazioni governative americane per la sicurezza in Internet e i produttori e/o costruttori delle infrastrutture software e hardware utilizzati nell'ambiente di produzione di INAIL.
- **Analysis:** In questa fase si effettua l'analisi della vulnerabilità software per valutare e classificare il loro impatto potenziale sulle risorse IT di INAIL sulla base di parametri ad esse correlati. Inoltre, si controllano attentamente le contromisure per l'eliminazione delle vulnerabilità e gli aggiornamenti software proposte per stabilire se pertinenti per l'infrastruttura IT dell'Istituto. Nell'analisi, si determinano la priorità e la classificazione delle vulnerabilità per stabilire la rapidità del processo di aggiornamento e l'impatto potenziale sui sistemi e sui servizi nell'ambiente di esercizio. Si è adottato un modello di valutazione delle priorità strutturato su 3 livelli (Alto, Medio e Basso) e dell'impatto su due livelli (Rosso e Verde).
- **Planning:** In questa fase si pianificano le modalità di aggiornamento software, in base al livello di classificazione delle vulnerabilità e si valuta la possibilità di aggiornare direttamente il software in ambiente di produzione o se è necessario testarne prima la funzionalità e stabilità nell'ambiente di test. Alla fine di questa fase viene prodotto un report, inviato al Responsabile della Sicurezza dell'UQS che in caso di approvazione provvede al rilascio ai responsabili dei settori IT di INAIL coinvolti.

- **Deployment:** A seguito dell'analisi effettuata sull'impatto che le minacce potrebbero avere, sono pubblicate le contromisure volte a mitigarle.
- **Verifica:** In questa ultima fase si verifica, dopo la bonifica, l'effettiva rimozione della vulnerabilità e che non siano state compromesse le funzionalità e le prestazioni dei dispositivi di rete, degli applicativi e dei servizi erogati, mediante la conduzione di audit preventivamente definiti e concordati con i responsabili dei settori IT di INAIL coinvolti.

SECURITY TOPIC DISCLOSURE

Il servizio di Security Topic Disclosure ha l'obiettivo di provvedere alla pubblicazione sul portale interno del CERT di INAIL di linee guida su tematiche di sicurezza relative alla messa in sicurezza di apparati di rete, di server Web o Database o alla corretta implementazione delle politiche di sicurezza e antivirus. È possibile consultare sul portale le linee guida in modalità on-line o effettuare il download della documentazione.

14.11. Firma Digitale Centralizzata

L'Inail, per semplificare l'utilizzo e per risolvere la problematica delle firme massive, ha acquisito un sistema di Firma Elettronica basato su una soluzione SAS Infocert che espone i servizi di:

- Firma qualificata;
- Firma automatica;
- Sigillo Elettronico - ESeal.

I benefici risultanti, oltre la ovvia riduzione dei costi attribuibili all'impiego della carta, risiedono anche nell'elevato standard di sicurezza adottato dalla soluzione il quale, mediante accorgimenti sia a livello hardware che software, soddisfa i più stringenti standard internazionali di sicurezza.

I sistemi di firma digitale sono utilizzabili dalle procedure applicative tramite l'utilizzo di due tipologie di componenti:

- **Websigner:** componente di Front-End che consente agli utenti di digitare le informazioni di sicurezza necessarie all'utilizzo del certificato di firma remota – UserId, Pin, OTP;

14.12. Privacy e sicurezza delle informazioni

L'Istituto ha ritenuto importante realizzare questo Canale Tematico di Orientamento e accesso al mondo Privacy e della Sicurezza delle Informazioni, che permetta di mettere a disposizione degli utenti ciò di cui hanno bisogno, sia per le necessità primarie del loro lavoro e sia per le funzioni di supporto alle attività giornaliere, risultando quindi un asset di potenziamento per il business primario. Permette una facilitazione delle attività principali degli utenti coinvolti direttamente nella gestione della sicurezza, e un coinvolgimento maggiore e più immediato di tutti gli altri utenti, facilitando così una buona attuazione delle

politiche per la sicurezza ed una sensibilizzazione a tutte le problematiche che per vari aspetti possono avere impatti su di essa.

Nel Portale gli utenti, profilati secondo i diversi ruoli, possono accedere a documentazione, riservata o meno, suddivisa per le varie aree tematiche, ossia Servizi erogati, Aree della norma 27001 e la normativa sulla Privacy. La documentazione contiene Policy, procedure, Linee Guida dell'Istituto, normative interne ed esterne.

Le necessità che portano a tale intervento progettuale sono:

- Riunire in un unico punto tutte le informazioni inerenti all'argomento sicurezza.
- Facilitare la gestione di tutta la documentazione, da parte di chi se ne occupa direttamente attraverso:
 - strumenti di collaborazione;
 - gestione della versione dei documenti;
 - uso efficace del Sistema di pubblicazione in modalità web da parte di tutti gli attori coinvolti utilizzando funzioni di ricerca su aree tematiche (servizi contrattuali, ambiti contrattuali, categorie documentali) e su parole chiave.
- Semplificare la fruizione da parte di tutti gli utenti delle informazioni disponibili e necessarie per una corretta applicazione delle policy di sicurezza dell'Istituto:
 - garantire maggior efficacia nella comunicazione dei contenuti informativi gestiti, in termini di completezza, loro aggiornamento e soprattutto di fruibilità delle informazioni da parte dei diversi attori coinvolti;
 - consultazione on-line mirata di leggi, norme e linee guida interne;
 - accessi diretti agli strumenti utili;
 - supporto alla soluzione delle problematiche più importanti e comuni (ad es. segnalazione virus o incidente di sicurezza).

Per lo sviluppo del Portale, si è scelto di utilizzare Microsoft SharePoint Services 3.0. Le aree tematiche del portale sono divise in sezioni:

- Nella sezione Sicurezza si archiviano tutti i documenti della Sicurezza - Politiche, Linee Guida, Regole Tecniche - che tutti gli utenti dell'Istituto devono conoscere ed applicare nella conduzione delle attività giornaliere per garantire il livello di protezione atteso dall'Istituto e raggiungere gli obiettivi di sicurezza prefissati.

In questa sezione, i documenti sono organizzati secondo i domini individuati dalla norma ISO/IEC 27001:2022

- Nella sezione Privacy si archiviano tutti i documenti relativi al D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", Codice che recepisce i principi comunitari basati sulla tutela dei diritti e delle libertà delle persone interessate al trattamento, con adozione di adeguate misure tecniche ed organizzative atte a garantire la sicurezza dei dati personali e impedire, in tal modo,

qualsiasi trattamento non autorizzato. L'Istituto, sulla base delle prescrizioni del Codice e dei provvedimenti del Garante, ha adottato una serie di disposizioni, obbligatorie e non, riportate nei documenti consultabili attraverso le varie voci di menu della sezione.

Operativamente il cuore dello standard è l'allegato A (Annex A "Control objectives and controls") che contiene tutti i controlli a cui, l'organizzazione che intende applicare la norma, deve attenersi.

L'organizzazione deve motivare quali di questi controlli non sono applicabili all'interno del suo sistema di sicurezza (ISMS- Information Security Management System), per esempio un'organizzazione che non attua al suo interno 'commercio elettronico' può dichiarare non applicabili i relativi controlli.

Privacy

Il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n.196), a decorrere dal 1° gennaio 2004, disciplina in maniera organica l'intera materia relativa alla tutela dei dati personali.

Il testo rappresenta il primo modello di codificazione organica della privacy in Europa e stabilisce il diritto soggettivo, per chiunque, alla protezione dei dati personali.

I soggetti pubblici, che effettuano trattamento dei dati, hanno l'obbligo di adottare misure di garanzia volte a tutelare la riservatezza delle informazioni di natura personale e sensibile in possesso degli stessi per l'espletamento dell'attività istituzionale.

Pertanto, l'Istituto, quale soggetto pubblico che tratta dati personali, sensibili e giudiziari, ha provveduto a porre in essere gli adempimenti di seguito indicati:

Adozione delle misure di sicurezza atte a configurare elevati livelli di protezione;

Adozione del "Documento Programmatico sulla Sicurezza";

Predisposizione del "Regolamento attuativo del Decreto legislativo 30 giugno 2003 n.196"; Adozione del nuovo modello organizzativo sulla privacy.

Politiche, Normative e Standard

L'Istituto, avendo l'obiettivo di seguire tutte le "raccomandazioni" legate alla sicurezza e alla privacy, oltre agli standard da attuare (Decreto legislativo 30 giugno 2003, n.196, ISO/IEC 27001:2013), si è fornito di una serie di normative interne, atte a chiarire, informare e divulgare regole, policy e linee guida. In questa area oltre a tutti i documenti relativi alla legislazione nazionale ed europea (normative Generali), vengono riportate le circolari interne dell'Istituto ed ogni altro documento che ufficializzi modalità di lavoro o di comportamento (Normative Interne, Politiche, Linee Guida).

Documenti per la Sicurezza

Tutti i documenti relativi alla sicurezza non riservati distribuiti dall'Istituto, verranno riportati in quest'area, dove potranno essere consultati o scaricati dai dipendenti.

L'area sarà aggiornata inserendo ogni nuovo documento o versione che faccia riferimento alla sicurezza interna di INAIL.

Classificazione dei documenti

Il Portale dovrà consentire di classificare i documenti in Riservati e Pubblici e di definire a quale area essi appartengono. Quindi sia in fase di definizione iniziale che in fase di manutenzione del portale gli utenti, all'atto dell'inserimento di un documento in una determinata area, dovranno poter definire se il contenuto di tale documento è Pubblico o Riservato.

Storicizzazione dei documenti

Il Portale dovrà conservare tutte le versioni dei documenti in esso contenuti.

Requisiti di Interoperabilità

Il Portale dovrà integrarsi con il portale intranet di INAIL non richiedendo ulteriore autenticazione. Si farà invece carico di gestire la profilazione degli stessi.

Requisiti di Sicurezza

Il software prodotto dovrà essere conforme a quanto indicato nel documento "INAIL-DCSIT-Linee guida per la progettazione e lo sviluppo di applicazioni WEB sicure_v1 0_20090508.doc.

Audit interni

Periodicamente le applicazioni sono sottoposte ad audit di sicurezza, per valutarne la conformità alla norma ISO 27001 e l'aderenza alle Policy dell'Istituto.

15. PROGETTAZIONE E SVILUPPO DELLE APPLICAZIONI

Per la digitalizzazione e l'automazione di processi complessi occorre ricorrere ad attività di progettazione e sviluppo di software custom che devono seguire specifiche indicazioni di metodo, a partire dalla "Linea guida per la realizzazione dei siti web e i servizi digitali della PA" (https://www.agid.gov.it/sites/default/files/repository_files/design-linee-guida-docs.pdf) emanata dall'AgID (versione 7/22).

Per la progettazione delle applicazioni esiste un *design system* di riferimento in cui sono differenziate le risorse per servizi internet e intranet. Per designers e sviluppatori, che devono essere stati accreditati nei sistemi Dcod, sono disponibili risorse documentali e componenti riutilizzabili per la progettazione delle interfacce in coerenza con le indicazioni del design system.

Tutte le interfacce utente sono standardizzate in *template* e consistono di:

- **Header:** logo, nome utente e profilo, tasto Esci, breadcrumb interna all'applicazione
- **Body:** menu principale e secondari, *form* per la gestione dei dati applicativi
- **Footer:** link di accesso rapido, loghi delle iniziative di finanziamento

L'applicazione può procedere solo nella parte *body* del template, non è consentito modificare in alcun modo il *template* standard. Tutti i servizi digitali Inail devono essere integrati nel design system, nel sistema di autenticazione e profilazione e in quelli di tracciatura, nonché resi disponibili attraverso i menu del portale.

I servizi applicativi devono essere progettati secondo il paradigma modulo / componente. Sono disponibili *template* per la realizzazione rapida di applicazioni Java.

Per le attività di progettazione e realizzazione dei servizi è necessario consultare il processo omonimo e relazionarsi con il team di supporto alla progettazione, Dwork, che contribuisce al mantenimento e svolge attività di *advisoring* e *adoption* delle risorse disponibili.

Le applicazioni possono essere composte da più moduli applicativi, per ognuno dei quali esiste una sola componente applicativa di *frontend*, e sono autoconsistenti. È disponibile un sistema centralizzato per la gestione dei differenti ruoli applicativi (vedi cap. Sicurezza).

Le linee guida architetturali e di sviluppo consentono di indirizzare le attività realizzative verso la soluzione applicativa più idonea ed il team di sviluppo è tenuto ad osservare le indicazioni ricevute. È raccomandato il riuso dei moduli e dei componenti applicativi già disponibili. Non è favorito lo sviluppo di *app* per dispositivi *mobile* se non nei casi in cui l'automazione richiesta non preveda l'utilizzo delle caratteristiche specifiche di smartphone e tablet, come la fotocamera, la geolocalizzazione, il salvataggio dei dati *offline* e simili.

Le tecnologie e le risorse disponibili coprono tutte le possibili necessità realizzative. Le proposte di innovazione seguono un rigido processo di selezione e *adoption*. I team di sviluppo devono essere composti da personale con competenze avanzate sui temi della sicurezza applicativa (es. Owaps) e dell'accessibilità

(norme tecniche nazionali e WCAG 2.x, uso di Lighthouse) e sono tenuti a sviluppare secondo le *best practices* conosciute nonché a ridurre i tempi di certificazione del software.

Le API devono essere nominate, catalogate, descritte e mantenute secondo standard Inail vigenti.

Tecnologie utilizzate: webkit HTML/Css/js, template Springboot, Java 11, Angular, Jsp, API rest, db relazionali e non relazionali, DevOps, risorse *cloud*

15.1. Servizi internet

Il portale risponde all'indirizzo www.inail.it, attraverso contesti specifici (/portale, /intracs, /API, /sol-, ecc.) vengono raggiunte sia le pagine informative che le applicazioni e i backend che sfruttano canali sicuri e strong authentication. Alcune applicazioni sono attestate su domini di terzo livello di inail.it, comportamento fuori standard in via di abbandono. Le risorse statiche dei componenti sono disponibili sulla Cdn inailcloud.it e vengono richiamate attraverso il sistema di integrazione *header/footer*. E' possibile utilizzare la piattaforma di integrazione PLAP e nPLAP (vedi cap. Il portale pubblico).

La progettazione delle interfacce delle applicazioni web deve procedere attraverso le componenti presenti nel webkit di riferimento e secondo i principi di buona progettazione delle linee guida nazionali e interne, con il supporto della Dwork. Il team Dwork può essere consultato anche nelle fasi di certificazione e post rilascio in esercizio del software.

Il portale pubblico non mette a disposizione informazioni o servizi riservati, che vengono invece messi a disposizione dopo autenticazione nella apposita area di post login (PLAP -> MyInail) e nelle applicazioni. Le applicazioni possono integrare elementi informativi e multimediali del portale pubblico attraverso link. Il manuale dell'applicazione va pubblicato nella sezione specifica del portale pubblico.

È necessario integrare le applicazioni nei sistemi di monitoraggio dell'esperienza utente (analytics) nonché di assistenza analogica (contact center) e digitale (*chatbot*). Il chatbot offre assistenza in linguaggio naturale e indirizza l'utente al canale di assistenza più idoneo, occorre quindi dedicare risorse all'addestramento del dominio di conoscenza e all'aggiornamento della matrice di correlazione utente-canale-applicativo.

A seconda delle esigenze sono da valutare le integrazioni nel sistema centralizzato di notifica più idoneo, nonché dei canali e delle politiche di consegne più indicati (vedi cap. Strumenti di notifica applicativa).

15.2. Servizi internet con funzionalità intranet

Alcune applicazioni possono dover offrire funzionalità sia ad utenti interni Inail che esterni, contemplando contemporaneamente profilazione sia internet che intranet. Questo tipo di soluzione presuppone una più attenta attività di progettazione delle interfacce e della sicurezza in modo che le differenti anime dell'applicativo non producano problemi nell'esperienza utente o incidenti di sicurezza. In questo caso la progettazione delle interfacce deve seguire uno dei due modelli:

- Integrare le funzionalità intranet nel contesto internet;

- Realizzare moduli applicativi specifici per internet e intranet.

15.3. I servizi intranet

La scrivania digitale attraverso il *widget* Applicativi offre l'accesso alle applicazioni intranet custom e package per lo svolgimento delle attività lavorative dei dipendenti presso le varie sedi e strutture.

Come per i servizi internet, per lo sviluppo di applicazioni intranet sono messe a disposizione risorse, linee guida e team di supporto cui fare ricorso, secondo la stessa impostazione. È necessario valutare con i team specifici la possibilità di integrare nei widget della Scrivania dati e informazioni specifiche, in modo di aggiungere all'esperienza utente già nota altri elementi di lavoro.

È necessario integrare le applicazioni nei sistemi di monitoraggio dell'esperienza utente (anche APM MS Application Insight) nonché di assistenza analogica.

A seconda delle esigenze sono da valutare le integrazioni nel sistema centralizzato di notifica più idoneo, nonché dei canali e delle politiche di consegne più indicati (vedi cap. Strumenti di notifica applicativa).