

APPENDICE 1 AL CAPITOLATO TECNICO

CONTESTO TECNOLOGICO E APPLICATIVO

Sommario

2	Infrastrutture di rete	4
2.1	Architettura Sede Via Vitorchiano	6
2.2	Architettura "Wifi@DPC"	7
2.3	Log Management	8
2.3.1	Architettura Log Management.....	8
2.4	Architettura Sedi Via Ulpiano e Via Affile	8
2.4.1	Architettura Sede Via Ulpiano.....	9
2.4.2	Architettura Sede Via Affile.....	10
2.5	Architettura Sede Disaster Recovery - Palmanova	11
2.6	Enti esterni connessi alla rete	12
3	Postazioni di Lavoro.....	13
4	Infrastrutture tecnologiche dipartimentali.....	14
4.1.1	Fileserver e Sharepoint.....	15
4.1.2	Servizio di Active Directory.....	16
4.1.3	Servizio NTP (Network Time Protocol).....	18
4.1.4	Servizio di Posta Elettronica	19
4.1.5	Servizio di fax server.....	20
4.1.6	Sistemi per la videoconferenza	21
4.2	Monitoraggio.....	Errore. Il segnalibro non è definito.
4.3	Osservatorio delle Strutture Sismiche (OSS).....	26
4.4	Rete Accelerometrica Nazionale (RAN).....	28
4.5	Centro Funzionale Centrale (CFC)	30
4.5.1	<i>MeteoSync</i>	31
4.6	Backup	32
4.7	Telefonia Fissa	34
4.8	Direzione di Comando e Controllo - DICOMAC.....	35
5	Centri Funzionali.....	37
6	Apparati Audio Video	40
6.1	Sistema Audio-Video installato nella sede del DPC di via Vitorchiano	40
6.2	Sistema Audio-Video installato nella sede del DPC di via Ulpiano	53
8.	APPLICAZIONI	56

8.1 Antincendio boschivo – COAU	56
8.2 Benemerienze - PIB	57
8.3 Verifiche sismiche - SIV3274.....	59
8.4 Sistema informativo territoriale - SITDPC	60
8.5 Gestione delle emergenze - Brogliaccio	63
8.6 Beni culturali - CSRS.....	67
8.7 Sistema informativo territoriale - SITDPC.....	71
9. Gestione del Sito web istituzionale in Cloud Computing.....	75

2 Infrastrutture di rete

Le sedi del Dipartimento della Protezione Civile sono ubicate in Roma:

1. Via Vitorchiano: rete di accesso per il personale del Dipartimento; in questa sede è presente il CED principale, dal quale vengono erogati la maggior parte dei servizi; può essere considerato come un hub presso il quale convergono le altre nuvole di connettività;
2. Via Ulpiano: rete di accesso per il personale del Dipartimento; vi è collocato un CED dal quale vengono erogati alcuni servizi per il personale dislocato presso tale sede;
3. Via Affile: rete di accesso per il personale del Dipartimento.

Di seguito uno schema generalizzato della rete:

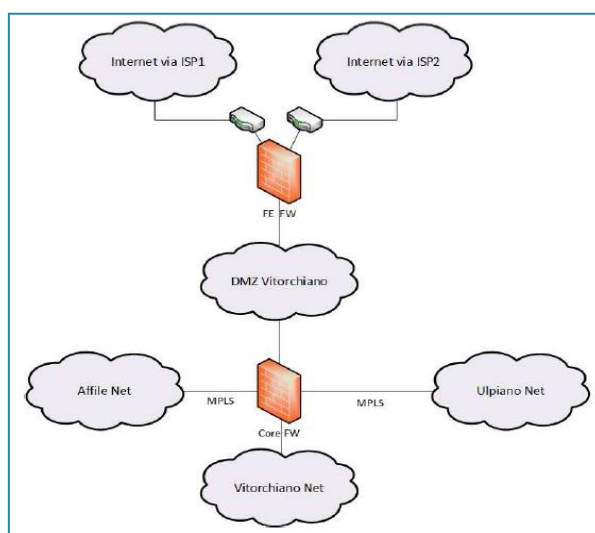


Figura 1 - Schema della rete del Dipartimento

La sede di via Vitorchiano è inoltre il centro stella della rete ed offre la raggiungibilità ai seguenti servizi:

- Datacenter;
- APN (Access Point Name per il trasferimento dati da rete mobile);
- SPC (Sistema Pubblico di Connettività);
- Ex Rete Rupa;
- Palazzo Chigi;
- Accesso ad Internet.

Per poter erogare i propri servizi ed essere indipendenti dagli eventuali problemi dei singoli carrier, il Dipartimento ha deciso di diventare un Autonomous System (AS), in modo da poter annunciare le rotte in modo autonomo per il raggiungimento dei propri IP pubblici (e quindi dei servizi ad essi associati). La connettività verso internet avviene attraverso due carrier distinti, Fastweb e Telecom Italia. Disponendo di due distinti collegamenti con due differenti provider, è possibile annunciare sulla rete gli stessi IP (con pesi diversi) così da bilanciare una linea o l'altra a seconda

delle necessità o di eventuali fault. In caso di caduta di una delle due linee, il traffico di rete viene instradato automaticamente su quella rimasta attiva.

La sede di via Vitorchiano è collegata alla rete tramite connettività MPLS con livello di affidabilità L5, livello che prevede le seguenti caratteristiche:

- Disponibilità del servizio di tipo Mission Critical, pari al 99,99%.
- Tempo di ripristino (in caso di guasti) veloce (per Roma 4h nel 95% dei casi e comunque entro 8h nel 100% dei casi)
- Finestra di erogazione estesa (24/7/365).

Le sedi di Via Ulpiano e di via Affile sono connesse alla rete attraverso un collegamento in MPLS.

La tabella seguente elenca il numero di apparati di rete collocato presso le sedi.

Sede	Router	Switch	Firewall
Roma - via Vitorchiano	2	77	12
Roma - via Ulpiano	-	21	2
Roma - via Affile	-	4	2

I paragrafi seguenti entrano nel merito delle tecnologie di networking e sicurezza impiegate in ciascun sito dipartimentale.

2.1 Architettura Sede Via Vitorchiano

La sede di Via Vitorchiano rappresenta il centro nevralgico per quanto riguarda l'architettura IT.

All'interno di tale sede è presente infatti il Datacenter principale che ospita tutti i sistemi che erogano servizi sia interni che su connettività pubblica.

Inoltre tale sede ospita gli apparati adibiti alla gestione della connettività Internet

L'architettura di rete centrale è organizzata seguendo il paradigma "collapsed network". È dunque presente:

- Un'architettura di core (layer 3) centrale implementata con una coppia di next-generation firewall Sonicwall Supermassive in alta affidabilità
- Un'architettura di accesso (layer 2) implementata con apparati Extreme Network Black Diamond e Summit-X series.
- L'architettura di sicurezza è invece realizzata utilizzando tre differenti bastioni ciascuno a difesa di un'area di rete ben specifica:
- Firewall perimetrale: implementato attraverso una coppia di next-generation firewall Fortigate
- Firewall di core: implementato attraverso una coppia di next-generation firewall Sonicwall Supermassive
- Firewall Intranet/Infranet: implementato attraverso una coppia di next-generation firewall Fortigate

Lo scopo dei firewall perimetrali è quello di proteggere l'architettura da eventuali attacchi provenienti da connettività pubblica. Oltre a fungere da default gateway per le reti DMZ svolgono funzionalità di VPN Concentrator su tecnologie IPSEC e SSL. Svolgono inoltre controlli UTM approfonditi come ad esempio Web Filtering, Application Control, IPS Control e similari

Lo scopo dei firewall di core è quello di proteggere le reti interne (utenti e server Back End) oltre che fungere da default gateway per tali reti. Svolgono inoltre controlli UTM approfonditi come ad esempio Web Filtering, Application Control, IPS Control e similari

Lo scopo dei firewall Intranet/Internet è quello di proteggere l'architettura da eventuali attacchi provenienti da connettività Intranet o Infranet. Tali firewall non svolgono alcun controllo UTM

Il livello network è totalmente gestito dai firewall descritti e non è utilizzato alcun protocollo di routing.

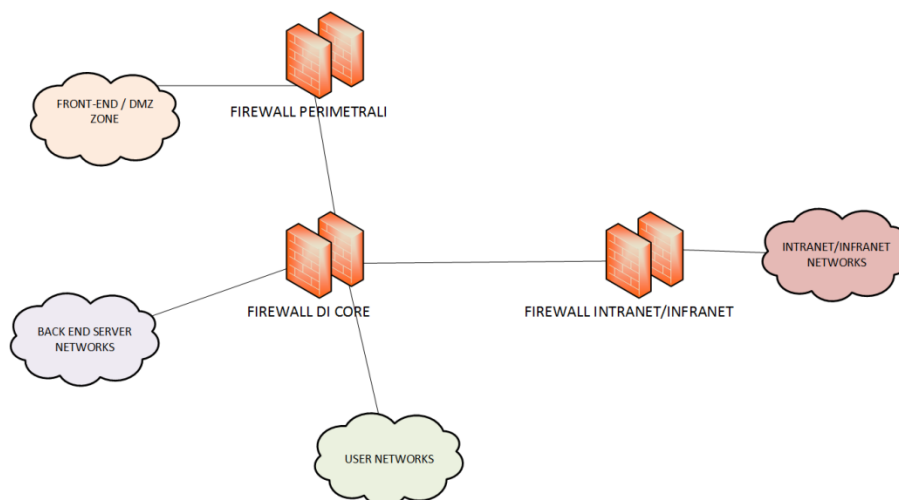


Figura 2 – Architettura Infrastruttura di Rete Via Vitorchiano

L'architettura interna è suddivisa in zone a cui è associato un differente livello di sicurezza. Le principali zone implementate sono:

- **Back End Network:** in questa zona sono ospitati tutti i server in grado di erogare servizi interni (es. Active Directory, Fileshare)
- **DMZ Network:** in questa zona sono ospitati tutti i server in grado di erogare servizi esposti su connettività pubblica (es. Mail, siti web)
- **User Network:** in questa zona sono ospitati tutte le reti utenti interne
- **Intranet/Infranet Network:** questa zona comprende tutte le reti esterne, siano esse di tipo Intranet che Infranet. Ad esempio rientrano in questa categoria le reti implementate nei siti remoti di Via Ulpiano e Via Affile, le reti appartenenti a differenti amministrazioni pubbliche (es. Palazzo Chigi) e le reti gestite dislocate nei centri regionali di protezione civile.

La sicurezza dell'intera infrastruttura è realizzata oltre che sfruttando i servizi Next-Gen Firewall e UTM a bordo dei rispettivi firewall di core e perimetrale, anche sfruttando avanzati controlli ATP svolti dalla suite di prodotti Fireeye.

Nello specifico nel sito di Via Vitorchiano sono implementati i seguenti prodotti:

- FireEye NX serie 7xxx : utilizzato per analizzare il traffico web diretto verso applicazioni interne o Internet
- FireEye EX serie 3xxx: utilizzato per rilevare la presenza di threat avanzati all'interno dei messaggi di posta elettronica inviati o ricevuti
- FireEye HX serie 4xxx: utilizzato per rilevare la presenza di threat avanzati sulle postazioni di lavoro

2.2 Architettura "Wifi@DPC"

Il progetto "WiFi@DPC" propone l'introduzione della tecnologia WiFi presso il Dipartimento Nazionale Protezione Civile.

Scopo principale dell'architettura è quello di garantire massima libertà nella navigazione e di fruizione dei servizi su internet agli utenti, unitamente al pieno rispetto delle leggi vigenti e attinenza alle politiche di necessaria sicurezza attualmente implementate presso DPC

L'infrastruttura wireless è nata con lo scopo di fornire servizi di Hotspot Guest Internet per visitatori e personale interno. Nello specifico le aree coperte sono quelle di maggior aggregazione come ad esempio Auditorium, sale riunioni, sale emergenza e sala Comitato Operativo.

L'infrastruttura wireless e la rete di distribuzione è implementata per mezzo di tecnologie Extreme Network Summit, WM200 controllers e Altitude 450 AP.

Il livello di routing dell'infrastruttura è svolto in parte dai controller proprietari Extreme Network, in parte da una coppia di firewall perimetrali Fortigate entrambi configurati in alta affidabilità. Quest'ultimi hanno tra l'altro il compito di erogare un servizio Captive portal indispensabile per l'autenticazione di accesso alla rete.

Infine, una coppia di Domain Controller Active Directory implementati su sistemi Microsoft Windows server sono impiegati come repository remoti delle utenze.

I sistemi operativi impiegati per il corretto funzionamento dell'infrastruttura sono implementati in tecnologia virtuale e installati a bordo di host VMware.

Per la distribuzione ai piani dei segnali wireless sono utilizzati infine una serie di switch Extreme Network Summit series configurati in modalità stacking e interconnessi con i nodi centrali Black Diamond.

2.3 Log Management

La soluzione DPC di Log Management & Correlazione si compone di una piattaforma di sicurezza HPE ArcSight dedicata a:

- Collezionare, aggregare, conservare, ricercare ed analizzare centralmente i log provenienti dai sistemi, database, applicazioni, apparati e dispositivi del Dipartimento della Protezione Civile.
- 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;
- **Cyber Security**
Per collezionare e mantenere eventi generati dagli apparati di sicurezza, apparati di rete e sistemi informativi, al fine di consentire indagini a seguito di incidenti di sicurezza, e di generare allarmi in caso di violazioni di policy, accessi non autorizzati o atti ostili.

2.3.1 Architettura Log Management

L'infrastruttura di LM & CO è composta dalle seguenti tipologie di appliance distribuite presso il CED di Vitorchiano (sito primario).

- 9 **Connector** dedicati alla funzione di raccolta degli eventi di rete in esecuzione su 4 macchine virtuali;
- 1 **Logger** appliance L7600 dedicato alla funzione di Log Management degli eventi di privacy, sicurezza e di rete;
- 1 **Correlator** appliance Express EE-7600 (**ESM**) dedicato alla funzione di correlazione per gli eventi di tipologia network e sicurezza

2.4 Architettura Sedi Via Ulpiano e Via Affile

L'architettura IT delle sedi di Via Affile e Via Ulpiano sono abbastanza simili. In ciascuna sede è presente una coppia di firewall (tecnologia Sonicwall per Ulpiano e Fortigate per Affile) aventi come unico obiettivo quello di interfacciare la sede con quella principale di Via Vitorchiano. Tali firewall fungono da default gateway per le reti interne e svolgono solo funzionalità di access filtering. Nessun altro controllo aggiuntivo è attualmente implementato.

L'infrastruttura di accesso è invece realizzata:

- Da apparati Extreme Network Summit series presso la sede di Via Affile. La ridondanza in tal caso è implementata facendo ricorso alle tecnologie di Stacking
- Da apparati Extreme Network Summit series e Black Diamond series e Cisco 3xxx e 4xxx Series presso la sede di Via Ulpiano. In tal caso la ridondanza è implementata oltre grazie alle tecnologie di Stacking anche per mezzo del protocollo PVST+.

2.4.1 Architettura Sede Via Ulpiano

La sede di Via Ulpiano rappresenta la sede istituzionale storica del Dipartimento di Protezione civile. Al suo interno è presente un Datacenter di ultima generazione interconnesso per mezzo di una rete altamente performante e ridondata realizzata principalmente con tecnologie Extreme Networks Black Diamond e Summit series.

Attualmente il datacenter ospita alcuni sistemi utilizzati all'interno della sede basati principalmente su sistemi operativi Microsoft.

Nel complesso l'architettura prevede dunque:

- Un'infrastruttura di rete verticale impiegata per interconnettere i sistemi e le PDL all'interno del palazzo
- Un'infrastruttura di rete orizzontale impiegata per interconnettere i rack e i sistemi presenti all'interno del Datacenter presente al piano terra della sede istituzionale. Quest'ultima è realizzata principalmente con tecnologie Cisco 3xxx e 4xxx

Gli apparati Extreme Network summit series sono configurati in modalità stacking al fine di avere da un lato un elevato livello di ridondanza dall'altro una maggior semplicità di gestione.

Il livello di routing è svolto unicamente da una coppia di firewall Sonicwall Supermassive che fungono quindi da elemento centrale. I firewall sono implementati in configurazione cluster high-availability Active/Passive con abilitazione della funzionalità Preempting Mode.

I firewall Sonicwall Supermassive svolgono inoltre anche funzionalità avanzate di firewalling sul traffico in transito.

All'interno della sede di Via Ulpiano non è presente alcun link WAN Internet. L'unica connettività WAN è attestata su una linea ridondata multi-VRF impiegata per mettere in comunicazione tale sede con quella principale di Via Vitorchiano. L'intera connettività Internet/Intranet viene fatta dunque confluire attraverso tale collegamento

Lo schema seguente illustra l'architettura logica di massima dell'infrastruttura di rete implementata presso la sede di Via Ulpiano.

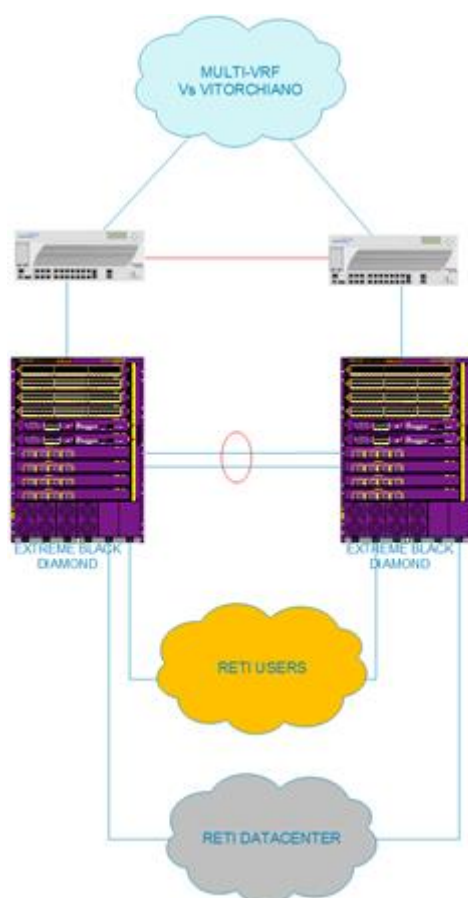


Figura 3 - Layout logico dell'architettura di rete di Via Ulpiano

2.4.2 Architettura Sede Via Affile

La sede di Via Affile rappresenta il principale polo logistico del Dipartimento di Protezione Civile.

L'architettura di rete implementata all'interno di tale sede ha il solo compito di interconnettere i sistemi e le PDL presenti all'interno della sede; non è pertanto presente alcun datacenter al suo interno.

Così come Via Ulpiano, neanche la sede di Via Affile è dotata di un accesso WAN Internet autonomo. Anche in tal caso è infatti presente un singolo collegamento WAN MultiVRF utilizzato per interconnettere la sede con Via Vitorchiano. Ancora una volta l'intera connettività Internet/Intranet è fatta dunque confluire sul link privato multiVRF.

Le principali distinzioni rispetto alla sede di Via Ulpiano sono:

- L'intero livello di routing e firewalling è svolto da una coppia di apparati Fortigate
- Il livello data-link è implementato per mezzo di una coppia di apparati Summit Extreme Networks configurati in modalità stacking.

2.5 Architettura Sede Disaster Recovery - Palmanova

La sede di Via Natisone, Palmanova agisce come sito di Disaster Recovery per i servizi erogati dal datacenter principale di via Vitorchiano.

Tale sede replica fedelmente l'architettura di rete del sito principale: di conseguenza è composta da:

- Un'architettura di core (layer 3) centrale implementata con una coppia di next-generation firewall Sonicwall Supermassive in alta affidabilità
- Un'architettura di accesso (layer 2) implementata con apparati Extreme Network Black Diamond e Summit-X series.
- L'architettura di sicurezza è invece realizzata utilizzando tre differenti bastioni ciascuno a difesa di un'area di rete ben specifica:
 - Firewall perimetrale: implementato attraverso una coppia di next-generation firewall Fortigate
 - Firewall di core: implementato attraverso una coppia di next-generation firewall Sonicwall Supermassive
 - Firewall Intranet/Infranet: implementato attraverso una coppia di next-generation firewall Fortigate

L'interconnessione con il sito principale è realizzata per mezzo di un collegamento MPLS multi-VRF dedicato, come illustrato in figura

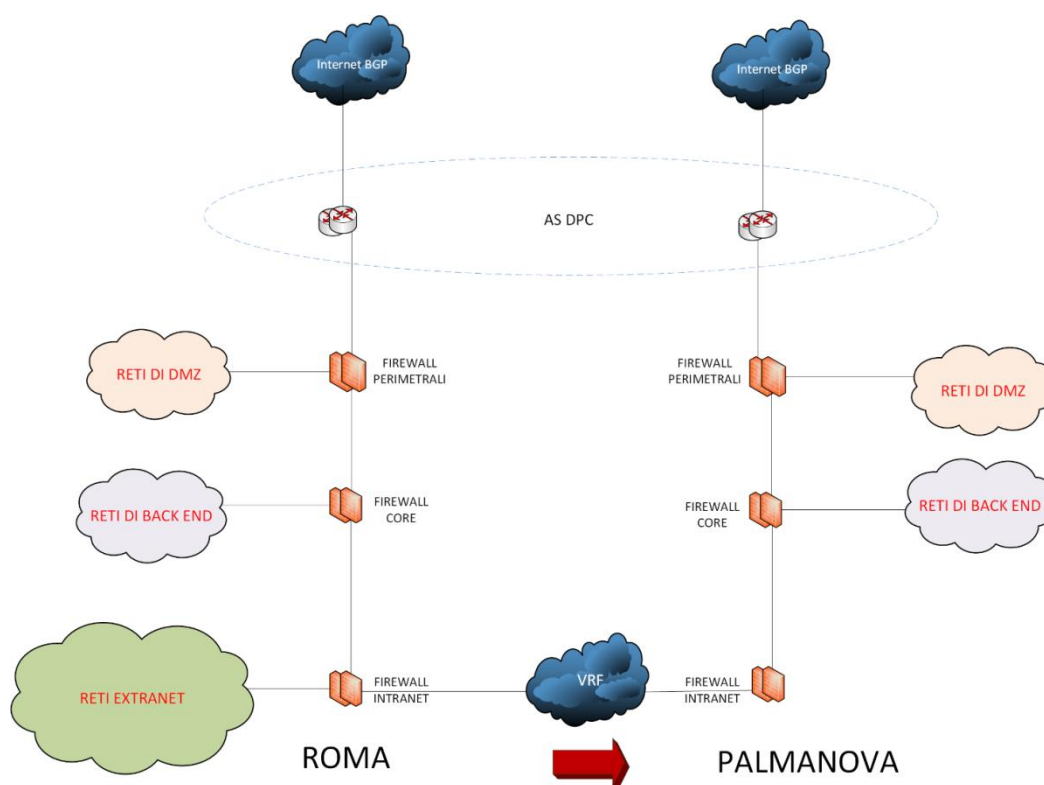


Figura 4 – Schema logico Disaster Recovery

Nella situazione attuale l'indisponibilità della sede di via Vitorchiano, a causa di un evento disastroso, porterebbe alla non raggiungibilità di tutti i servizi (compresa la posta elettronica del Dipartimento), con l'eccezione del sito web istituzionale che è connesso a Internet con una sua connessione distinta.

In questo modo, in caso di disastro, la connettività sarà ripristinata riconfigurando i router internet di Palmanova. Le operazioni di riconfigurazione possono essere effettuate per via remota, con l'obiettivo di ristabilire le connessioni nel più breve tempo possibile, entro tre ore dalla proclamazione del disastro. Per il Disaster Recovery verrà configurata sul centro di Palmanova una subnet IP sempre attiva, che non necessiterà quindi di essere annunciata sulla rete dal sito di Vitorchiano, in modo da rendere raggiungibile il sito di Palmanova direttamente per le necessità di manutenzione. In caso di disastro, tutti i restanti IP verranno riconfigurati nel più breve tempo possibile, in modo da rendere raggiungibili tutti i servizi man mano che questi verranno ripristinati sul centro di Palmanova. Sono attualmente allo studio prodotti che consentono di allineare automaticamente anche le configurazioni dei firewall.

2.6 Enti esterni connessi alla rete

Dati i compiti istituzionali del Dipartimento a livello nazionale, esistono alcune realtà che hanno necessità di connessione verso l'hub di via Vitorchiano, per lo scambio di dati o per l'accesso ai servizi erogati.

3 Postazioni di Lavoro

Nella seguente tabella è riportata la configurazione delle postazioni di lavoro e dei componenti accessori attualmente installati presso gli utenti del Dipartimento Protezione Civile.

Tipologia	n. pezzi
WORKSTATION	1.082
NOTEBOOK	272
STAMPANTI	507
SCANNER	328
ETICHETTATRICI	121

4 Infrastrutture tecnologiche dipartimentali

L'infrastruttura tecnologica di supporto alle attività informatiche del Dipartimento si articola nelle seguenti sette aree.

1. **Applicazioni di supporto** (Fileserver e Sharepoint).
2. **Autenticazione e indirizzamento** (Active Directory, DNS e proxy).
3. **Connettività e sicurezza** (Cyber security e malware protection, servizio NTP, infrastruttura Wi-Fi)
4. **Messaggistica** (Fax server, piattaforma per le comunicazioni unificate, posta elettronica e sistemi di videoconferenza.)
5. **Monitoraggio** (Service management, sistema di monitoraggio, CMDB, asset management).
6. **Sistemi di backup.**
7. **Telefonia fissa.**

Nel seguito una sintetica descrizione di ciascuna area e una valutazione della criticità del servizio per l'operatività del Dipartimento

4.1.1 Fileserver e Sharepoint

I Fileserver (due) sono server virtuali che consentono di condividere documenti tra i vari utenti del dipartimento.

Il prodotto Microsoft Sharepoint viene utilizzato per realizzare alcuni siti di condivisione documentale per diverse applicazioni dipartimentali.

L'architettura Fileserver è basata su due server virtuali Windows Server 2012 R2.

L'architettura Sharepoint è invece composta da otto server virtuali Windows Server 2012 R2

4.1.2 Servizio di Active Directory

Il servizio effettua la gestione centralizzata delle funzioni di identificazione, autenticazione e autorizzazione degli utenti. L'infrastruttura Active Directory (AD) è un raggruppamento logico di utenti e computer in un dominio, gestito centralmente da alcuni server detti "Domain Controller". AD fornisce informazioni sugli oggetti, li organizza, controlla l'accesso e ne imposta la sicurezza. Ciascun oggetto rappresenta una singola entità (ad esempio un utente, un computer, una stampante oppure un gruppo di utenti) con e i suoi attributi. Alcuni oggetti possono anche essere contenitori di altri oggetti. Un oggetto è identificato univocamente dal suo nome e ha un insieme di attributi — le caratteristiche e l'informazione che l'oggetto può contenere — definiti da uno schema, che determina anche il tipo di oggetti che possono essere registrati.

La foresta Active Directory del Dipartimento è composta da un unico dominio Root "PROTEZIONECIVILE.IT", in modalità Windows2008 r2. È poi presente un unico site che comprende le sedi di Via Vitorchiano e Via Ulpiano. Ogni Domain Controller ha i seguenti ruoli:

- DHCP (configurati in modalità *failover hot standby*);
- GC (Global Catalog);
- DNS

Complessivamente sono presenti quattro sistemi Domain Controller Microsoft Windows Server 2012. Servizio DNS e Proxy

L'infrastruttura DNS può essere suddivisa nel seguente modo:

- Infrastruttura atta ad erogare il servizio di DNS interno:
 - ✓ Gestione centralizzata delle utenze (servizio erogato da due DC Microsoft Windows Server dominio snipc.dpc.local)
 - ✓ Gestione record DNS interni (servizio erogato da quattro DC Microsoft Windows Server dominio protezionecivile.it)
- Infrastruttura atta ad erogare il servizio di DNS pubblico (servizio erogato da due server Linux)

L'infrastruttura proxy dipartimentale è composta da tre Server Linux che erogano servizio di navigazione proxy, webfiltering e caching. Nello specifico il servizio utilizzato è Squid.

I server Proxy sono presenti all'interno dell'infrastruttura di Via Vitorchiano e collocati nell'area logica DMZ.

La figura seguente illustra l'ubicazione logica dell'area DMZ.

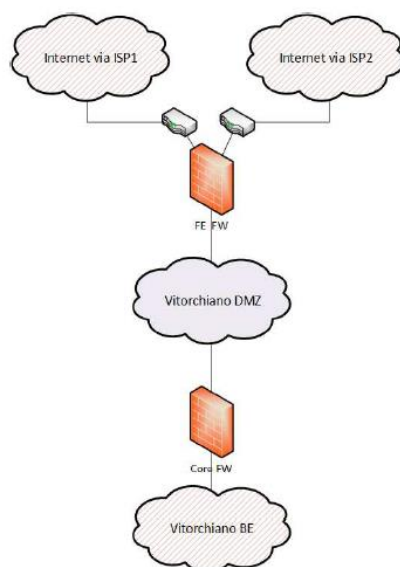


Figura 5 – Zone architettura Via Vitorchiano

Il compito dell'infrastruttura di Reverse Proxy è quello di pubblicare all'esterno applicativi e siti web dipartimentali. L'architettura si compone di due server Linux e due bilanciatori. Anche in tal caso i sistemi risiedono all'interno dell'area logica DMZ di Via Vitorchiano e anche in tal caso Squid è il servizio utilizzato per implementare la funzionalità di Reverse Proxy.

4.1.3 Servizio NTP (Network Time Protocol)

La sincronizzazione degli orari dei dispositivi all'interno delle reti dipartimentali è garantita da quattro server virtuali Linux (Debian GNU/Linux) che mantengono l'orario sincronizzato con il servizio di sincronizzazione dell'Istituto Nazionale di Ricerca e Metrologica e redistribuiscono tale segnale ai Domani Controller Active Directory ed agli altri dispositivi dipartimentali.

La Figura riporta l'architettura utilizzata

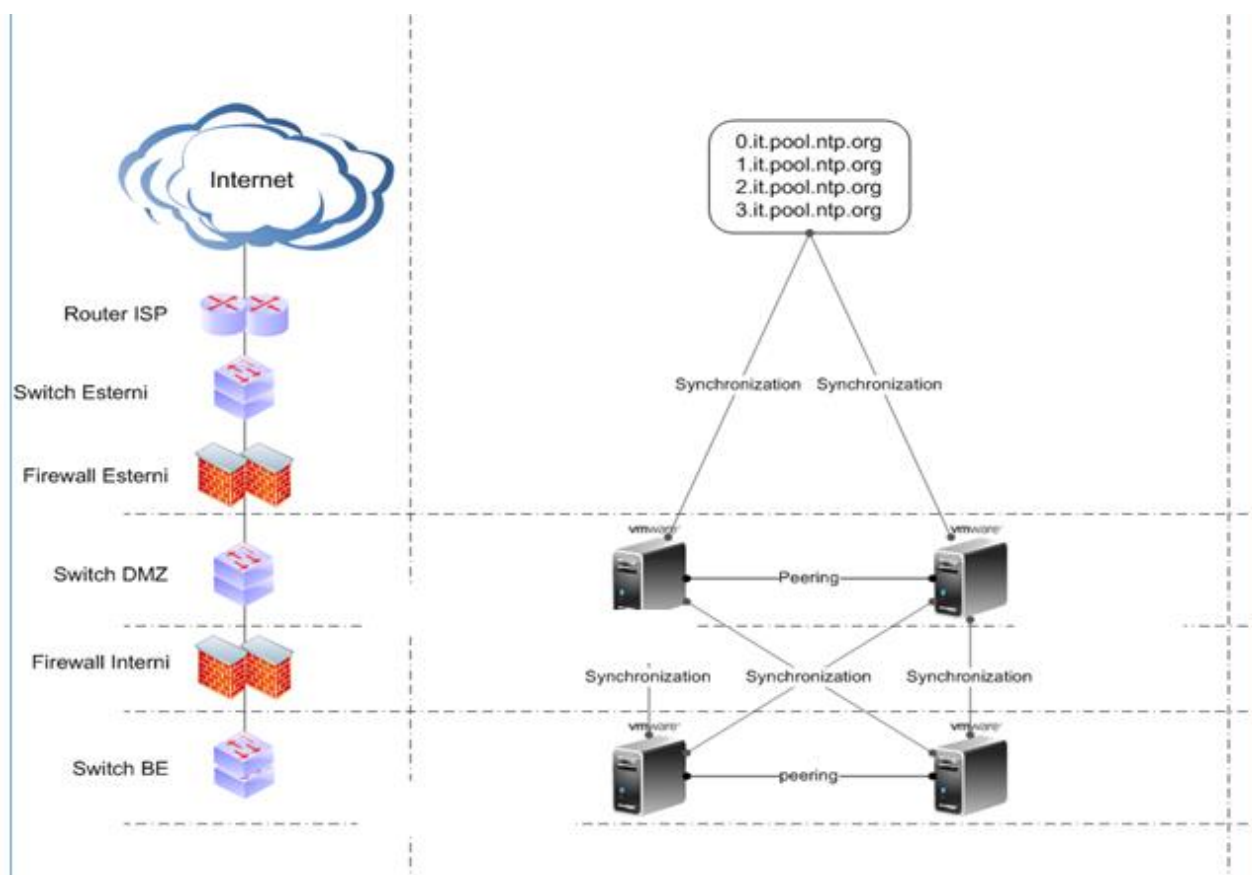


Figura 6 - Architettura del servizio NTP

4.1.4 Servizio di Posta Elettronica

Il servizio di posta elettronica del Dipartimento si basa su un'infrastruttura Microsoft Exchange 2103 ed è interamente ospitata nel datacenter di Via Vitorchiano. Il servizio è erogato da 6 server virtuali (4 server Exchange e 2 server Application Request Routing).

Attualmente il servizio ospita circa 1000 mailbox divise in 21 database, più 47 mailbox su un ulteriore database, dedicate a ricevere i report di Journaling per le mailbox per cui è previsto il servizio.

Il servizio DAG (Database Availability Group) fornisce il ripristino automatico del database in caso di guasti ed è configurato per avere una copia di ogni database attivo. DAG è implementato sui sistemi associati al ruolo Mailbox Server. Quest'ultimi incorporano inoltre tutte le funzionalità di accesso dei client, del trasporto, di gestione dei database e di unified messaging.

I Client Access Server incorporano le funzionalità di accesso al servizio di tutti i client (per tutti i protocolli), preoccupandosi dell'autenticazione degli utenti e della redirectione delle connessioni verso il mailbox server che ospita il database attivo.

I server Exchange 2013 sono in area di Back End ed iscritti al dominio Active Directory del dipartimento.

I server Application Request Routing sono invece in area DMZ e fungono da reverse proxy dei servizi esposti su internet.

I client dalla rete interna accedono direttamente attraverso i CAS Exchange in DNS round robin.

4.1.5 Servizio di fax server

L'applicativo Zetafax consente agli utenti la possibilità di ricevere ed inviare fax da Client, Outlook, Web Client e da una macchina fax (se collegata ad una ATA - Analog Telephone Adaptor).

Il servizio si articola in quattro componenti funzionali:

- 6 Zetafax Client: consente la gestione, invio e ricezione fax da PC
- 7 Zetafax Server Monitor: consente di monitorare lo stato del servizio, cronologia eventi e messaggi real time dei fax in transito
- 8 Zetafax Configuration: consente la configurazione del servizio, gestione utenti
- 9 Manager Zetafax Server service: consente di avviare o bloccare il servizio Zetafax

4.1.6 Sistemi per la videoconferenza

Il sistema di Telpresence installato presso la sede di Vitorchiano, si compone di una serie di macchine che permettono la trasmissione dei segnali audio-video, e di gestione della stessa:

Il sistema si compone di:

- MCU Cisco Codian (Multi-Suite Control Units);
- VCS (Video Communication Control, deployed inside the firewall);
- VCS (Video Communication Control Expressway, deployed outside the firewall);
- TCS (Telepresence Content Server, gestisce le registrazioni);
- ISDN Gateway (per chiamate H320);
- TMS Server (Software di gestione);
- Endpoint (apparati di videoconferenza);
- Jabber (software di videoconferenza).

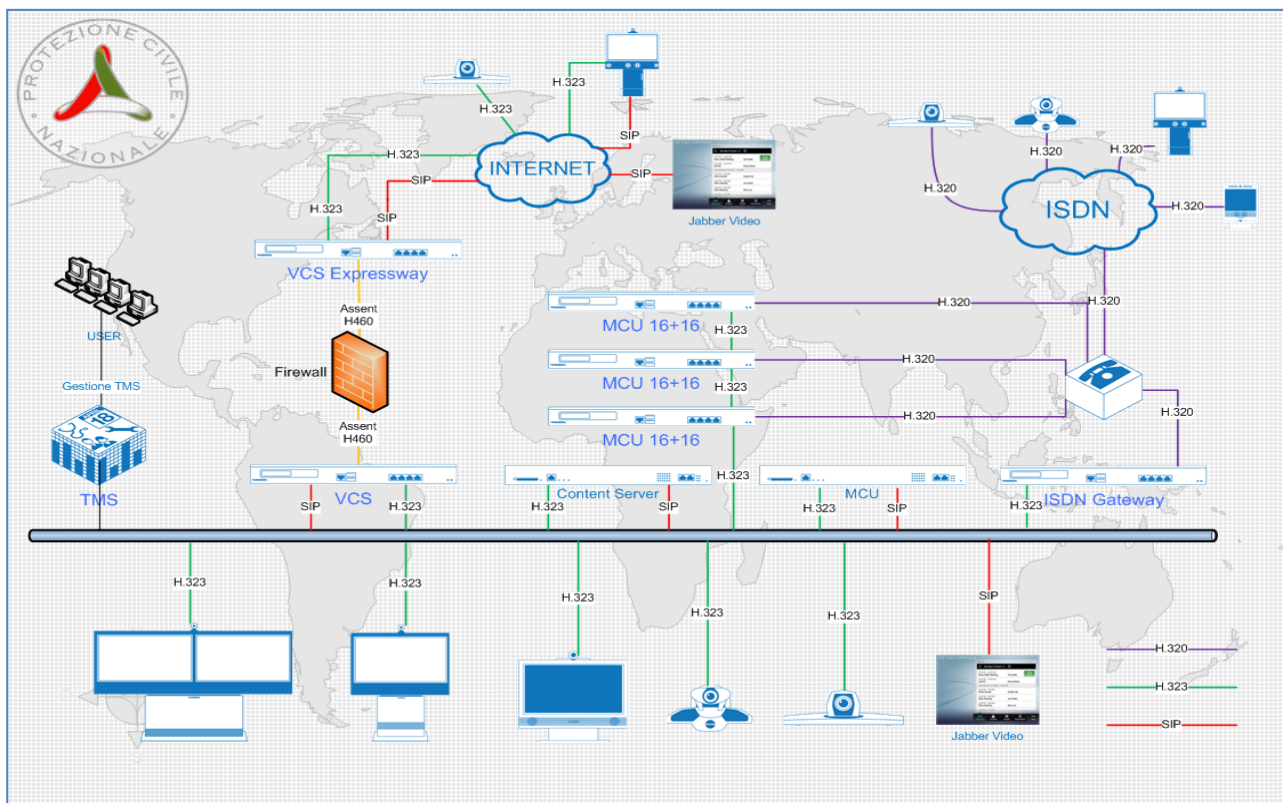


Figura 7 - Architettura del sistema di videoconferenza

Il sistema consente di ricevere chiamate H323, H320, SIP, mediante apparati di sala o mediante applicativi software installati su dispositivi fissi o mobile.

Il Server TMS è installato su un server virtuale, in modo da consentire la gestione del sistema.

4.2 Strumenti di gestione

Gli strumenti di gestione attualmente in uso presso il Dipartimento si compongono di:

- Una piattaforma di monitoraggio dei sistemi e dei servizi e delle applicazioni in logica end-to-end;
- Una piattaforma di Service Desk per la gestione del ciclo di vita delle segnalazioni informative/malfunzionamento/richieste di change da parte degli utenti;
- Una piattaforma di service management articolata in:
 - Un sistema di Trouble Ticketing;
 - Un sistema di Asset e Configuration Management (CMDB);
 - Una Knowledge Base;
 - Un sistema di reportistica.

Di seguito sono descritti i principali componenti che costituiscono le infrastrutture suddette.

4.2.1 Piattaforma di Monitoraggio

La Piattaforma di Monitoraggio tiene controllo lo stato operativo dei sistemi, delle loro componenti e degli apparati di rete, rilevando automaticamente le informazioni relative a:

- stato dei diversi sistemi, sottosistemi, servizi ed apparati;
- parametri critici per la funzionalità dei diversi sistemi, sottosistemi, servizi ed apparati, definendo dei valori di soglia che denuncino la prossimità di situazioni critiche. In particolare i parametri riguardano:
 - le allocazioni di spazio disco;
 - l'utilizzo della memoria;
 - l'utilizzo della CPU;
 - l'utilizzo delle interfacce di rete;
 - lo stato dei processi applicativi che siano di particolare rilevanza per la funzionalità dei servizi erogati;
 - i parametri critici per la funzionalità dei processi applicativi, in base ai valori di soglia che determinano la prossimità di situazioni critiche.

La Piattaforma di Monitoraggio è attualmente costituita dalle seguenti componenti:

HPE	HPE Operations Manager i 10.00, Build 172	Dashboard Centralizzata eventi/topologia
HPE	HPE Business Service Management 9.25.221, Build 378	Monitoraggio applicativo Manager
HPE	Business Process Monitor Version 9.23 Build 541	Monitoraggio applicativo (numero di transazioni)
HPE	HPE Operations Manager Build: A.17.0.120.29 Version: A.09.00	Monitoraggio Sistemi

HPE	NNMi Version 10.00.701,10.01.001,10.01.002	Monitoraggio Network
HPE	HPE SiteScope 11.24.421 64-bit JVM, Build 498	Monitoraggio Applicativo Agentless
HPE	uCMDB 10.20.CPU1.545	Configuration Manager
HPE	BSM Connector (integrazione SCOM e NNMi) 12.00.052	Connettore eventi e topologia SCPM e NNMi
HPE	OO Core Version 10.20 Build 49	Automazione: operation orchestration
HPE	SM Version: 9.35.4001 P4	Service Manager
HPE	Connect IT: version 9.50	Connettore di integrazioni
HPE	AM: Version 9.41	Asset Manager
HPE	NNMSPI 10.00 NPS10P01	Collettore performance apparati di rete

4.2.2 Service Desk

Il Service Desk costituisce il punto centralizzato di tutte le attività di gestione dei servizi. Tutte le richieste di servizi dei clienti vengono inoltrate attraverso il Service Desk, sia che vengano iniziate da una telefonata, da un messaggio e-mail o dall'interfaccia web self service, permettendo così all'IT di centralizzare, assegnare task, gestire e risolvere i problemi con efficienza.

Fornisce all'operatore di primo livello tutti gli strumenti per documentare, catturare e aggiornare le informazioni su una richiesta o problema legato ad un cliente; esso può massimizzare le possibilità di risoluzione della richiesta alla prima chiamata grazie alla sua base di conoscenza interna sullo stato di avanzamento di attività in corso e su problemi affini verificatisi in passato.

Questo permette ai tecnici specializzati di essere più veloci nel risolvere le chiamate e quindi dedicarsi a questioni più complesse. Quando i problemi sono ricorrenti, le loro soluzioni sono raccolte nella base di conoscenza, per essere riutilizzate; infine possono essere facilmente generati rapporti sulle performance globali del servizio di service desk.

Completato il modulo, la richiesta viene evasa indirizzandola alla struttura organizzativa preposta.

Gli utenti finali possono controllare via web lo stato delle proprie richieste, ed eventualmente modificarle e chiuderle.

La piattaforma di service desk per gli utenti è costituita da un applicativo web custom in ASP con database di appoggio MS SQL Server.

4.2.3 Service Manager

Il Service Manager è lo strumento a supporto dei processi di incident management e change management.

○ **Piattaforma di Incident Management**

Il modulo “Incident Management” automatizza l’intero ciclo di vita dell’incident migliorando l’efficienza dei tecnici incaricati del troubleshooting.

Il modulo comprende una potente categorizzazione degli incident pronta per l’uso, oltre a workflow di routing ed escalation che possono essere innescati sulla base di criteri quali SLA, impatto, urgenza, Configuration Item, localizzazione o cliente.

Una volta che un incident è risolto, il modulo HelpDesk fornisce un circuito automatizzato di feedback per convalidare la soluzione e salvarla per un uso futuro.

Viene fornito anche un aiuto a monitorare il rispetto dei livelli di servizio tramite segnalazioni in caso di violazione delle regole di business.

Il supporto del CMDB ai processi di incident e problem management è fornire una vista sullo stato effettivo del configuration item oggetto dell’incident per avere informazioni che possano aiutare l’operatore a risolvere il problema il più presto possibile, magari evidenziando un configuration item correlato che al momento risulta avere un funzionamento non idoneo.

○ **Change Management**

Lo scopo del processo di Change Management è la gestione dei processi di change e release management.

L’obiettivo del processo di Change Management è mettere a disposizione metodologie e procedure standardizzate per gestire in modo efficace ed efficiente tutte le modifiche ad elementi IT nell’ottica di minimizzare il numero e l’impatto di ogni incident correlato sui servizi.

Il Change Management si basa sull’implementazione di un workflow che gestisce il processo. Il workflow definisce le regole atte a controllare le modifiche per tutto il loro ciclo di vita: dalla richiesta iniziale all’approvazione, alla programmazione e implementazione, al monitoraggio e valutazione.

Il disegno e l’implementazione del processo di change management si basano sull’omonimo modulo “Change Management” di HP Service Manager, che fornisce potenti capacità di implementazione dei processi/workflow di modifica, con la definizione delle fasi e dei task.

Il motore interno del modulo documenta le modifiche nel tempo, categorizzando ed assegnando le risorse in modo più efficace, permettendo alle modifiche di percorrere vie seriali o parallele.

Il modulo Change Management fornisce gli strumenti per la gestione delle approvazioni, strumenti che permettono:

- l’adeguato livello di supervisione da parte di un Change Advisory Board (CAB) e dei vari responsabili organizzativi;
- di mantenere l’accordo tra le parti in causa su quali modifiche vengono apportate con l’assicurazione che tali modifiche sono state effettuate correttamente;

di aggiornare automaticamente i dati di gestione della configurazione, in modo che le modifiche all’infrastruttura IT siano accuratamente riportate nel CMDB.

4.1 Osservatorio delle Strutture Sismiche (OSS)

La strategia di monitoraggio sismico del Dipartimento si basa su tre reti di ambito nazionale. Scopo primario delle reti è quello di fornire informazioni sull'entità delle scosse sismiche e su eventuali danni provocati. I dati raccolti servono inoltre come base, a disposizione della comunità scientifica, per studi ed approfondimenti in campo sismico ed ingegneristico.

La prima rete, chiamata "Rete Sismometrica Nazionale", è costituita da circa trecento stazioni dislocate sul territorio nazionale ed è gestita dall'Istituto Nazionale di Geofisica e Vulcanologia (INGV) tramite il suo Centro Nazionale Terremoti (CNT). Essa opera la sorveglianza sismica per l'individuazione dell'epicentro e della magnitudo dei terremoti in tempo quasi-reale.

Le altre due reti sono gestite direttamente dal Dipartimento e sono: l'"Osservatorio Sismico delle Strutture" (OSS), descritta in questa sezione, e la "Rete Accelerometrica Nazionale" (RAN), descritta nel seguito.

L'Osservatorio Sismico delle Strutture ha l'obiettivo di acquisire dati dalla rete MOT OSS (Monitoraggio sismico del territorio) e di elaborarli al fine di identificare il danno subito dagli edifici monitorati. Tramite la rete dell'OSS vengono erogati una serie di servizi di informazione sull'attività sismica del territorio. Inoltre, è a questa rete che arrivano i segnali dei vari apparati che nel territorio controllano l'attività sismica in tempo reale.

Si tratta di una rete a "trigger", ossia le stazioni collegate alla rete delle strutture avviano la registrazione solo se la soglia minima di trigger viene superata. Una volta acquisito, il dato viene elaborato da particolari software che effettuano l'analisi dei dati e provvedono alla reportistica e all'allerta via e-mail e SMS. La trasmissione dei dati, in base alla collocazione geografica della stazione, può avvenire sia in ADSL, 3G, Satellitare o PSTN tradizionale. Questi dati, una volta scaricati sul proprio server (che varia in base al produttore della strumentazione), vengono inviati al server centrale (SMC), che ne permette l'archiviazione in un database.

La Figura riporta una descrizione ad alto livello della rete.

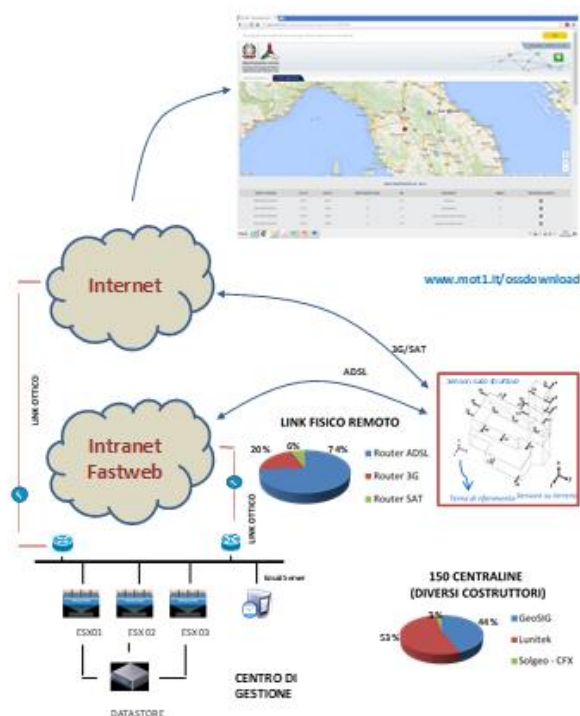


Figura 8 – Osservatorio Sismico delle Strutture

La rete OSS è composta da:

Numero di server: 16
Application server: Windows Server 2003 / Windows Server 2008 R2 / CENTOS 7
Web server: IIS, Apache
RDBMS: Microsoft SQL, MySQL, MariaDB (derivazione di MySQL)

L'infrastruttura server della rete osservatorio sismico nazionale in gestione è costituita da un cluster VMWARE ESX virtuale composto da tre nodi e da uno storage SAN; su di essi sono in esecuzione un insieme di macchine virtuali che erogano servizi per l'OSS. I nodi ESX e la SAN sono implementati con dei server IBM.

4.2 Rete Accelerometrica Nazionale (RAN)

Scopo della Rete Accelerometrica Nazionale è quello di misurare le accelerazioni indotte al suolo, lungo i tre assi di una terna cartesiana, da un sisma forte (strong motion) che interessi una porzione del territorio nazionale.

La misurazione è fatta tramite acquisitori “compatti”, che si interfacciano con tre sensori accelerometrici, disposti secondo i tre assi di una terna cartesiana di riferimento, le cui uscite, una volta campionate e digitalizzate, vengono memorizzate su una memoria locale. In caso di superamento di una certa soglia (0,1 % dell’accelerazione di gravità), vengono inviate, tramite collegamento TCP/IP, al Centro di Gestione RAN situato presso la sede del Dipartimento di via Vitorchiano in Roma.

L’accesso ad Internet delle singole centraline è ottenuta in modalità Mobile, sfruttando la tecnologia GPRS/EDGE/3G. Presso il Centro di Gestione RAN le forme d’onda vengono elaborate, allo scopo di individuare l’epicentro dei terremoti con una intensità superiore ad una certa soglia, nonché alcuni parametri indicativi dell’intensità del sisma. Le elaborazioni effettuate sono quindi archiviate in un Database e messe a disposizione della comunità scientifica per studi e approfondimenti. È attualmente attiva una connessione FTP che consente di inviare alcuni dei risultati delle elaborazioni all’INGV. È prevista anche la possibilità di inviare alcuni parametri del sisma ad una lista di cellulari di personale coinvolto nel monitoraggio.

La gestione dei dati che affluiscono al Centro di Gestione si basa sul DBMS (Data Base Management System) Antelope. Si tratta di un insieme di Software, su piattaforma Linux, espressamente sviluppati per trattare l’acquisizione, la distribuzione, l’archiviazione e l’elaborazione dei dati di monitoraggio ambientale.

La figura seguente riporta una descrizione ad alto livello della rete.

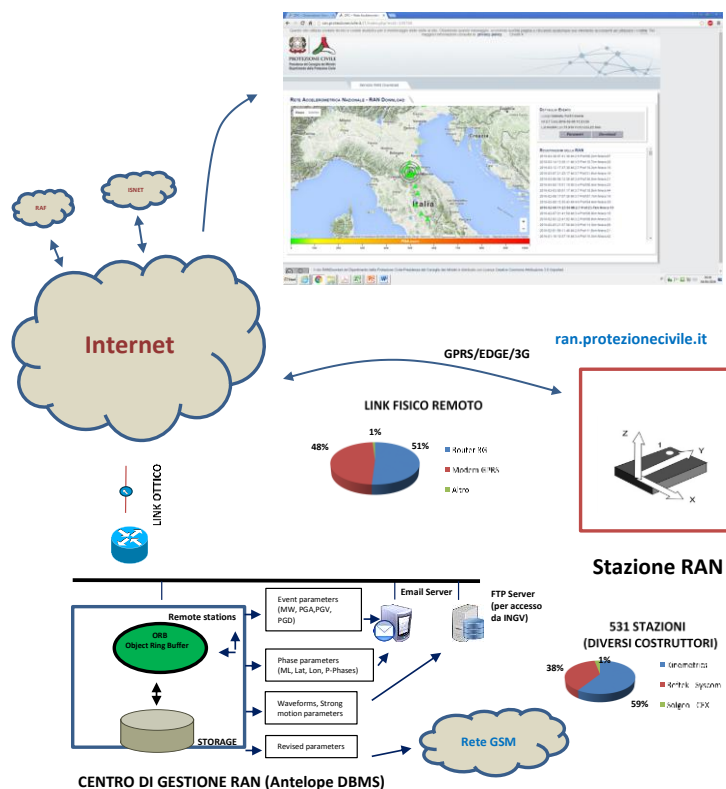


Figura 9 – Rete Accelerometric Nazionale

4.3 Centro Funzionale Centrale (CFC)

La gestione del sistema di allertamento nazionale è assicurata dal Dipartimento e dalle Regioni attraverso la rete dei Centri Funzionali, ovvero Soggetti preposti allo svolgimento delle attività di previsione, monitoraggio e sorveglianza in tempo reale degli eventi e di valutazione dei conseguenti effetti sul territorio.

La rete dei Centri Funzionali è costituita da un Centro Funzionale Centrale (CFC) presente all'interno della sede di Via Vitorchiano e da 21 Centri Funzionali Decentrati (CFD) presso le Regioni e le Province Autonome di Trento e Bolzano.

I compiti del CFC vengono svolti attraverso una serie di apparati hardware e di moduli software che, in sinergia, consentono agli operatori di raccogliere e condividere con gli altri CFD:

- i dati parametrici relativi ai diversi rischi provenienti dalle diverse reti di monitoraggio presenti e distribuite sul territorio;
- le informazioni provenienti dalle attività di vigilanza e contrasto degli eventi svolte sul territorio.

Il CFC elabora un'analisi in tempo reale degli eventi in atto, sulla base di modelli previsionali e di valutazione, e ne sintetizza i risultati concertati, ove del caso, tra CFC e CFD operativi interessati. Ogni CFD è equipaggiato di firewall e switch ed è interconnesso tramite rete MPLS Fastweb. I CFD inviano continuamente dati in tempo reale riguardanti il territorio al CFC, che è dislocato presso la sede operativa del Dipartimento.

Per mezzo del CFC il Dipartimento, insieme alle Regioni, garantisce il coordinamento del sistema di allertamento nazionale.

Sulla base del principio di sussidiarietà, nei casi in cui i CFD non siano attivi o siano temporaneamente non operativi, il CFC può svolgere tutti i compiti operativi loro assegnati.

Presso il CFC operano le seguenti applicazioni/servizi, meglio descritte nel seguito:

- **METEORA** (ora **METEOSYNC**): server ftp per l'acquisizione e l'esportazione di dati e modelli meteo;
- **CAE/ETG/CIMA**: server di accentramento dati idropluviometrici;
- **VDISK**: software utilizzato per esportare i bollettini di criticità e per condividere informazioni metereologiche e pluviometriche con le Regioni.

4.3.1 *MeteoSync*

L'infrastruttura Meteosync ha il compito di rendere fruibili dati meteo al sistema regionale del Dipartimento. L'infrastruttura è formata da 4 diversi sistemi virtuali basati su tecnologia Linux. Una coppia di server è interconnessa con un server presente presso l'Aeroporto militare di Pratica di Mare dal quale vengono prelevati i dati meteo tramite FTP, che a sua volta sincronizza tali dati con il cluster Linux, dove opera un server ftp a cui accedono i centri di protezione civile regionali.

La figura seguente illustra il funzionamento dei sistemi descritti

I server non hanno servizi in runtime, ma bensì lavorano tramite script che utilizzano protocolli lftp e rsync.

I dati vengono archiviati giornalmente e conservati per un anno. I dati sono conservati sul sistema storage EMC².

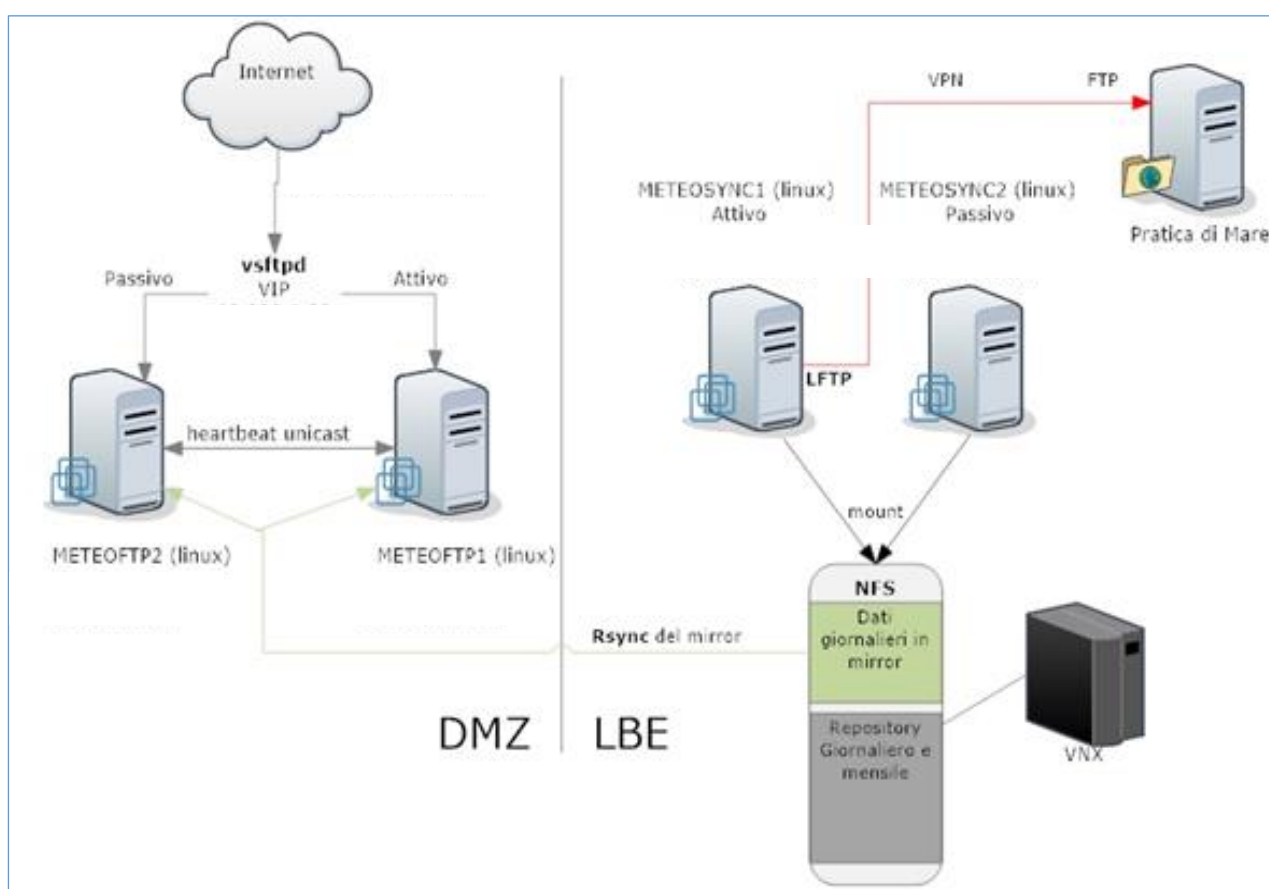


Figura 10 - Architettura dei sistemi Meteosync

4.4 Backup

Nel Dipartimento il servizio di backup viene effettuato in tre distinte modalità:

- Avamar
- Vcenter
- Portale SNIPC (Sistema Nazionale Integrato della Protezione Civile)

4.4.1 Infrastruttura backup EMC² Avamar Solution.

Avamar è la soluzione backup EMC che offre il ripristino rapido ed efficiente di ambienti fisici e virtuali (grazie all'integrazione con le architetture VmWare), in linea con le crescenti esigenze IT che prevedono la gestione di grandi quantità di macchine virtuali. Mette a disposizione varie modalità per effettuare il ripristino ed il backup, ponendo in primis come obiettivo la riduzione della banda utilizzata per la trasmissione dei dati attraverso l'utilizzo di sofisticati algoritmi di deduplica. In questo modo il ripristino di dati critici all'interno del Dipartimento avviene in tempi rapidi, diminuendo drasticamente il tempo di disservizio. L'architettura Avamar è costituita da:

- Cinque Nodi Storage per i dati;
- Un nodo Utility che gestisce le policy di backup;
- Un Media Access Node che trasmette via fibra ottica i dati in un archivio esterno ad Avamar;
- Due switch ethernet;

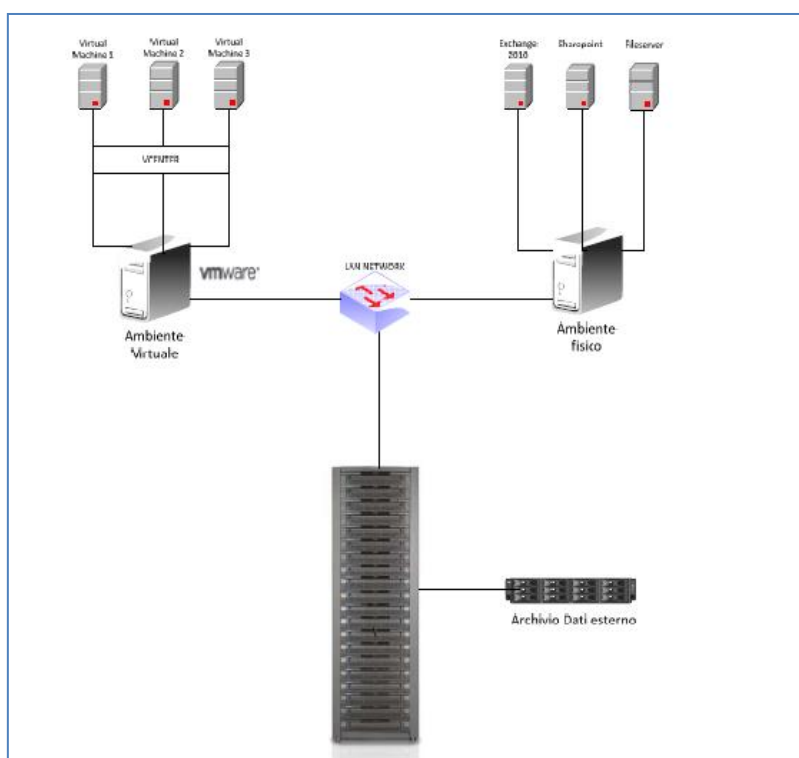


Figura 11 – Architettura del servizio di backup (EMC² Avamar)

Esiste all'interno del Data Center di Via Vitorchiano un secondo backup server che effettua il salvataggio dei dati per le applicazioni o i Database che non possono essere virtualizzati o che richiedono specifiche particolari (es. Microsoft SqlServer, Microsoft Exchange, Oracle Database, Microsoft Sharepoint).

Ogni Backup ha una schedulazione distinta e una retention dedicata (di solito è di 60gg); il salvataggio avviene su dischi dedicati e ridondati. Il salvataggio avviene quotidianamente con schedulazioni distinte a seconda delle indicazioni fornite dai referenti applicativi.

4.4.2 Backup Infrastruttura virtuale Vcenter.

Si tratta di una tipologia di Backup specializzata per l'infrastruttura virtuale. È presente nel Vcenter VmWare un server virtuale dedicato che effettua il backup di tutti i server virtuali presenti. Il backup viene eseguito quotidianamente.

4.4.3 Portale SNIPC (Sistema Nazionale Integrato della Protezione Civile).

Questa modalità di Backup avviene tramite il portale SNIPC che ospita le applicazioni più critiche del Dipartimento. Il backup delle applicazioni viene effettuato tramite un Backup Server virtuale, che si occupa di eseguire la copia di tutto il sistema presente in VmWare. Questa tipologia di Backup è una modalità distinta, rispetto alle precedenti e si basa sullo snapshot (immagine del server virtuale), e preclude una gestione delle immagini dei server virtuali. I dati sono salvati tramite disco EMC2.

4.5 Telefonia Fissa

Il dipartimento ha a disposizione 3 centrali Alcatel così dislocate:

- 1 centrale nella sede di Via Ulpiano
- 2 centrali nella sede di Via Vitorchiano

Inoltre il dipartimento ha a disposizione una centrale telefonica Alcatel omnipcx enterprise per la gestione delle emergenze.

4.6 Direzione di Comando e Controllo - DICOMAC

La struttura “DICOMAC” rappresenta il centro di coordinamento nazionale delle Componenti e Strutture operative di Protezione civile attivato sul territorio interessato dall’evento, se ritenuto necessario, dal Dipartimento della Protezione Civile in caso di emergenza.

La struttura possiede una propria infrastruttura tecnologica attivata all’occorrenza e in grado di:

- Fornire connettività Internet e Extranet alle utenze presenti all’interno dell’infrastruttura
- Fornire servizi di connettività Wifi di tipo Hotspot
- Fornire servizi di telefonia

Per facilitarne la movimentazione, i sistemi che compongono l’infrastruttura sono fisicamente preinstallati su rack mobili.

Nello specifico l’infrastruttura “DICOMAC” eroga in locale i seguenti servizi:

- Servizio Active Directory
- Servizio DNS/DHCP
- Servizio Fileshare
- Servizio di Protocollo

L’architettura è inoltre protetta da una coppia di sistemi di sicurezza perimetrali (FIREWALL) che svolgono, oltre al firewalling, i seguenti servizi supplementari:

- Layer 3 Routing
- UTM
- VPN Concentrator
- Wifi Controller

I sistemi di sicurezza perimetrale offrono la possibilità di interconnettere la struttura “DICOMAC” con ulteriori sedi istituzionali (come ad esempio la sede centrale di Via Vitorchiano) facendo utilizzo della rete Extranet.

I sistemi sono interconnessi tra loro per mezzo di una coppia di switch.

Nel complesso l’architettura “DICOMAC” è composta dunque da:

- Due sistemi Server per la gestione del dominio Active Directory e dei servizi DHCP/DNS
- Un sistema Server per la gestione del servizio Fileshare
- Un sistema Server per la gestione del servizio di Protocollo
- Un sistema Storage per il salvataggio dei dati gestiti dal sistema Fileshare
- Due Switch configurati in Alta affidabilità per mezzo della tecnologia Stacking
- Due firewall tecnologia Fortinet configurati in Alta affidabilità in modalità “Active/Standby”

- Numero variabile di Access Point Wireless in tecnologia Fortinet

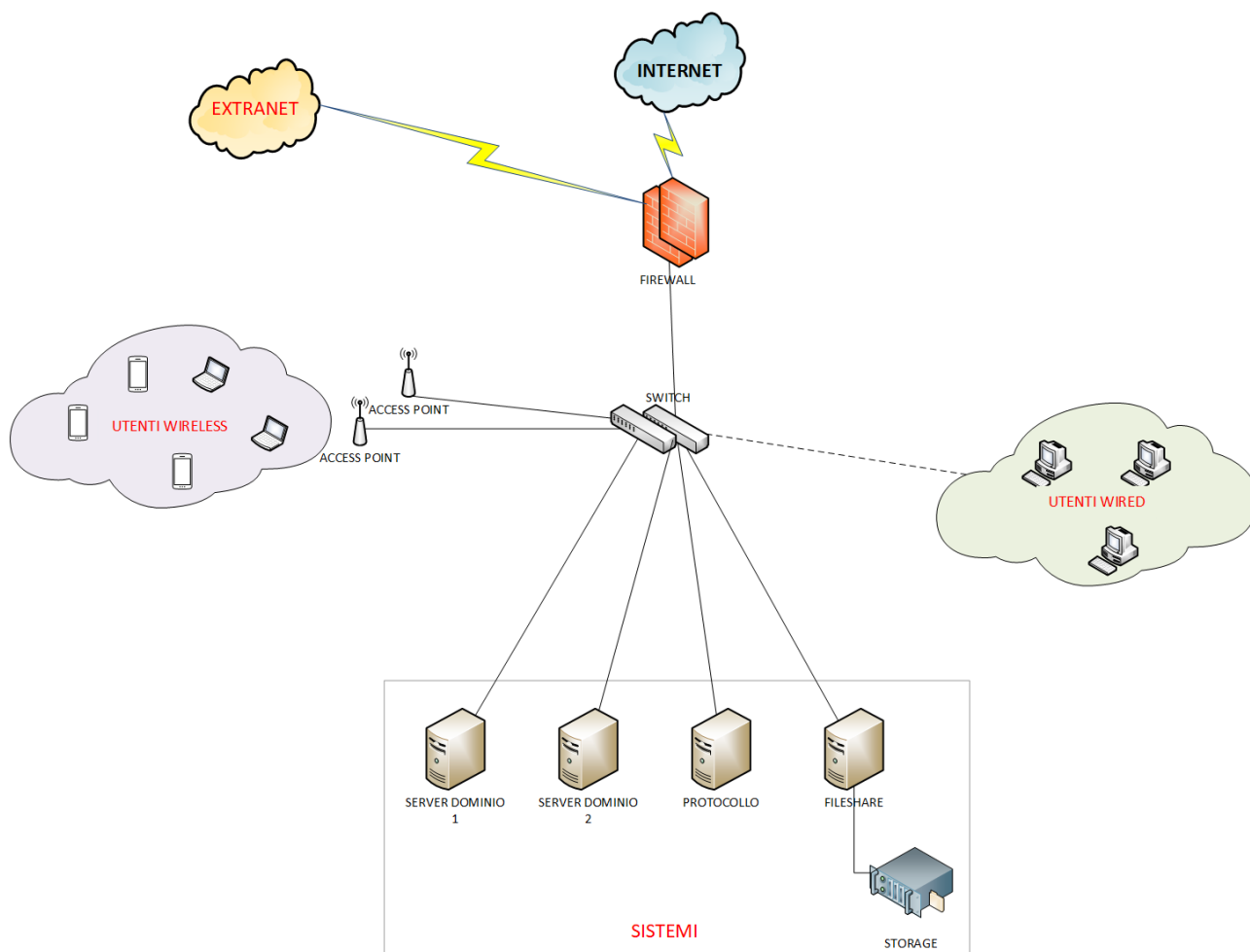


Figura 12 – Architettura logica DICOMAC

5 Centri Funzionali

La rete dei Centri Funzionali è costituita da un Centro Funzionale Centrale (CFC) presso il Dipartimento e da 21 Centri Funzionali Decentrati (CFD) presso le Regioni e le Province Autonome di Trento e Bolzano. I compiti di ciascun Centro Funzionale sono ottemperati ogni giorno attraverso una serie di apparati hardware e di moduli software che in sinergia consentono agli operatori di raccogliere e condividere con gli altri Centri Funzionali, sia i dati parametrici relativi ai diversi rischi provenienti dalle diverse reti di monitoraggio presenti e distribuite sul territorio, sia le informazioni provenienti dalle attività di vigilanza e contrasto degli eventi svolte sul territorio, ed elaborare un'analisi in tempo reale degli eventi in atto sulla base di modelli previsionali e di valutazione, nonché di sintetizzarne i risultati concertati, ove del caso, tra il Centro Funzionale Centrale ed i Centri Funzionali Decentrati operativi interessati. I Centri Funzionali trasmettono in continuo dati in tempo reale riguardanti il territorio nazionale. Ogni singolo centro funzionale è interconnesso attraverso la rete MPLS di Fastweb.

La tabella seguente mostra l'ubicazione geografica dei centri funzionali decentrati.

SCHEDA	Elenco Centri Funzionali		
Centro Funzionale	Ruolo	ENTE	Indirizzo
DPC	CFC	Dipartimento Protezione Civile	Via Vitorchiano, 2 00189 Roma
Abruzzo	CFD	Amministrazione Regionale	Via Salaria Antica est, 27 67010 L'Aquila
Basilicata	CFD	Amministrazione Regionale Dipartimento Infrastrutture, OO.PP. e Mobilità Ufficio Protezione Civile	c.so Garibaldi, 139 85100 Potenza
Bolzano	CFD	Provincia Autonoma Ripartizione 26.4	Via Druso, 116 39100 Bolzano
Calabria	CFD	Ufficio Idrografico e Mareografico di Catanzaro	Viale degli Angioini, 143a 88100 Catanzaro
Campania	CFD	Amministrazione Regionale Settore Programmazione Interventi di Protezione Civile sul Territorio	Centro Direzionale di Napoli - Isola C3 80143 Napoli
Emilia Romagna	CFD	ARPA Emilia-Romagna	Viale Silvani, 6 40122 Bologna

Friuli Venezia Giulia	CFD	Regione Autonoma Direzione Regionale della Protezione Civile	Via Natisone, 43 33057 Palmanova (UD)
Lazio	CFD	Amministrazione Regionale Direzione Regionale Protezione Civile – Attività della Presidenza Ufficio Idrografico e Mareografico	Via Monzambano, 10 00185 Roma
Liguria	CFD	ARPA Regione Ligure	Viale Brigate Partigiane, 2 16129 Genova
Lombardia	CFD	Amministrazione Regionale Ufficio Protezione Civile	Via Rossellini, 17 20124 Milano
Marche	CFD	Amministrazione Regionale Servizio Protezione Civile	Centro Operativo di Passo Varano Via Cameranense, 1 60100 Ancona
Molise	CFD	Amministrazione Regionale Assessorato Protezione Civile	C.da Selva del Campo 1 86020 Campochiaro (CB)
Piemonte	CFD	ARPA Regione Piemonte Area Previsioni e Monitoraggio Ambientale	Via Pio VII, 9 10135 Torino
Puglia	CFD	Amministrazione Regionale	Via Enzo Ferrari Aerostazione Bari Palese - 70128 Bari
Sardegna	CFD	Servizio di protezione civile	Via Biasi, 7 09031 Cagliari
Sicilia	CFD	Dipartimento regionale della protezione civile	Via Gaetano Albela, 5 90141 Palermo
Toscana	CFD	Amministrazione Regionale Servizio Idrologico	Lungarno Pacinotti, 49 56126 Pisa
Trento	CFD	Provincia Autonoma	Via Vannetti, 41
		Dipartimento Protezione Civile e Tutela del Territorio	38100 Trento

Umbria	CFD	Amministrazione Regionale Ufficio Protezione Civile	Via Romana Vecchia 06034 Foligno (PG)
Valle d'Aosta	CFD	Amministrazione Regionale	Via Promis, 2 11100 Aosta
Veneto	CFD	Segreteria Regionale Lavori Pubblici - Unità di Progetto Protezione Civile	Via Longhena,14 30175 Marghera - Venezia

Tabella 1 – Dislocazione Centri funzionali

La tabella seguente illustra le tecnologie utilizzate all'interno di ciascun centro funzionale.

UNITA'	Apparati	Marca	Modello	Q.tà
Server Cluster	Net Server:	IBM	x346, Intel Xeon 3.2 GHz/800 MHz, S.O. Linux	1
	Back-up Server:	IBM	x346, Intel Xeon 3.2 GHz/800 MHz, S.O. Linux	1
	SAN Storage Server:	IBM	TotalStorage DS4300 12 dischi connessi in fibra ottica RAID e Hot Spare	1
	Tape Unit	IBM	TotalStorage 3581 Ultrium Autoloader	1
Switch Unit	Switch	CISCO	Catalyst 3750G 24 10/100/1000T c/2 SFP MULTILAYER	2
WAN Unit	Router	CISCO	2811 SEC/K9	3
LAN Gateway	Router	CISCO	2611XM	2
UPS set	UPS	APC	Smart-UPS 5000RmiB	2
Accessori	Armadio Rack	IBM	Netbay 42U	1

Tabella 2 – Infrastruttura tecnologica Centro Funzionale

6 Apparati Audio Video

Il Dipartimento di Protezione Civile detiene un'architettura audio video interna dislocata nelle principali sedi. Le funzioni di tale architettura possono essere così sintetizzati:

- Distribuzione di segnali audio/video
- Videoconferenza
- Registrazione eventi

Nel seguito sono riportate le tecnologie coinvolte e gli apparati attualmente facenti parte dell'architettura audio video.

6.1 Sistema Audio-Video installato nella sede del DPC di via Vitorchiano

Posizione	Descrizione Apparato	Quantità
Sala Regia seminterrato	Monitor Barco 42	4
	Monitor Barco 46	2
	Telecamera Canon VC-C4R	1
	Tandberg T1000	1
	Pc Gestione VideoWall	2
	Pc Gestione MTX Vikinx 64x64	1
	PC Gestione MTX Sierravideo 32x32	1
	Pc Gestione Videoconferenza	1
	PC Gestione Audio	2
	Monitor Dell controllo audio	2
	Monitor Albiral 056RK03VFA	2
	Monitor Albiral 084RK02VFA	1
	Panasonic MFC AW-RP655	1

Posizione	Descrizione Apparato	Quantità
Sala Regia seminterrato	Panasonic AW-SW350	1
	Panasonic AW-PS505A	6
	Switch vga 2x1	1
	Radiomicrofono Mipro Act 707H	5
	Mipro Act 707	2
	Biamp Audia Expi	2
	Dvd Recorder LG RHT397H	2
	Ddv Recorder Panasonic DMR-EH50	2
	Vhs Samsung SV-500W	1
	Dvd Recorder Panasonic DMR-EX86EC-K	1
	Vhs Sony SLV-SE740D	1
	Monitor jvc TM-A10E	2
	Telecomando Crestron	1
	Pannello Luxmate	4
	Bonifex RedBox	1
	Cuffia Audio DT 770	1
	Diffusori Audio Penton Rcs 8/t	2
	Apart BuzzStop III	5
	Monitor Barco	4

Posizione	Descrizione Apparato	Quantità
CED seminterrato	Diffusori Audio da soffitto	2
COAU seminterrato	Monitor Barco	2
	Pc Slim Pro	2
	Videowall	1
	Pc Controllo Colorimetria Vw.	1
	Telecamera Canon VC-C4R	1
	Telecamera Canon VB-C50iR	1
	Proiettore Barco IqPro 210	1
	Pc controllo Iq 210	1
	Diffusori Audio Penton Rcs 8/t	4
	Base Microfono da tavolo AVL6305S	1
	Telo Proiezione Motorizzato	1
STRUTTURE OPERATIVE seminterrato	Philips TV	16
	Pc Slim	16
	Videowall Barco	3
	Proiettore Barco IqPro 210	1
	Telo proiezione motorizzato	1
	Microfono da Tavolo	1
	Telecamera Canon VC-C4R	3

Posizione	Descrizione Apparato	Quantità
	Telecamera Canon VB-C50iR	3
	Diffusori Audio Penton Rcs 8/t	9
	Base Microfono da tavolo AVL6305S	1
	Switch iview vga 2x1	13
	Pc Controllo Colorimetria Vw.	1
SALA EMERGENZE seminterrato	Monitor Barco	2
	Tandberg 3000 MXProfile	1
	Proiettore Barco IqPro 210	1
	Telo Proiezione	1
COMITATO OPERATIVO seminterrato	Monitor Barco	16
	Pc slim	16
	Lindy Switch kvm Cpu Lite Lindy vga 2x1	40
	Switch Iview 1x8	2
	Videowall Barco	1
	Telecamere Panasonic AW-E650E	4
	Telecamera Sony	1
	Motore Saliscendi Hafele	22
	Switch Iview vga 1x8	4
	Switch Iview vga 1x4	1
	Switch Kramer vga 2x1	1

Posizione	Descrizione Apparato	Quantità
	Telecamere Canon VC-C4R	4
	Microfoni Stelo	23
	Pulsantiera Accensione Mic.	23
	Switch commutazione video	22
	Diffusori Audio Penton Rcs 8/t	10
	Network Conquer V0106DEQ	4
	Pc gestione tavolo	24
	Monitor Tavolo	24
CESI – Sala Operativa seminterrato	Monitor Barco	5
	Pc Slim Pro	5
	Videowall Barco	1
	Telecamera Canon VC-C4R	1
	Telecamera Canon VB-C50iR	1
	Diffusori Audio Penton Rcs 8/t	5
	Base Microfono da tavolo AVL6305S	1
COEM seminterrato	Monitor Barco	3
	Pc Slim Pro	3
	VideoWall Barco	1
	Telecamera Canon VC-C4R	1
	Telecamera Canon VB-C50iR	1

Posizione	Descrizione Apparato	Quantità
	Diffusori Audio Penton Rcs 8/t	2
	Base Microfono da tavolo AVL6305S	1
Direzione Emergenze seminterrato	Monitor Barco	2
	Pc Slim Pro	2
	Proiettore Barco IqPro 210	1
	Diffusori Audio Penton Rcs 8/t	2
	Telo per Proiezione	1
Unità di Crisi Cielo Stellato seminterrato	Monitor Barco Cielo Stellato	1
	Pc Slim Pro Cielo Stellato	1
	Telecamera Canon VC-C4R	1
	Telecamera Canon VB-C50iR	1
	Diffusori Audio Penton Rcs 8/t	4
	Base Microfono da tavolo AVL6305S	1
	Telo Proiezione motorizzato	1
	Proiettore Barco IqPro 210	1
	Tandberg Mpx 85+Telecamera	1
	Apart BuzzStop III	1
	Pc Slim Pro	2
	Telecamera Canon VC-C4R	1
	Diffusori Audio Penton Rcs 8/t	1

Posizione	Descrizione Apparato	Quantità
	Monitor Sharp 70" Big Pad	1
	Tv Sharp 50"	2
	Matrice DVI 8x8	1
	Radio microfoni	4
Sala Apparati seminterrato	Cisco Mcu 4220 Codian	1
	Cisco Vcs-Video Comm.Server	1
	Cisco Content Server (tcs)	1
	Cisco Vcs Express	1
	Barco Argus+Omnibus A7 (Coem)	1
	Barco Argus+Omnibus A8 (Regia)	1
	Barco Argus+Omnibus A6 (Coau)	1
	Barco Argus+Omnibus A4 (Cesi)	1
	Barco Argus+Omnibus A5 (Com.Op.)	1
	Barco Argus+Omnibus A1 (Strop.1)	1
	BarcoArgus+Omnibus A2 (Strop.2)	1
	Baco Argus+Omnibus A3 (Strop.3)	1
	Cisco Catalyst 4506	2
	Zodiac DZR-1900CI	5
	Zodiac DZR-40PVRDTT	4
	Sky decoder	1

Posizione	Descrizione Apparato	Quantità
Sala Apparati	Zodiac DZR-1200DTT	3
	Zodiac DZR-30DTT	1
	Apart Buzzstop III	7
	Tandberg Gatekeeper	
	Tandberg 2500 TTC7-06 (Coau)	
	Tandberg 2500 TTC7-06 (Com.Op.)	
	Tandberg 2500 TTC7-06 (Str.op.)	
	Tandberg Gateway Isdn	
	Tandberg Mcu 1	
	Tandberg Mcu 2	
	Tandberg Mcu	
	Tandberg Mxp 85 (Coem)	
	Leich Panacea Matrice video 16x16	
	Leich FR-684 Ampli-Distributore video	
	Creston St-com	
	Gen Electric 517EPS1	
	Apart Buzzstop	5
	Albiral 0560RK03VF	3
	Switchcraft I/O Module	6
	Viknix 64-Proxy 00088	6

Posizione	Descrizione Apparato	Quantità
Sala Apparati	Viknix V6464 00114	
	Viknix V0106DEQ	2
	Viknix V0106	15
	Kramer VP501 Scan Convert	
	6 Sch.LowbitRate-7 HighbitRate	
	Sieeravideo Proxl Mtx 32x32 vga (RGB-HV)	
	Vcs Vip 10	50
	Symetrix 581E	6
	Audia EXPI Biamp	
	Audia Audiaflex	4
	D.I.S. Cu6010	
	D.I.S. A06008	
	Apart MB150	16
	Apart DT150	8
	Audia EXPI Biamp	
Reception Piano terra	Solaris Barco	2
	Pc Slim Pro	2
Stanza Capo Dipartimento piano primo	Solaris Barco	1
	Pc Slim Pro	1

Posizione	Descrizione Apparato	Quantità
Stanza Capo Vulcanologico piano primo	Solaris Barco	1
	Pc Slim Pro	1
	Tandberg T1000	1
Sala Cassisi piano primo	Solaris Barco	2
	Pc Slim Pro	1
	Proiettore Barco IqPro 210	1
	Telo Proiezione	1
	Tandberg Mxp 85+Telecamera	1
Sala Centro Funzionale piano secondo	Monitor 72 " Sharp Bigpad	2
	Solaris Barco	5
	Pc Slim Pro	1
	Telecamera Unit IV wave	1
	Radiomicrofono Mipro Act 707H	2
	Diffusori Audio	4
	Telecamera Canon VC-C4R	1
Sala Apparati Centro Funzionale piano secondo	Mirpo Act 707D	1
	Audia Flex Biamp	1
	Argus Barco	1
	Omnibus Barco	1
	MB150	2

Posizione	Descrizione Apparato	Quantità
	DT150	1
Sala Emergenze piano secondo	Monitor Barco	2
	Tandberg 3000 MXProfile	1
	Proiettore Barco IqPro 210	1
	Telo Proiezione	1
Direttore Emergenze piano secondo	Monitor Barco	2
	Pc Slim Pro	2
Sala Losavio piano secondo	Proiettore Barco IqPro 210	1
	Telo Proiezione	1
	Tandberg TTC7-06	1
	Telecamera Unit IV wave	1
	Base Microfono da tavolo AVL6305S	3
	Diffusori Audio	2
	Microfono ambientale da Tavolo	1
Auditorium piano terra	Creston AV2	1
	Creston DVP HD	1
	Kramer VS-3232	1
	Viewtek LRM-6521	1
	Kramer VM-10XL	1

Posizione	Descrizione Apparato	Quantità
	30 System Maxx Image Server	1
	Tandberg 2500	2
	Leitch Neo Suite	4
	Kramer VP-128H	1
	Kramer VP-61N	1
	AnalogWay BSC730 Broadscan	4
	Viewtek LRM-6521	1
	Lectrosonic Lecnet 2 DSP DH812	1
	Sony RDR-VX450	1
	Panasonic DMR-EH50	1
	Samsung DVD-HR 755	1
	Bosch VK0748	1
	Bose Entero4400	1
	Viewtek LRM-6521	1
	DBX 1215	1
	Shonner ALP 299	1
	Crestron Isys 10	1
	Leitch 700/T-R	1
	G.E. Security 517EPS1	1
	Mipro ACT-707	1

Posizione	Descrizione Apparato	Quantità
	Logitech R-RB5	
	Elmo P-30	
	Logitech DiNovo Y-RZ42	
	Logitech M-RBA97	
	Logitech C-UV35	
	Eizo Flexscan HD2441W	
	EizoFlexscan S1901	
	Empire R-1000	
	Eizo Flexscan HD2441W	
	Eizo Flexscan S1901	
	Barco CLM HD8	3
	Samsung LTM213U6-L01	
	JVC KY-F560E complete di obiettivi e motori Crestron	4
	Bose Panaray MA12 Modular Line Array	

Tabella 3 – Apparati Audio Video sede Via Vitorchiano

6.2 Sistema Audio-Video installato nella sede del DPC di via Ulpiano

Posizione	Descrizione Apparato	Quantità
Sala Ippolito	Australian Monitor ProSeries SM12	1
	Australian Monitor Synergy SY4200	2
	DIS CU 6010 Central Unit	1
	SABINE Adaptive Audio GRAPHI-Q ² GRQ3120 series	1
	SABINE Adaptive Audio GRAPHI-Q ² GRQ3120 series FBX®1200 feedback exterminator	1
	CLOCKAUDIO CWR9000R Diversity Receiver CW9000T Hand held transmitter	1
	Elpro INOX/4 PLUS	1
	Elpro TZW 803 switcher 8x1 VGA/XGA	1
	HITACHI CP-X608	1
	Tandberg EDGE 85 MXP + Precision HD camera	1
	Clock Audio C3 Series Cardioid Condenser Microphones	28
	DIS FD 4010	1
	DIS FD 4011	27
	PANASONICDMR-EX83	1

Tabella 4 – Apparati Audio Video sede Via Vitorchiano

8. APPLICAZIONI

Di seguito sono riportate schede di sintesi che descrivono l'ambiente applicativo del Dipartimento.

8.1 Antincendio boschivo – COAU

Obiettivi/Funzioni

Il Dipartimento è quotidianamente impegnato in attività di ricognizione, soppressione e contenimento di incendi boschivi che possono verificarsi sul territorio nazionale. In tale ambito l'Ufficio IV - Gestione delle emergenze, tramite la Sala Operativa del **COAU** (Centro Operativo Aereo Unificato) è responsabile del coordinamento e dell'impiego degli aeromobili della flotta di Stato per la lotta attiva agli incendi boschivi. Tale attività viene espletata con la concorrenza delle Regioni, le Amministrazioni dello Stato e gli Enti Esercenti.

Il **COAU** è un'applicazione web che fornisce servizi, configurabili tramite apposita profilazione, a tutti gli Attori coinvolti nella lotta AIB. Le richieste di concorso aereo, inoltrate al **COAU** attraverso la compilazione di un apposito form direttamente dai COR (Centri Operativi Regionali)/SAOP (Sale Operative Regionali), vengono validate dal personale del **COAU**. Oltre ad effettuare le richieste, le Regioni hanno facoltà di richiedere l'annullamento o la chiusura delle stesse, controllandone lo stato in ogni momento. La presentazione dei dati (richieste, mappe, statistiche) si limita esclusivamente al proprio territorio di competenza e alle zone confinanti.

Il personale del **COAU** provvede, dopo aver validato la richiesta, ad assegnare i velivoli sull'incendio; questi ultimi sono per gran parte radiolocalizzati: la visualizzazione dei suddetti come layer sull'applicativo del **COAU** ha come vantaggio quello di creare un unico strumento di supporto alle decisioni, comprendente anche dati effettivi di volo disponibili in tempo reale durante le missioni. Tra le opzioni a supporto del personale del **COAU**, vi sono anche la possibilità di gestire gli aeromobili componenti la flotta di Stato, le basi di decollo ed atterraggio degli stessi, la gestione delle frequenze radio per le comunicazioni con il direttore delle operazioni di spegnimento, nonché la gestione dei provider di radiolocalizzazione degli aeromobili.

Le attività svolte dai velivoli impiegati nella lotta agli incendi boschivi sono integrate dai dati direttamente inviati, sempre via web, dagli Enti Esercenti, i quali collaborano col personale del **COAU** alla creazione della richiesta prontezze, ovvero l'attività di stabilire la dislocazione degli aeromobili sul territorio nazionale in base alle previsioni relative al rischio incendi boschivi.

Principali criticità per l'Amministrazione connesse all'interruzione del servizio

L'applicativo viene utilizzato, a vario titolo, principalmente dal personale dell'Ufficio IV - Gestione delle emergenze, dell'Ufficio II - Rischi idrogeologici e antropici, dell'Ufficio Stampa del Capo del Dipartimento e dell'Ufficio V - Amministrazione e bilancio.

Oltre all'utenza interna, l'applicativo viene utilizzato anche dal personale del Corpo Forestale dello Stato, dei Vigili del Fuoco, delle Capitanerie di Porto, dei COR/SOUP delle Regioni/Province Autonome e degli Enti Esercenti.

La non disponibilità del servizio può essere causa di forti ritardi nella gestione della flotta aerea dello Stato coordinata dal **COAU** per la lotta agli incendi boschivi, nonché di un consistente aumento dei carichi di lavoro per il personale del **COAU**.

Principali danni per l'Amministrazione in caso di interruzione del servizio

Oltre al grave intralcio nello svolgimento dei propri delicati compiti istituzionali, un'interruzione prolungata del servizio può causare danni di immagine (inefficienza) al Dipartimento.

Procedure alternative

È possibile utilizzare la procedura preesistente in area intranet dipartimentale, avvalendosi dei fax per la ricezione delle richieste di concorso aereo da parte delle Regioni e dei riepiloghi delle sortite da parte degli Enti esercenti.

Architettura

Il sistema integrato a supporto delle attività aeronautiche coordinate dal COAU è realizzato con Web Application realizzate in tecnologia ASP. Il sistema operativo lato server è Windows Server 2003 Standard Edition a 32 bit con installato Autodesk MapGuide Enterprise 2011. Lato client è necessario l'utilizzo di Internet Explorer 7.0 o superiore come browser.

L'architettura del sistema è del tipo Three-Tier basata su server tutti virtuali:

- 8 un server per la gestione delle Web Application;
- 9 un server per la gestione dell'RDBMS;
- 10 un server per la gestione cartografica;
- 11 un numero variabile di Client ed un videowall con Internet Explorer 7.0 o superiore installato.

Sistema Operativo: Windows Server 2003.

Application Server: IIS 6.

Database: SQL Server 2005.

Software installato: Autodesk Mapguide, in fase di aggiornamento.

8.2 Benemerenze - PIB

Obiettivi/Funzioni

Benemerenze (http://www.protezionecivile.gov.it/jcms/it/benemerenze_istituzionale.wp) è un applicativo web per l'acquisizione, la consultazione e il consolidamento dei dati relativi alle pubbliche attestazioni di benemerenza del Dipartimento della protezione civile della Presidenza del Consiglio dei Ministri che fa riferimento al DPCM 22 ottobre 2004.

L'acronimo PIB sta per Progetto Informatico Benemerenze.

Con la pubblicazione in Gazzetta Ufficiale del decreto del Capo Dipartimento, dal 9 giugno 2015 è in vigore la nuova procedura per richiedere l'attestazione di pubblica benemerenza.

Il sistema prevede una parte pubblica a libero accesso dove è possibile consultare la documentazione informativa, circolari, risposte alle domande frequenti, eccetera.

Nella parte pubblica è disponibile il modulo elettronico con cui inoltrare la richiesta di accreditamento di un referente del segnalante per l'accesso alla parte riservata. La richiesta di accreditamento è valutata e approvata dal Dipartimento. L'approvazione della richiesta viene effettuata sul sistema che provvede ad inoltrare al richiedente le credenziali, codice fiscale e password, per l'accesso.

L'area ad accesso riservato è gestita in modalità sicura (protocollo https) e richiede il riconoscimento dell'utente tramite codice fiscale e password. L'utente autenticato ha visibilità solo ed esclusivamente sui dati dei soggetti da lui segnalati. Il sistema prevede due profili di utenza per l'accesso alle funzioni dell'area riservata:

- 12 **Referente:** rappresenta il segnalante, e deve essere accreditato con apposita procedura. Ha accesso alle funzioni di gestione della propria anagrafica, segnalazione soggetti e consultazione dati dei propri soggetti.
- 13 **Amministratore:** è una persona del dipartimento che ha accesso alle funzioni di accreditamento e revoca dei referenti, gestione soggetti per l'accettazione della forzatura di un codice fiscale e l'attribuzione delle benemerienze. Ha libero accesso ai dati di tutti i soggetti segnalati.

La procedura di accreditamento si articola nelle seguenti fasi:

- compilazione della richiesta di accreditamento sul sito istituzionale;
- stampa della richiesta e delle condizioni del servizio, ed invio al Dipartimento via fax;
- verifica di congruità tra i dati ricevuti e quelli presenti sul sistema da parte del Dipartimento;
- valutazione ed eventuale accettazione della richiesta da parte del Dipartimento;
- in caso di accettazione della richiesta invio automatico al referente della password per posta elettronica;
- il referente accreditato può gestire le informazioni inviate con la richiesta accedendo ad una specifica pagina del portale dopo essersi autenticato.

Il sistema prevede:

- Forms per inserimento, modifica e revoca dati di richiesta accreditamento;
- Forms per inserimento, modifica accettazione/respingimento dei dati di richiesta;
- Gestione anagrafica dei referenti.

L'applicativo viene utilizzato (tramite web) per l'acquisizione, la consultazione e il consolidamento dei dati relativi alle pubbliche attestazioni di benemerienza del Dipartimento, conferite a persone, amministrazioni, enti, istituzioni o organizzazioni del Servizio Nazionale della Protezione Civile che dimostrano di aver partecipato con merito a operazioni di protezione civile.

L'iter prevede la segnalazione dei nominativi del personale partecipante alle suddette operazioni, da parte dei referenti degli organismi. Tali segnalazioni vengono analizzate da una Commissione permanente per la successiva valutazione e approvazione al Presidente del Consiglio dei Ministri.

L'area ad accesso riservato è gestita in modalità sicura (protocollo https) e richiede il riconoscimento dell'utente tramite codice fiscale e password.

Principali criticità per l'Amministrazione connesse all'interruzione del servizio

Non vi sono criticità gravi a fronte di una interruzione del servizio.

Principali danni per l'Amministrazione in caso di interruzione del servizio

Non vi sono danni per l'Amministrazione, tranne il danno di immagine per inefficienza amministrativa nel caso di una interruzione prolungata.

Procedure alternative

Eventuale ma non necessario utilizzo di fogli Excel e di stampe con *merge*.

Architettura

- Lo schema architetturale dell'applicazione (riportato nella figura a lato) è così costituito:
- **Sistema Operativo:** Microsoft IIS
- **Database:** SQL
- **Linguaggio:** ASPX.

La piattaforma hardware è composta da:

Classificazione del documento: Public

58 di 75

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l'appalto di servizi di gestione, sviluppo e supporto per il sistema informativo del Dipartimento della Protezione Civile della Presidenza del Consiglio dei Ministri - ID 2005

Appendice 1 al Capitolato tecnico - Contesto tecnologico e applicativo

- Web-Tier - due macchine virtuali che risiedono su ambiente virtuale VMWare 4.1;
- Data-Tier - due server fisici.

8.3 Verifiche sismiche - SIV3274

Obiettivi/Funzioni

L'OPCM 3274 del 20 marzo 2003, che ha introdotto in Italia la nuova classificazione sismica ed una normativa tecnica coerente con gli standard internazionali sull'ingegneria antisismica, ha anche previsto (art. 2, comma 3) che le opere strategiche per finalità di protezione civile e quelle suscettibili di conseguenze rilevanti in caso di collasso fossero sottoposte a verifica entro il mese di maggio 2008 a cura dei rispettivi proprietari. Le tipologie di opere da assoggettare a verifica sono state individuate, per quanto riguarda lo Stato, con Decreto n. 3685 del 21 ottobre 2003 del Capo del Dipartimento pro-tempore e per quanto riguarda le Regioni con propri atti di Giunta o con specifiche norme regionali.

In linea generale, le verifiche sono suddivise in tre livelli:

- **livello 0:** relativo a censimento anagrafico, dimensioni generali, data di costruzione, dati di esposizione, ubicazione in relazione alla pericolosità, inventario e dati statistici di rischio;
- **livello 1:** relativo a verifiche sismiche di opere ad alta priorità, strutturalmente regolari, con fondazioni allo stesso livello, che non si trovino su categorie di suolo S1 o S2 e che non siano realizzati in prossimità di dirupi o creste o su corpi franosi;
- **livello 2:** relativo a verifiche sismiche di altre opere ad alta priorità (i livelli 1 e 2 si differenziano per il diverso grado di conoscenza della struttura ed i diversi strumenti di analisi e di verifica richiesti). La scadenza predetta è stata successivamente prorogata al 31/03/2013, per effetto della legge di stabilità 2013.

Dal 2006 è stato realizzato uno strumento informativo in grado di gestire la mole di dati derivanti dalle verifiche. L'applicativo, denominato Sistema Informativo Verifiche sismiche per OPCM 3274 (SIV3274) consente di:

- raccogliere e consultare i risultati del censimento effettuato con le schede di livello 0 (L0), che fornisce un quadro della distribuzione sul territorio degli edifici ed opere strategiche e rilevanti;
- raccogliere e consultare i risultati delle verifiche sismiche eseguite sugli edifici ed i ponti strategici e rilevanti, (schede di livello 1-2 (L1/2)), dati di interesse nelle attività di mitigazione del rischio sismico;
- gestire i DPCM di finanziamento per le verifiche e gli interventi previsti dalle OPCM 3362 e 3376 del 2004 ed OPCM 3502 e 3505 del 2005, favorendo il monitoraggio delle tempistiche di attuazione e le reportistiche alla Corte dei Conti.

Il sistema consente di raccogliere e consultare i risultati di verifiche sismiche eseguite in campo sugli edifici e i ponti, nonché di gestire i DPCM di finanziamento per le verifiche e gli interventi. Inoltre, il SIV3274 consente di visualizzare su mappa tutti i dati inseriti.

Principali criticità per l'Amministrazione connesse all'interruzione del servizio

Non vi sono criticità gravi in caso di interruzione del servizio, tuttavia l'interruzione non consentirebbe la possibilità di caricamento, aggiornamento e consultazione dei dati.

Principali danni per l'Amministrazione in caso di interruzione del servizio

L'interruzione del servizio è causata da inefficienza amministrativa per il Dipartimento, non in grado di fare fronte completamente ai suoi compiti istituzionali.

Procedure alternative

È disponibile una versione off-line dell'applicativo, realizzata per operare su computer locali. Il software è scaricabile dal sito web dedicato ed è dotato di funzionalità per il successivo riversamento dei dati raccolti nel server del Dipartimento. La versione off-line consente di conservare i dati in locale, di accodarli e di esportarli in formati di larga diffusione; il sistema memorizza l'utenza e l'ente per cui viene eseguito il download. Sul personal computer deve essere disponibile jdk1.6.0_25 o versioni successive e deve essere presente anche la variabile di ambiente JAVA_HOME. L'application server utilizzato è JBoss-4.2.3.GA, mentre il DB utilizzato per allocare i dati in locale è Microsoft Access 2003.

Architettura

Il **SIV3274** opera in ambiente Internet, con caricamento diretto dei dati sul server del Dipartimento da remoto. L'accesso avviene attraverso un sistema di autenticazione, con utenti aventi differenti gradi di operatività all'interno dell'applicativo a cui si accede tramite un portale web.

L'Application Server è costituito da un server con le seguenti caratteristiche:

- a) 2 CPU 2Ghz, 4GB di RAM e 30GB di Hard Disk;
- b) Windows 2003 Enterprise Edition R2, 32 bit;
- c) JBoss-4.2.3.GA;
- d) Java JDK (ver. 1.6.0.27 con java DB 10.6.2.1);
- e) Microsoft Office Professional 2007 a 32 bit;
- f) librerie software specifiche per l'accesso ai dati, l'export in access e la stampa in pdf.

La componente DB server è costituita da due server fisici Red Hat Enterprise Linux 5.4 a 64 bit posti in cluster tra loro in condizioni di alta affidabilità, e che utilizzano uno storage EMC esterno per l'allocazione dei dati. Il DBMS è Oracle RAC 11gR2.

8.4 Sistema informativo territoriale - SITDPC

Obiettivi/Funzioni

Il **SITDPC** (Sistema Informativo Territoriale del Dipartimento di Protezione Civile) è il sistema cartografico utilizzato per organizzare i dati territoriali del Dipartimento e interoperare con gli altri soggetti del Servizio Nazionale della Protezione Civile, in primo luogo con le Regioni, al fine di costituire un sistema di supporto alle decisioni nelle attività di pianificazione e di gestione delle emergenze.

Il sistema è stato implementato sulla base del framework Geo-Platform, sviluppato come progetto open source dal CNR-IMAA (Consiglio Nazionale delle Ricerche-Istituto di Metodologie per l'Analisi Ambientale), ed ha nel portale Geo-Portal la principale interfaccia utente, attraverso la quale è possibile utilizzare o accedere a quasi tutte le funzionalità del sistema.

Il sistema ha una piattaforma che, anche grazie all'utilizzo di standard, lo rende in grado di interagire e interoperare con altri sistemi, sia interni che esterni al Dipartimento, per poter integrare dati, di diverse tipologie e provenienti da diverse fonti, in un'unica visualizzazione di tipo geografico.

Principali criticità per l'Amministrazione connesse all'interruzione del servizio

In caso di interruzione del servizio non sarebbe possibile integrare in un unico servizio di consultazione le informazioni cartografiche provenienti da più fonti (sia interne che esterne al Dipartimento).

Principali danni per l'Amministrazione in caso di interruzione del servizio

In caso di interruzione del servizio non sarebbe possibile integrare in un unico servizio di consultazione le informazioni cartografiche provenienti da più fonti (sia interne che esterne al Dipartimento).

Procedure alternative

Le fonti esterne (se disponibili) sono consultabili con altri strumenti, mentre le fonti interne, se servite esclusivamente tramite questo servizio, non sarebbero comunque consultabili.

Architettura

Il sistema **SITDPC** è un sistema client-server costituito da diverse Macrocomponenti:

- un insieme di Geodatabase e di file system per archiviare ed organizzare i dati territoriali;
- un Catalogo per la gestione dei relativi metadati;
- un server che rende disponibili i dati mediante servizi web standard previsti dalla normativa vigente;
- un geoportale (webgis) che consente, all'utente, di integrare dati provenienti da fonti e livelli territoriali diversi, permettendone la consultazione, l'analisi e l'editing e, all'amministratore, di gestire il sistema (utenti, ruoli, permessi, inserimento di nuovi dati, ecc.).

Lo schema logico dell'architettura del **SITDPC** è raffigurato in figura.

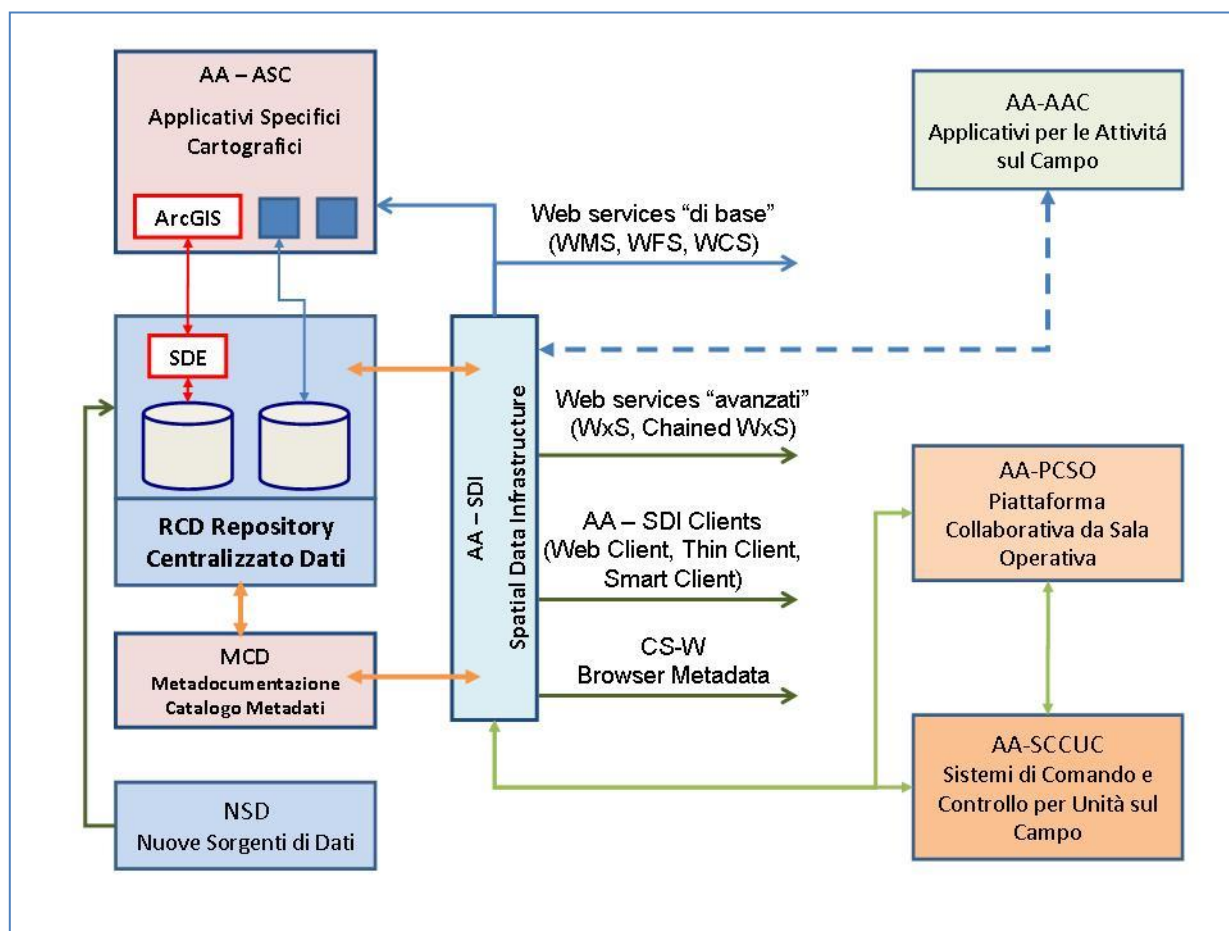


Figura 13 - Architettura del SITDPC

La configurazione hardware della piattaforma è composta dai seguenti server e postazioni:

Servizi mappa, geoWebCache e Web process service:

- 2 postazioni di bilanciamento.
- 16 postazioni geoServer.

Catalogo:

- 1 postazione di bilanciamento;
- 2 postazioni geoNetwork;
- 1 postazione postgresSQL.

Web service

- 1 postazione di bilanciamento;
- 2 postazioni di elaborazione dei servizi WS.

geoPortale

- 1 postazione di bilanciamento;
- 2 postazioni geoPortale.

Messaggistica jabber

(Il server jabber garantisce lo scambio di messaggi applicativi fra i diversi moduli del sistema, in formato XMPP)

Classificazione del documento: Public

62 di 75

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l'appalto di servizi di gestione, sviluppo e supporto per il sistema informativo del Dipartimento della Protezione Civile della Presidenza del Consiglio dei Ministri - ID 2005

Appendice 1 al Capitolato tecnico - Contesto tecnologico e applicativo

- 1 postazione di bilanciamento;
- 2 postazioni jabber server.

Data Server

- 1 postazione di bilanciamento PostGIS pool;
- 8 postazioni PostGIS;
- 1 storage SAN con dischi raid da 40 terabyte.

Per l'accesso alle funzionalità gestionali, dedicate all'utente amministratore, (geoData, geoServer, Admin, geoBatch UI) si aggiunge un nodo dedicato, con accesso all'archivio dati ed al cluster di geoServer, caratterizzato anch'esso da una postazione di bilanciamento e due nodi server.

8.5 Gestione delle emergenze - Brogliaccio

Obiettivi/Funzioni

Presso la Sala Situazione Italia del Dipartimento è attivo un centro di coordinamento nazionale, denominato **SISTEMA**, con il compito di monitorare e sorvegliare il territorio nazionale al fine di individuare le situazioni emergenziali, previste o in atto, e seguirne l'evoluzione, nonché di allertare ed attivare le diverse componenti e strutture operative del Servizio Nazionale della Protezione Civile che concorrono alla gestione delle emergenze.

Per assicurare l'impiego razionale delle risorse, è indispensabile che le componenti e le strutture operative del Servizio Nazionale della Protezione Civile garantiscano l'immediato e continuo scambio delle informazioni, sia a livello territoriale che centrale. Al verificarsi di una situazione emergenziale eccezionale, il Dipartimento deve disporre di tutti gli elementi necessari per valutare la gravità dei rischi di compromissione dell'integrità della vita umana.

I compiti di **SISTEMA** sono quelli di:

- Raccogliere informazioni dal territorio;
- Garantire il flusso delle comunicazioni all'interno della struttura (componenti e strutture operative);
- Mantenere uno stretto raccordo con:
 - Il Centro Funzionale Centrale (CFC);
 - Il Centro Operativo Aereo Unificato (COAU)
 - Le altre Componenti del Dipartimento;
 - Le Strutture Operative (vedi sotto).

Gli eventi, segnalati presso la Sala Situazione Italia del Dipartimento vengono registrati, dai Capi Sala del Dipartimento, in apposite schede che vengono di volta in volta aggiornate dagli operatori delle diverse strutture operative presenti in sala.

SISTEMA opera 24 ore su 24, tutti i giorni dell'anno, con la presenza di personale, ciascuno dotato di una propria postazione, appartenente a:

Dipartimento:

- 1 Capo Turno
- Turnisti

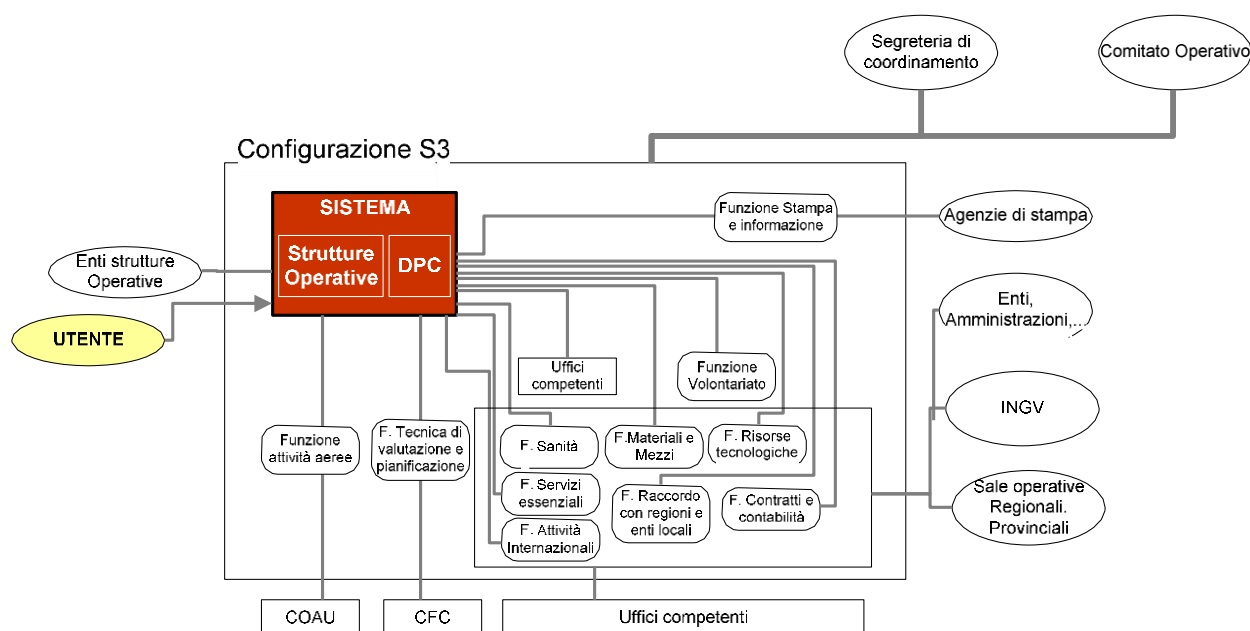
Strutture operative:

- Corpo Nazionale dei Vigili del Fuoco
- Forze Armate (attraverso il Comando Operativo di vertice Interforze)

- Polizia di Stato
- Arma dei Carabinieri
- Guardia di Finanza
- Corpo Forestale dello Stato
- Capitanerie di Porto
- Guardia Costiera

La situazione di emergenza può assumere quattro possibili Stati di Configurazione della struttura, in base alla tipologia e alle caratteristiche dell'evento nonché dei relativi impatti - potenziali o reali - sulla popolazione.

Ad ogni stato corrisponde un grado crescente di attivazione del Dipartimento con il coinvolgimento progressivo di uffici e servizi. La configurazione **S3 (Unità di Crisi)** della Sala Situazioni Italia è riportata in Figura. Nella configurazione **S3** si prevede l'attivazione di postazioni ("isole") che ospitano tutte le funzioni di supporto. In questa configurazione la Sala si predispose come Sala Operativa effettiva.



Principali criticità per l'Amministrazione connesse all'interruzione del servizio

Il servizio non presenta un livello di criticità elevato. Una sua indisponibilità è causata dall'impossibilità di inserire nuove informazioni e di ricercare le vecchie.

Principali danni per l'Amministrazione in caso di interruzione del servizio

Una prolungata interruzione del servizio rende complessa la ripartenza delle attività e degli eventi della Sala Situazione Italia del Dipartimento.

Procedure alternative

In caso di indisponibilità di SISTEMA le informazioni possono essere raccolte in locale (documenti word) per essere poi inserite a sistema riavviato.

Architettura

La base di dati del sistema informativo per la gestione delle emergenze è costituita da un'unica applicazione software denominata **GEM**, realizzata come "web application", la cui interfaccia utente è presentata all'interno di un "internet browser" e la cui logica applicativa è contenuta in un "web server" che si interfaccia a sua volta con una base dati. Il modello architetturale è quindi a tre livelli come evidenziato dalla seguente figura.

L'Application Server è costituito da un server con le seguenti caratteristiche:

- 2 CPU 2Ghz, 4GB di RAM e 30GB di Hard Disk;
- RedHat Enterprise Linux 5.4;
- JBoss-5.1.0-GA.
- La componente DB server è costituita da due server fisici Red Hat Enterprise Linux 5.4 a 64 bit posti in cluster tra loro in condizioni di alta affidabilità, e che utilizzano uno storage EMC esterno per l'allocazione dei dati. Il DBMS è Oracle RAC 11gR2.

La configurazione è la seguente:

- Linguaggio: Java jdk 1.6;
- Web Server: Web container JBoss;
- Piattaforma Java EE;
- Implementazione Ejb: 3.1;
- Application server: JBoss 5.1.0 GA;
- Persistenza: Hibernate 3.3;
- Web Services: Axis2 1.5.1;
- Database: Oracle.

Amministrazione e bilancio - SIAB

Obiettivi/Funzioni

Il Sistema di Amministrazione e Bilancio (SIAB) implementa le seguenti funzionalità:

- Gestione del bilancio del Dipartimento;
- Gestione dei pagamenti e dell'interfaccia con il sistema informativo di contabilità integrata delle Pubbliche Amministrazioni (SiCoGe);
- Gestione degli straordinari e delle indennità varie;
- Gestione delle schede fiscali e dei conguagli;
- Gestione dei collaboratori Co.Co.Co. (pagamento degli stipendi);
- Gestione dei dati relativi alle missioni nazionali ed estere del personale;
- Gestione dei fondi relativi ai diversi Progetti che il Dipartimento gestisce;
- Gestione fiscale e previdenziale;
- Gestione dell'anagrafica di dipendenti, beneficiari, collaboratori, ecc.;
- Amministrazione del sistema stesso: accessi, credenziali utente, profili utente, ecc..

Il sistema viene utilizzato dai diversi uffici per produrre i rispettivi documenti, come quelli relativi ad autorizzazioni di cassa, impegni di pagamento, mandati di pagamento, pagamento straordinari, pagamento collaboratori, schede fiscali, ecc.

Una volta preparati, i documenti vengono inviati a SICOGE, il Sistema per la Gestione Integrata della Contabilità Economica e Finanziaria. Tale sistema è esterno al Dipartimento ed è sviluppato e mantenuto dalla CONSIP, una società per azioni del Ministero dell'Economia e delle Finanze - MEF.

Principali criticità per l'Amministrazione connesse all'interruzione del servizio

Non vi sono criticità gravi in caso di interruzione del servizio. A lungo termine ci potrebbero essere inadempienze contabili.

Principali danni per l'Amministrazione in caso di interruzione del servizio

In caso di una interruzione prolungata oltre alla inefficienza amministrativa si potrebbero verificare anche conseguenze economiche.

Procedure alternative

L'elaborazione può proseguire in locale, in assenza dell'applicativo, rinviando l'elaborazione fino al ripristino del sistema.

Architettura

L'architettura si sviluppa sui tre livelli logico-funzionali (Three-Tier) di presentazione, intermedio e dati. Il sistema è realizzato tramite diverse Web-application che implementano le funzionalità richieste e l'integrazione è garantita a livello dati tramite la gestione di un unico database al quale tutte le Web-Application accedono in lettura e/o scrittura. Il Sistema comunica con il SICOGE attraverso un flusso di dati via Web Services con interfacce opportunamente standardizzate dalla CONSIP. Tutti i server della presente infrastruttura sono virtuali. La piattaforma è composta da un server per il Data-Tier ed un server per il Web-Tier.

Data Tier:

- Sistema Operativo: Linux Enterprise RH 5.4;
- Database: Oracle 11g Enterprise Edition R2.

Web Tier:

- Sistema Operativo: Linux Enterprise RH 5.4 64 bit;
- Framework: J2EE;
- Web Server/Application Server: JBoss Application Server, Liferay Portal Server, Eclipse

8.6 Beni culturali - CSRS

Obiettivi/Funzioni

Il sistema **Centri Storici e Rischio Sismico (CSRS)** nasce come strumento condiviso di indagine per completare ed aggiornare, attraverso una rete nazionale di scambio di informazioni tra diversi livelli di governo territoriale (Dipartimento, Ministero per i Beni e le Attività Culturali, Regioni, Province, Enti Locali), la banca dati riferita ai centri storici esposti a rischio sismico.

Il sistema **CSRS** raccoglie e visualizza via web, anche in forma cartografica, mappe e dati tabellari relativi ai centri storici, elabora scenari di Interesse ed Esposizione Culturale dei suddetti Centri Storici e delle relative perdite a seguito di evento sismico, predispone report tabellari e cartografici, elabora scenari post-evento sismico di Impatto sul patrimonio culturale.

La prima versione è attualmente in produzione ed è accessibile via Internet. La seconda versione (che viene descritta nel presente documento) è esposta solo su Intranet ed è oggetto attualmente di una attività evolutiva per un aggiornamento architetturale che consentirà di esporla anche su Internet.

Al sistema accedono utente interni del Dipartimento, sia tramite intranet che tramite internet (se abilitato con VPN) e, in prospettiva, ricercatori universitari o studiosi.

In caso di emergenza può essere consentito l'accesso al sistema anche ad altri utenti esterni, appartenenti comunque al Servizio Nazionale della Protezione Civile (SNPC).

Principali criticità per l'Amministrazione connesse all'interruzione del servizio

In caso di interruzione del servizio non è possibile fornire le informazioni cartografiche al sistema cartografico SITDPC e non è possibile consentire l'accesso e l'uso agli utenti del sistema. In una situazione di emergenza questa impossibilità è particolarmente rilevante soprattutto nelle primissime fasi dell'evento, dato che il sistema predispone uno scenario post-evento di impatto da condividere. Nelle fasi post-evento l'interruzione impedirebbe la fornitura di

cartografie aggiornate sull'evento (es. zone rosse) e la precompilazione delle schede di rilievo del danno subito dai Beni Culturali.

Principali danni per l'Amministrazione in caso di interruzione del servizio

Un'interruzione prolungata del servizio, in caso di emergenza, è causa di un danno di immagine (inefficienza) per il Dipartimento, non in grado di fare fronte ai suoi delicati compiti istituzionali.

Procedure alternative

Prevedendo una copia dei dati rilevanti dagli schemi SSN_Carto (dati georeferenziati) e SSN_DATA (dati alfanumerici) alcune attività potrebbero essere realizzate tramite un sistema GIS DESKTOP.

Architettura

Il **CSRS** consiste in un applicativo realizzato in tecnologia asp.net, su web server Microsoft IIS con DBMS Oracle.

All'applicazione si accede tramite interfaccia web. La piattaforma hardware è composta da: Web-Tier: due macchine virtuali in ambiente virtualizzato VMWare 4.1;

- Data-Tier: due server fisici.

La componente Data-Tier ha una configurazione in cluster che assicura al sistema una High Availability dell'intero database. Il cluster è costituito da due server gemelli aventi uno storage in comune. Inoltre, esiste un ulteriore storage condiviso, su cui vengono depositati i backup eseguiti quotidianamente.

I due server gemelli sono equipaggiati ciascuno con 2 CPU Intel Xeon 5670 @2.93GHz 6 Core.

Lo storage in comune tra i due server gemelli è un VNX5700. Nello storage viene memorizzato il database e tutte le eventuali copie di back-up.

Componenti SW	
Sistema Operativo	RHEL 5.11
Database	<i>Oracle 11gR2 Enterprise Edition</i>

La componente Web-Tier è realizzata attraverso l'utilizzo di due server in configurazione ridondata ed un DB Oracle.

Componenti SW	
Sistema Operativo	Microsoft Windows Server 2012 R2 Enterprise Edition a 64 bit
Framework Microsoft	PHP 5.6

Il sistema informativo della Protezione Civile è accessibile da diverse tipologie di utenti e da diverse tipologie di rete (internet, intranet): dipendenti che accedono dalla rete dipartimentale e da internet e partner (p.e. Enti esterni). L'apertura dell'accesso ai dati ed ai servizi da diversi canali e la necessità di gestire identità interne ed esterne è guidata da una soluzione robusta e centralizzata basata su standard aperti.

Il prodotto di access management utilizzato è OpenAM ed è in grado di centralizzare la gestione dell'autenticazione e l'autorizzazione all'accesso alle risorse protette, collegandosi a repository degli utenti implementati con directory server (ldap), database e altri sistemi.

Rappresenta una soluzione all-in grazie alle funzioni di autenticazione, federazione, SSO, social sign-on, adaptive authentication. Consiste in una java application accessibile tramite console grafica, servizi REST e diversi protocolli come OpenID Connect, SAML.

Il seguente diagramma illustra l'implementazione del sistema di IAM.

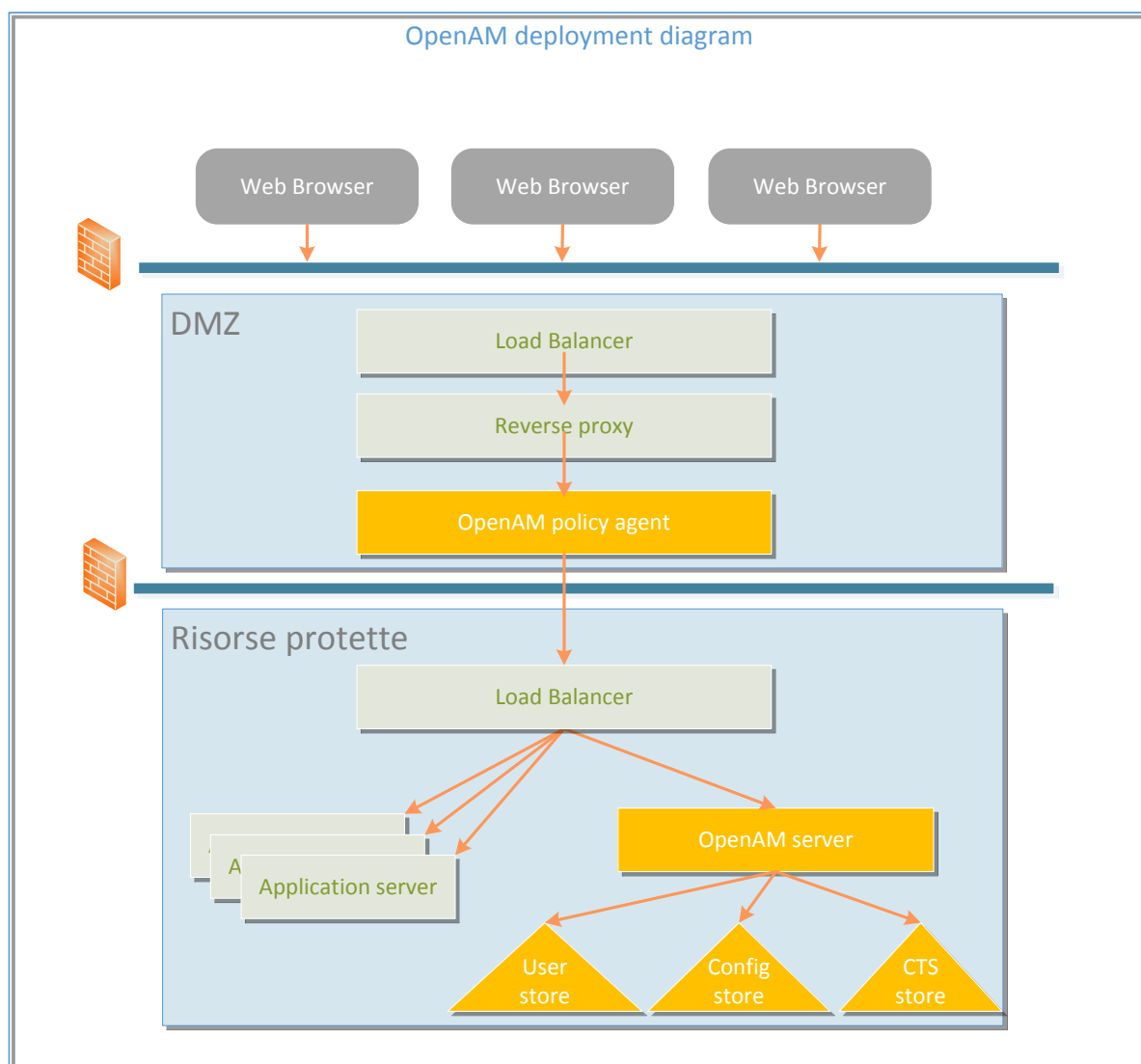


Figura 14 - OpenAM deployment diagram

L'application layer, dove risiedono tutte le risorse protette dai policy agent sono accessibili in base alle regole definite in OpenAM server.

Le componenti di OpenAM per la gestione degli accessi sono:

- **OpenAM server** installato nel layer applicativo, componente centrale nel quale sono configurate tutte le policy di accesso; java-based e quindi installabile nei più popolari application server (si consiglia JBOSS);
- **Web Policy Agent** installati nel front end che, intercettando le richieste alle risorse protette, consentono l'accesso in funzione delle policy configurate in OpenAM server e abilitano il Single Sign On, propagando all'application layer, le informazioni dell'utente collegato;

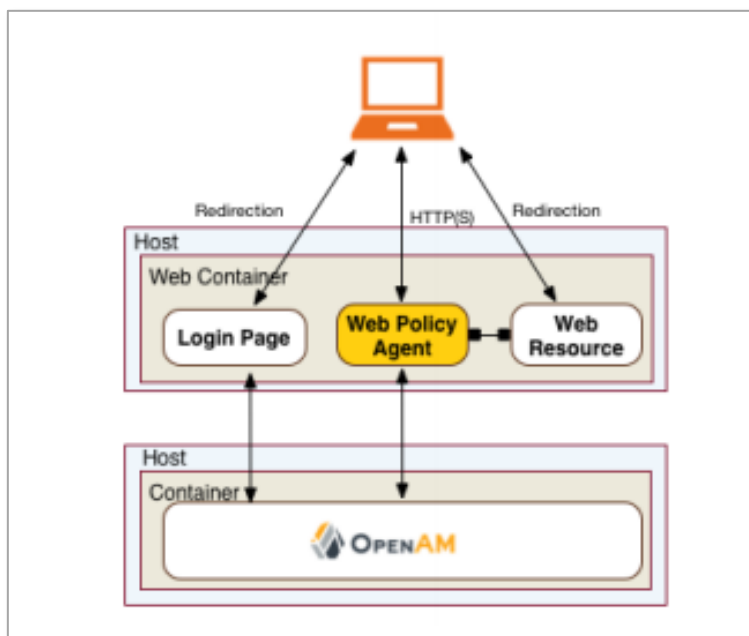


Figura 15 - OpenAM policy agent

- **Configuration Data Store** per la memorizzazione delle policy di accesso configurate (autenticazione e autorizzazione), implementato da OpenDJ, directory server della stessa community di OpenAM, che può essere installato in modalità embedded a OpenAm o esternamente come moduli separati;
- **CTS Data Store** per la persistenza e l'alta affidabilità delle sessioni utente di OpenAM (token), implementato sempre da OpenDJ;
- **User Data Store** il repository degli utenti, di solito un directory server

8.7 Sistema informativo territoriale - SITDPC

Premessa:

Il sistema in oggetto costituisce lo strumento di condivisione attraverso il quale è possibile la visione e il monitoraggio delle risorse di Protezione Civile in termini di reperimento, custodia, movimentazione, utilizzo e recupero.

Il programma è in grado di recepire le informazioni degli Enti e delle Amministrazioni appartenenti al Servizio Nazionale di Protezione Civile, sia in un'ottica di censimento che di gestione della logistica in tempo di pace o al verificarsi di situazioni di emergenza.

Il programma si compone di dati sulle risorse, definiti statici, ed altre informazioni che, se implementate, ne consentiranno un'articolazione dinamica per un'effettiva gestione delle risorse. Il sistema sarà tanto più efficace nel soddisfare le esigenze di gestione nella misura in cui potrà contare nella condivisione e nel concorso degli Enti e delle Amministrazioni appartenenti all'intero Sistema Nazionale di Protezione Civile.

La peculiarità del progetto consiste nella capacità di interfacciarsi con analoghi programmi già in uso da parte dei vari Attori del Sistema Nazionale di Protezione Civile e nella possibilità che lo stesso garantisce nell'integrazione della gestione della logistica nei vari livelli di competenza che vedono, in emergenza, la catena di comando e controllo svilupparsi sul territorio, a partire dalla DICOMAC, attraverso le forze locali attivate nell'ambito dei Centri Operativi istituiti, fino a rappresentare uno strumento di gestione dei siti di emergenza: di ricovero della popolazione (aree, centri, strutture ricettive) e di ammassamento dei soccorritori.

Il sistema, operando in ambiente web sarà fruibile dagli utenti attraverso il rilascio delle necessarie credenziali di accesso.

INFORMAZIONI GENERALI SUL SISTEMA

Il sistema di Logistica del Dipartimento di Protezione Civile assicura le seguenti macro funzionalità:

- a) Gestione dati comuni:
 - Indirizzo;
 - Proprietario;
 - Fornitore;
- b) Gestione anagrafica dei materiali:
 - Anagrafica e stoccaggio del bene;
 - Suddivisione beni in categorie;
 - Identificazione del proprietario e del fornitore del materiale;
 - Manutenzione e prestito dei materiali e relativi alert;
- c) Gestione anagrafica dei mezzi:
 - Identificazione categorie;
 - Identificazione proprietario e fornitore;
 - Manutenzione e prestito dei materiali e relativi alert;
 - Regole di stoccaggio;
- d) Gestione poli logistici e dei siti di accoglienza:
 - Individuazione del proprietario;
 - Identificazione mezzi e materiali presenti;
 - Monitoraggio mezzi e materiali presenti;

- Gestione del personale facente parte di un'area di ricovero, centro di accoglienza o area di ammassamento;
- Associazione di file di tipo multimediale contenenti informazioni aggiuntive;
- e) Movimentazione dei materiali e dei mezzi:
 - Operazioni di carico/scarico del magazzino;
 - Organizzazione imballaggi e produzione etichette di trasporto;
 - Produzione documenti di trasporto, presa in carico o di resa;
- f) Motore di ricerca mezzi e materiali:
 - Ricerca di un bene mediante tutti i suoi attributi, con evidenza dell'ente proprietario;
 - Ricerca geografica di un bene;
- g) Reportistica e ricerche:
 - Beni impiegati in una determinata missione e relativi movimenti;
 - Beni in prestito e beni non restituiti;
 - Beni che necessitano di manutenzione;
 - Produzione report di analisi di supporto alle decisioni della Logistica;
- h) Amministrazione:
 - Creazione utenti e gruppi;
 - Associazioni tra utenti gruppi e funzionalità;
 - Gestione degli accessi;
- i) Distribuzione del sistema:
 - Accesso capi area ammassamento o centro e area di accoglienza;
 - Accesso utenti strutture operative esterne al DPC.

A) Dati Comuni

La funzionalità "Dati Comuni" consente di gestire tutte quelle informazioni che saranno rese disponibili in modo trasversale a tutto il sistema, vale a dire la località, il proprietario, il fornitore, il donatore, le ditte di manutenzione.

I dati salvati sono visualizzabili nelle altre finestre dell'applicativo mediante menu a tendina o finestre di pop up.

Molte informazioni non potranno che derivare da altre banche dati presenti all'interno del Sistema di Protezione Civile.

Il concetto di proprietario sarà di estrema importanza nell'ottica di una distribuzione estesa dell'applicativo, al di fuori del Dipartimento di Protezione Civile e presso le altre Strutture operative; infatti, da un lato quest'informazione permetterà ad ogni Ente di identificare in modo corretto i dati di propria competenza, dall'altro sarà possibile la gestione della condivisione dell'informazione, che vedrà comunque nel Dipartimento di Protezione Civile l'Amministratore di tutto il sistema.

B) Gestione Materiali

Il programma fornirà, mediante la funzionalità di "Gestione dei Materiali", la capacità di inserire, reperire e modificare un qualunque materiale utilizzato dal Servizio Nazionale di Protezione Civile.

I materiali avranno un proprietario che sarà colui che mette a disposizione il bene nel momento dell'emergenza.

Il sistema tratterà il materiale anche in termini di manutenzione, dismissione e caratteristiche di imballaggio. Queste ultime risulteranno indispensabili nel momento in cui, nell'ambito della gestione di un'emergenza, si vorrà pianificare o eseguire una determinata spedizione.

Sarà contemplata anche la gestione dei kit e dei lotti (aggregazioni di materiali e mezzi: moduli) con la relativa tracciatura.

C) Gestione Mezzi

La funzionalità di "Gestione dei Mezzi" permette all'utente del sistema di inserire, modificare e ricercare un qualunque mezzo di trasporto persone o cose.

Un mezzo avrà una categoria di appartenenza e potrà avere una o più dotazioni necessarie a compiere il lavoro cui è destinato.

L'utente potrà collegare ad un mezzo le sue regole di stivaggio, che permetteranno di rendere automatizzata la spedizione dei beni necessari all'intervento in emergenza o alla preparazione del grande evento.

D) Poli Logistici e Siti di Accoglienza

Il sistema fornirà lo strumento di inserimento e di gestione dei poli logistici, delle aree e dei centri di accoglienza. Essi saranno organizzati in modo gerarchico e, in emergenza, a partire dalla DICOMAC fino al Centro di Ammassamento Comunale o al Centro di Accoglienza; alcuni poli logistici esisteranno in modo permanente, altri potranno essere creati solo al momento del verificarsi dell'emergenza o a scopo esercitativo.

Il sistema è in grado di gestire anche l'iter di richiesta di un bene, dal suo reperimento, al documento di trasporto, alla presa in carico, alla resa.

Il sistema, consente inoltre, all'interno di un'area di ricovero della popolazione o in una struttura ricettiva, la gestione anagrafica degli assistiti, attraverso l'inserimento dello stato di famiglia e delle necessità e monitorando gli ingressi e l'utilizzo delle risorse.

E) Movimentazione Materiali

Il sistema permette di organizzare una spedizione consentendo anche di calcolare in modo automatico gli imballaggi, i colli di un lotto o di un kit e le etichette contenenti informazioni relative al contenuto, alla deperibilità o all'urgenza di distribuzione del bene.

Il programma consente la creazione del documento di trasporto che accompagna i beni da distribuire o in uso temporaneo presso altra organizzazione, nonché il relativo documento di presa in carico del bene, segnalando, al termine eventualmente preventivato di assegnazione, la necessità di recupero.

F) Motore di Ricerca Mezzi e Materiali

Il sistema permetterà la ricerca di un bene in anagrafica utilizzando un suo qualunque attributo.

G) Reportistica e Ricerche

Il programma permetterà di ottenere report di consuntivo degli interventi già effettuati, sotto punti di vista modificabili dall'utente ed in modo da costituire un valido supporto alle decisioni.

H) Amministrazione

Classificazione del documento: Public

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l'appalto di servizi di gestione, sviluppo e supporto per il sistema informativo del Dipartimento della Protezione Civile della Presidenza del Consiglio dei Ministri - ID 2005

Appendice 1 al Capitolato tecnico - Contesto tecnologico e applicativo

La funzionalità di “Amministrazione” permetterà la gestione dell’autenticazione e delle autorizzazioni necessarie per accedere alle funzionalità del sistema.

Le normali operazioni di creazione, eliminazione, blocco e sblocco dell’utente, gestione moderna di password comprensiva almeno di validità a scadenza, saranno gestite all’interno del sistema stesso tramite un’autenticazione applicativa.

Tale scelta è motivata dalla necessità di poter agevolmente consentire e controllare gli accessi di utenti agevolando il lavoro degli amministratori di sistema, anche quando si vorrà permettere l’accesso all’applicativo ad un utente “estraneo” al Dipartimento di Protezione Civile, proprietario e gestore del sistema stesso.

Tramite la funzione di amministrazione sarà possibile modificare alcune caratteristiche degli utenti e il loro profilo di accesso alle funzionalità del sistema.

Gli utenti con ruolo di “Amministratore” avranno accesso completo alle funzionalità di amministrazione del sistema.

I) Distribuzione del Sistema

Il sistema potrà essere condiviso, mediante accesso via web, tra le aree di ricovero ed i centri di accoglienza, in modo da poter essere utilizzato per le normali attività di registrazione, gestione e richiesta del bene.

Caratteristiche tecniche e di compatibilità

L’Application Server è costituito da un Server con le seguenti caratteristiche:

- Red Hat Enterprise Linux 5 (64-bit)
- JBoss-6.0.0
- Java JDK (ver. 1.6.0_26 con java DB 10.6.2.1)
- librerie software specifiche per l’accesso ai dati, l’export in formato Microsoft Access e la stampa in pdf.

Tale postazione è caratterizzata da 1 CPU, 8GB di RAM e 20GB di Hard Disk.

Il database sul quale l’applicativo alloca i propri dati, è Oracle RAC 11gR2, costituito da due server fisici RedHat Enterprise Linux 5.4 a 64 bit posti in cluster tra loro in condizioni di alta affidabilità, e che utilizzano uno storage EMC esterno per l’allocazione dei dati.

9. Gestione del Sito web istituzionale in Cloud Computing

Il contratto per la fornitura dei servizi di Cloud Computing per le Pubbliche Amministrazioni nell'ambito del Contratto Quadro SPC Lotto 1 prevede la fornitura dei seguenti servizi di Cloud Computing nell'ambito del Sistema Pubblico di Connettività e Cooperazione (SPC):

- servizi di tipo Infrastructure as a Service (IaaS);
- servizi di tipo Platform as a Service (PaaS);
- servizi di tipo Software as a Service (SaaS);
- servizi di Cloud Enabling.

Il ricorso ai servizi di Cloud Computing risulta idoneo a rispondere alle esigenze attuali del Dipartimento della Protezione Civile, di gestire in completa autonomia i server remoti virtuali dell'infrastruttura del sito web istituzionale, acquistare e gestire in completa autonomia un servizio base di backup (BaaS).

Per quel che riguarda la componente IaaS, l'architettura Cloud DPC è composta da due differenti VDC (Virtual Data Center): "Model Office" e "Produzione" composti rispettivamente da:

Ambiente "Model Office":

- 9 sistemi Red Hat,
- 1 sistema FreeBSd
- 1 sistema Microsoft Server Windows 2008

Ambiente "Produzione":

- 22 sistemi Red Hat,
- 2 sistemi FreeBSd

Inoltre è gestito in completa autonomia dal Dipartimento della Protezione Civile anche il Virtual Storage Object interconnesso ai sistemi precedentemente descritti.