

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP CONFIDENTIAL

**APPENDICE 5 AL CAPITOLATO TECNICO
CONTESTO TECNOLOGICO**

**GARA A PROCEDURA APERTA IN DUE LOTTI PER L'ACQUISIZIONE DI SERVIZI
PROFESSIONALI A SUPPORTO DELLA GOVERNANCE E BUSINESS OPERATIONS DI
INAIL - ID 2208**



SOMMARIO

Sommario

1. PREMESSA	4
2. SISTEMI.....	7
2.1. Sistemi Centrali.....	8
2.1.1. MAINFRAME	8
2.1.2. Sistemi IBM System P 795 Power	9
2.1.3. Sistemi Intel x86 e Web Farm	10
2.1.4. Ambiente CLOUD	12
2.2. Sistemi Periferici.....	12
2.3. Sistemi Centro Protesi INAIL	12
2.4. Postazioni di lavoro	13
2.5. Cooperazione Applicativa	14
2.5.1. Porta di Dominio (PDD).	14
2.6. Posta Elettronica PEL e PEC	17
2.7. Infrastruttura Active Directory.....	19
2.8. Sistema Documentale Centralizzato	20
2.9. Data Warehouse	20
3. SERVICE ORIENTED ARCHITECTURE (SOA).....	21
3.1. Architettura	21
3.2. Componenti infrastrutturali	22
4. API REST GATEWAY	26
4.1. Interfacce di esposizione	27
4.2. Standard costruzione URL servizi REST	27
4.3. Servizi Trasversali esposti dall'API-REST-GTW e JWT	28
4.4. Servizio checkSession	28
4.5. JWT 28	
4.6. JWTNames	28
5. INFRASTRUTTURE DI RETE.....	29
5.1. Architettura generale di Rete.....	29
5.2. Connettività verso Infranet	30
5.3. Reti Locali	30
5.4. Connettività verso Internet.....	31
5.5. Architettura Sedi, Direzioni Regionali e Direzione Generale	31
5.6. Architettura Sedi di tipo C.....	31
5.7. Architettura Agenzie	31
5.8. Collegamento ADSL Telelavoratori.....	31
5.9. Biometria	32
5.10. VOIP (Voice over IP).....	32

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



5.11.	RFID (Radio Frequency Identification)	32
5.12.	Wireless (Mobile e WI-FI)	32
6.	PUNTO DI ACCESSO POLISWEB.....	34
6.1.	Servizio PDA PolisWeb	34
6.1.1.	Architettura del PDA PolisWeb	34
6.1.2.	Autenticazione ed Autorizzazione	36
7.	SICUREZZA	40
7.1.	Identity Management.....	40
7.2.	Tracciatura	40
7.3.	Single Sign On INAIL	44
7.4.	Sistema unico di profilazione	48
7.5.	Servizi del Security Operations Center (SOC).....	53
7.5.1.	SOC – Log Management e Correlazione.....	55
7.5.2.	SOC – Vulnerability Assessment	55
7.5.3.	SOC – Sicurezza DB e Applicazioni	56
7.5.4.	SOC – Network Forensics	56
7.6.	Web Application Firewall (WAF)	56
7.7.	System Center Configuration Management	56
7.8.	Security Patch Management	57
7.9.	Sicurezza delle connessioni	58
7.10.	Sicurezza Applicativa	59
7.11.	CERT	63
7.12.	Firma Digitale Centralizzata.....	69
7.13.	Canale di orientamento e accesso al mondo della privacy e della sicurezza delle informazioni.....	70
8.	ARCHITETTURE APPLICATIVE	73
8.1.	Architettura a tre livelli.....	73
8.2.	Architetture Applicative per il Cloud Ibrido	74
8.2.1.	Applicazioni a Container	75
8.2.2.	Architetture a Micro e Mini-servizi	76



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 e dei datori di lavoro 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, compresa la gestione dei processi medico-legali);
- Protesi, Riabilitazione, Prime cure e Reinserimento al lavoro;
- 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 (sistemi grandi e medi) siti presso due Data Center della Direzione Centrale Organizzazione Digitale, da sistemi elaborativi siti presso le Direzioni Regionali, le Sedi Locali nonché da sistemi elaborativi siti presso il CED del Centro Protesi di Vigorso di Budrio (sistemi medi).

Il Centro Protesi ospita, in particolare, il sistema informatico del Centro di Riabilitazione Motoria (CRM) di Volterra, il CTO di Roma e il Centro Protesi di Lamezia Terme e centralizza i servizi per le proprie filiali e i Punti Cliente.

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 2003, 2008 e 2012. Server per la realizzazione della architettura aperta, che affiancano il preesistente sistema centralizzato basato essenzialmente su Mainframe IBM e sistema operativo z/OS, e RDBMS standard di mercato quali DB2, Oracle, SQL Server.

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 centrali grandi (mainframe e open) e intermedi (open) siti presso i Data Center della DCOD;
- sistemi di elaborazione medi siti presso il CED del Centro Protesi di Vigorso di Budrio;
- sistemi di elaborazione periferici medi siti presso le Direzioni Regionali, 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, test 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, prevalentemente, a dirigenti, professionisti e personale direttivo e ispettivo;
- diverse tipologie di software di base;
- patrimonio applicativo e informativo che supporta tutte le attività istituzionali e gestionali dell'Istituto.



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 di $\frac{1}{4}$, 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 (sistemi grandi e medi) siti presso il DC Primario e Secondario, da sistemi elaborativi al servizio del territorio (sistemi medi) siti presso le Direzioni Regionali, le Sedi Locali, da sistemi siti presso il Centro Protesi di Vigorso di Budrio, interconnessi mediante la rete geografica SPC (Sistema Pubblico di Connettività).

Il DC Secondario garantisce l'erogazione del servizio anche in caso di disastro del DC Primario.

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

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



2.1. Sistemi Centrali

L'ambiente centrale è costituito da un mainframe in ambiente z/OS, e sistemi open su piattaforme Linux e Windows. L'ambiente mainframe funge essenzialmente da data server, tramite il DB2, per gli ambienti collegati, inoltre il DB2 si avvale della presenza di un'Appliance che funge da acceleratore di query (IDAA). Sulle piattaforme Linux e Windows sono presenti le basi dati ORACLE e SqlServer relative dei servizi online interni esterni, del portale INAIL e del sistema di autenticazione.

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, Opendata, Autoliquidazione, Contabilità Finanziaria, Gestione Risorse Umane, Data Warehouse, Controllo di Gestione e l'Avvocatura.

2.1.1. MAINFRAME

Il sistema centrale Mainframe si è evoluto verso una configurazione di tipo Active-Active, pertanto non ha più senso distinguere il Sito Primario dal Secondario, si tratta quindi di due elaboratori attivi sui due siti più una Coupling Facility esterna agli stessi così configurati per CPU e Memoria:

1 - ELABORATORE IBM 2827 MODELLO H43 604 CON

- 4 CPU di tipo General Purpose di livello 6 che sviluppano una potenza di ca. 3404 Mips con sw capping a MIPS;
- 4 CPU di tipo zIIP (Processori Specializzati per carico DB2) che sviluppano una potenza di 5033 Mips;
- 608 GB di Memoria suddivisa tra 5 LPAR z/OS con 200 GB, 2 LPAR z/VM con 308 GB, 1 LPAR Linux on System Z nativa con 50 GB e 2 LPAR di Coupling Facility interne con 9 GB.

2- ELABORATORE IBM 2827 MODELLO H43 604 CON

- 4 CPU di tipo General Purpose di livello 6 che sviluppano una potenza di ca.3404 Mips con sw capping a 1450 MIPS;
- 3 CPU di tipo zIIP che sviluppano una potenza di 3836 MIPS (Processori Specializzati per carico DB2);
- 608 GB di Memoria suddivisa tra 6 LPAR z/OS con 208 GB, 2 LPAR z/VM con 308 GB, 1 LPAR Linux on System Z nativa con 50 GB e 2 LPAR di Coupling Facility interne con 9 GB.

3 - ELABORATORE (COUPLING FACILITY) IBM 2828 CON:

- 2 CPU con funzioni di Coupling Facility esterna con 2 LPAR (1 di Produzione e 1 di Test) con 32 GB di Memoria.

Il sistema operativo attualmente in uso è z/OS 2.1;

Il sistema Mainframe funge essenzialmente da data server.Sui sistemi z/OS gira il DB2 for z/OS, attualmente alla versione 11.1, in configurazione Data Sharing grazie all'architettura Parallel Sysplex implementata sul sistema operativo; sul DB2 for z/OS risiedono prevalentemente i dati delle Applicazioni Istituzionali e del Flussi Monetari;

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



Accanto al Mainframe, fisicamente collegata ad esso tramite fibra, con l'ultimo contratto di adeguamento è stata inserita una nuova componente Hardware con lo scopo di agevolare e rendere più performanti le attività di query nei confronti del DB2; IDAA for z/OS (IBM DB2 Analytics Accelerator) è un'appliance ad alte prestazioni usata allo scopo di accelerare l'elaborazione e migliorare in modo esponenziale i tempi di risposta delle query più pesanti, e che può essere utilizzato anche come data storage grazie alle feature di compressione estremamente performanti, attualmente è installata la versione 5.1.

INAIL sta conducendo il progetto di "Rehosting", avente l'obiettivo di trasferire su una infrastruttura basata su sistemi IBM Power 8, con database DB2 LUW, le applicazioni attualmente in esecuzione su mainframe Z/OS. Si tratta essenzialmente di trasferire banche dati DB2 e procedure scritte in COBOL o PL/SQL, mentre i front end delle applicazioni già operanti su sistemi indipendenti dal mainframe se non per la parte dati e batch.

La prima applicazione sulla nuova infrastruttura è stata rilasciata in produzione all'inizio del mese di novembre 2019. Il progetto prevede un passaggio graduale di applicazioni e dati dai DB zOS dei mainframe ai DB2 LUW secondo un approccio a rilasci incrementali. Per tutta la durata del periodo transitorio ci sarà, quindi, uno spostamento di applicazioni, e dei relativi dati, dai mainframe ai nuovi sistemi fino a quando tutte le applicazioni e tutti i dati saranno stati spostati sulla nuova infrastruttura. Solo allora i mainframe potranno essere spenti e dismessi.

2.1.2. Sistemi IBM System P 795 Power

L'infrastruttura comprende due elaboratori IBM 9119-FHB System P 795 in tecnologia Power7, uno presso il Sito Primario e uno presso il sito Secondario, con sistema operativo AIX 7.2 e Linux Distribuzione Suse SLES 11 SP2, ogni macchina è composta di 76 CPU con capacità di gestire 4 thread contemporaneamente per ogni core, 1024 Gb di memoria, e sono collegate alla SAN EMC VMAX.

Su questi sistemi sono installati, su LPAR (partizioni virtuali), i seguenti ambienti con architetture in alta affidabilità sia in business continuity che disaster recovery:

- BPM IBM (Business Process Management) dove girano le applicazioni critiche come flussi monetari, fatturazione elettronica e POM massivo (posta multicanale);
- Websphere Application Server ND in fase di dismissione con migrazione delle applicazioni verso ambienti Jboss, Weblogic con sistema operativo RedHat su X86;
- 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 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;
- IBM SPSS per attività di analisi statistica e predittiva dei fenomeni di interesse per le missioni dell'istituto;



- IBM infosphere Optim Archive per le necessità di archiviazione di dati storici che non necessitano di essere tenuti in linea, ma possono essere restorizzati selettivamente;
- IBM TWS (Tivoli Workload Scheduler) schedulatore per DB2 in ambiente distribuito).

2.1.3. Sistemi Intel x86 e Web Farm

I sistemi Intel x86 comprendono, principalmente, le seguenti tipologie di sistemi elaborativi:

- HPE Proliant DL560 Rack-mount System (Gen 8 e Gen 9) quadriprocessore e con RAM variabile tra I 256 e 512 GB
- HPE Proliant Blade BL460c System (Gen8 e Gen 9) bi processore e con RAM variabile tra I 128 e 516 GB
- HPE Proliant Blade BL 460c System (G7 - generazione obsoleta) bi processore a 64 GB RAM
- Una soluzione Iperconvergente della famiglia Nutanix

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.

Tralasciando la soluzione di iperconvergenza Nutanix, attualmente utilizzata esclusivamente per l'infrastruttura di monitoraggio, i sistemi HPE Proliant svolgono ruoli di

- DBMS Oracle o SQL Server
- Hypervisor per farm VMWARE

Si può senz'altro affermare che, buona parte buona parte dei DBMS dell'Istituto insiste su server fisici HPE Proliant e, più precisamente:

- DBMS Oracle in configurazione RAC con Dataguard su sistema Operativo Red hat Enterprise Linux;
- MS SQL server in configurazione cluster geografico Active / Passive sui due siti

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 VPLEX 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 Web Hosting prevede i seguenti elementi:

- Connettività di rete & Sistemi di Load Balancing
- Sistemi Server Wintel & Linux
- Web Server & Application Server
- 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 è gestita dall'Ufficio Reti dell'Inail. La componente di rete è alla base del servizio. Con l'obiettivo di erogare servizi in alta affidabilità si utilizzano schede ACE (netscaler) della Cisco che garantiscono un meccanismo efficiente e stabile di alta affidabilità dei servizi.

L'elemento dei sistemi è caratterizzata da una architettura a processori Intel principalmente a 64 bit. È prevista la manutenzione hardware dei sistemi ossia l'insieme delle attività inerenti l'installazione e la manutenzione degli apparati server (fisici e virtuali), la gestione degli upgrade e delle sostituzioni dei componenti difettosi in caso di malfunzionamenti.

Il monitoraggio dei sistemi e delle applicazioni – raccoglie tutte le attività di monitoraggio inerenti lo stato di funzionamento della rete e dei sistemi. Il monitoraggio continuo è rivolto alla disponibilità ed alle prestazioni dei servizi e dei sistemi. Le attività comprendono la gestione delle anomalie e la risoluzione dei problemi.

Predisposizione degli ambienti - Comprende le attività per la predisposizione delle configurazioni dell'infrastruttura applicativa e dei sistemi (Databases, Application server, file di log, parametri di monitoraggio, definizione delle autorizzazioni, etc.) sia nell'ambiente di collaudo, certificazione che in quello di produzione. Fra tali attività si inseriscono inoltre quelle atte alla definizione ed alla realizzazione degli ambienti di sviluppo, secondo i requisiti definiti dalle necessità individuate in fase progettuale, a seconda dei contesti applicativi non forniamo ambienti di sviluppo per wls,jboss e db.



2.1.4. Ambiente CLOUD

L'Istituto dispone di una infrastruttura distribuita come servizio (IaaS) ospitata su cloud pubblico Microsoft Azure Windows. Attualmente l'infrastruttura da oltre 120 server virtuali con sizing diverse per soddisfare le diverse esigenze. L'infrastruttura ospita server Windows 2008/2012, DBMS SQL Server 2008 e cloni Linux, per un totale di 2 TB di RAM, 500 core virtuali e da 30 TB di spazio disco utile, a supporto di infrastrutture dedicate ai servizi Documentale, Collaboration, Mobility, Big Data. Una VLAN dedicata collega direttamente le macchine in cloud con l'infrastruttura on-premise di INAIL per consentirne l'integrazione.

2.2. Sistemi Periferici

Ogni Sede di tipo A e B e ogni Direzione Regionale è caratterizzata da un sistema Windows 2012 R2 Server per la piattaforma CA-Unicenter R11.

2.3. Sistemi Centro Protesi INAIL

Il sistema informatico del Centro Protesi INAIL è costituito attualmente da più sistemi di elaborazione siti presso il CED del Centro Protesi di Vigorso di Budrio (BO). Esso serve circa 200 utenti distribuiti in diverse unità territoriali:

- il Centro di Riabilitazione Motoria di Volterra;
- la Filiale di Roma del Centro Protesi;
- la Filiale di Lamezia Terme;
- i Punti Cliente del Centro Protesi di Roma e Milano.

Il sistema informatico del Centro è inserito nel ben più ampio contesto infrastrutturale dell'Istituto (rete geografica SPC - Sistema Pubblico di Connettività) e prevede, tra l'altro, 2 host VmWare VSphere 4.1 in configurazione cluster, 1 sistema di elaborazione Fujitsu PRIMERGY Rx300 S5 Windows 2008 per il VCenter VmWare e la centrale di Backup Exec, 1 Storage IBM DS3950. Il 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, sistema di "produzione" del Centro di Riabilitazione Motoria di Volterra.

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

Il sistema del Centro Protesi INAIL è costituito da quattro server in produzione:

- un Web server/Report server implementato con Microsoft Windows 2003 e un IIS Server su cui risiedono le applicazioni;
- un Database Server, implementato con Microsoft Windows 2008, RDBMS Oracle v. 11.0.0;



- un Database Server, implementato con Microsoft Windows 2003 SQL Server dedicato al controllo di due magazzini semiautomatici “Bertello”.

Inoltre, è stato realizzato un ambiente di test che comprende un server web, con configurazione analoga al server di produzione, ed un Database Server, implementato con Microsoft Windows 2003 – Microsoft Windows 2008, Oracle 11.0.0.

In seguito alla ristrutturazione delle stanze dei degenti, all’interno di alcune di esse, il Centro Protesi di Vigorso è stato dotato di un “Terminale Bordo Letto” per ciascun ospite. Si tratta di un dispositivo “touch screen” resistivo che può essere utilizzato anche da chi fa uso di protesi, alimentato a corrente e munito di porta ethernet per la connessione in rete, montato su un braccio meccanico ancorato alla parete adiacente a ciascun letto.

L’Istituto ha così progettato e sviluppato per il terminale una suite di applicazioni dotata di un’interfaccia grafica “semplificata” e lineare nonché accessibile da qualsiasi utente (ai sensi della Legge “Stanca” n. 4 del 9 gennaio 2004 recante “Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici”).

Il Terminale Bordo Letto offre una suite di applicazioni di immediato utilizzo da parte dell’utente, tra cui, navigazione su internet tramite un browser semplificato ad hoc, utilizzo e visualizzazione dei canali TV e radio via ethernet, visualizzazione delle notizie del Centro, oltre a una serie di opzioni di configurazioni e multilingue coadiuvate da un help in linea.

Inoltre, il Terminale offre la possibilità ai medici di visionare la cartella clinica del paziente.

È in fase di immediato avvio anche la possibilità di effettuare chat audio/video da parte degli utenti verso l’esterno.

2.4. Postazioni di lavoro

L’Istituto dispone di postazioni di lavoro (PC Desktop e stampanti) ad uso del personale, postazioni di servizio, personal computer portatili in dotazione a Dirigenti Medici, Avvocati, Professionisti, Ispettori, Telelavoratori e personale informatico dell’Istituto.

I PC Desktop dell’Istituto (circa 14.000) sono composti principalmente da 5 modelli:

- Olidata X2 (circa il 7,14% del totale);
- Fujitsu Esprimo P5730 (circa il 16,43% del totale);
- Gateway DT50 (circa il 14,29% del totale);
- Olidata Alicon T4000 (circa il 32,14% del totale);
- HP PRO SFF 6300 (circa il 30,00% del totale).
- I Notebook (circa 2.800) sono composti da 2 modelli:
- Fujitsu-Siemens Esprimo Mobile V5505 (circa il 78,57% del totale)



- HP ProBook 6550b (circa il 21,43% del totale).
- Le postazioni di lavoro sono dotate di sistema operativo Windows 7 sp1, acquisiti in convenzione CONSIP.

Il produttore fornisce le macchine con il S.O. pre-installato e la pila software verificata e approvata da INAIL.

2.5. 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 (offerti da un Dominio o da un Dominio di Cooperazione per il tramite del soggetto coordinatore responsabile) sono offerti attraverso un unico elemento (logico) denominato

2.5.1. Porta di Dominio (PDD).

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 dispiegate 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.

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:

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

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 (ad oggi le piattaforme supportate sono Jboss/Wildfly e Weblogic 7.x e 9.x), 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 i seguenti servizi:

Comunicazione unica

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

La PDD è logicamente suddivisa in due elementi logici:

1. 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.
2. 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.

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 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 di 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).

2.6. 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
- McAfee Security for Microsoft Exchange



- NetWorker

Attualmente sono presenti on-premise circa 2000 caselle.

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

- a. PEC Base. Attualmente ve ne sono in esercizio 206, 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.
- b. Caselle PEC Strutturate. Attualmente ve ne sono in esercizio 680, 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.
- c. 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.
- d. 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.

2.7. Infrastruttura Active Directory

L'attuale infrastruttura di Active Directory INAIL si compone di un'unica foresta Windows 2012 r2 denominata INAIL.PRI che risulta ramificata in 3 domini: un dominio root (**inail.pri**) e due domini child.

Il primo dominio child è il dominio di "logon" denominato **inailutenti.inail.pri**, ovvero il contesto di sicurezza nel quale si trovano le risorse INAIL (utenti, personal computers, stampanti, cartelle condivise, ecc.).

Il secondo dominio child - **inailservizi.inail.pri** - è un dominio dedicato alla gestione di sistemi e applicazioni "legacy" dell'Istituto.

Alla foresta di produzione si è aggiunta una nuova foresta Active Directory per la sola gestione delle utenze amministrative denominata **inailadmin.local**.

La soluzione di business continuity prevede nel sito Secondario la replicata la foresta INAIL per tutti i domini Active Directory. Inoltre, nell'ambito dei servizi INAIL esternalizzati, si è reso necessario replicare parte della directory direttamente sul cloud per una migliore gestione dei contesti di logon e di replica.

Nello specifico, per i servizi ospitati sul cloud Microsoft (es: Documentale, Mobility) sono stati replicati direttamente su Azure i due domini child.

Infine, nell'ambito del servizio di Posta Elettronica ospitata su Office 365 è stato necessario implementare una foresta dedicata, denominata **tiucc.local**.



2.8. Sistema Documentale Centralizzato

Applicazione è per la componente dati su Oracle EXADATA la componente Database Oracle RAC 11.2.0.4 e ambiente X86 (DL560 HP) per la parte di Document Management (Oracle Web Center Content) evoluzione WEB della precedente piattaforma Oracle UCM. La nuova piattaforma del sistema documentale centralizzato per le Unità Centrali e periferiche (GESTDoc, Protocollo Informatico e DocWeb) è in funzione su 6 server HP DL560, con 4 processori Intel Xeon 3.40 GHz, 8 core da 128 GB di RAM per nodo, dei quali 4 nodi dedicati al DBMS Oracle 11R2 in configurazione RAC e 2 nodi con Oracle Content Server (Document Management). I dati sono memorizzati sia sulla soluzione Oracle EXADATA sia su sistema storage EMC VMAX. Il precedente sistema (GESTDoc, Protocollo Informatico e DocWeb) interamente su piattaforma X86 rimarrà in esercizio per la parte storica delle immagini.

2.9. Data Warehouse

Il Data Warehouse è stato migrato da Oracle DWH ad Enterprise Data HUB di Inail basato sul prodotto Cloudera versione 5.15.1 basato su Hadoop e composto dal Data Lake, Data Hub e Data Lab. L'infrastruttura è on-premises su macchine Dell configurate per gli ambienti di collaudo, certificazione e produzione. Ogni ambiente prevede nodi master, worker e spare. L'hardware è composto da Dell PowerEdge R730xd processore 2 x Intel Xeon E5-2680 v4 2.4GHz (14 core) 128GB (256Gb per worker) network 1Gb Ethernet (2 x 10GbE, 2x 1GbE) disk 2 x 1,2TB 10K Bay Disk 2 x 300GB .



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.

3.1. Architettura

La soluzione SOA realizzata prevede, in termini di architettura, la presenza di un ESB e di un Registry realizzati con la suite Aqualogic di BEA-ORACLE. Al momento la situazione comprende ambienti di sviluppo, test e produzione ospitati nella sede INAIL Santuario.

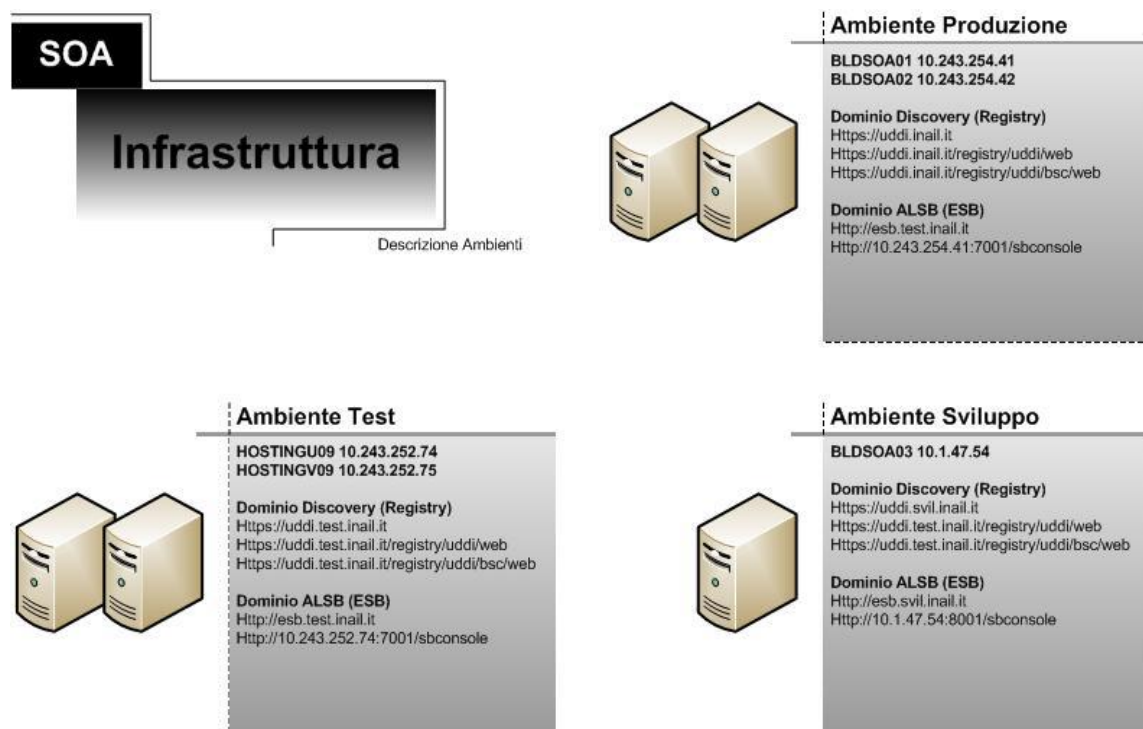


Figura 1 – Architettura SOA in INAIL

Di seguito la descrizione delle attuali architetture/strati che sono stati progettati e sono implementati in INAIL.

Infrastructure Services

L'Infrastruttura dei servizi è il meccanismo per esporre componenti dell'infrastruttura della SOA come servizi. Ad

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



esempio i servizi per il monitoraggio e l'amministrazione, i servizi di registry, nonché servizi di utilità comune, come quelli relativi alle tracciature e alle notifiche. Questi servizi possono essere utilizzati da tutti i servizi degli altri strati. Essi possono essere acceduti tramite il Services bus, in quanto registrati e amministrati come un qualsiasi altro servizio. Il Service Bus fornisce servizi essenziali per il trasporto, la conversione di protocollo, la trasformazione dei dati, e il routing dei messaggi tra i servizi dei vari strati. Il Service Bus fornisce uno stile di trasporto dei messaggi sia sincrono che asincrono.

Security Architecture

Gli elementi di sicurezza adottati sono:

- firewall e gateway XML;
- sicurezza a livello di messaggio;
- domini di sicurezza e zone custodite;
- identità, ruoli, applicazione delle policy e relativa gestione;

Data Architecture

Gli elementi di sicurezza adottati sono:

- Background sulle responsabilità dei dati (che possiede e gestisce i dati);
- Introduzione all'architettura dei dati (MDM, DNA, ecc);
- Il ruolo del servizio dati;
- Come gli schemi saranno definiti in relazione ai modelli canonici e altre iniziative di dati.

3.2. Componenti infrastrutturali

Ambiente di Sviluppo

L'ambiente di sviluppo consiste in un sistema stand alone con le seguenti caratteristiche tecniche:

Componente Hardware

- 2 x CPU Intel(R) Xeon(R) E5405 2.00GHz Quad Core
- RAM 8 Gb
- File System /space/ 40 Gb (il file system /space è quello dedicato all'installazione di tutto ciò che concerne l'erogazione di servizi tramite i prodotti BEA-ORACLE).

Componente Software

- Sistema Operativo: Red Hat Enterprise Linux Server release 5.3 (Tikanga)



- Enterprise Service Bus: Oracle Service Bus 10.3.1
- Registry: Aqualogic Service Registry 3.0
- Application Server: Oracle Web Logic 9.2.1

Il sistema di sviluppo, raggiungibile esclusivamente dall'intranet INAIL, è identificato da un nome host e dal corrispondente IP address. Questo IP è stato virtualizzato, tramite un dispositivo di rete chiamato CSM, e ai virtuali sono stati associati i nomi DNS relativi ai servizi erogati.

La gestione dei sistemi, per quanto di competenza, si realizza con modalità relative al tipo di attività da svolgere sulle stesse, ad esempio:

- Connessione SSH - Per tutto quanto riguarda la modifica di file di configurazione piuttosto che script, quali quelli di avvio/arresto dei motori, o la consultazione di file di log.
- Connessione VNC - Per tutte quelle attività che necessitano le funzioni grafiche tramite applicazioni X, ad esempio l'installazione di patch BEA-ORACLE.
- Connessione Browser - Tramite l'utilizzo di un browser è possibile accedere alle console di amministrazione web dei prodotti BEA-ORACLE.

Ambiente di Test

L'ambiente di Test consiste in un cluster applicativo realizzato con una coppia di sistemi. Ognuno di questi sistemi, speculare all'altro, ha le seguenti caratteristiche tecniche:

Componente Hardware

- 2 x CPU Intel(R) Xeon(R) 5110 1.60GHz Dual Core
- RAM 4 Gb
- File System /space/ 19 Gb (il file system /space è quello dedicato all'installazione di tutto ciò che concerne l'erogazione di servizi tramite i prodotti BEA-ORACLE).

Componente Software

- Sistema Operativo: Red Hat Enterprise Linux AS release 4 (Nahant Update 3)
- Enterprise Service Bus: Oracle Service Bus 10.3.1
- Registry: Aqualogic Service Registry 3.0
- Application Server: Oracle Web Logic 9.2.1.

I nodi del cluster di sviluppo, raggiungibili esclusivamente dall'intranet INAIL, sono identificati da un nome host



e dal corrispettivo IP address, questi IP sono stati virtualizzati tramite un dispositivo di rete chiamato CSM che realizza il bilanciamento del traffico, inoltre gli indirizzi IP sono associati a relativi nomi DNS.

La gestione dei sistemi, per quanto di competenza, si realizza con modalità relative al tipo di attività da svolgere sulle stesse, ad esempio:

- Connessione SSH - Per tutto quanto riguarda la modifica di file di configurazione piuttosto che script, quali quelli di avvio/arresto dei motori, o la consultazione di file di log.
- Connessione VNC - Per tutte quelle attività che necessitano le funzioni grafiche tramite applicazioni X, ad esempio l'installazione di patch BEA-ORACLE.
- Connessione Browser - Tramite l'utilizzo di un browser è possibile accedere alle console di amministrazione web dei prodotti BEA-ORACLE.

Ambiente di Produzione

L'ambiente di produzione consiste in un cluster applicativo realizzato con una coppia di sistemi. Ognuno di questi sistemi, speculare all'altro, ha le seguenti caratteristiche tecniche:

Componente Hardware

- 4 x Intel(R) Xeon(TM) E7420 2.13GHz Quad Core.
- RAM 8 Gb
- File System /space/ 78 Gb (il file system /space è quello dedicato all'installazione di tutto ciò che concerne l'erogazione di servizi tramite i prodotti BEA-ORACLE).

Componente Software

- Sistema Operativo: Red Hat Enterprise Linux Server release 5.3 (Tikanga)
- Enterprise Service Bus: Oracle Service Bus 10.3.1
- Registry: Aqualogic Service Registry 3.0
- Application Server: Oracle Web Logic 9.2.1

I nodi del cluster di produzione, raggiungibili esclusivamente dall'intranet INAIL, sono identificati da un nome host e dal corrispettivo IP address, questi IP sono stati virtualizzati tramite un dispositivo di rete chiamato CSM che realizza il bilanciamento del traffico, inoltre questi IP virtuali sono stati associati a relativi nomi DNS.

La gestione dei sistemi, per quanto di competenza, si realizza con modalità relative al tipo di attività da svolgere sulle stesse, ad esempio:

- Connessione SSH - Per tutto quanto riguarda la modifica di file di configurazione piuttosto che script, quali



quelli di avvio/arresto dei motori, o la consultazione di file di log.

- Connessione VNC - Per tutte quelle attività che necessitano le funzioni grafiche tramite applicazioni X, ad esempio l'installazione di patch BEA-ORACLE.

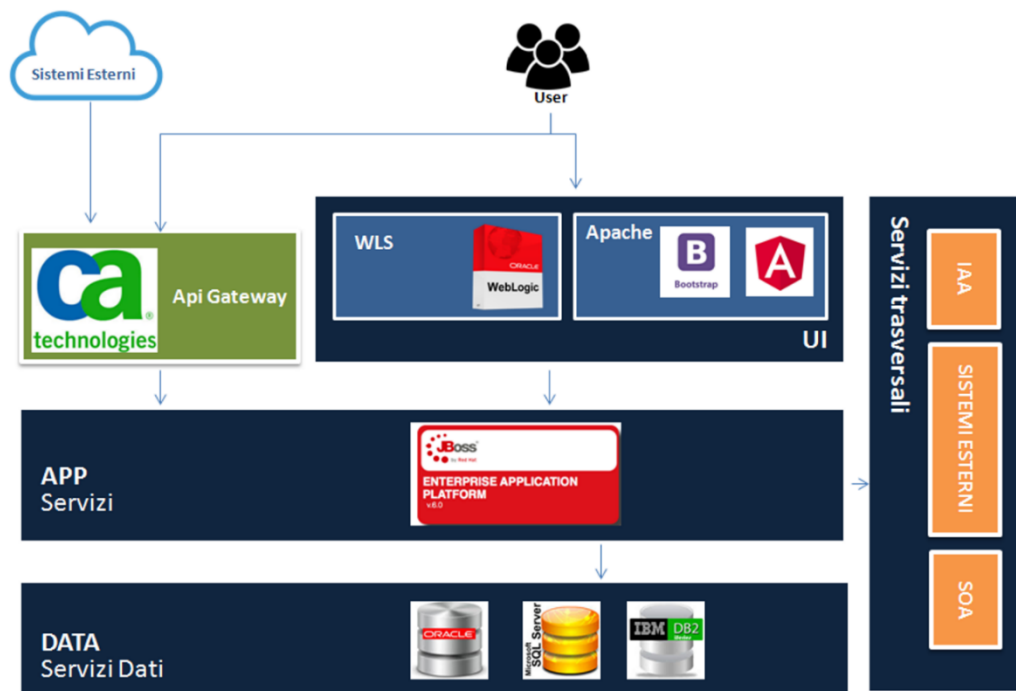


4. API REST GATEWAY

Nell'architettura applicativa generale INAIL, nell'ambito della gestione dei servizi, è presente, oltre alla componente SOA, una componente API Rest Gateway utilizzata dall'Istituto per l'orchestrazione dei servizi REST esposti verso l'esterno.

Questo layer infrastrutturale permette di orientarsi verso un'architettura API-Based/HTTP Rest 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", come verrà meglio descritto nel capitolo dedicato alle Architetture Applicative.



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 REST erogati da soggetti esterni all'Istituto.

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

Il suo unico front-end è rappresentato dal layer di Reverse proxy dell'Istituto che protegge e disaccoppia l'API-



REST-GTW dall'esterno.

L'API Gateway è integrato con il Sistema di Controllo degli Accessi, interagendo con il sistema di Single Sign ON per la gestione delle policy di autenticazione, autorizzazione, verifica dei token di sessione e dei workflow di controllo per ciascuna chiamata ad API.

4.1. Interfacce di esposizione

I servizi REST sono pubblicati, via API Gateway, su Endpoint differenti in funzione delle loro caratteristiche, in particolare elementi discriminanti sono:

- Esposizione:
 - Internet: servizi esposti su Internet (e raggiungibili quindi anche dalla intranet)
 - Intranet: servizi esposti solo su Intranet
 - B2B: servizi esposti sono per i Backend invocabili quindi solo da tale layer

Nel caso i servizi dovessero essere esposti su più interfacce, mantenendo lo stesso pacchetto applicativo, verranno pubblicati su tutte le interfacce necessarie dall' API-REST-GTW.

- Protezione:
 - Protetti: servizi che necessitano di Autenticazione
 - Pubblici: servizi che possono essere esposti senza autenticazione

4.2. Standard costruzione URL servizi REST

Le URL dei Servizi Rest pubblicati, eccetto specifiche eccezioni che vengono valutate di volta in volta, è tipicamente costituito da:

- Protocollo: HTTPS → "https://"
- Dominio base: <baserest> → www.inail.it / collportale.inail.it / certportale.inail.it
- Context Base: "/api" → contesto comune a tutti i servizi
- Context tipologia: "/public" oppure "/" (per private)
- Context Area Applicativa: "/denunce" → contesto relativo all'Area applicativa.
- Context Servizio: "/pratica" → nome del servizio (anche multipath).
- Nome Metodo: "/getPratica" → metodo del servizio invocato.



- Query String (o POST): “?param1=value1” → parametri veicolati verso il servizio Rest in GET o in POST.

4.3. Servizi Trasversali esposti dall’API-REST-GTW e JWT

Sono elencati di seguito i servizi e features esposti dall’API-REST-GTW per supportare la pubblicazione di servizi protetti e pubblici

4.4. Servizio checkSession

Per poter gestire correttamente la sessione per applicazioni Single Page Application è stato creato un servizio “sentinella” che permette di avere informazioni base sulla validità della sessione.

Tale servizio può essere invocato:

- On Demand: ogni qualvolta l’applicazione vuole verificare se l’utente ha una sessione valida o meno (es. Per inizializzare la sessione prima di invocare i REST)
- Via polling: l’applicazione può invocare periodicamente il servizio per verificare la sessione e mantenerla attiva (non facendo scattare l’Idle Timeout)

4.5. JWT

I JWT sono degli oggetti (Tokens) che permettono di inviare dati ad un server usando il formato JSON. E’ uno standard utilizzato per veicolare claims in modalità interoperabile tra i servizi REST in modalità standard, indipendente dalla piattaforma e sicura.

E’ stato scelto per uniformità ed indipendenza dai servizi di inviare il JWT a tutti i servizi protetti da API-REST-GTW.

Il JWT può essere arricchito da informazioni di profilo con Ruoli/Ambiti in funzione delle specifiche richieste dell’applicazione.

In caso i servizi non necessitassero di attributi particolari o ruoli verrà inviato un JWT costituito dalla sola UUID (in caso di servizi comunque protetti) firmato dal REST Gateway.

4.6. JWTNames

All’interno del sistema Inail, nel caso in cui i servizi richiedano Ruoli/Ambiti in funzione delle specifiche di funzionamento, queste informazioni saranno contenute nel JWT. Per consentire una corretta ed agevole definizione dei livelli di accesso degli utenti ai servizi, l’Api Gateway consente di suddividere i servizi in categorie identificate da un parametro denominato “JWTName”. I servizi omogenei, che sulla base delle specifiche fornite dai gruppi di sviluppo condividono gli stessi “Domini di dati”, saranno identificati dallo stesso JWTName.



5. INFRASTRUTTURE DI RETE

5.1. 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 DCIT 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 40 Mbit/s secondo la quantità di traffico effettuato.

Le strutture della Direzione Generale hanno tutte collegamenti in fibra a 200 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 xDSL a 10 Mbit/s.

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 ridonati su dark fiber.

Sullo stesso DWDM insistono anche i collegamenti Infiniband e ISL che permettono la sincronizzazione continua e la comunicazione rispettivamente dei sistemi Mainframe e dello storage.

Tramite tali collegamenti ad alta velocità i due siti si comportano, dal punto di vista della rete, come se fossero un sito unico erogando servizi da entrambi i siti e ognuno è in grado di sopperire ad un eventuale fault dell'altro in qualsiasi momento.

La rete Lan del data center è costituita principalmente da collegamenti in fibra a 10 Gb in tecnologia Unified fabric (LAN e SAN unificate) pur residuando alcuni 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 7000;5000;2000;1000 e catalyst 6509 in configurazione vss.



Negli switch Catalyst risiedono anche i firewall che permettono la creazione dei vari domini di sicurezza in cui è divisa la rete; per i servizi bilanciati vengono utilizzati apparati Netscaler.

5.2. 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".

La connettività verso Infranet è composta da due Links, uno attivo a 200Mbit e uno di backup presso il CED del BCRS di Acilia Via DI Macchia Palocco, attestati entrambi su SPC, mediante operatore Vodafone.

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.

5.3. Reti Locali

La LAN della DCOD è realizzata con cablaggi certificati in categoria 5E e 6 fino a 1Gbit/s con dorsali 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 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.

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

Al completamento dei lavori di ogni singola Sede viene effettuata la migrazione al VoIP per quanto riguarda la fonia. Successivamente è prevista la sostituzione degli IP statici delle postazioni di lavoro (PdL) con IP dinamici tramite server DHCP e l'autenticazione 802.1x al punto d'accesso.

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.



5.4. Connettività verso Internet

La connettività verso internet è fornita da Vodanofe S.p.A 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.

5.5. Architettura Sedi, Direzioni Regionali e Direzione Generale

Per il collegamento delle Sedi (di tipo A e B) e delle Direzioni Regionali sul territorio nazionale vengono utilizzati link a 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.

5.6. Architettura Sedi di tipo C

Le Sedi di tipo C utilizzano esclusivamente collegamenti a 10 Mbit/s. Anche in questo caso i collegamenti sono ridondati verso il sito Primario sia dal punto di vista dell'apparato Hardware L3 (tramite l'utilizzo di 2 Router Cisco), sia dal punto di vista dei flussi del fornitore di connettività (tramite l'utilizzo di 2 linee HDSL da 10Mbit/s, una primaria e l'altra di backup attestata su POP diverso dalla principale) con livello di affidabilità L3 o L5.

5.7. 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.

5.8. 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.



5.9. Biometria

L'Istituto, ad oggi, non ha in corso progetti che prevedano l'utilizzo della biometria per finalità di accesso fisico e/o logico per l'identificazione delle persone fisiche.

Si ritiene opportuno, comunque, segnalare che il Centro Protesi di Vigorso di Budrio (Bologna) utilizza la biometria, impiegando la caratteristica della geometria della mano esclusivamente per la finalità istituzionale di produzione protesi.

Più in particolare, per realizzare la protesi in silicone nel distretto della mano, oltre a rilevare la forma dell'arto superstite (mano, dito, ecc.) e dell'arto controlaterale, nel processo lavorativo si rileva anche l'impronta della persona, effettuando tale rilievo con del materiale da copiatura come l'alginato, il silicone, il gesso. Tali modelli vengono poi conservati nell'archivio interno degli stampi che il reparto del Centro Protesi ha in carico.

5.10. VOIP (Voice over IP)

La sostituzione nelle strutture della Direzione Generale di Roma e nelle Sedi periferiche degli apparati di LAN, tra le cui caratteristiche avanzate c'è la possibilità di supportare ed implementare la Voce su Ip con telefoni che vengono alimentati dagli stessi apparati, ha consentito l'installazione di telefoni IP per un totale di circa 12.000 utenze tra Direzione Generale e Unità periferiche.

Il sito per la fonia VoIP è presente presso il DC Primario ed anche esso ha una soluzione di disaster recovery.

5.11. RFID (Radio Frequency Identification)

Presso il Centro Protesi di Vigorso di Budrio è stato definito ed ingegnerizzato l'utilizzo dei tag passivi RFID, al fine di memorizzare un codice univoco nella protesi, per essere chiaramente identificata nel processo produttivo. Il tag registrato nel sistema informatico di produzione all'inizio della costruzione

del presidio ortopedico, consente la successiva identificazione durante le fasi di avanzamento della lavorazione.

5.12. Wireless (Mobile e WI-FI)

È stato realizzato ed inserito in esercizio il progetto INAIL "Mobile" che prevede l'attivazione dei canali "mobile" di accesso ai servizi online tramite apparati mobili, servizi nomadici, l'attivazione del Captive Portal (Portale mobile) per le Wi-Fi Area.

Relativamente ai servizi su dispositivi mobili sono fruibili, oltre che il sito m.inail.it, le app per smartphone, sia Apple che Android, Inail Informa, Rapporto Annuale 2010, e per tablet, sia Apple che Android, Rapporto



Annuale 2010, iNAPO, Scaffale INAIL.

Relativamente al Wi-Fi sono stati installati access-point interni per consentire il collegamento wireless, ad esempio, nelle sale riunioni, nelle aule didattiche o in punti non cablati o di difficile cablatura, 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. Inizialmente presso il Centro Protesi di Vigorso di Budrio è stato realizzato un hot-spot “pubblico” per consentire il collegamento internet ai pazienti del Centro, 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.

Lo stesso 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.



6. PUNTO DI ACCESSO POLISWEB

6.1. 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 DCOD. 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.

6.1.1. 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.

6.1.2. Autenticazione ed 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

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



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.





7. SICUREZZA

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

7.1. 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 (cod. fiscale, CNS, CIE, etc.) superando le credenziali proprietarie (ES: matricola, codice ditta, ecc).

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.*

7.2. 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, ecc).

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);
- elabora 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.

7.3. Single Sign On INAIL

L'obiettivo del nuovo sistema SSO è creare un'architettura unitaria fortemente integrata, idonea a sostenere l'evoluzione dei servizi e di minimizzare nel contempo 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 UserName/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, sottoforma 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.

Data la suddivisione sia logica che fisica delle applicazioni sono definiti due user store: uno su DB SQL server 2016 per gli utenti internet; uno user store definito dentro il Policy Server collegato al dominio

Active Directory degli utenti, per gli utenti intranet. Nel corso del 2009 è prevista la migrazione dei database da SQL 2000 a SQL 2005.

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. Una volta definiti i ruoli gestibili in una procedura è possibile assegnarli a gruppi tramite la "console di profilazione". 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 fornisce strumenti centralizzati per gestire i livelli di accesso alle procedure; si compone di una base dati SQL 2016, di console web e di web-services di interrogazione, entrambi sviluppati in linguaggio C#, frame work 4.5.

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



La console web fornisce gli strumenti che consentono ad utenti autorizzati di popolare i gruppi di sicurezza definiti dall'istituto e il web-services veicola 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.

La documentazione completa dei componenti di profilazione applicativa è reperibile sulla Intranet dell'Istituto all'indirizzo <http://intranet.inail.it/AreaInternet/default.asp>.

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.

Le credenziali di accesso degli utenti Intranet risiedono su dominio AD; le credenziali di accesso degli utenti Internet risiedono su un DB Microsoft SQL Server 2016, le informazioni di profilo di entrambi gli utenti risiedono su un DB Microsoft SQL Server 2016.

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) gli agent installati richiedano le credenziali di accesso (user e password, Smart Card ,SPID, Federazione) che saranno verificate uno dei due Users Store (DB SQL o Active Directory).

Se la fase di autenticazione non va a buon fine, l'utente è invitato a immettere nuovamente le credenziali, altrimenti, ha inizio la fase successiva di identity assertion.

Autenticazione

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 (protocollo SOAP) 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".

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 il web services di profilazione.

Il profilo completo dell'utente contiene i suoi dati anagrafici, i gruppi di appartenenza, le proprietà. 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 rappresentato da un documento XML.

7.4. 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 basi dati istituzionali (HR per le utenti interni e DB2 per le aziende ed i patronati) ed in parte in quelle infrastrutturali (Cercapersona 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).

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

IL "PROFILO APPLICATIVO"

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

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.

Es: i "validatori pratiche" del GRA ed i "gestori anomalie" di GPA sono due gruppi "applicativi".

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#, frame work .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.

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



7.5. Servizi del Security Operations Center (SOC)

Nell'infrastruttura dell'Istituto sono installate e attive diverse soluzioni di sicurezza a protezione sia dei server che dei client. E' 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 McAfee 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 ed ecc... 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.
- McAfee ePO 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 McAfee. 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 DXL McAfee permette a tutti agli altri prodotti della suite McAfee (ENS, IPS, MWG ed ecc...) 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 McAfee 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 – E' 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 – E' 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 – E' 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;
- McAfee Endpoint Security – É 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 dalla minacce esterne, controllando e bloccando le attività potenzialmente pericolose;
- File and Removable Media Protection – É 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;

7.5.1. SOC – Log Management e Correlazione

Il servizio INAIL di Log Management & Correlazione (LM & CO) si compone di una piattaforma di sicurezza HPE ArcSight dedicata a:

- 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.

7.5.2. 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

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



dell'Istituto in conformità alle normative vigenti, agli standard ed alle best practices.

7.5.3. SOC – Sicurezza DB e Applicazioni

Le sonde della piattaforma Imperva SecureSphere sono costantemente attive sul traffico di pertinenza analizzando le connessioni verso i DB.

7.5.4. 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.

7.6. Web Application Firewall (WAF)

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

7.7. 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.

7.8. 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.

7.9. 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.

7.10. Sicurezza Applicativa

FINALITÀ DEL SERVIZIO DI SICUREZZA APPLICATIVA

Il servizio di Sicurezza Applicativa è finalizzato a verificare la sicurezza delle applicazioni web prima del loro rilascio in produzione.

L'attività si basa sulla metodologia ISECOM/OSSTMM (open source Security Testing Methodology Manual) e comporta l'utilizzo di strumenti software automatizzati e non, per l'analisi delle vulnerabilità

applicative note, l'utilizzo di tecniche più evolute per valutare la possibilità che una vulnerabilità sia sfruttata per perpetrare un attacco a opera di un utente esperto. Nel corso della verifica,

l'interpretazione e la verifica manuale dei risultati e delle vulnerabilità effettivamente esistenti sono volte a individuare i punti di debolezza riscontrati, i falsi positivi, a correlare i risultati e ad assegnare un livello di gravità, per definire le contromisure necessarie. Al termine dell'attività viene prodotto un report dettagliato, contenente la descrizione dei risultati emersi, la gravità delle vulnerabilità riscontrate e le possibili contromisure da adottare.

Il processo di verifica e correzione delle vulnerabilità si suddivide in tre fasi distinte:

- preparazione,
- processo di verifica,
- processo di correzione.

Il processo di individuazione delle vulnerabilità applicative e della loro correzione richiede il coinvolgimento diretto del Responsabile dell'Applicazione Web, del Responsabile dello Sviluppo per la gestione e la correzione delle URI vulnerabili, con la revisione del codice sorgente.

Fase preliminare

Nella fase preliminare sono svolte le attività necessarie per la pianificazione delle verifiche e l'allestimento dell'ambiente di test.

Identificazione del Responsabile dell'Applicazione WEB

Per consentire lo svolgimento dei test, occorre identificare un referente per le attività di sviluppo dell'applicativo, che viene indicato di seguito come Responsabile dell'Applicazione Web, e che concorda con il Responsabile del Gruppo Sicurezza Applicativa le attività di verifica dell'applicazione, riceve la notifica delle



vulnerabilità rilevate e valuta l'opportunità di sospendere i servizi vulnerabili.

Attivazione dell'ambiente di test

Per non compromettere la riservatezza, l'integrità delle informazioni e la disponibilità dei servizi erogati dai sistemi in produzione, deve essere predisposto un ambiente di test, identico all'ambiente di produzione, costantemente allineato a fronte di qualsiasi modifica infrastrutturale o di versione del software, con le medesime utenze e profili di accesso definite in base alla politica per la gestione degli accessi definita per l'ambiente di esercizio.

Aggiornamento del processo di collaudo

Il processo di collaudo delle applicazioni Web dell'Istituto è stato aggiornato, includendo una nuova fase di controllo, finalizzata a valutare la sicurezza applicativa del software prima del suo rilascio in produzione. Questa fase è stata introdotta dopo le prove di accessibilità e prima dei test di carico ed è finalizzata a verificare la conformità delle misure di sicurezza e protezione delle informazioni ai requisiti di sicurezza minimi previsti dal D. Lgs. 196/2003 e dai regolamenti interni dell'Istituto.

Identificazione e classificazione dei servizi

Le funzionalità dei sistemi sono state raggruppate in una serie di moduli, cui fanno capo una o più URI.

Per ogni modulo è stato identificato un Responsabile dello sviluppo, cui sono notificate le vulnerabilità riscontrate e che deve attivarsi per la correzione e revisione del codice.

La priorità con cui effettuare i test delle applicazioni è stabilita in funzione dell'effettiva disponibilità dell'applicazione per i test e/o di specifiche esigenze contingenti. La verifica delle applicazioni in rilascio avviene nell'ambito delle prove di collaudo così come specificato nel paragrafo precedente.

Redazione delle linee-guida per la programmazione

È stata avviata la redazione di un documento contenente le linee guida per la programmazione di applicazioni Web sicure, rivolto agli analisti, per consentire la definizione di un'architettura capace di resistere almeno agli attacchi più comuni, e ai programmatori, che dovranno applicare le direttive degli analisti evitando, allo stesso tempo, di non cadere in errori che possano compromettere la sicurezza del sistema.

Le linee guida consentono di valutare la gravità delle vulnerabilità individuate affinché il responsabile dell'applicazione Web possa decidere se un servizio vulnerabile debba essere sospeso o debba essere rilasciato comunque in produzione, con l'impegno però di sanare in tempi brevi le vulnerabilità segnalate.



Processo di verifica

L'attività di verifica di ciascun servizio è effettuata esclusivamente dal personale del Gruppo di Sicurezza Applicativa su richiesta del Responsabile dell'Applicazione Web che determina anche la priorità di intervento.

Per ogni servizio deve essere identificata una URI di "ingresso" dalla quale è possibile l'accesso alle diverse funzionalità da verificare. Il Responsabile dell'applicazione Web deve indicare, per ciascun servizio, la URI iniziale, il percorso necessario a raggiungerla (per esempio, Home > Sala Stampa > Notiziario INAIL) e qualora l'accesso alle pagine richieda un'autenticazione, anche le credenziali di accesso (username e password) per tutte le classi di utenze previste.

Partendo dalla URI segnalata, viene effettuata dapprima una scansione di sicurezza automatica e, in base agli esiti dell'esame, le URI del sistema sono classificate come possibili positivi e possibili negativi.

Successivamente, le URI sono assegnate ai componenti del Gruppo Sicurezza Applicativa con le informazioni specifiche di dettaglio (per esempio protocollo http, linguaggio SQL, programmazione ASP) per ulteriori test e permettere un'analisi approfondita e la verifica dell'effettiva vulnerabilità. Alla fine delle prove, si classificano le URL esaminate in base ad un livello di pericolosità.

Il modello di classificazione delle categorie di vulnerabilità adottato si basa su una scala che ne indica il livello di pericolosità:

- **colore giallo** - le prove hanno evidenziato una o più vulnerabilità, ma non è stato possibile sfruttarle per portare a termine un attacco o le condizioni per sfruttare la vulnerabilità sono molto basse;
- **colore rosso** - le prove hanno evidenziato una o più vulnerabilità che hanno permesso di portare a termine un attacco senza particolari difficoltà;

Le classificazioni di seguito riportate indicano due ulteriori stati di esecuzione dei test:

- **colore verde** - le prove eseguite non hanno rilevato vulnerabilità;
- **colore grigio** - le vulnerabilità individuate non rientrano nella pertinenza delle verifiche di sicurezza afferenti il servizio.

Al termine delle verifiche viene prodotto e consegnato al Responsabile dell'Applicazione Web, un report dettagliato che descrive le vulnerabilità rilevate, e se necessario anche il tipo di attacco effettuato.

Tutti i report sono classificati come riservati e generalmente, a meno di esplicite richieste da parte del Responsabile dell'applicazione Web, eventuali brani di codice relativi all'attacco sono parzialmente oscurati, al fine di prevenire la possibilità di occorrenza che un utente malintenzionato possa riprodurre l'attacco, sfruttando le informazioni contenute nel documento.



A fronte della rilevazione delle vulnerabilità, il Responsabile dell'Applicazione Web con il supporto del Responsabile dello Sviluppo dell'applicazione, procede alla valutazione dell'opportunità di sospendere il servizio in attesa che le vulnerabilità siano sanate o avviare le correzioni senza provocare soluzioni di continuità, e determina la priorità degli interventi.

Processo di correzione

Le attività di correzione devono essere effettuate per tutte le applicazioni che non hanno superato il test di sicurezza applicativa e sono svolte dal personale preposto allo sviluppo o alla gestione e/o manutenzione del software.

In funzione dell'esito delle prove di sicurezza, il Responsabile dell'applicazione Web può valutare l'opportunità di sospendere il rilascio del servizio vulnerabile in attesa che le anomalie rilevate siano corrette.

Il processo di correzione delle vulnerabilità e di revisione del codice sorgente è avviato dal Responsabile dello sviluppo dell'applicazione, che assegna a un programmatore la o le vulnerabilità riscontrate, la loro possibile causa e le azioni correttive da intraprendere.

Infine, al termine della revisione, il codice sarà sottoposto alle verifiche funzionali previste dal piano di collaudo dell'Istituto e, in caso di esito positivo, sarà inviato dal Responsabile dell'Applicazione Web al team di Sicurezza Applicativa per una nuova verifica.

Gestione del sistema di verifica e correzione

Per garantire la riservatezza delle informazioni trattate, la gestione dell'intero processo di verifica e correzione delle applicazioni avviene mediante un sistema "Web-based", provvisto di un meccanismo di autenticazione basato su userid e password, accessibile solo dalla intranet dell'Istituto.

L'accesso al sistema di gestione è consentito esclusivamente al personale coinvolto nei processi di verifica e correzione delle vulnerabilità e, nel rispetto del principio del need to know, a ogni utente è assegnato un profilo che permette di accedere solo e soltanto alle informazioni e risorse necessarie per lo svolgimento della propria attività lavorativa.

Le informazioni sulle vulnerabilità non possono essere inviate per posta elettronica o su documenti cartacei, ma risiedono nella base-dati del sistema.

Inoltre, il sistema tiene traccia del lavoro svolto dai Responsabili dello sviluppo delle applicazioni e dal Gruppo Sicurezza, sullo stato di avanzamento delle attività di verifica e di correzione, permette di generare reportistica sulle applicazioni verificate, elaborare statistiche sulla percentuale di applicazioni esaminate, vulnerabili e corrette.



7.11. 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 CNIPA 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 un tool di trouble ticketing, Mantis, scritto in linguaggio PHP ed integrabile anche con diversi database, per esempio MySQL, Microsoft SQL, PostgreSQL e con un server web. Il tool permette anche la comunicazione fra i soggetti coinvolti nelle diverse fasi del processo.

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 dell'UQS 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;

Classificazione del documento: Consip Public

Gara a procedura aperta in due lotti per l'acquisizione di servizi professionali a supporto della governance e business operations di Inail - ID 2208

Appendice 4 al Capitolato tecnico – Contesto tecnologico



- 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), al Centro Gestione Sicurezza SPC, e a GOV-CERT, mediante l'analisi degli eventi ed allarmi provenienti dai dispositivi di sicurezza monitorati;
- alle Strutture operative delle Aree Interne alla DC. SIT, 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 dell'UQS o di un suo delegato, qualora il personale coinvolto per il livello precedente non abbia le conoscenze e competenze sufficienti.
- 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 DCOD 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.



7.12. Firma Digitale Centralizzata

L'Inail, per semplificare l'utilizzo e per risolvere la problematica delle firme massive, ha acquisito un sistema di Firma Elettronica, costituito da due apparati HSM (tecnologia CoSign) configurati in alta affidabilità, nei quali sono memorizzate in maniera centralizzata e sicura le chiavi della firma (Chiavi Private). 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 per l'utilizzo della crittografia digitale, garantendo, inoltre, che ogni accesso non autorizzato, sia fisico che logico, all'apparato sia tempestivamente individuato.

Gli apparati HSM sono integrati nel servizio di Directory d'Istituto di modo che si possa usufruire di una base dati, centralizzata, costantemente aggiornata, monitorata e sicura, contenente le credenziali d'accesso dei Richiedenti ritenuti idonei per la fruizione del Servizio di Firma Digitale.

L'apparato costituente la soluzione permette agli utilizzatori di firmare digitalmente transazioni, documenti ed altre tipologie di dati. Per assolvere a questa funzionalità, la soluzione può essere fruita

sia in modalità client che client-less.

Nella prima funzionalità, l'apposizione della firma sul documento è realizzata mediante l'utilizzo del client software fornito con la soluzione. In questo modo è possibile firmare digitalmente, sia in maniera massiva che puntuale, la documentazione da approvare, mediante inoltre della stessa con sessione crittografata, in modalità trasparente all'utente, all'apparato di firma.

Nella seconda funzionalità, l'apposizione della firma sul documento è realizzata mediante l'utilizzo dei web services esposti dall'apparato. In questo modo è possibile integrare la funzionalità di firma elettronica nei servizi dell'Istituto erogati mediante applicazioni web. In entrambi i casi l'apposizione della firma viene effettuata solo se l'apparato conclude con successo l'autenticazione delle credenziali dell'utente.

Per garantire un adeguato livello di riservatezza alle informazioni trattate, il servizio di Firma Digitale Centralizzata è gestito tramite due processi, relativi alla gestione di certificati ad uso interno (selfsigned) o ad uso esterno (PKI pubblica certificata).

Entrambi i processi sono scomposti in due sotto-processi:

- Il primo, inerente la richiesta e relativa approvazione del rilascio di un certificato, è gestito mediante comunicazioni non ripudiabili tra il Richiedente, l'unità di Sicurezza "Firma Digitale", il Referente della Sicurezza d'Istituto, ed i responsabili delle aree coinvolti.



- Il secondo, inerente il rilascio e l'eventuale revoca, è gestito mediante comunicazioni non ripudiabili tra l'unità di Sicurezza "Firma Digitale", l'unità Operativa "Gestione Dominio" e i responsabili delle aree coinvolti.

7.13. Canale di orientamento e accesso al mondo della privacy e della 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 l'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 27001:2013.
- 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 ed divulgare regole, policy e linee guida.

In questa area oltre a tutti i documenti relativi alla legislazione nazionale ed europea (normative Generali), vengono riportare 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.



8. ARCHITETTURE APPLICATIVE

Le applicazioni che vengono sviluppate per INAIL sono disegnate secondo standard di architettura applicativa che variano in base alla mission, alla tipologia di dati gestiti e all'eventuale storia pregressa dell'applicazione stessa.

Vengono riportate di seguito le due tipologie architetture presenti in Istituto.

8.1. Architettura a tre livelli

All'interno della DCOD è stata stabilita una suddivisione architetture per la maggior parte delle applicazioni nei classici three-tier:

- Presentation layer;
- Business logic layer;
- Data layer.

A questa suddivisione logica per tier corrisponde una suddivisione fisica delle applicazioni in componenti, con una ripartizione delle stesse su piattaforme hardware/software diverse, secondo gli attuali standard tecnologici dell'istituto.

Ai livelli descritti sono state associate le due ulteriori componenti infrastrutturali descritte nei capitoli precedenti:

- SOA: per realizzare l'implementazione di un ESB dell'Istituto, secondo la logica Publisher/Subscriber;
- API Manager Rest Gateway: per l'orchestrazione dei servizi REST.

L'architettura appena presentata è stata declinata ed adattata alle esigenze degli ambiti applicativi specifici, ma mantiene una funzione di Architettura di Riferimento dell'Istituto.

Per Front-End Container si intende l'area tecnologica attraverso la quale vengono presentate le interfacce grafiche ed i servizi di frontiera delle applicazioni all'utente finale.

Quest'area dovrebbe contenere essenzialmente la logica di presentazione, grafica e funzionale, esposta sul web front-end delle applicazioni e deve dialogare con il layer inferiore attraverso l'uso di servizi http.

Per Business Logic Container, si intende l'area dedicata alla gestione della logica di business delle applicazioni, alla realizzazione di servizi eleggibili all'uso generalizzato tramite la SOA, alla comunicazione e gestione dei dati, attraverso framework standard di gestione della persistenza.

La funzione del modulo HTTP-Rest sarà quella di centralizzare la gestione di API HTTP esposte verso applicazioni



in mobilità o widget stateless dei front-end esposti agli utenti finali.

Attualmente le soluzioni tecnologiche utilizzate in corrispondenza degli standard indicati in figura sono i seguenti ambienti Java-Based:

- Front-End Container: Oracle Weblogic;
- Business Logic Container: Red Hat JBoss;
- SOA: Oracle SOA Suite;
- DBMS: Oracle, DB2 e MS SQL Server.

Lo standard di esposizione dei servizi REST verso l'esterno prevede l'utilizzo di un apposito Rest Gateway – CA API Gateway, integrato con CA Siteminder.

I servizi devono essere deployati su AS di back-end, ossia su AS Jboss.

Per il dettaglio sulle versioni dei singoli prodotti e sui framework standard che sono accettati per le applicazioni on top di essi si rimanda ai documenti di dettaglio nei riferimenti.

Per il dettaglio su processi e modalità di sviluppo di applicazioni sui layer standard si rimanda alla documentazione operativa e di processo relativa.

Per il workflow management sono presenti in Istituto due prodotti:

- Oracle BPEL Process Manager
- IBM Business Process Manager

Entrambi i prodotti presentano un throughput adeguato all'interazione con applicazioni in produzione e hanno funzionalità simili ma non equivalenti, si consiglia quindi un'analisi approfondita dell'ambito di utilizzo prima di selezionarne uno rispetto all'altro.

8.2. Architetture Applicative per il Cloud Ibrido

Il contesto di riferimento dell'Istituto è un modello di Cloud Ibrido.

Tale modello è costituito da una infrastruttura “on premise” a cui fa riferimento il Private Cloud dell'INAIL con la componente legacy/enterprise ed un contesto “off premise” a cui fa riferimento la parte Public Cloud dell'Istituto.

In entrambi i casi l'Istituto si poggia su una PaaS (Platform as a service).



Nel caso di infrastruttura “on premise” la PaaS di riferimento sarà RedHat - OpenShift.

Nel caso di infrastruttura “off premise” potrebbe essere una PaaS proprietaria del vendor.

Le applicazioni sviluppate secondo l’architettura a Micro/Mini servizi, dovranno essere realizzate in maniera indipendente dal contesto infrastrutturale “on premise” / “off premise”.

Per i dettagli si rimanda al documento “Guida alle Architetture Cloud e standard applicativi di riferimento DCOD” indicato nella tabella riferimenti.

Di fatto un’applicazione esercita sulla PaaS on premise dovrà poter continuare a funzionare sulla PaaS off premise.

8.2.1. Applicazioni a Container

A fronte di specifiche esigenze funzionali e operative che consentano lo sviluppo di applicazioni in ottica di Cloud Ibrido, è possibile la realizzazione delle applicazioni stesse con un architettura a micro/mini servizi, ospitati su Container.

L’architettura a Microservizi è una variante delle Architetture Orientate al Servizio (SOA) che struttura un’applicazione come una raccolta di servizi integrati.

Un Container è un modello di pacchettizzazione software leggero, eseguibile autonomamente che include tutto ciò che serve per eseguirlo: codice, runtime, strumenti e librerie di sistema, impostazioni.

Lo standard di containerizzazione scelto dall’Istituto per la realizzazione di applicazioni a microservizi è Docker.

Tale standard, può essere utilizzato per la realizzazione di nuove applicazioni e in caso di decomposizione di applicazioni “monolitiche” tramite l’applicazione di “Pattern di Trasformazione” verso i nuovi ambienti containerizzati.

L’Istituto ha definito una serie di immagini Docker base su cui possono essere basate le applicazioni realizzare su tale standard, che rappresentano lo “stack tecnologico” consentito per l’esercizio di Docker in DCOD, supportato dalla PaaS on premise di riferimento, Red Hat –OpenShift, con l’indicazione di privilegiare per quanto possibile prodotti open source.

Dockerfile di base e Docker Images non presenti nei repository ufficiali dell’Istituto non potranno essere utilizzate se non preventivamente concordate con gli uffici preposti.

In generale il software prodotto dovrà comunque rispettare tutti i vincoli già in essere in Istituto riguardanti test di qualità statica del codice, sicurezza e di performance opportunamente rimodulati secondo il nuovo contesto di sviluppo.



Per renderne più agevole la consultazione, le fonti e i rimandi al dettaglio di Best Practice e riferimenti tecnologici presenti nel testo saranno inseriti direttamente come note a piè pagina.

8.2.2. Architetture a Micro e Mini-servizi

Come già accennato, per "microservizio", si intende una singola componente di un'applicazione che compie un'operazione specifica rispetto ad un ambito applicativo molto articolato e complesso, agente in modo proprietario sui dati e che può essere rilasciata in modo indipendente su macchine diverse con un ciclo di vita autonomo.

La derivazione di tale paradigma dalla SOA consente di darne una definizione più sintetica a partire dai principi base che indentificano un servizio nella SOA stessa:

- Separazione degli ambiti
- Incapsulamento
- Basso accoppiamento

A detti principi base, nel caso di un microservizio, vengono aggiunte le seguenti direttive:

- Indipendenza (deploy & Scaling)
- Singola responsabilità
- Ownership esclusiva propri dati
- Non pubblicazione diretta di interfacce per uso esterno

In INAIL DCOD al momento non si ha l'obiettivo di applicare il concetto di "Architettura a Microservizi" in senso esclusivo e diretto, poiché la stessa può essere di difficile attuazione rispetto alla realtà del parco applicativo esistente in Istituto, ma se ne cercherà di sfruttarne i benefici sulle applicazioni ragionando in termini di miniservizi.

Per "miniservizio", si intende un insieme di operazioni facenti parte di un ambito funzionale omogeneo. Può anche essere inteso come un aggregato di "microservizi" in senso stretto contenuti in un unico docker container, un insieme di componenti autonomi che possono rappresentare un insieme di funzionalità di uno specifico ambito.

Condividendo la parentela con i servizi SOA, anche le caratteristiche di un miniservizio possono essere schematizzate a partire dai principi base SOA, aggiungendo le seguenti indicazioni:

- Indipendenza (deploy & Scaling)



- Componente di un'applicazione
- Con responsabilità verticale (contiene tutte le funzionalità di un singolo ambito)
- Ownership esclusiva propri dati in caso di gestione di stato persistente
- Espone API request/response

La scelta della realizzazione di micro o miniservizi dipenderà strettamente dal contesto di business e dalla tipologia delle Applicazioni che tali micro o miniservizi dovranno comporre.