



Ministero della Salute

Direzione Generale del Sistema Informativo e Statistico
Sanitario

Architetture dell'infrastruttura del Sistema Informativo Sanitario Nazionale del Ministero della Salute



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

SOMMARIO

1	INTRODUZIONE.....	3
2	CONTESTO TECNICO: LE ARCHITETTURE DEL SISTEMA INFORMATIVO SANITARIO NAZIONALE.....	4
2.1	<i>L'architettura logica.....</i>	<i>4</i>
2.2	<i>L'architettura applicativa.....</i>	<i>14</i>
2.3	<i>La piattaforma tecnologica.....</i>	<i>16</i>
2.4	<i>L'infrastruttura tecnica di riferimento.....</i>	<i>25</i>
2.5	<i>Raggruppamenti omogenei dei sistemi - Le isole.....</i>	<i>32</i>
2.6	<i>Le caratteristiche statiche e dinamiche del SIS-N.....</i>	<i>36</i>



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

1 INTRODUZIONE

Il presente documento descrive le architetture nelle diverse viste del Sistema Informativo Sanitario Nazionale del Ministero della Salute.

Dopo una breve parte introduttiva tali viste vengono presentate nelle quattro componenti principali (l'architettura logica, l'architettura applicativa, la piattaforma tecnologica e l'infrastruttura tecnica), al fine di illustrare in modo dettagliato lo scenario attuale in termini di "AS IS".



2 CONTESTO TECNICO: LE ARCHITETTURE DEL SISTEMA INFORMATIVO SANITARIO NAZIONALE

Il Sistema Informativo Sanitario Nazionale (SIS-N) è un sistema informativo unitario, basato sulla cooperazione e l'integrazione dei diversi sistemi informativi gestiti in piena autonomia dalle singole amministrazioni regionali e locali, inteso quale strumento essenziale per migliorare la fruizione dei servizi da parte dei numerosi soggetti coinvolti.

L'attuale architettura del SIS-N, in continua evoluzione, è il risultato di una profonda revisione che ha portato, attraverso un periodo di sostanziali mutamenti ed evoluzioni in tutte le sue componenti, ad adeguarla ai requisiti di tipo funzionale, normativo e tecnologico da parte dei numerosi soggetti coinvolti, assicurando nel contempo la condivisione e la sicurezza del patrimonio informativo del Sistema Sanitario Nazionale.

Il disegno architettuale è basato sugli attuali standard *de iure* e *de facto*, in piena aderenza rispetto alle linee guida indicate dagli organismi competenti in materia di informatizzazione della Pubblica Amministrazione.

Nei paragrafi seguenti viene presentato l'attuale contestotecnico (modelli architetture, soluzioni, prodotti software, infrastrutture tecnologiche, ecc.), attraverso una descrizione strutturata su quattro livelli:

- **l'architettura logica di riferimento:** descrive il sistema dal punto di vista delle componenti logiche che lo compongono e mostra le relazioni che intercorrono tra esse;
- **l'architettura applicativa:** descrive la strutturazione in componenti logiche delle applicazioni sviluppate;
- **la piattaforma tecnologica:** esplicita i prodotti utilizzati e le soluzioni software per realizzare le componenti descritte nell'architettura logica;
- **l'infrastruttura tecnica:** illustra l'organizzazione e le componenti dell'infrastruttura necessaria al supporto delle funzionalità erogate e del software installato.

Vengono sinteticamente descritte tutte le componenti infrastrutturali del SIS-N, secondo lo schema sopra riportato, rimandando agli specifici allegati per le descrizioni di maggior dettaglio.

2.1 L'ARCHITETTURA LOGICA

Le linee guida che hanno portato alla realizzazione dell'attuale modello architetture sono scaturite sostanzialmente dall'esigenza di disaccoppiare la logica di business delle applicazioni dalle evoluzioni tecnologiche, di interagire con facilità con altri sistemi e tecnologie esistenti sul mercato e di aderire ai principali standard vigenti, con uno sguardo particolare alle indicazioni provenienti dall'evoluzione normativa ed in particolar modo dalle linee guida AGID, soprattutto per quanto concerne l'impiego di prodotti "open source" rispetto a quelli proprietari.

Si è quindi realizzata un'architettura "trasversale", mediante un insieme di componenti architetture predisposti per erogare una serie di servizi comuni alle singole applicazioni. Su tali componenti si basa gran parte delle applicazioni del SIS-N, che possono così contenere la sola logica applicativa e risultano inoltre meglio disaccoppiate dalle specificità dell'infrastruttura



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

tecnologica adottata. Tale modello è rappresentato nella successiva Figura 1 dai sottosistemi ricompresi nell'area tratteggiata; per completezza, sono presenti anche alcuni sistemi indipendenti e realizzati con architetture diverse o facenti uso di soluzioni e/o prodotti ulteriori rispetto al modello trasversale citato (ad esempio il Sistema Informativo Trapianti/Sistema informativo dei servizi trasfusionali (SIT-SISTRA) o il Sistema di Protocollo e gestione documentale).

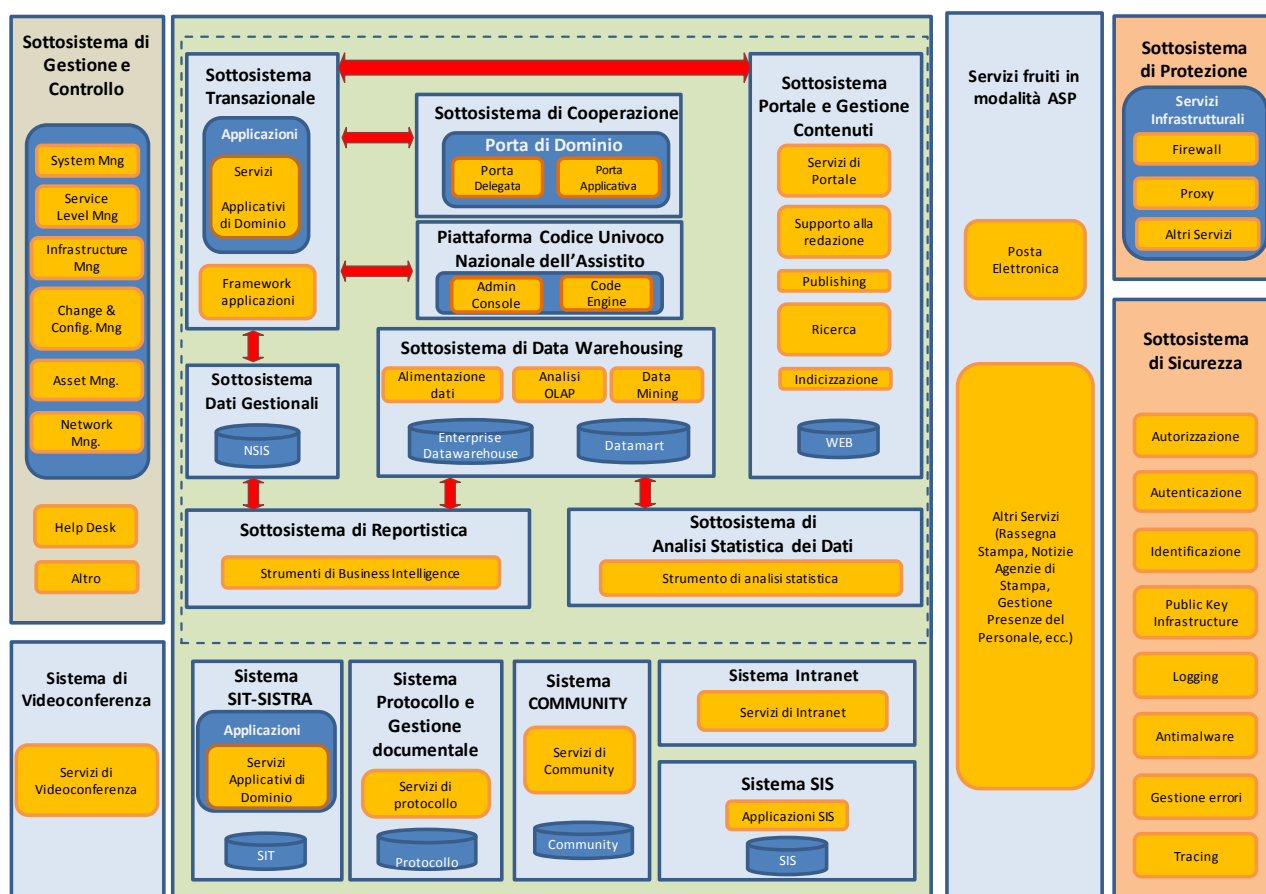


Figura 1: Modello logico dell'Architettura SIS-N 'as-is'

L'architettura logica è pertanto composta dai seguenti sottosistemi (area tratteggiata - NSIS):

- Sottosistema Transazionale;
- Sottosistema Dati Gestionali;
- Sottosistema di Data Warehousing;
- Sottosistema di Cooperazione;
- Sottosistema Portale e Gestione Contenuti;
- Sottosistemi Reportistica e Analisi Statistica dei Dati;
- Sottosistema Piattaforma Codice Univoco Nazionale dell'Assistito

e dai seguenti ulteriori sistemi:



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

- Sistema SIT-SISTRA (Sistema Informativo Trapianti e Servizi trasfusionali);
- Sistema di Protocollo e Gestione documentale;
- Sistema di Community;
- Sistema Intranet;
- Sistema SIS (Applicazioni Sistema Informativo Sanitario);
- Sistema "Polo SBN" (sistema per gestione biblioteca e sistema per cataloghi on line – in corso di realizzazione).

L'architettura SIS-N inoltre comprende i sottosistemi di Protezione e Sicurezza e di Gestione e Controllo che erogano servizi di natura intrinsecamente trasversale al fine di trattare in maniera omogenea problematiche comuni. Sono inoltre rappresentati i servizi erogati in modalità 'ASP' come la posta elettronica o altri servizi come la rassegna stampa o la gestione delle presenze del personale, nonché il servizio di videocomunicazione del Ministero (Sistema di Videoconferenza) ed il servizio di Web Application Firewall (WAF) ospitati in housing presso l'attuale Data Center.

Nel seguito del presente capitolo sono illustrate sinteticamente le componenti elencate; quelle più complesse sono descritte in maggior dettaglio all'interno dei seguenti documenti tecnici:

- Appendice 9 - Architettura SI – Community
- Appendice 10 - Architettura SI – Cooperazione
- Appendice 11 - Architettura SI – Datawarehousing
- Appendice 12 - Architettura SI – Intranet
- Appendice 13 - Architettura SI - Portale e Gestione Contenuti
- Appendice 14 - Architettura SI – Sicurezza
- Appendice 15 - Architettura SI - SIT SISTRA
- Appendice 16 - Architettura SI - Transazionale e Dati Gestionali
- Appendice 17 - Architettura Piattaforma CUNA

2.1.1 Il Sottosistema Transazionale

Il sottosistema Transazionale fornisce i servizi necessari alle applicazioni che richiedono una stretta interazione utente/sistema. In genere si tratta di applicazioni che permettono l'inserimento e la cancellazione di nuove informazioni, o semplici elaborazioni sui dati inseriti. La quantità dei dati trattati non è particolarmente estesa, ma è data particolare importanza agli aspetti di velocità nella risposta del sistema e alla transazionalità che deve essere garantita per ogni operazione eseguita dall'utente. Tale sottosistema costituisce il **punto unificato di accesso** per l'insieme di informazioni potenzialmente a disposizione nel sistema.

I servizi offerti dall'architettura transazionale si possono racchiudere in servizi di:

- **Front End e Presentazione:** realizzano le interfacce presentate all'utente tramite le diverse tipologie di dispositivi (tipicamente in tecnologia internet) e gestiscono: il *Layout*, in relazione alle caratteristiche del canale con il quale l'utente sta interagendo; la *Navigazione*, che supporta il percorso fra i diversi steps; la *Sessione*, che consente di mantenere il contesto durante la navigazione e i *Dispositivi*, che mascherano alle applicazionile peculiarità dello specifico dispositivo.
- **Applicazioni:** realizzano la logica di business dei processi automatizzati garantendo adeguati tempi di risposta e la transazionalità delle operazioni eseguite dall'utente.



2.1.2 Il Sottosistema Dati Gestionali

Il sottosistema Dati Gestionali è preposto alla gestione dei dati relativamente alle componenti gestionali. Tale sottosistema è quindi utilizzato dalle applicazioni del sottosistema Transazionale, dalle componenti del sottosistema di Gestione Contenuti e dalle applicazioni batch. E' la fonte primaria di alimentazione del sottosistema di Data Warehousing, ma è logicamente disaccoppiato da esso.

2.1.3 Il Sottosistema Data Warehousing

Il sottosistema Data Warehousing permette l'esecuzione di applicazioni per analisi complesse su elevate quantità di dati. Le sorgenti da cui si attingono i dati d'interesse spesso sono formate da un insieme di sistemi informativi interni al Servizio Sanitario Nazionale, e da sistemi esterni di particolare interesse (ad esempio le società farmaceutiche, o anagrafi provenienti da altri ministeri). Il sottosistema di Data Warehousing, che ricopre gran parte dell'architettura tecnologica, deve consentire l'estrazione dei dati sia dal sottosistema Dati Gestionali sia da altre fonti esterne. Inoltre deve garantire la correttezza delle elaborazioni svolte. Le sue funzioni infatti devono essere raggiungibili tramite qualsiasi tipologia di *Browser* o applicazioni del SIS-N da parte degli utenti interni ed esterni all'Amministrazione.

Il modello adottato prevede che il Data Warehouse sia strutturato in due livelli:

- l'*Enterprise Data Warehouse (EDW)* che contiene i dati storicizzati al massimo livello di dettaglio;
- i *Data Mart (DM)* che contengono un sottoinsieme di dati normalmente molto aggregati e disegnati per uno specifico ambito di analisi.

Nel sottosistema di Data Warehousing, sono comprese le funzioni ed i relativi strumenti sia per il caricamento e pulizia dei dati (ETL) e sia per la loro fruizione diversificati in relazione alla tipologia di analisi e in particolare per attività di:

- query e reporting
- OLAP
- data mining

2.1.4 Il Sottosistema di Cooperazione

L'architettura di cooperazione è il "tessuto connettivo" che mette in comunicazione, attraverso i corrispondenti Sottosistemi di Cooperazione che la compongono, i diversi enti che partecipano a SIS-N.

Il Sottosistema di Cooperazione ha un duplice compito:

- supportare la comunicazione tra le applicazioni di un ente e quelle presenti in sistemi informativi di altri enti e che collaborano nell'erogazione di servizi.
- interfacciare fra loro applicazioni realizzate con tecnologie diverse che le rendono non integrabili in modo nativo.

Tale sottosistema ha l'obiettivo di permettere l'esecuzione di processi complessi su differenti sistemi informativi, garantendo il controllo del flusso delle attività componenti il processo stesso. La Porta Di Dominio di tale sottosistema ha la caratteristica di poter effettuare cooperazione applicativa con enti sia pubblici che privati, e quindi senza l'utilizzo del protocollo e-Gov. E' inoltre integrata con il sistema di autenticazione ed autorizzazione del SIS-N e conforme sia agli standard di sicurezza OASIS 1.0 che a quelli della busta e-Gov 1.1. Dal punto di vista tecnologico è basata su software open source "JBOSS – Redhat".



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

2.1.5 Il Sottosistema Portale e Gestione Contenuti

Il Portale del Ministero rende disponibili contenuti e servizi on line di tipo pubblico, utilizzando il sottosistema di pubblicazione dei contenuti e banche dati residenti alimentate dai sistemi gestionali tramite appositi servizi applicativi. Inoltre integra contenuti on line realizzati anche esternamente all'architettura del Ministero: tramite appositi servizi applicativi è integrata la sezione della normativa sanitaria e della rassegna stampa. Sono anche presenti strumenti di forum, newsletter e iscrizione a convegni.

La componente di Gestione dei contenuti ha il compito di supportare il ciclo di vita dei medesimi, nei canonici passi di *redazione*, *validazione*, *publishing*, *categorizzazione*, e di integrarli con i servizi applicativi del sottosistema transazionale, puntando così ad ottenere il maggior valore possibile dall'aggregazione. Consente alle redazioni di procedere con la predisposizione e la pubblicazione di materiale sul portale web del Ministero ed in particolare:

- creare nuovi contenuti;
- effettuare ricerche nel data base dei contenuti;
- inserire i contenuti nelle pagine del sito;
- visualizzare l'anteprima delle pagine coi nuovi contenuti;
- gestire il workflow di pubblicazione;
- pubblicare pagine e contenuti sui vari canali distributivi.

2.1.6 I Sottosistemi Reportistica e Analisi Statistica dei dati

Il sottosistema di reportistica fornisce elaborazioni preconfigurate (report) a oltre 3.000 utenti, sia interni al Ministero della Salute che esterni.

La reportistica si riferisce a 25 differenti ambiti, per un totale di oltre 1.000 report disponibili a sistema. In genere l'accesso ai report avviene tramite le applicazioni, nelle quali viene gestita la profilazione degli utenti. Solo ad alcuni di questi è consentito l'accesso nativo al sistema di reportistica (Business Objects); questi ultimi sono in genere utenti più avanzati, con privilegi di modifica dei report a sistema per l'effettuazione di analisi più mirate.

Le interrogazioni vengono effettuate su tutte le basi di dati dell'Amministrazione (EDW, Gestionale, Data Mart, SIT, SIS) attraverso, quando possibile, un sistema appositamente dedicato (Data Mart); su di esso, utilizzando prodotti software di ETL (Extraction, Transformation & Loading) vengono trasferiti i dati dai sistemi operazionali (Gestionale, SIT, SIS) e di Data Warehouse (EDW).

Il sottosistema di analisi statistica serve utenti con particolari esigenze di analisi dei dati più approfondite rispetto al sistema di reportistica.

2.1.7 La Piattaforma Codice Univoco Nazionale dell'Assistito

La "Piattaforma Codice Univoco Nazionale dell'Assistito" è stata realizzata con la finalità di rispondere pienamente ed integralmente alla regolamentazione delle procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio Sanitario Nazionale.

La piattaforma ha quindi, come requisito fondamentale, quello di essere un sistema di sicurezza che, dato in ingresso un codice fiscale CFX dalle amministrazioni periferiche, produca sempre in uscita un codice univoco CUX, ovvero che sia invariante dal luogo geografico, dal contesto informativo e dal momento temporale di effettuazione di tale operazione, al fine di



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

garantire il cosiddetto "record linkage" che abilita la ricostruzione dei percorsi sanitari dell'assistito senza soluzione di continuità.

Per quanto attiene il sistema di sicurezza, si è prevista l'applicazione combinata di diverse soluzioni tecnologiche (cifratura, autenticazione forte, sistemi infrastrutturali dedicati, ecc.) e di processo (elaborazioni automatizzate con accessi controllati e per le sole finalità di gestione e manutenzione), volte a minimizzare i rischi di violazione dei dati.

La "Piattaforma Codice Univoco Nazionale dell'Assistito" si avvale, per la funzionalità di generazione del CUNA, di un dispositivo denominato Hardware Security Module ("HSM"), che presenta le seguenti caratteristiche:

- Prevede una gestione esclusivamente automatizzata delle procedure di generazione, assegnazione ed utilizzo del codice univoco;
- Dispone di algoritmi di hashing e di cifratura simmetrica o asimmetrica volti all'elaborazione del CUNA a partire dal codice univoco non invertibile (CUNI) ed alla cifratura e decifratura del codice fiscale per le deroghe concesse dal decreto;
- Genera, memorizza e protegge per l'intero ciclo di vita, le chiavi che consentono il calcolo del codice univoco e la cifratura e decifratura dei codici fiscali per le deroghe concesse dal decreto;
- Prevede l'autenticazione forte per gli amministratori della piattaforma che accedono al sistema esclusivamente per finalità di gestione e manutenzione (il sistema di autenticazione è integrato con il sistema di autenticazione del NSIS) e per gli utenti autorizzati ad accedere direttamente od indirettamente alle funzionalità di hashing, cifratura e decifratura.

Nella figura seguente è rappresentato lo schema dell'architettura logica della piattaforma.

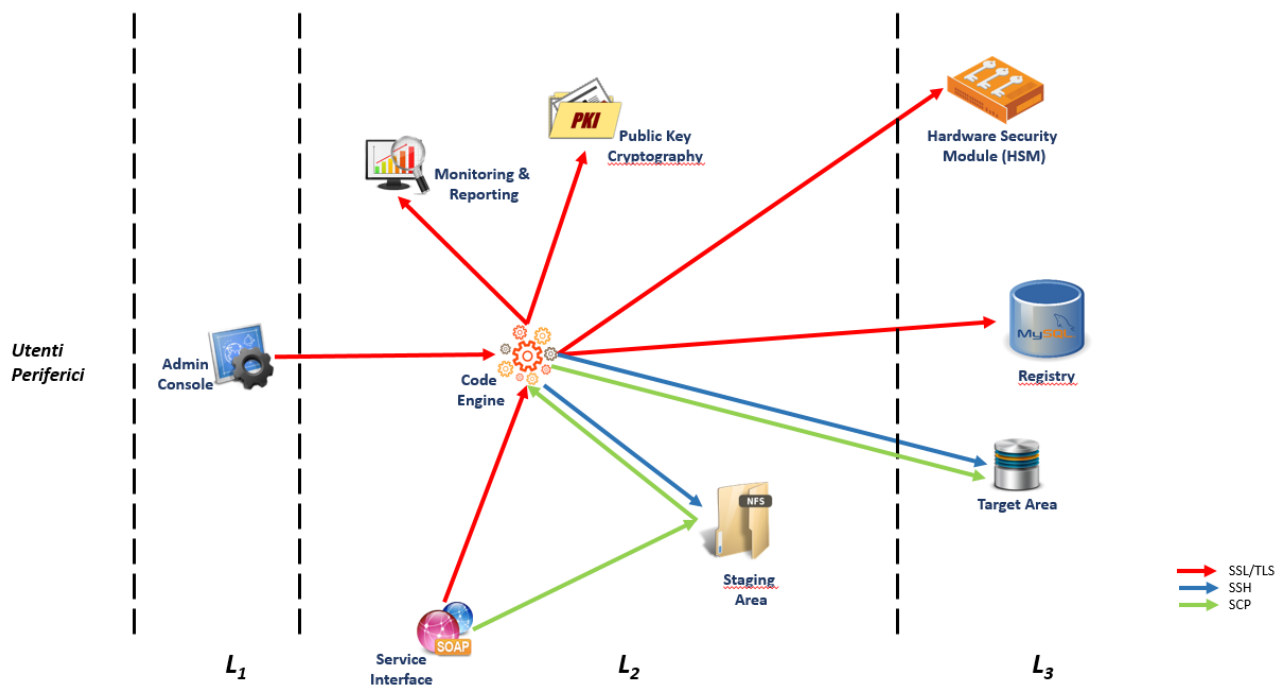


Figura 2: Schema architettura logica della piattaforma



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

2.1.8 Gli altri sistemi

Come specificato in precedenza, oltre alle applicazioni realizzate secondo il modello trasversale sopra descritto, vi sono alcuni sistemi che afferiscono a diversi modelli architetturali. Pur essendo comunque basati su tecnologia Internet, la sostanziale differenza rispetto a quanto precedentemente esposto risiede nel fatto che le corrispondenti applicazioni non utilizzano le componenti infrastrutturali trasversali, ma realizzano al loro interno tutti i servizi di cui necessitano, quali ad esempio data layer, controllo degli accessi, logging, etc.. Esse non presentano invece sostanziali differenze dal punto di vista dell'architettura applicativa essendo comunque sviluppate secondo uno schema che mantiene logicamente separati i tre livelli elaborativi (Presentazione, logica di business ed accesso ai dati).

2.1.9 Il Sistema SIT-SISTRA (Sistema Informativo Trapianti e Servizi Trasfusionali)

2.1.9.1 Sistema Informativo dei Trapianti (SIT)

Il SIT, nato per dare supporto informatico alle attività della Rete nazionale dei trapianti, garantendo la tracciabilità e la trasparenza dell'intero processo "donazione - prelievo - trapianto", consente lo svolgimento delle seguenti attività:

- notifica tempestiva della presenza di un potenziale donatore in una rianimazione;
- tracciatura del livello di rischio del donatore dalla fase che precede il prelievo degli organi alle fasi successive al trapianto;
- gestione delle iscrizioni in lista unica di attesa e della raccolta standardizzata dei dati clinici del paziente durante il periodo di permanenza in lista;
- caratterizzazione delle iscrizioni in lista unica con particolari requisiti di urgenza, o sul protocollo degli anticipi;
- caratterizzazione delle iscrizioni in lista unica su protocolli nazionali (Pediatrico, Iperimmuni) con relativa gestione e allocazione di organi secondo quanto previsto dai protocolli corrispondenti;
- gestione delle attività di donazione e trapianto, da cadavere e da vivente, registrazione del follow-up dei trapianti effettuati;
- raccolta delle dichiarazioni di volontà di donazione di organi e tessuti da parte dei cittadini;
- registrazione del flusso dei dati sulle attività di donazione e prelievo di organi e tessuti, di trapianto di organi e di distribuzione di tessuti alle banche certificate;
- registrazione dei dati semestrali del registro cerebrolesi trasmessi dai coordinamenti per ogni unità di rianimazione;
- gestione del registro del trapianto da vivente;
- accettazione formale, da parte delle Banche Tessuti delle donazioni offerte loro e importazione all'interno dei propri sistemi informativi del CUD della donazione di loro pertinenza;
- gestione delle informazioni inerenti alle fasi perioperatorie del trapianto utili alla valutazione della qualità dei trapianti.

2.1.9.2 Sistema Informativo dei Servizi Trasfusionali (SISTRA)

Il SISTRA è stato realizzato dal Ministero della Salute, sulla base delle esigenze del Centro Nazionale Sangue in collaborazione con le Regioni e Province Autonome, relativamente alla definizione, raccolta e elaborazione dei flussi informativi relativi alle seguenti macro-aree:

- anagrafiche strutture che partecipano all'attività trasfusionale;
- programmazione e pianificazione del fabbisogno nazionale;
- raccolta e utilizzo del sangue e dei suoi componenti;



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

- produzione e utilizzo di farmaci plasma derivati;
- emovigilanza e sorveglianza epidemiologica dei donatori;
- compensazione emocomponenti e plasma derivati;
- informazioni concernenti la qualità dei processi e dei prodotti/servizi.

Sono previste due diverse modalità di trasmissione delle informazioni verso SISTRA:

- modalità interattiva, che consente l'inserimento delle informazioni mediante collegamento al sito e compilazione online delle schermate di notifica. Questa modalità è disponibile per tutti gli utenti, in particolare per i Servizi Trasfusionali e le Strutture Regionali di Coordinamento che non dispongono di un proprio sistema informativo compatibile con il sistema nazionale SISTRA;
- attraverso lo scambio di file XML (eXtensible Markup Language), strutturati secondo uno schema reso noto alle regioni tramite la pubblicazione dei relativi XSD (XML Schema Definition). Questa modalità di interazione consente alle regioni che dispongono di un proprio sistema informativo di inoltrare i dati preventivamente estratti dal proprio sistema.

Per l'invio dei file è disponibile un'apposita funzione di upload all'interno di SISTRA e specifici servizi applicativi (web services) per la raccolta e la registrazione dei flussi informativi. Il sistema utilizza per la connettività i servizi del Sistema Pubblico di Connettività (SPC) e l'interazione tra Amministrazioni si basa sul modello di cooperazione del SPC con requisiti di elevata sicurezza, intesa come capacità sia di mantenere l'integrità dei dati sia di garantire la loro riservatezza e la continuità di servizio.

2.1.10 Il Sistema di Protocollo e Gestione documentale

Il Sistema di Protocollo e Gestione documentale realizza le funzioni di protocollazione elettronica ai sensi del DPR 445/2000 e s.m.i. e gestisce oltre 20 registri di protocollo integrati con una o più caselle di Posta Elettronica Certificata. Tale sistema realizza inoltre la trasmissione elettronica dei documenti che, se pervenuti in forma cartacea, sono preventivamente dematerializzati, la classificazione degli stessi e la gestione dei fascicoli elettronici. Esso viene allineato, tramite apposite funzionalità, rispetto alle variazioni organizzative dell'Amministrazione. Il sottosistema è interoperabile, via web services, con alcuni sottosistemi del SIS-N per assicurare la corretta gestione e conservazione della documentazione amministrativa.

2.1.11 Il Sistema Intranet

Il Sistema Intranet del Ministero costituisce la "Bacheca elettronica" e la scrivania virtuale del personale dell'Amministrazione. Fornisce una serie di servizi on line. In particolare è disponibile la rubrica telefonica che, tramite servizi applicativi, accede al sottosistema gestionale per l'interrogazione dei dati logistici e dell'organizzazione del personale. Inoltre sono disponibili funzionalità che, previa autenticazione, consentono l'inserimento di avvisi su bacheche (sindacali e del dopolavoro) con contestuale invio di mail informative a tutto il personale e documenti su diverse sezioni.

2.1.12 Il SistemaCommunity

Il Sistema di Community soddisfa l'esigenza di un ambiente web di condivisione di contenuti e documentale per gruppi di individui che debbono condividere e scambiarsi materiali di lavoro per esigenze istituzionali (Community web).

Per la gestione e fruizione delle funzionalità del sistema viene utilizzato il framework Drupal opportunamente personalizzato e contestualizzato per renderlo maggiormente aderente alle esigenze degli utenti dell'Amministrazione.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Tale framework dispone di funzionalità di base che consentono l'implementazione di istanze di community web concernenti gli ambienti di condivisione e scambio documentale circoscritti a bacini di utenti ben delimitati nei quali l'accesso è consentito unicamente a coloro che dispongono delle credenziali di accreditamento (user-id e password). Il sistema è stato opportunamente integrato con il Sottosistema di Sicurezza.

2.1.13 Il Sistema SIS (Sistema Informativo Sanitario)

Il sistema SIS comprende alcune, residuali, applicazioni eterogenee, generalmente antecedenti all'architettura trasversale descritta in precedenza. In particolare, si segnalano i sistemi per la raccolta delle timbrature (personale e visitatori), per la successiva trasmissione dei dati a due distinte applicazioni: 'Gerip Web' di Data management che, in modalità ASP, gestisce le presenze del personale dell'Amministrazione presso le sedi centrali e periferiche, e 'Check and In' che gestisce il controllo accessi presso le sedi.

2.1.14 Il Sottosistema di Sicurezza

Il sottosistema di sicurezza realizza le funzionalità di gestione delle utenze e delle risorse informatiche (applicazioni, funzionalità) da proteggere, offrendo i propri servizi in particolare all'insieme dei sistemi trasversali sopra descritti. Tali servizi sono brevemente elencati e descritti nel seguito.

■ Registrazione / Identificazione

Il servizio fornisce gli strumenti per effettuare un controllo capillare dell'accesso alle risorse tramite l'identificazione degli utenti e la loro registrazione all'interno del sistema. Dal punto di vista utente vi è garanzia di semplicità d'uso e di confidenzialità ed integrità delle informazioni fornite.

■ Autenticazione

I Servizi di Autenticazione consistono nel verificare la veridicità delle credenziali inserite da un utente. Attualmente sono supportate le seguenti modalità:

- ▶ autenticazioni basate sulla Conoscenza: l'utente è colui che dice di essere poiché conosce qualcosa (ad esempio una password);
- ▶ autenticazioni basate su Token: l'utente è colui che dice di essere poiché possiede qualcosa (ad esempio una smartcard).

■ Single Sign-On

La modalità di accesso implementata è di tipo 'Single Sign-On', in base alla quale l'utente si autentica una sola volta per accedere a tutte le applicazioni per il cui uso è stato abilitato.

■ Autorizzazione

Il servizio di autorizzazione consente di definire e gestire un insieme di regole che indicano sia gli oggetti cui ha accesso ogni utente, sia il tipo di accesso cui l'utente ha diritto relativamente a tali oggetti. Tale servizio ha il compito di effettuare l'autorizzazione di primo livello (l'utente è autorizzato a utilizzare una determinata applicazione/funzione), lasciando eventuali autorizzazioni di secondo livello (l'utente nell'ambito dell'uso di una determinata funzione è autorizzato ad accedere a un particolare dato) alle singole applicazioni.

■ Cifratura



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Il servizio di cifratura utilizza diversi algoritmi simmetrici e asimmetrici e può operare sia a livello dei dati (cifratura permanente delle informazioni) che del canale trasmissivo (creazione di un canale cifrato fra la postazione utente e il server).

■ Firma Digitale

Il servizio consente l'apposizione e la verifica di una firma digitale basandosi sugli standard vigenti, senza imporre vincoli sull'uso di una specifica soluzione offerta da una particolare *Autorità di Certificazione*.

■ Logging

Il servizio di Logging registra eventi di particolare interesse per la sicurezza, permettendo di identificare eventuali rischi in modo unificato e consentendo di eseguire procedure di analisi notevolmente semplificate. Inoltre, ove necessario, è richiamato anche dalle applicazioni, in modo da centralizzare tutte le informazioni sugli accessi al sistema.

Nella figura seguente è rappresentato lo schema dell'architettura logica del sistema di controllo degli accessi.

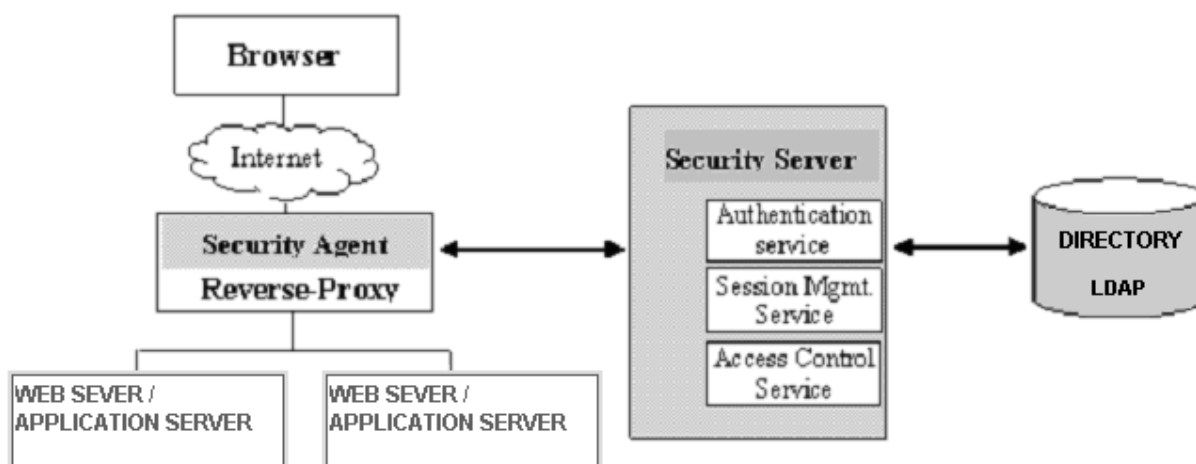


Figura 3: Schema architettura logica del sistema di controllo degli accessi

Vi sono, inoltre, alcuni servizi trasversali messi a fattor comune di tutte le applicazioni, che svolgono una serie di operazioni accessorie alla logica di business, ma che possono essere convenientemente centralizzate al fine di assicurarne l'omogeneità (come nel caso del controllo degli errori), ottimizzare il reperimento di informazioni e analizzare gli eventi, come nel caso del logging centralizzato.

I principali servizi disponibili in questa area sono.

- Logging
- Tracing
- Gestione Errori

2.1.15 Il Sottosistema di Protezione

Il Sottosistema di protezione eroga trasversalmente al SIS-N i servizi delegati a proteggere in modo sicuro le risorse e i dati dell'Amministrazione.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

2.1.16 Il Sistema di Videoconferenza

Il sistema di Videoconferenza consente agli utenti dell'Amministrazione la comunicazione in tempo reale ed in modalità interattiva con utenti (dell'Amministrazione o meno) dislocati remotamente su postazioni di lavoro o in sale attrezzate per videoconferenze.

Tale sistema si avvale di un tool per prenotazioni via web. Attraverso tale meccanismo gli utenti inseriscono la richiesta per poter effettuare una videoconferenza, corredata da tutte le informazioni necessarie al suo svolgimento (data, ora, partecipanti, eventuali presentazioni da effettuare nel corso della videoconferenza, etc.). La richiesta viene presa in carico dal gruppo di gestione che si occupa di organizzare nel dettaglio sia la fase di test che la video conferenza effettiva, definendo sempre via web un identificativo della videoconferenza che via mail raggiunge tutti i partecipanti, fornendo un promemoria dell'evento e le informazioni necessarie per collegamento. Il sistema di Videoconferenza dell'Amministrazione è inserito in housing nell'infrastruttura CED. Per una descrizione dettagliata si rimanda al successivo par. 2.3.14.

2.1.17 Il Sistema Web Application Firewall

Il sistema Web Application Firewall è ospitato in housing presso il Data Center ed integrato nella sua infrastruttura. Per una descrizione dettagliata si rimanda al successivo par. 2.3.15

2.1.18 Il Sistema "Polo SBN "

La piattaforma prevede, come descritto più avanti, la virtualizzazione, il BC/DR, la componente "SBNWeb" (gestionale di biblioteca) e la componente OPAC (On-line public access catalogue). Ciascuna componente prevede il livello di http /application server ed il livello di DB. Si rimanda al successivo paragrafo 2.3.17 per maggior dettaglio.

.

2.1.19 Il Sistema "MDS Drive"

Il Sistema MdS Drive è stato realizzato con la finalità di offrire agli utenti dell'Amministrazione una soluzione open source realizzata sul Cloud privato del Ministero per la conservazione e condivisione di file online. Si rimanda al successivo paragrafo 2.3.16 per maggior dettaglio.

2.2 L'ARCHITETTURA APPLICATIVA

L'architettura applicativa descrive il modello logico con cui sono realizzate le applicazioni.

Le applicazioni sono sviluppate nell'ambito dell'infrastruttura del SIS-N e condividono quindi dal punto di vista dell'architettura logica il modello generale trasversale previsto per il sistema informativo nel suo complesso, presentato nel paragrafo precedente.

L'architettura applicativa prevede applicazioni web strutturate sui tre seguenti livelli:

- **presentazione (front-end)**, che gestisce il colloquio con l'utente, facendosi carico dei controlli sintattici sui dati e delle diverse modalità di fruizione in relazione al canale di comunicazione usato.
- **applicazione o logica di business**, dove vengono effettuati i controlli semantici sui dati e si svolgono le elaborazioni che realizzano i diversi processi informatizzati. Tale livello deve essere del tutto indipendente dalle modalità di presentazioni dei dati all'utente e dalle peculiarità di memorizzazione dei dati.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

- **accesso ai dati**, che sovrintende tutte le operazioni di scrittura e lettura dei dati, garantendo per la sua centralità il rispetto delle medesime regole nell'accesso ai dati per le diverse applicazioni.

I diversi livelli, oltre ad essere logicamente separati, lo sono anche fisicamente, essendo ospitati su server diversi, collocati in LAN distinte e separati dai sistemi integrati di firewall.

2.2.1 Il livello Presentazione

Il livello Presentazione gestisce il colloquio con l'utente, facendosi carico dei controlli sintattici sui dati e delle diverse modalità di fruizione in relazione al canale di comunicazione usato. Da quelli classici (PC con Web Browser) a quelli alternativi (PDA, Wireless, Voce, etc).

Nell'ambito di tale livello viene effettuata l'interazione con il sistema di controllo degli accessi che è centralizzato e realizza un single sign-on integrato con tutte le applicazioni. Il controllo degli accessi svolge funzioni di *Identificazione ed Autenticazione* degli utenti, basandosi, in relazione ai requisiti specifici delle singole applicazioni, sia su meccanismi di user id e password, che su smart-card. Superata la fase di identificazione ed autenticazione il controllo degli accessi può, se previsto, effettuare verifiche autorizzative di primo livello prima di passare il controllo all'applicazione richiesta.

L'applicazione richiamata riceve l'identità dell'utente ed un insieme di informazioni relative al suo profilo, con cui effettua eventuali ulteriori verifiche di autorizzazione (autorizzazioni di secondo livello). Naturalmente non ripete i controlli di identificazione dell'utente.

2.2.2 Il livello applicazione

Tale livello eroga tutti i servizi forniti dal SIS-N, indipendentemente dal fatto che questi siano richiesti da utenti interni o esterni al sistema o che siano invocati tramite interfacce di cooperazione direttamente da processi attivi su altri sistemi informativi.

Tali servizi sono inoltre organizzati in modo modulare al fine di favorire il riuso e quindi tutte le possibili economie di scala realizzabili fra le diverse applicazioni.

In particolare, a questo livello di descrizione è importante sottolineare le seguenti caratteristiche dei componenti software che realizzano i servizi.

- Sono dedicati esclusivamente alla implementazione della logica elaborativa, non hanno alcuna conoscenza delle caratteristiche peculiari degli strati di presentazione e accesso ai dati a cui si interfacciano.
- Adottano per il colloquio con le altre componenti dell'applicazione interfacce standard per il colloquio con il livello di presentazione e quello di accesso ai dati.
- In virtù delle caratteristiche precedenti sono invarianti rispetto alla modalità di attivazione, nel senso che possono essere invocati indifferently sia da componenti di presentazione di tipo interattivo e quindi integrati nel portale, sia da componenti di interfaccia di tipo Web Services afferenti al sottosistema di cooperazione.
- Sono in grado a loro volta di attivare servizi resi disponibili da sistemi informativi esterni, o tramite interfacce dedicate alle applicazioni legacy interne al sistema o tramite componenti centralizzati dedicati all'integrazione verso i Sistemi sviluppati in tempi precedenti. Quest'ultima funzionalità attribuisce ai servizi un ruolo assolutamente rilevante nel rendere disponibili all'esterno, tramite modalità di cooperazione standard le applicazioni già presenti. In questo modo è sufficiente incapsulare l'applicazione legacy con uno strato software che ne converte l'input e l'output in formato XML per trasformarla



in un servizio che risulti aperto alla cooperazione e invocabile dalle componenti di front end.

- Sono sviluppati, ove non sussistano problemi di integrazione con l'ambiente pregresso, con linguaggi portabili, come Java, e quindi non legati a specifiche piattaforme tecnologiche.
- Sono, ove necessario, classificati e catalogati, in ottica Web Services, tramite la registrazione nel catalogo dei servizi, che consente la pubblicazione delle specifiche del servizio. Possono essere eseguiti sotto il controllo di strumenti che forniscono il supporto della transazionalità TP Monitor, MOM (Message Oriented Middleware) o Workflow, per garantire la congruenza certa delle operazioni di aggiornamento dei dati trattati, sia interni al sistema che esterni nel caso di elaborazioni distribuite fra più sistemi.

Poiché molti servizi comuni sono realizzati da componenti trasversali (Logging, Tracing e Gestione Errori), tali funzionalità non vengono naturalmente ripetute nelle applicazioni.

2.2.3 Il Livello di accesso ai dati

A questo livello, oltre ai dati veri e propri, appartengono anche le componenti (metodi) che incapsulano i dati, mascherando verso l'esterno le caratteristiche specifiche della loro struttura. Tali metodi possono essere componenti software a se stanti o integrati nel database (stored procedure). In entrambi i casi adottano con il layer di logica elaborativa un colloquio con protocolli standard come XML o, per il diretto accesso ai dati, il linguaggio SQL mediato tramite gli standard JDBC od ODBC nel caso di componenti esterni al Database, ovvero attraverso meccanismi di stored procedure.

L'uso delle stored procedure resta in ogni caso limitato alla realizzazione di metodi di incapsulamento dei dati.

2.3 LA PIATTAFORMA TECNOLOGICA

La piattaforma tecnologica descrive i prodotti software utilizzati per realizzare le diverse componenti individuate nell'Architettura Logica.

2.3.1 Il Sottosistema Transazionale

Il front end, la presentazione e le applicazioni che compongono il sottosistema transazionale sono realizzate con componenti java ospitate in application server Red Hat JBoss Enterprise Application Platform. Tali componenti non sono contattabili direttamente dall'utente, ma sono mascherate da reverse proxy Novell Access Gateway.

2.3.2 Il Sottosistema Dati Gestionali

Il sottosistema dati è gestito per la quasi totalità da DBMS Oracle, in configurazione di load balancing, attraverso la componente Oracle RAC 12c. E' presente anche un DB MySQL in load balancing utilizzato nell'ambiente di Community Drupal ed un DB MySQL in load balancing utilizzato nell'ambito della Piattaforma Codice Univoco dell'Assistito. In alcune realtà residuali o per pacchetti applicativi esterni i dati sono gestiti con Microsoft SQLServer.

2.3.3 Il Sottosistema Data Warehousing

Il sottosistema di Data Warehousing è basato sulla tecnologia Oracle per la componente di Database e su tecnologie Oracle e SAP per la componente ETL.



2.3.4 Il Sottosistema di Cooperazione

La Porta Di Dominio è sviluppata in conformità allo standard J2EE ed utilizza componenti standard de facto quali Apache CXF e Hibernate. Il seguente schema descrive l'infrastruttura del componente Porta Di Dominio.

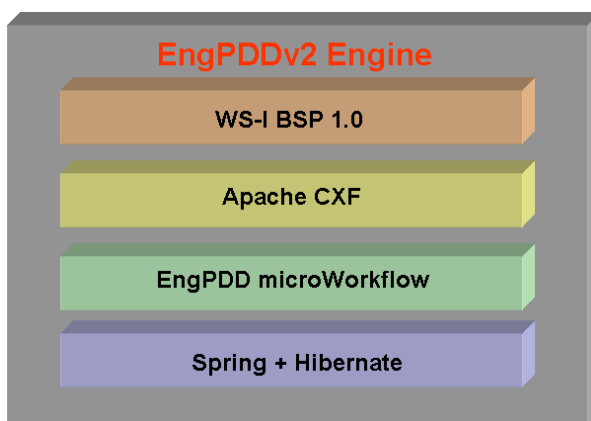


Figura 4: Infrastruttura della porta di dominio

2.3.5 Il Sottosistema Portale e Gestione Contenuti

La gestione dei contenuti e il portale di esposizione verso internet sono realizzati con il prodotto Polymedia di PIKSEL. Il data base utilizzato è Oracle Rac11g. L'Http server per il portale è Apache, mentre l'application server è Tomcat.

2.3.6 I Sottosistemi Reportistica e Analisi Statistica dei dati

Le funzionalità di query e reporting e OLAP sono realizzate tramite il prodotto Business Objects usato prevalentemente nella versione Web (WEBI). Le funzionalità statistiche e di DataMining sono implementate attraverso gli strumenti SPSS e SAS.

2.3.7 La piattaforma Codice Univoco Nazionale dell'assistito

La piattaforma Codice Univoco Nazionale dell'assistito si poggia su una architettura a tre livelli come evidenziato nello schema sottostante.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

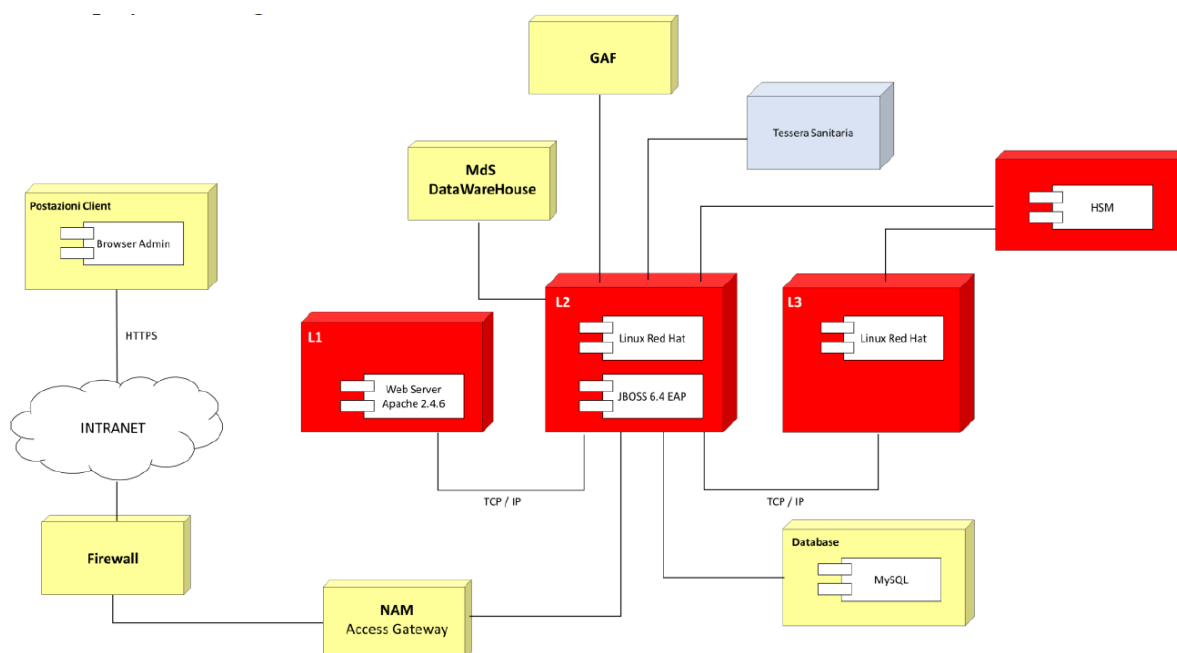


Figura 5: Infrastruttura della piattaforma CUNA

L'estensione dell'attuale infrastruttura NSIS, ai fini di rendere interconnettibili le informazioni a livello nazionale dei sistemi informativi su base individuale del Servizio Sanitario Nazionale, ha previsto l'introduzione di:

- 1) Layer 2 della piattaforma – 2 virtual machine con FileSystem (shared) di tipo NFS. La componente di Application Server su cui sono installate le applicazioni è gestita con il prodotto JBOSS 6.4 EAP;
- 2) Layer 3 della piattaforma – 2 virtual machine con Cluster FileSystem (shared);
- 3) Un dispositivo di tipo Hardware Security Module (HSM) per la componente responsabile della gestione del ciclo di vita di chiavi di cifratura;
- 4) Una componente di Database composta da una istanza HA MySQL Enterprise Edition.

La configurazione, nel suo complesso, è inserita in un ambiente accessibile attraverso il servizio GAF - Gestione Accoglienza Flussi. Il flusso di comunicazione avviene in modalità sicura tramite l'utilizzo del protocollo SSL (Secure Sockets Layer) con autenticazione mutua delle parti tramite l'utilizzo di certificati digitali. La piattaforma Gestione Codice Univoco è anche integrata con il SAA secondo le seguenti caratteristiche:

- Il modulo "Admin Console", deployato nella componente Layer 2, espone le proprie funzionalità attraverso l'autorizzazione ed autenticazione prevista dal SAA. I fruitori della piattaforma, devono pertanto registrarsi e, previa autorizzazione del SAA, accedere tramite un portale di accesso web del NSIS al fine di ottenere il token di autenticazione. L'applicazione, in fase di primo accesso, provvede ad accertare la presenza e la validità del token. Il passaggio da Access Portal verso il modulo viene effettuato attraverso la configurazione di una junction sotto NAM che punta alla componente Admin Console presente in L2.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Le informazioni tecniche di dettaglio relative alla Piattaforma sono documentate all'interno del documento tecnico allegato: ARCHITETTURA TECNICA - Piattaforma Codice Univoco Nazionale Assistito (file "Architettura Piattaforma CUNA").

2.3.8 Il Sistema SIT-SISTRA

Il Sistema SIT-SISTRA è caratterizzato da una architettura ad alta affidabilità, da un ambiente elaborativo completamente separato e dedicato e da elevati livelli di sicurezza per la tutela del corrispondente patrimonio informativo. Tali applicazioni sono basate su architetture standard con utilizzo del formato XML e del modello "business to business", per realizzare la cooperazione applicativa tra organismi diversi. Il sistema è affiancato da un sistema di data warehouse dedicato alle attività di indirizzo e governo del Centro Nazionale Trapianti (CNT), degli uffici di coordinamento regionali della Rete Nazionale Trapianti e del Centro Nazionale Sangue.

La potenza elaborativa è concentrata presso l'attuale Data Center, che fornisce servizi di web, application e data server. Gli apparati sono protetti mediante un sistema firewall e configurati in modo da garantire l'alta affidabilità grazie alla duplicazione di tutte le componenti critiche.

La rete geografica, che collega il CNT e i centri di coordinamento regionali al CED del SIT utilizza la rete SPC su VPN Mpls dedicata e chiusa. Tale rete non è accessibile da sistemi esterni e ha caratteristiche di elevatissima disponibilità grazie alla ridondanza dei collegamenti e degli apparati.

La sicurezza per il sistema SIT è garantita tramite l'autenticazione degli utenti con certificati digitali standard X.509 e smart card conformi allo standard PKCS11, la protezione dei messaggi scambiati (segretezza ed integrità dei dati), il tracciamento degli eventi e il non ripudio della consegna dei messaggi. Sono inoltre attuate tutte le misure di sicurezza logica e fisica a garanzia della disponibilità e riservatezza dei dati gestiti.

L'interazione con i sistemi esterni, quali ad esempio sistemi informativi regionali, che cooperano alla erogazione dei servizi, avviene attraverso la disponibilità di web services realizzati nel SIT-SISTRA e fruibili tramite la rete internet con protocolli SOAP su HTTPs.

L'attivazione dei web services, sia per le funzioni di interrogazione che per quelle di aggiornamento delle informazioni raccolte nel SIT-SISTRA richiede la mutua autenticazione con l'utilizzo di certificati digitali da parte dei sistemi che cooperano nella erogazione dei servizi.

L'ambiente operativo è costituito da:

- Sistema operativo MS Windows 2016
- Web server WebMethods Integration server e MS IIS
- Il Datawarehouse del SIT-SISTRA è integrato nel Datawarehouse del SIS-N
- Un sistema di Posta Elettronica ad uso esclusivo degli utenti del SIT, basato su sistemi dedicati MS Exchange
- Posti di lavoro con sistema operativo MS windows

Le informazioni tecniche di dettaglio relative agli ambienti SIT-SISTRA sono documentate all'interno del documento tecnico allegato: ARCHITETTURA TECNICA - Sistema SIT-SISTRA (file "Architettura SI-SIT SISTRA").

2.3.9 Il Sistema Protocollo e Gestione documentale

Il sistema per la gestione del protocollo informatico utilizza la piattaforma DOCSPA di NTT DATA Italia, adeguatamente personalizzata in base alle esigenze dell'Amministrazione. Tale sistema documentale è utilizzato dalle applicazioni "Protocollo e Flussi Documentali", accessibile sia dalla Intranet del Ministero della Salute che via Internet attraverso i sistemi di autenticazione e autorizzazione descritti in precedenza, e dall'applicazione "Piani di Rientro e



LEA" fruibile attraverso i sistemi di autenticazione e autorizzazione descritti in precedenza. L'architettura tecnica prevede un insieme dedicato di sistemi server con funzioni di front-end e application server in bilanciamento di carico. Tali sistemi sono dotati di http server MS IIS e ospitano il prodotto DOCSPA. Inoltre l'architettura dell'applicazione comprende anche due sistemi MS Windows in configurazione cluster attivo/passivo con funzioni di Repository dei documenti e un RDBMS Oracle Rac 12c composto da due nodi che ospitano i database utilizzati dalle due applicazioni.

2.3.10 Il Sistema SIS

Le applicazioni del Sistema SIS generalmente sono realizzate in ambiente Active Server Pages (ASP) Microsoft ed utilizzano Html con Script per le componenti di presentation e moduli Visual Basic per la logica elaborativa con chiamate al database SQL Server tramite connessioni ODBC. Lo schema architetturale per tali, residuali, realtà è schematizzato dalla figura seguente.

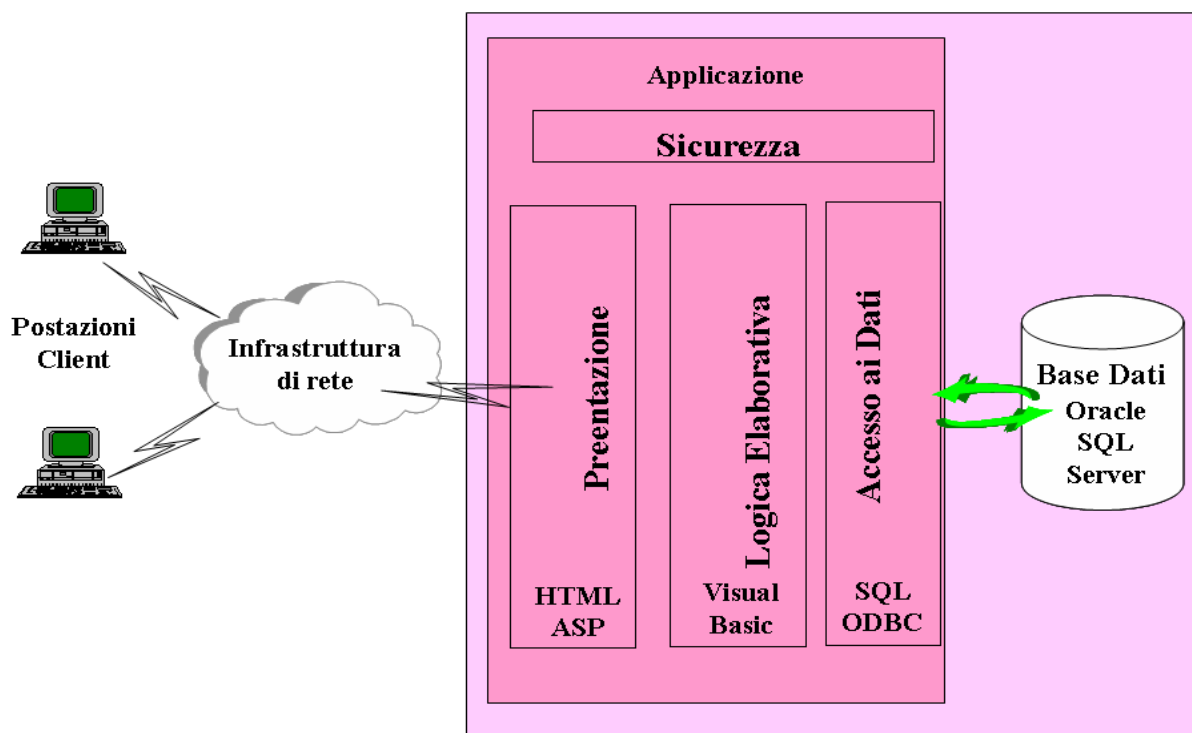


Figura 6: Schema architetturale (applicazioni SIS)

Dal punto di vista della piattaforma tecnologica, tali applicazioni utilizzano principalmente un'architettura basata su tecnologia Internet ed organizzata su più livelli elaborativi. Mentre una minima parte del sistema, relativa alla elaborazione delle informazioni, è realizzata invece in ambiente client-server.

I prodotti

WEB e Application Server

Sistema preposto come:

- Front End - svolge le funzioni di HTTP Server;
- Application Server – fornisce le funzioni necessarie e presiede alla gestione dei componenti che implementano la logica elaborativa.



Utilizza:

- sistema operativo Microsoft Windows ed Internet Information Server
- protocollo Secure Sockets Layer (SSL).

Data Server

Preposto alle funzioni di memorizzazione e accesso ai dati

Utilizza:

- sistema operativo Microsoft Windows;
- accessi ai dati effettuati tramite chiamate ODBC;
- database relazionale Oracle 9i o SQL Server Microsoft

2.3.11 Il Sistema Intranet

Per la descrizione tecnica di dettaglio del sistema Intranet si rimanda all'allegato ARCHITETTURA TECNICA - Sistema Intranet (file "Architettura SI-Intranet").

2.3.12 Il Sottosistema di sicurezza

Il Sistema di controllo degli accessi si avvale della suite di prodotti CrossIdeas e NetIQ/Microfocus. Nella figura seguente è sinteticamente rappresentato lo schema dei prodotti utilizzati per erogare i servizi di sicurezza descritti.

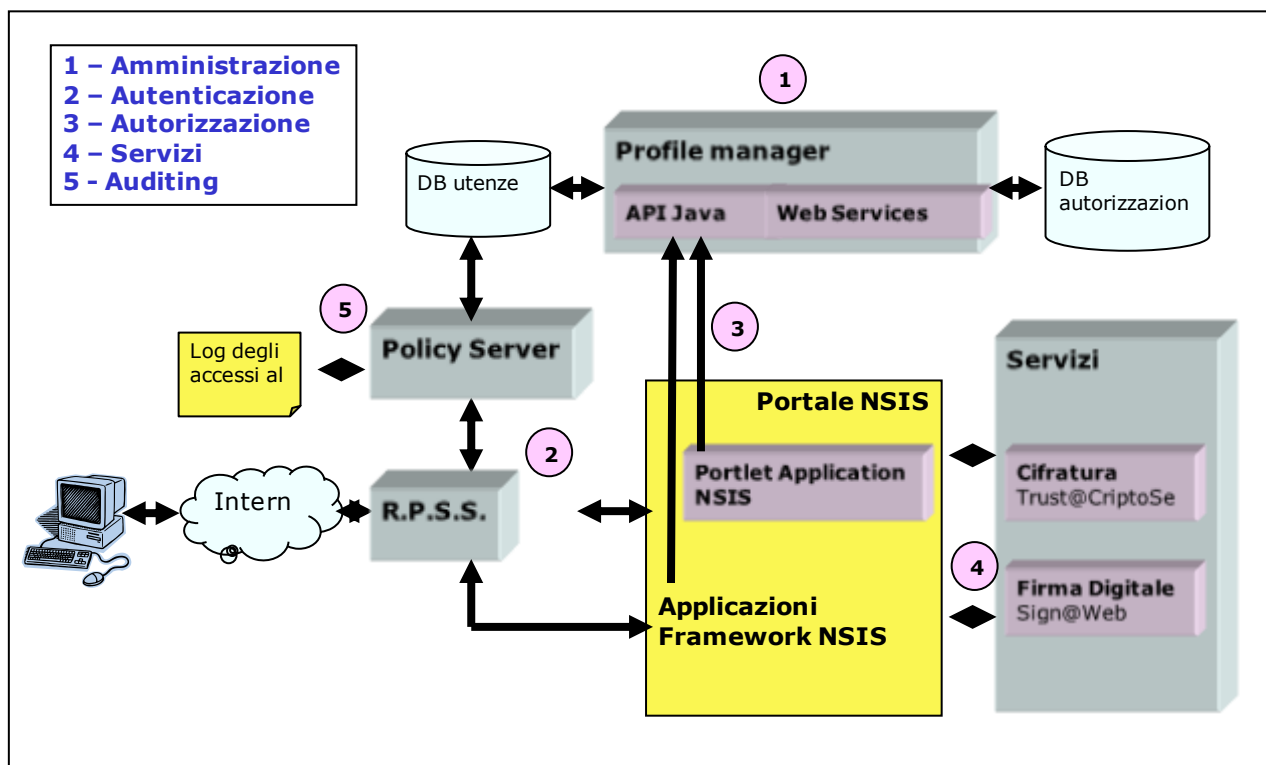


Figura 7: Prodotti per i servizi di sicurezza

1. Amministrazione (Profile Manager);
2. Autenticazione ((Novell Access Gateway;



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

3. Autorizzazione (Profile Manager);
4. Cifratura - Firma Digitale (Trust@CryptoServer – Sign@Web);
5. Auditing (NetIQ-IBM).

Per la descrizione tecnica di dettaglio si rimanda all'allegato ARCHITETTURA TECNICA – Sottosistema di Sicurezza (file "Architettura SI- Sicurezza");

E' anche presente presso il CED un sistema per la conservazione dei dati richiesti in ottemperanza alla normativa sulla tracciatura delle attività degli Amministratori di sistema.

2.3.13 Il Sottosistema di protezione

2.3.13.1.1 [Il Sistema di firewalling](#)

L'architettura di rete e sicurezza del SIS-N è una configurazione con doppio bastione di firewall dedicati, posti in alta affidabilità.

La configurazione adottata consente di isolare tre aree:

- Area Reti Esterne, dove sono attestati tutti i collegamenti geografici SPC;
- Area DMZ-MZ, posta dietro il primo livello di firewall, dove sono attestati i server di front end raggiungibili dalle reti geografiche e gli application server raggiunti dai sistemi di front-end;
- Area Reti Interne, posta dietro il secondo livello di firewall, dove sono attestati i server che necessitano di un maggiore livello di sicurezza, quali i server DB e i sistemi attestati sulla sottorete di back-office del SIT.

A tale configurazione si aggiungono i firewall e le sonde IPS/IDS che governano gli aspetti di sicurezza messi a disposizione dal gestore della rete SPC per i collegamenti Internet e Infranet, nonché gli apparati che consentono la realizzazione di accessi ai sistemi mediante VPN Internet anch'essi messi a disposizione dal fornitore della connettività SPC.

2.3.13.1.2 [URL Filtering](#)

La navigazione internet viene veicolata dai Firewall che implementano la funzione di proxy e la funzione di URL Filtering basata su policy associate all'utenza di dominio per gli utenti interni all'Amministrazione. Sono implementate black list e grey list. In particolare, le grey list consentono a gruppi di utenti autorizzati l'accesso a siti normalmente vietati.

2.3.13.1.3 [L'antivirus](#)

La gestione del software anti-malware (i. e. antivirus, anti-spyware, ecc.) è attualmente effettuata con l'utilizzo dei prodotti McAfee.

2.3.13.1.4 [Disaster Recovery](#)

Per la descrizione del sito di DR si rimanda al successivo paragrafo 2.4.2

2.3.14 Il Sistema di videoconferenza

L'architettura tecnica del sistema di videoconferenza è composta da un'infrastruttura centrale localizzata presso i due CED Primari del Ministero della Salute, da sale di videoconferenza situate presso le sedi centrali, da postazioni mobili di videoconferenza e da webcam dotate di cuffia microfonica installate sia al centro che nella periferia.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Vengono ospitati in housing presso i due CED primari le apparecchiature centrali previste per l'erogazione di questo servizio. La componente centrale del nuovo sistema di videoconferenza è al momento composta da 6 server virtuali VMware che ospitano i corrispondenti prodotti applicativi. L'architettura è scalabile e può prevedere espansioni future.

La configurazione prevede tre server ubicati presso ciascuno dei due CED in cluster tra i due siti e attestati su una VLAN dedicata esclusivamente al sistema di videoconferenza; il cluster dei sistemi è stato integrato nell'infrastruttura di BC dei due CED Primari (vedere descrizione di seguito).

La funzionalità Layer 3 (default-gateway della rete videoconferenza) viene svolta dai Firewall Fortigate del fornitore SPC Conn.

Sui Firewall del Ministero della Salute, oltre che su quelli Fortigate citati, sono state implementate tutte le policy e il routing necessario al corretto funzionamento e all'utilizzo del sistema di videoconferenza da parte degli utenti dell'Amministrazione.

Di seguito lo schema dell'architettura del sistema:

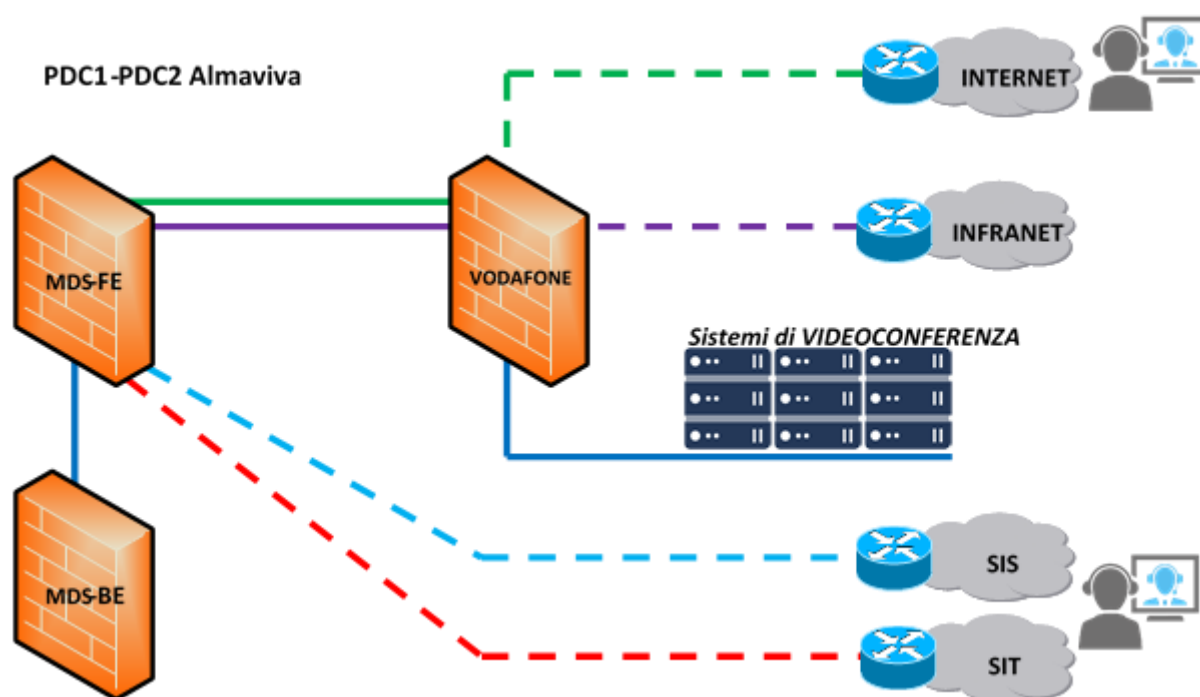


Figura 8: Architettura di Videoconferenza

2.3.15 Il Sistema di Web Application Firewall

Il servizio Web Application Firewall è erogato da due appliance Fortinet FortiWeb installate presso i due CED primari. Ogni appliance è collegata con 2 cavi in link aggregation per un totale di 2Gbit di banda disponibile. La configurazione è stata effettuata in modalità High Availability, active-passive, con CED attivo quello di Scalo Prenestino.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

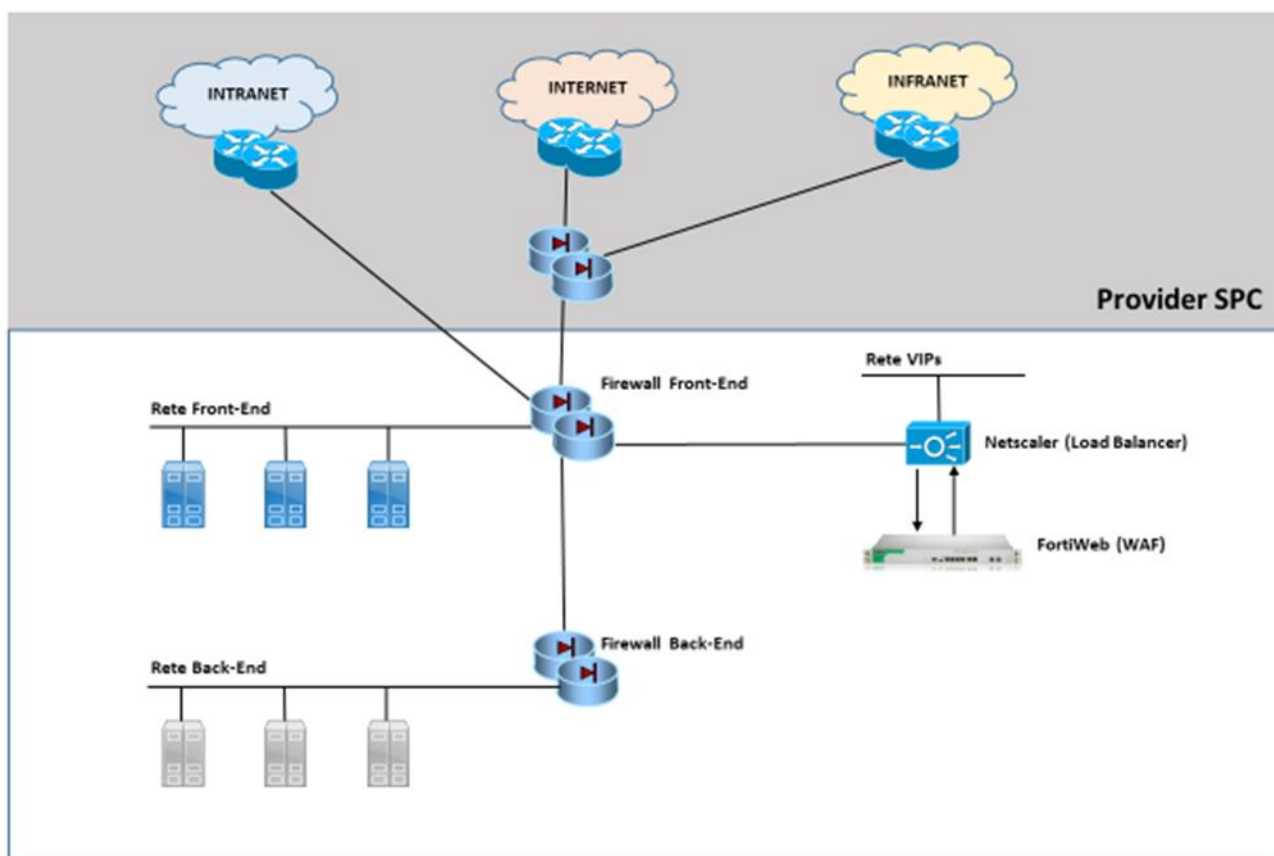


Figura 9: Il sistema WAF (Web Application Firewall)

Il FortiWeb è stato collocato a valle del bilanciatore hardware Netscaler in modo da poter usufruire dell'alta affidabilità dei portali aggiungendo uno strato di sicurezza: le richieste che raggiungono il bilanciatore vengono analizzate e filtrate dal WAF, in caso fosse necessario, per poi essere smistate verso i server.

La nuova architettura è stata progettata e realizzata per essere fault tolerant, dotando i due FortiWeb di doppi collegamenti elettrici e di rete.



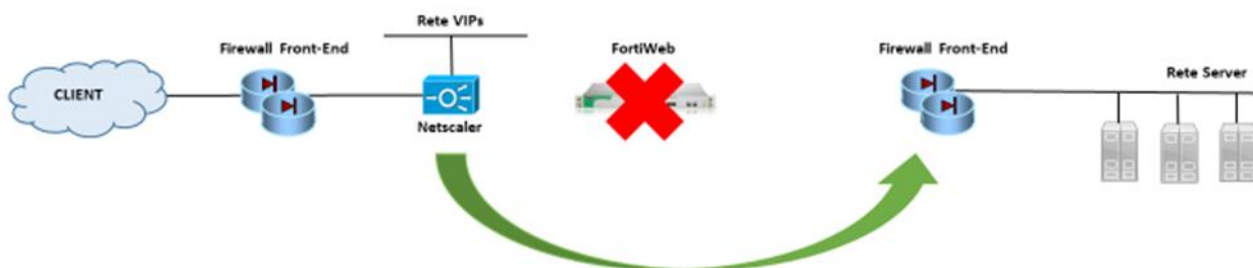
Per rendere ancora più affidabile il servizio è stato configurato un sistema di health check da parte del bilanciatore Netscaler che riconosce un eventuale malfunzionamento del FortiWeb ed esegue un bypass automatico del traffico direttamente verso i server bilanciati.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

FortiWeb non risponde agli health check, bypass attivato dal Netscaler



2.3.16 Il Sistema Mds Drive

Il Sistema MdS Drive è stato realizzato con la finalità di offrire agli utenti dell'Amministrazione una soluzione open source realizzata sul Cloud privato del Ministero per la conservazione e condivisione di file online.

La share può essere acceduta remotamente da PC, tramite software di sincronizzazione, o via web e da tablet o smartphone, tramite l'app di riferimento.

L'architettura logica è realizzata su 2 livelli di sicurezza, riportando nella rete più interna e protetta i dati residenti su file system e sul db. Gli accessi alla share verranno effettuati accedendo alla url mdsdrive.sanita.it su protocollo https.

La piattaforma nel suo complesso è costituita da un Sistema di front end ed un sistema di back end con Sistema operativo Linux CentOS e sw applicativo Owncloud.

2.3.17 Il Sistema Polo SBN

La piattaforma prevede la componente "SBNWeb" (gestionale di biblioteca) e la componente OPAC (On-line public access catalogue). Ciascuna componente prevede il livello di http /application server ed il livello di DB.

2.3.17.1 [SBNWeb – gestionale biblioteca](#)

Questa componente è accessibile tramite domain name in https , prevede l'esposizione di web service, l'inoltro mail ed il colloquio applicativo con il sistema Indice (Catalogo Centrale del Servizio Bibliotecario Nazionale) residente nel CED dell'Istituto Centrale per il Catalogo Unico delle Biblioteche Italiane (ICCU).

L'ambiente sw previsto per ospitare l'applicazione è costituito da Sistema Operativo Linux CentOS , HTTP Server Apache, Application server JBOSS e RDBMS PostgreSQL.

2.3.17.1.2 [OPAC – OnLine public access catalogue](#)

Questa componente è accessibile tramite domain name, prevede l'inoltro mail prevalentemente agli utenti della biblioteca, il colloquio applicativo con applicazioni residenti nel CED ICCU (anagrafe biblioteche) ed il colloquio applicativo con web-service esposto da SBNWEB.

L'ambiente sw previsto per ospitare l'applicazione è costituito da Sistema Operativo Linux CentOS , HTTP Server Apache, Application server Tomcat, Solr e RDBMS PostgreSQL

2.4 L'INFRASTRUTTURA TECNICA DI RIFERIMENTO



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

L'infrastruttura tecnica può, nelle sue linee generali, essere schematizzata in:

- **Architettura CED,,** che illustra l'organizzazione delle zone logiche in cui è suddiviso il CED e le caratteristiche salienti delle apparecchiature hardware;
- **Infrastruttura telematica di rete,** che fornisce una panoramica delle dislocazioni geografiche delle sedi del Ministero della Salute e le relative interconnessioni di rete;
- **Postazioni di lavoro,** che descrive le caratteristiche delle principali categorie di postazioni di lavoro informatiche presenti nelle diverse sedi.

2.4.1 Architettura CED

La soluzione tecnologica adottata per il Sistema Informativo del Ministero della Salute è basata su una infrastruttura distribuita su due Data Center che costituiscono un "cluster metropolitano", in cui i servizi sono erogati da 2 siti, entrambi con funzioni di Data Center Primario (PDC1 e PDC2), ubicati a Roma rispettivamente presso le sedi Almaviva in Via dello Scalo Prenestino 15 e in Via di Casal Boccone 188.

La soluzione adottata permette di realizzare un unico "data center globale", in cui il concetto di virtualizzazione è applicato a livello di:

- Sistemi, dove tutti i sistemi (a meno di eccezioni per esigenze specifiche) sono ospitati su macchine virtuali;
- Rete, che viene virtualizzata e condivisa a livello layer 2 tra i due Data Center Primari, realizzando di fatto una infrastruttura di rete unica;
- Storage, che viene virtualizzato e condiviso uniformemente sia all'interno di ognuno dei 2 Data Center Primari, sia come condivisione geografica della SAN tra i 2 DC Primari.

La virtualizzazione dei sistemi su cui si basa l'infrastruttura, a seconda della tecnologia utilizzata, viene supportata da appropriate tecnologie e strumenti per realizzare la soluzione di BC/DR.

In condizioni di normale funzionamento il carico viene ripartito sulle strutture virtualizzate dei 2 CED Primari a seconda delle necessità e delle condizioni generali.

In caso di fault sia parziale che totale di uno dei due CED Primari la soluzione implementata è in grado di garantire la continuità del servizio grazie all'infrastruttura realizzata

- a livello storage perché i dati sono in replica su entrambi i siti ed utilizzabili a prescindere della locazione fisica;
- a livello rete per la realizzazione dell'infrastruttura unica di rete tra i due CED;
- a livello sistemi per i meccanismi delle soluzioni di virtualizzazione che consentono di spostare virtual machines senza interruzione del servizio.

2.4.2 Disaster Recovery

In questo scenario si inserisce l'ulteriore sito di Disaster Recovery ubicato presso il Data Center Telecomitalia di Rozzano (Milano) da attivare nel caso di indisponibilità contemporanea di entrambi i Data Center che costituiscono il sito primario.

L'architettura complessiva è omogenea con le scelte tecnologiche di PDC1 e PDC2 e



l'allineamento dei dati viene assicurato dalla tecnologia EMC . La soluzione garantisce la protezione dei dati integrando una replica remota continua. La piattaforma è interamente virtualizzata e basata sulla stessa tecnologia adottata presso i due siti primari.

2.4.3 Configurazione HW dei sistemi

L'infrastruttura server di erogazione utilizza due tipologie di ambienti: x86 e Risc.

Gli ambienti x86 sono installati su una farm composta da Blade Cisco UCS utilizzate per erogare gli ambienti x86 Virtuali, con virtualizzazione basata su VMware.

Gli ambienti Risc sono ospitati su sistemi IBM pSeriesPower7 con virtualizzazione basata su LPAR.

Di seguito è riportato un prospetto di sintesi dell'infrastruttura hardware predisposta presso i due siti primari .

Apparati	Marca	Modello	Processore	Q.tà
Blade	Cisco	B200 M3	E5-2670	14
P-Series	IBM	P795	P7	2
Firewall	Checkpoint	12600		4
Storage	EMC2	VNX		2 apparati per un totale di 80 TB ciascuno
Bilanciatori	Citrix Netscaler	Sdx11500		2

I sistemi virtuali utilizzano come piattaforma di sistema operativo MS Windows, Linux e AIX.

2.4.4 Storage Area Network

Per quanto riguarda l'infrastruttura Storage\SAN gli elementi principali sono:

- **EMC2 VPLEX –componenti Local e Metro:** sistema di virtualizzazione e federazione dello storage;



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

- **EMC2 VNX**: unified storage per lo storage multiprotocollo a livello di file, blocchi e oggetti, con provisioning dello storage semplificato per gli ambienti virtualizzati;
- **EMC2 RecoverPoint**, sistema di replica remota per storage eterogenei.

Lo spazio SAN, oltre che allo storage utilizzato dai DB, è dedicato anche allo spazio disco dei sistemi di elaborazione virtuali.

La figura seguente fornisce una rappresentazioni schematica delle zone logiche del CED

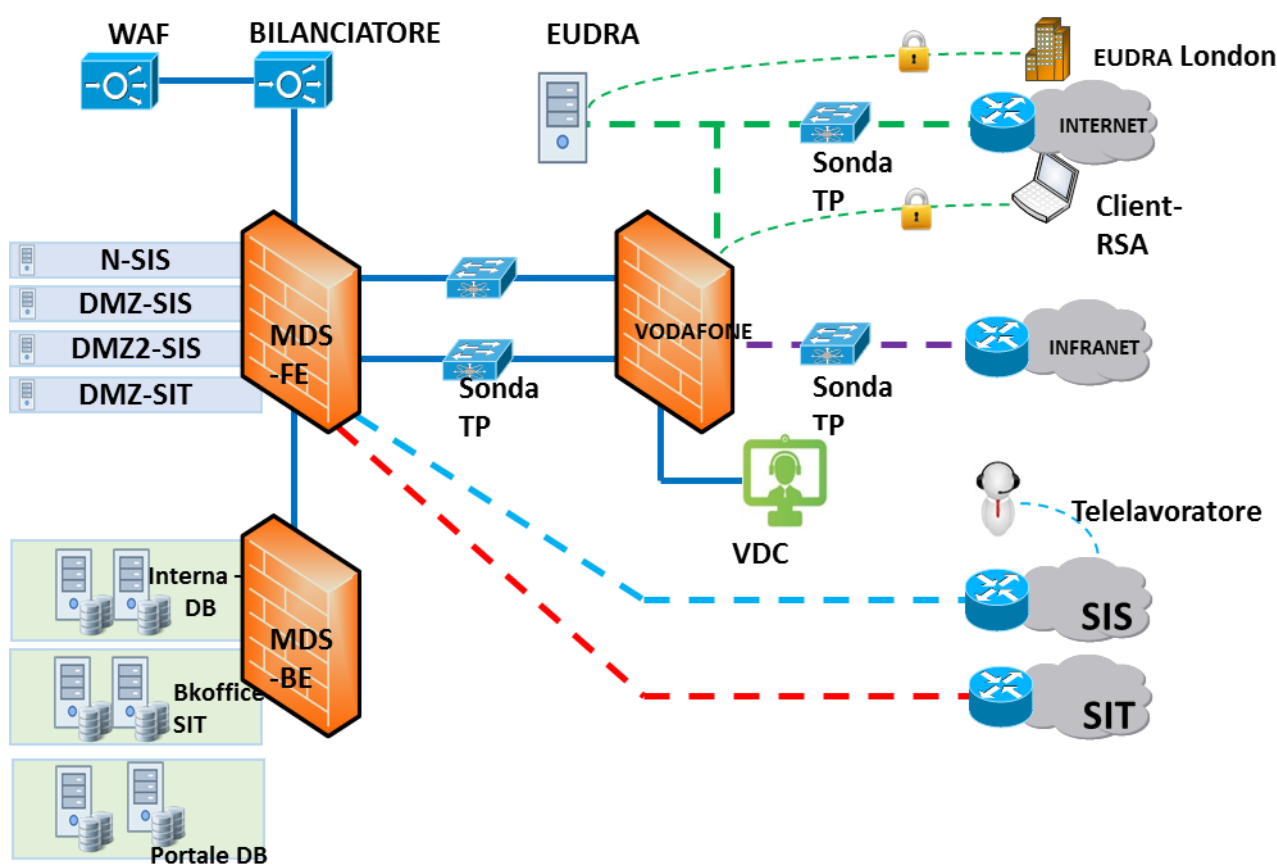


Figura 10: Le zone logiche del CED

2.4.5 Infrastruttura telematica di rete

L'infrastruttura realizzata per il Ministero della Salute prevede che i due siti primari siano interconnessi tra loro tramite anello ottico ridondato a percorso differenziato.

Ciascuno dei due siti primari è inoltre collegato con il sito di DR con 1 trunk MPLS.

Presso i due Data Center Primari sono utilizzati apparati Cisco, firewall Checkpoint, switch SAN Cisco tutti in configurazione di alta affidabilità.

L'infrastruttura di rete e connettività utilizza inoltre i Fabric Interconnect della serie Cisco UCS.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Come già illustrato precedentemente L'architettura di rete e sicurezza del SIS-N è una configurazione con doppio bastione di firewall dedicati, posti in alta affidabilità.

La configurazione adottata consente di isolare tre aree:

- Area Reti Esterne, dove sono attestati tutti i collegamenti geografici SPC;
- Area DMZ-MZ, posta dietro il primo livello di firewall, dove sono attestati i server di front end raggiungibili dalle reti geografiche e gli application server raggiunti dai sistemi di front-end;
- Area Reti Interne, posta dietro il secondo livello di firewall, dove sono attestati i server che necessitano di un maggiore livello di sicurezza, quali i server DB e i sistemi attestati sulla sottorete di back-office del SIT.

A tale configurazione si aggiungono i firewall e le sonde IPS/IDS che governano gli aspetti di sicurezza messi a disposizione dal gestore della rete SPC per i collegamenti Internet e Infranet, nonché gli apparati che consentono la realizzazione di accessi ai sistemi mediante VPN Internet anch'essi messi a disposizione dal fornitore della connettività SPC.

Il Ministero della Salute attualmente si avvale, attraverso i servizi di trasporto e interoperabilità SPC (Sistema Pubblico di Connettività), di una infrastruttura telematica che realizza l'interconnessione delle sedi centrali a Roma e dei suoi uffici periferici distribuiti sul territorio nazionale.

E' possibile distinguere:

- **reti di tipo locale (LAN):** reti ad estensione locale a cui afferiscono postazioni di lavoro e dispositivi di rete, dotati, nella quasi totalità dei casi, di agent SNMP; appartengono a questa categoriale LAN di edificio degli uffici centrali e periferici del Ministero della Salute;
- **rete geografica (SPC Mpls):** rete che permette il collegamento geografico di tutti gli uffici del Ministero della Salute.

In tale contesto i due siti **CED** primari si configurano logicamente quale centro stella dei collegamenti sopra descritti e si interconnettono inoltre:

- alla rete Internet;
- alla rete Infranet SPC

Nell'ambito del SIT, i due siti **CED** primari si configurano logicamente quale centro stella di collegamenti che dipartono:

- dai Centri Regionali (CR);
- dal Centro Nazionale Trapianti (CNT);
- dall'Istituto Superiore della Sanità (ISS).

Di seguito si riporta una sintesi per tipologia dei collegamenti forniti dal provider SPC:



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Profilo	BMA (Kbps)	Q.tà
STDE-A10	1.024	3
STDE-A9	512	7
STDE-S3	512	1
STDE-S4	1.024	17
STDE-S5	2.048	73
STDE-S6	4.096	69
STDO-1	10.000	21
STDO-2	20.000	2
STDO-3	40.000	1
STDO-4	100.000	1
STDO-6	300.000	2
STDO-9	2,5 Gbps	2

Le sedi periferiche sono tutte dotate di reti locali, realizzate tramite cablaggi strutturati di categoria 5e o 6.

L'interconnessione di tutte le sedi con la rete SPC avviene mediante l'utilizzo di apparati router; ogni sede periferica è dotata di un doppio collegamento (primario e back-up) e di un ulteriore backup 4G.

Gli uffici periferici del SIT si attestano su una rete MPLS (sempre in ambito SPC) dedicata e separata dalla rete MPLS SPC dedicata agli altri uffici periferici del Ministero della Salute (UVAC-PIF, USMAF-SASN, NAS, Dipartimenti)

2.4.5.1.1 Rete VPN per il collegamento EUDRA

Il Ministero della Salute si collega ad una rete europea di scambio di informazioni realizzata e presieduta dall'Agenzia Europea per la Valutazione dei Medicinali (EMA).

I principali obiettivi e funzioni realizzate sono:

- mutuo riconoscimento dei farmaci
- rapid alert
- reazioni avverse dei farmaci
- scambio documentazione tra ditte ed Enti Nazionali
- servizi di posta condivisi
- accesso a banche dati europee

La VPN viene realizzata tramite l'utilizzo di un sistema di terminazione dedicato ed installato presso il CED, come riportato sullo schema generale del CED .

2.4.5.1.2 CED del Ministero della Salute

I due siti primari ed il sito di DR sono interconnessi alla rete SPC per l'erogazione dei servizi agli utenti.

In particolare il Data Center di Scalo Prenestino è equipaggiato con i seguenti collegamenti SPC ridondati per ciascuna tipologia:



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

- mpls sis, infranet, internet sono attestati su una coppia di router multiambito con un throughput di 2,5 Gbit/s in bilanciamento (per un totale di 5 Gbit/s)
- mpls sit attestato su una coppia di router a 20 Mbit/s

Il data Center di Casal Boccone è equipaggiato con gli stessi collegamenti come tipologia e velocità.

Il sito di DR è equipaggiato con gli stessi collegamenti come tipologia, ma con velocità inferiore.

2.4.5.1.3 Interconnessione alla rete Internet

Attraverso il collegamento Internet vengono esposti i siti pubblici del Ministero. Inoltre, a tutti gli uffici centrali e periferici viene fornito l'accesso ad Internet veicolato per ragioni di sicurezza dalle funzioni di proxy e URL filtering dei firewall di Front End.

2.4.5.1.4 Servizi offerti dall'infrastruttura

L'architettura del servizio di Hosting è completata con i servizi infrastrutturali necessari al corretto funzionamento del servizio.

I servizi offerti sono i seguenti:

- funzioni di Active Directory, Url filtering e reverse proxy.
- funzioni di DHCP,
- funzioni di capacity planning,
- gestione dell'antivirus,
- controllo degli accessi alle reti LAN mediante il protocollo 802.1x,
- accesso ai servizi attraverso rete WIFI
- backup dei server e relativa gestione della nastroteca,
- monitoraggio della componenti di rete,
- monitoraggio delle componenti hw e sw dei sistemi,
- monitoraggio della end-user experience.

2.4.5.1.5 Le reti locali degli uffici centrali del Ministero

Ogni sede centrale del Ministero della Salute è ubicata a Roma ed è dotata di una rete locale LAN a cui afferiscono le postazioni informatiche del personale dell'Amministrazione.

In particolare si distinguono le seguenti LAN:

- LAN della Sede del Ministero di Lungotevere Ripa (Roma);
- LAN della Sede del Ministero di Via Ribotta (Roma);
- LAN della Sede del Ministero di V.le dell'Aeronautica (NAS Roma);
- LAN della Sede del Ministero di Via Carri Armati (Roma).

Le sedi di Ripa, Ribotta e V.le dell'Aeronautica prevedono dorsali in fibra ottica multimodale e cablaggio orizzontale di categoria 5e o 6. La topologia di rete è di tipo stellare: il centro stella della rete è costituito da una coppia di switch ridondati a cui sono connessi i vari switch di piano. Tutte le postazioni utente sono collegati agli switch di piano.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

2.4.5.1.6 Le reti locali degli uffici periferici del Ministero

Tutte le sedi periferiche sono dotate di cablaggio strutturato di categoria 5e o 6 e più dispositivi switch layer 2 Fast Ethernet. A tali switch afferiscono:

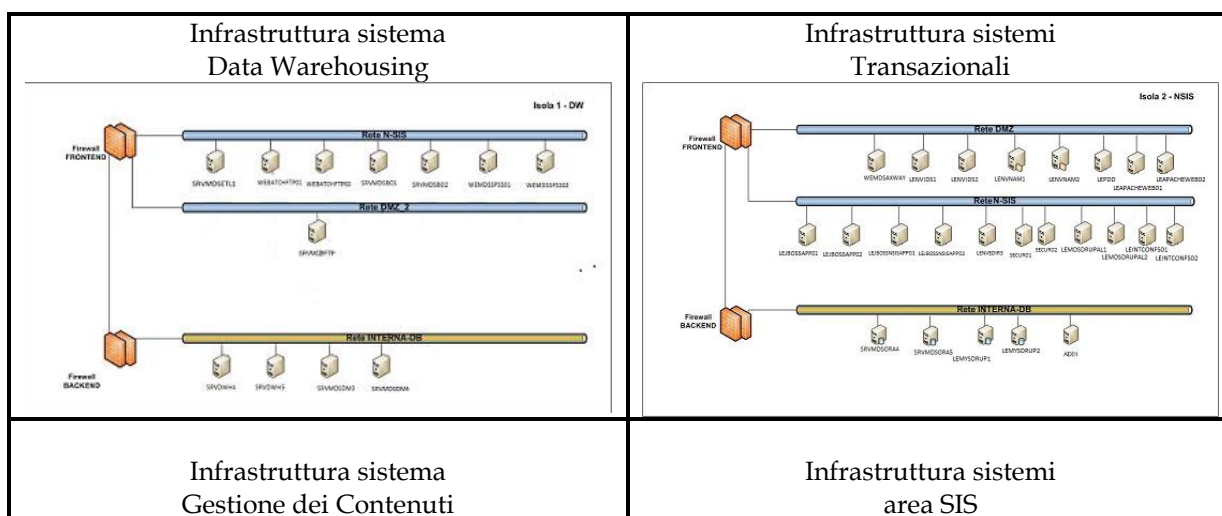
- PC, lettore rilevazione presenze, stampanti di rete ed altri eventuali dispositivi di rete;
- router per l'interconnessione alla rete SPC MPLS del Ministero.

2.4.6 Postazioni di lavoro informatiche

Le postazioni di lavoro del Ministero sono collegate alle LAN degli uffici centrali e periferici dell'Amministrazione. Tali postazioni sono costituite da personal computer e stampanti, di produttori eterogenei, di proprietà del Ministero. Ciascuna postazione è dotata di base di Sistema Operativo MS Windows nelle versioni Seven, Windows8 e Windows10, di prodotti di office automation della Suite MS Office Professional e Standard e di antivirus McAfee. L'intero parco delle apparecchiature in uso è oggetto di continuo e progressivo rinnovamento con contestuale dismissione delle apparecchiature obsolete. Attualmente, il numero complessivo delle PDL operative ammonta a circa 4000 PC e circa 3000 tra stampanti e scanner.

2.5 RAGGRUPPAMENTI OMOGENEI DEI SISTEMI - LE ISOLE

Data la complessità e le dimensioni dell'intero sistema, l'infrastruttura tecnica è stata suddivisa in gruppi di server applicativi e/o infrastrutturali omogenei e il più possibile autoconsistenti, denominati 'isole', nelle quali i sistemi possono essere raggruppati. Si noti che tale suddivisione è una rappresentazione "logica" basata sulle principali aree di applicazioni e di servizi infrastrutturali e non rappresenta una separazione fisica di tali ambienti. I criteri per definire tali raggruppamenti sono l'omogeneità delle funzioni svolte (tipicamente sistemi applicativi di frontend e relative basi dati sono attestati nella stessa isola) e la minimizzazione degli scambi di dati fra server di isole differenti.





Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

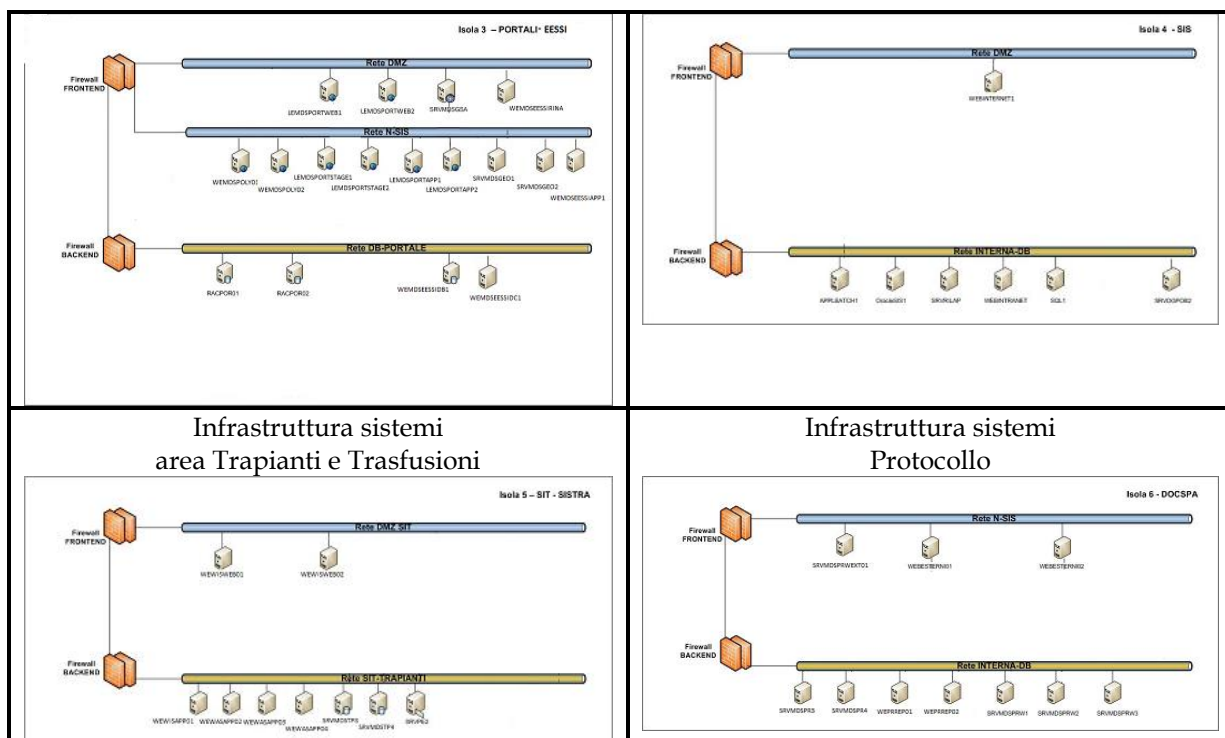


Figura 11 La suddivisione in isole

Le isole, pur essendo in massima parte autoconsistenti, sono tra loro comunque interconnesse sotto l'aspetto delle reti interne, in base alle funzionalità esposte da ogni singola applicazione.

Nella matrice seguente vengono fornite le principali interazioni presenti tra le varie isole. Si noti come, ad esempio, le isole infrastrutturali/firewall, essendo di natura trasversale, interagiscono con tutte le restanti isole.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Matrice Interazione Isole										
Descrizione Isola	Cod. Isola	DWH	NSIS	PORTALI	SIS	SIT-SISTRA	DOCSPA	PE	VDC	Config_Infrast fw_ips
Isola1 - DWH	DWH									
Isola2 - NSIS	NSIS	Strettamente correlate. Funzioni ETL da NSIS a DWH; BI dell'NSIS su DWH								
Isola3 - Portali EESSI	PORTALI_EESSI	Correlati. Esposizione dati su Portale da DWH	Correlati. Esposizione dati su Portale da NSIS							
Isola4 - SIS	SIS	Strettamente correlate. Funzioni ETL da SIS a DWH; BI del SIS su DWH	Strettamente correlati. Applicazioni che utilizzano funzioni SIS ed NSIS	Correlati. Esposizione dati su Portale da NSIS						
Isola5 - SIT - SISTRA	SIT-SISTRA	Funzioni ETL da SIT a DWH; BI del SIT su DWH	Correlati. Area Business Intelligence	Correlati. Esposizione dati su Portale da NSIS						
Isola 6 - DOCSPA	DOCSPA		Strettamente correlati. Gestione del protocollo da aree applicative							
Isola 7 - Posta	PE		Strettamente correlati. Utilizzo della Posta Elettronica da aree applicative		Strettamente correlati. Utilizzo della Posta Elettronica da aree applicative		Strettamente correlati. Utilizzo della Posta Elettronica da aree applicative			
Isola Videoconferenza	VDC									
Isole Configuration e infrastrutturali e Firewall,IPS	Config_Infrast fw_ips	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	Area Infrastrutturale delle isole	

Di seguito viene riportata una breve descrizione di ciascuna isola e l'abbreviazione con la quale vengono referenziate nella documentazione.

Isola 1 – DWH (DWH). In questa isola applicativa sono ricompresi i server che svolgono le funzioni inerenti il sistema di Data Warehousing, come, ad esempio, le funzioni ed i relativi strumenti sia per il caricamento e pulizia dei dati (ETL) e sia per la loro elaborazione e fruizione. In tale isola sono anche ospitati i DB server del sistema di Datawarehouse.

Isola 2 – NSIS (NSIS). In questa isola applicativa sono ricompresi i server che ospitano i sistemi di autenticazione ed autorizzazione, gli Application server ed i DB server appartenenti al modello architetturale trasversale descritto in precedenza.

Isola 3 – Portali EESSI (PORTALI_EESSI). In questa isola applicativa sono compresi i server (Application server, DB server e server di Stage) che ospitano il portale pubblico del Ministero della Salute. Sono inoltre inseriti in questa isola anche gli eventuali server EESSI.



Ministero della Salute

Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica

Isola 4 - SIS (SIS). In questa isola sono compresi i server su cui risiedono le applicazioni SIS; come già descritto in precedenza, tali applicazioni afferiscono ad un particolare modello architetturale realizzando generalmente al loro interno tutti i servizi di cui necessitano. In tale isola è ospitato anche il sito Intranet del Ministero della Salute.

Isola 5 - SIT-SISTRA (SIT_SISTRA). In questa isola sono compresi i server del Sistema Informativo dei Trapianti e del Sistema Informativo dei Servizi Trasfusionali. Come già descritto in precedenza, il SIT-SISTRA è caratterizzato da una architettura dedicata ad alta affidabilità e da elevati livelli di sicurezza per la tutela del proprio patrimonio informativo. Pur facendo parte del SIS-N, si avvale di un ambiente elaborativo separato; in particolare i sistemi sono distribuiti su una sottorete dmz (sistemi di front-end) e su di una sottorete di back-end (dove sono ospitati gli application ed i DB server, nonché un sistema di posta "chiuso" e dedicato al sistema informativo dei trapianti). Tali sottoreti sono dedicate e separate tramite firewall dagli altri ambienti applicativi.

Isola 6 - DOCSPA (DOCSPA). In questa isola sono compresi i server per la gestione del protocollo informatico e gestione documentale.

Isola 7 - POSTA (PE). In questa isola sono compresi i server che erogano il servizio di Posta Elettronica per il Ministero della Salute. In tale ambito sono compresi i server interni, che gestiscono le caselle postali degli utenti (Back-end servers), server intermedi per lo scambio della posta da e verso il dominio di posta (Mail Gateway Server); server di Front End per gli accessi web/https, server per gli accessi tramite Blackberry. A tale infrastruttura si affiancano i sistemi perimetrali del fornitore SPC di Mail Gateway e di controllo Antispam/Antivirus.

Isola Configuration e Infrastrutturali (Config_Infrast). In questa isola sono compresi i server preposti alla gestione della configurazione dei sistemi informativi ed i server che gestiscono i servizi infrastrutturali tra cui le funzioni di Active Directory, DHCP, gestione dell'antivirus, controllo accessi apparati LAN, ecc..

Isola Videoconferenza (VDC). In questa isola sono compresi i server dedicati al sistema di Videocomunicazione che consente agli utenti dell'Amministrazione la comunicazione in tempo reale ed in modalità interattiva con utenti (dell'Amministrazione stessa e/o di altre Amministrazioni) dislocati remotamente su postazioni di lavoro o in sale attrezzate per videoconferenze, mediante l'utilizzo di immagini e suoni e lo scambio di dati elettronici.

Isola Firewall, IPS (fw_ ips). In questa isola sono ospitati i sistemi di infrastruttura; a titolo esemplificativo e non esaustivo, i firewall di front-end e di back-end, i proxy per la navigazione Internet, gli Appliance per accesso mediante VPN Internet e per la sicurezza (IPS/IDS) forniti dal fornitore dei servizi SPC, gli Appliance per accesso VPN Eudra, ecc..



Ministero della Salute

Direzione generale della digitalizzazione, del sistema
informativo sanitario e della statistica

2.6 LE CARATTERISTICHE STATICHE E DINAMICHE DEL SIS-N

Al fine di conoscere e valutare nel dettaglio il dimensionamento dei sistemi informativi dell'Amministrazione, vengono forniti in una serie di specifici documenti; nella tabella seguente si riporta l'elenco di questi documenti con l'indicazione del contenuto informativo di ciascuno di essi.

CONTENUTI	NOME DOCUMENTI
Report transazioni totali per applicazione – numero, per ogni applicazione, di transazioni totali per mese e percentuale di livello di servizio erogata (Anno 2017)	Appendice 18 al Capitolato Tecnico "Report transazioni totali per applicazione"
Report Asset banche dati – elenco, per ogni istanza del BD, degli identificativi e dello spazio occupato	Appendice 19 al Capitolato Tecnico – "Asset Banche Dati"
Report Licenziato MdS – elenco delle licenze software "middleware" di proprietà dell'Amministrazione	Appendice 20 al Capitolato Tecnico – "Elenco licenze middleware di proprietà del MdS"
Asset applicazioni	Appendice 21 al Capitolato Tecnico "Asset Applicazioni"