



consip

CLASSIFICAZIONE: CONSIP PUBLIC

APPENDICE 1 AL CAPITOLATO TECNICO - CONTESTO APPLICATIVO E TECNOLOGICO

GARA PER L’AFFIDAMENTO DEI SERVIZI DI GESTIONE, SVILUPPO E SUPPORTO PER IL SISTEMA INFORMATIVO DEL DIPARTIMENTO DELLA PROTEZIONE CIVILE DELLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI (ED. 3)

ID 2617



Sommario

1	INFRASTRUTTURE DI RETE	3
1.1	ARCHITETTURA DI RETE DELLA SEDE DIPARTIMENTALE DI Via VITORCHIANO	4
1.2	ARCHITETTURA DI RETE DELLE SEDI DIPARTIMENTALI DI Via ULPiano E Via DELLA MAGLIANA.....	5
1.3	ARCHITETTURA DELLA SEDE DI DISASTER RECOVERY	5
1.4	ARCHITETTURA WIFI	5
1.5	LOG MANAGEMENT	6
1.6	ENTI ESTERNI CONNESSI ALLA RETE	6
2	INFRASTRUTTURE TECNOLOGICHE	7
2.1	FILESERVER E SHAREPOINT.....	7
2.2	SERVIZIO DI ACTIVE DIRECTORY	7
2.3	REVERSE PROXY.....	7
2.4	SERVIZIO NTP (NETWORK TIME PROTOCOL)	8
2.5	SERVIZIO DI POSTA ELETTRONICA	8
2.6	SERVIZIO DI FAX SERVER	8
2.7	STRUMENTI DI GESTIONE	8
2.8	BACKUP	9
2.9	DELL EMC AVAMAR	9
2.10	VCENTER	10
2.11	PORTALE DEI SERVIZI DEL DIPARTIMENTO	10
2.12	TELEFONIA FISSA	10
2.13	APPARATI AUDIO-VIDEO.....	11
3	POSTAZIONI DI LAVORO	12
4	APPLICAZIONI	14
5	DIREZIONE DI COMANDO E CONTROLLO - DICOMAC.....	17
6	OSSERVATORIO SISMICO DELLE STRUTTURE (OSS)	18
7	RETE ACCELEROMETRICA NAZIONALE (RAN)	19
8	RETE DEI CENTRI FUNZIONALI.....	20



1 INFRASTRUTTURE DI RETE

Le tre sedi del Dipartimento della protezione civile della Presidenza del Consiglio dei Ministri sono ubicate a Roma, in:

- Via Vitorchiano (sede operativa): 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 considerata come un hub, presso il quale convergono le altre nuvole di connettività;
- Via Ulpiano (la sede storica): rete di accesso per il personale del Dipartimento, dov'è collocato un CED secondario, dal quale vengono erogati alcuni servizi per il personale dislocato presso tale sede;
- Via della Magliana (la sede dei mezzi): rete di accesso per il personale del Dipartimento.

La sede dipartimentale di via Vitorchiano è, inoltre, il centro stella della rete ed offre la raggiungibilità a molteplici servizi (Datacenter, APN per il trasferimento dati da rete mobile, SPC, ToIP, accesso ad Internet, ecc.).

Per erogare i propri servizi ed essere contestualmente indipendente dagli eventuali problemi dei singoli carrier, il Dipartimento si è impostato come Autonomous System, 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 le Società TIM e Fastweb: disponendo di due distinti collegamenti - con due differenti provider - è possibile quindi annunciare sulla rete gli stessi IP (con dei 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 istradato automaticamente su quella rimasta attiva.

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

- la disponibilità del servizio di tipo Mission Critical, pari al 99,99%;
- in caso di guasti, un veloce tempo di ripristino (4h nel 95% dei casi e, comunque, entro 8h nel 100% dei casi);
- una finestra di erogazione estesa (24/7/365).

Le sedi dipartimentali di Via Ulpiano e via della Magliana sono connesse alla rete attraverso un idoneo collegamento in MPLS.



1.1 ARCHITETTURA DI RETE DELLA SEDE DIPARTIMENTALE DI VIA VITORCHIANO

La sede dipartimentale di Via Vitorchiano rappresenta il centro nevralgico dell'architettura IT.

Infatti, in tale sede è presente il Datacenter principale, che ospita tutti i sistemi che erogano servizi, sia interni, che su connettività pubblica; inoltre, sono qui allocati gli apparati adibiti alla gestione della connettività Internet.

L'architettura di rete centrale è organizzata seguendo il paradigma "collapsed network", con:

- un'architettura di core (layer 3) centrale implementata con una coppia di next-generation firewall Fortigate, 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 PAN (Palo Alto Network);
- firewall di core: implementato attraverso una coppia di next-generation firewall Fortigate;
- 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, altresì, 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 anch'essi 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 (non svolgono alcun controllo UTM).

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

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

- Back End Network, dove sono ospitati tutti i server in grado di erogare servizi interni (es. Active Directory, Fileshare);
- DMZ Network: dove sono ospitate 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: che comprende tutte le reti esterne, siano esse di tipo Intranet che Infranet. Ad esempio, rientrano in questa categoria le reti implementate nei siti remoti (Via Ulpiano, Via della Magliana, le reti appartenenti a differenti amministrazioni pubbliche, ecc.).

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, in sostituzione per le medesime funzioni e superiori con la suite di prodotti endpoint e EDR/XDR Cybereason, in gestione ad un servizio di SOC operato da figure tecniche specialistiche in remoto.

1.2 ARCHITETTURA DI RETE DELLE SEDI DIPARTIMENTALI DI VIA ULPIANO E VIA MAGLIANA

L'architettura IT delle sedi di Via Ulpiano e Via della Magliana è abbastanza simile. In ciascuna sede è presente una coppia di firewall (tecnologia Fortigate), 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 comunque 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 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+;
- apparati Extreme Network Summit series presso la sede di Via Magliana. La ridondanza in tal caso è implementata facendo ricorso alle tecnologie di Stacking.

1.3 ARCHITETTURA DELLA SEDE DI DISASTER RECOVERY

Di prossima adozione una soluzione con un modello DRaaS, via WAN ed in modalità off-site backup, con la sede dipartimentale di via Ulpiano.

Il portale istituzionale www.protezionecivile.it e alcuni sistemi critici sono stati rilocati su architettura cloud AWS, non soggetti ad eventuali problemi di fault delle sedi (infrastruttura fisica e logica).

1.4 ARCHITETTURA WIFI

Scopo principale dell'architettura WiFi è quello di assicurare la 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 il Dipartimento.

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, Sala del Comitato Operativo, ecc..

L'infrastruttura wireless e la rete di distribuzione è implementata con tecnologie Fortinet e Fortinet AP Controller, con numero adeguato di AccessPoint WiFi5 e WiFi 6 managed (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, firewall di core 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 in parola 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.

1.5 LOG MANAGEMENT

La soluzione dipartimentale di Log Management & Correlazione si compone di una piattaforma di sicurezza HPE ArcSight, in sostituzione con una soluzione SIEM remota in gestione al servizio SOC dedicata a:

- collezionare, aggregare, conservare, ricercare ed analizzare centralmente i log provenienti dai sistemi, database, applicazioni, apparati e dispositivi del Dipartimento;
- 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 riuscire a 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.

L'infrastruttura è composta dalle seguenti tipologie di appliance:

- 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.

1.6 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.



2 INFRASTRUTTURE TECNOLOGICHE

Le infrastrutture tecnologiche dipartimentali si articolano, primariamente, nelle seguenti aree:

- Applicazioni di supporto;
- Autenticazione e indirizzamento;
- Connettività e sicurezza;
- Messaggistica;
- Monitoraggio;
- Sistemi di backup;
- Telefonia fissa;
- Apparatrici audio-video.

2.1 FILESERVER E SHAREPOINT

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

Il prodotto Microsoft Sharepoint 2016 viene utilizzato per realizzare alcuni siti di condivisione documentale, per diverse applicazioni dipartimentali.

L'architettura Fileserver è basata su due server virtuali Windows Server 2019 Standard in cluster Active/Passive MS.

L'architettura Sharepoint è invece composta da dodici server virtuali Windows Server 2016 e 2 server virtuali Windows Server 2012 R2, per l'autenticazione dei siti esposti su Internet.

2.2 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". L'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 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.

È presente, inoltre, un trust tra il dominio del Dipartimento e quello DiCOMAC, in uso per l'infrastruttura trasportabile a supporto della gestione dell'emergenza.

2.3 REVERSE PROXY

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 delle sede dipartimentale di Via Vitorchiano e NGINX è il servizio utilizzato per implementare la funzionalità di Reverse Proxy.

2.4 SERVIZIO NTP (NETWORK TIME PROTOCOL)

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

2.5 SERVIZIO DI POSTA ELETTRONICA

Il servizio di posta elettronica del Dipartimento si basa su un'infrastruttura Microsoft Exchange 2019 ed è interamente ospitata nel datacenter di Via Vitorchiano. Il servizio è erogato da 4 server virtuali.

Attualmente il servizio ospita circa 1000 mailbox divise in 28 database più 2 Journaled dedicati 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.

I server Exchange 2019 sono in area di Back End ed iscritti al dominio Active Directory del dipartimento.

I servizi erogati da Exchange 2019 sono pubblicati tramite il bilanciatore Kemp (due appliance virtuali). Quindi i client interni oppure da internet accedono attraverso il bilanciatore Kemp.

2.6 SERVIZIO DI FAX SERVER

L'applicativo Zetafax consente agli utenti la possibilità di ricevere ed inviare fax da Client e da Outlook.

L'applicazione è installata su due server in modalità active/stand by ed è interfacciata alle linee ISDN PRI attraverso due gateway Dialogic SR140 anche loro in modalità active/stand by.

Il servizio si articola in quattro componenti funzionali:

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

2.7 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 (Nagios Enterprise), che tiene controllo dello 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.
- una piattaforma di Service Desk per la gestione del ciclo di vita delle segnalazioni di change, da parte degli utenti (Zendesk, attualmente in corso d'acquisizione, da parte dell'Amministrazione).

2.8 BACKUP

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

- Dell EMC Avamar;
- Veeam (in corso d'acquisizione);
- Vcenter;
- Portale Servizi.

2.9 DELL EMC AVAMAR

Dell EMC Avamar garantisce backup e ripristino, grazie alla tecnologia integrata di deduplica a lunghezza variabile. L'infrastruttura è ottimizzata per backup giornalieri completi e veloci in ambienti virtuali e fisici, server NAS, applicazioni di livello enterprise.

In questo modo, il ripristino di dati all'interno del Dipartimento avviene in tempi rapidi, diminuendo drasticamente il tempo di disservizio. L'architettura Avamar è costituita da:

- un Dell EMC Data Domain;
- una VM Avamar;
- cinque VM Avamar Proxy.

Il backup avviene con l'ausilio di agenti installati sui server per le tipologie supportate (esempio file system, database SQL Server, DAG di Exchange Server, ecc.) oppure tramite i proxy vengono salvate le intere VM.

Ogni backup ha una schedulazione distinta e una retention dedicata (di solito di trenta/sessanta giorni); il salvataggio avviene su dischi dedicati e ridondati, quotidianamente per l'ambiente di esercizio o con diversa cadenza per gli ambienti di test/collaudato, comunque con schedulazioni e retention distinte a seconda delle indicazioni fornite dai referenti degli applicativi/servizi.



2.10 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.

2.11 PORTALE DEI SERVIZI DEL DIPARTIMENTO

Questa modalità di backup avviene tramite il portale dei servizi, 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: si basa sullo snapshot (immagine del server virtuale) e preclude una gestione delle immagini dei server virtuali. I dati sono salvati tramite disco EMC2.

2.12 TELEFONIA FISSA

La centrale telefonica Alcatel Oxe del Dipartimento è composta da due nodi principali (con altri secondari):

- nodo 2 situato a Via Vitorchiano (al quale è legato un media gateway esterno, situato nella sede di Via della Magliana);
- nodo 3 situato a Via Ulpiano.

Su un rack dedicato sono stati installati 4 server HP: su 2 sono virtualizzate le CPU OXE Main e Stand-By e sui restanti 2 sono virtualizzati gli SBC Main e Stand-by. Inoltre, è collegato un media gateway locale sul quale è installato l'hardware necessario per le comunicazioni IP (schede equipaggiate con compressori DSP), schede per la generazione di linee analogiche e schede per il collegamento di flussi ISDN.

I posti operatori di Vitorchiano (Centralino attivo) sono 6, con 2 gruppi di distribuzione chiamate, e sono attualmente attestati e gestiti tutti sul nodo 2, mentre quelli attestati sulla sede di Ulpiano sono 3, dormienti e di backup, pertanto attualmente non utilizzati.

I telefoni IP sono quasi nella totalità dei casi collegati in cascata ai personal computer, ovvero la porta è configurata sia con l'accesso alla VLAN dei telefoni, che con la VLAN dati per la connessione dei personal computer stessi.

Fisicamente, il cavo LAN, proveniente dalla torretta/presa RJ45 è collegato al telefono da cui riparte il cavo che serve il personal computer. Alcune postazioni, prevalentemente quelle dirigenziali, hanno porte telefono e porte personal computer singole e dedicate (separate).

I telefoni IP, senza entrare nella specificità di ogni modello, sono di due serie; la più diffusa e anche la più recente è la serie IPTouch 8xxx, che offre una connessione con velocità a 1Gb mentre; la meno recente e anche la meno diffusa è la serie IPTouch 4xxx, che offre una connessione a velocità massima di 100Mb.

Sono presenti, nel MD, anche delle utenze analogiche che servono dei Fax ancora attivi dopo la migrazione della maggior parte di essi al recente fax server.



Per completezza d'informazione, si rappresenta che alla centrale telefonica è collegato un altro server virtuale, su cui è alloggiata l'applicazione denominata Alcatel 8770, necessaria a gestire tutto ciò che si trova in "monitoraggio" (dal traffico telefonico, all'eventuale gestione addebiti, all'allarmistica).

2.13 APPARATI AUDIO-VIDEO

Il Dipartimento detiene un'architettura audio video analogica interna, dislocata presso tutte le sale riunioni presenti nelle sedi dipartimentali.

Tutti i segnali vengono gestiti e smistati da una Sala regia, dedicata allo scopo.

Il Dipartimento, per poter svolgere i propri compiti istituzionali, si avvale anche di appositi sistemi di videoconferenza: un sistema on-premise di Cisco e due sistemi in cloud, che consentono di svolgere riunioni con molti partecipanti.

Tali riunioni, in sede o in videoconferenza, su esplicita richiesta degli Organizzatori, possono essere anche registrate su dei dispositivi presenti in sede o utilizzando gli spazi a disposizione sul cloud.



3 POSTAZIONI DI LAVORO

Nella tabella in calce è riportata, in estrema sintesi, la configurazione delle postazioni di lavoro standard e dei relativi componenti accessori, attualmente in uso agli utenti del Dipartimento (ad esclusione delle stampanti).

Ad ogni buon fine, sono presenti anche due ulteriori tabelle, riguardanti il numero dei tickets gestiti:

- nelle sedi dipartimentali, dal 2019, al 2022;
- nella DiComaC istituita a Rieti, a seguito dagli eventi sismici verificatisi a far data dal 24 agosto 2016 nelle regioni del centro Italia.

Tipologia	N. apparecchiature
Workstation	995
Notebook	464
Scanner	306
Etichettatrici	107

Anno	Sede dipartimentale	N. tickets
2019	Via Ulpiano	954
	Via Vitorchiano e Via della Magliana	2538
2020	Via Ulpiano	866
	Via Vitorchiano e Via della Magliana	2138
2021	Via Ulpiano	975
	Via Vitorchiano e Via della Magliana	2488
2022	Via Ulpiano	1276
	Via Vitorchiano e Via della Magliana	2928



DiComaC - Rieti	
Anno	N. tickets
2016 (da agosto)	715
2017 (fino ad aprile)	380

A partire dal 2020, al Dipartimento è stato progressivamente implementato l'utilizzo dei computer portatili Azure AD Join, la cui principale caratteristica è rappresentata dalla possibilità di connettersi al dominio dell'Amministrazione con la propria utenza personale, anche al di fuori delle sedi dell'Ente, facilitando, contestualmente, lo svolgimento della prestazione lavorativa in modalità agile.

Lato sicurezza, rivestono una particolare importanza le impostazioni di criteri di crittografia del disco: infatti, tramite l'utilizzo della funzionalità BitLocker, i file lavorati all'interno del sistema operativo, per essere spostati su un dispositivo esterno devono per forza essere crittografati, come il disco dove è contenuto il sistema operativo stesso.

Le credenziali sono gestite tramite tecnologia Windows Hello (accesso con riconoscimento del volto, impronta digitale, PIN).

I client AD Join sono serviti da una rete cablata, così come da una rete Wi-Fi dedicata: all'interno della Struttura dipartimentale i computer portatili in argomento sono normalmente collegati alla rete cablata, ma c'è comunque la possibilità di passare alla rete Wi-Fi, in caso di necessità.



4 APPLICAZIONI

A titolo puramente informativo, di seguito è riportato un elenco di sintesi, con la denominazione dei principali servizi che, attualmente, compongono l'ambiente applicativo del Dipartimento.

Servizio
AGITEC - Gestione attività di censimento e sopralluogo edifici danneggiati
Brogliaccio - Centro Funzionale Centrale
Brogliaccio - Rischio Vulcanico
Brogliaccio - Sala Situazione Italia
Catalogo delle mappe interattive Web-GIS
Catalogo dei metadati
COAU - Antincendio boschivo
COS - Contributi di sostentamento
CSRS - Centri storici e rischio sismico
DataHub
Designa - Gestione della popolazione in emergenza
Dighe - Gestione informazione sulle dighe
Donazioni - Raccolte fondi per le emergenze
ELOG - Gestione emergenze - Rischio vulcanico
Logistica - Sistema di gestione della logistica di protezione civile
HSAF - Gestione applicazioni idrologiche operative
Identity and Access Management (IAM)
IT-Alert - Sistema di allarme pubblico per l'informazione della popolazione



MyDewetra - Sistema integrato per il monitoraggio, la previsione e la prevenzione dei rischi naturali in Italia e nel mondo
OSS - Osservatorio Sismico delle Strutture
Piattaforma radar
PIB - Procedura informatica per le benemerienze
PON - Piattaforma PON
RAN - Rete Accelerometrica Nazionale
SAE - Soluzioni abitative in emergenza
Scuola multimediale - Scuola multimediale di protezione civile
SIAB - Sistema integrato di amministrazione e bilancio
SIAM - Sistema di allertamento tsunami
Sicuro+ - Sistema informativo di comunicazione del rischio
SIGE - Supporto alle decisioni per la prima emergenza sismica
Sito Web istituzionale
Sito Web istituzionale - Io non rischio
Sito Web istituzionale - IT-Alert
SIV - Verifiche sismiche
Socialprociv
Stromboli - Sistema di gestione delle sirene d'allertamento
Volontariato - Gestione dei servizi al volontariato di protezione civile
SMS-Handler
SITDPC - Sistema informativo territoriale
SQL Server 2014 Always On



SQL Server 2016 Always On Applicativi
SQL Server 2016 Always On SP
PostgreSQL 9.6 Cluster

La stima degli interventi di manutenzione correttiva sul parco applicazioni eseguito nell'ultimo anno sono stati pari a 4 interventi/mese.



5 DIREZIONE DI COMANDO E CONTROLLO - DICOMAC

La DiComaC è 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 in caso di emergenza nazionale.

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

- in base al provider individuato, fornire connettività Internet e Extranet alle utenze presenti all'interno dell'infrastruttura;
- fornire servizi di connettività WiFi di tipo Hotspot;
- fornire servizi di telefonia;
- fornire supporto audio/video nelle sale riunioni.
- Garantire la connessione ad i servizi di microsoft adjoin su cloud azure per la corretta gestione delle pdl nel servizio active directory del dipartimento
- Fornire possibilità di connessione sicura ed affidabile ad i servizi di filesharing basati su piattaforma microsoft sharepoint.

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: DNS/DHCP. L'architettura è protetta da una coppia di sistemi di sicurezza perimetrali (firewall) che svolgono, oltre al firewalling, i seguenti servizi supplementari:

- Layer 3 Routing,
- UTM/SDWAN e controlli avanzati sulla qualità e la sicurezza del traffico verso internet ;
- VPN Concentrator;
- WiFi Controller.

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

I sistemi sono interconnessi tra loro per mezzo di una coppia di switch. Nel suo complesso l'architettura è composta dunque da:

- due Switch configurati in Alta affidabilità POE per mezzo della tecnologia Stacking;
- due firewall tecnologia Fortinet configurati in Alta affidabilità in modalità "Active/Standby", con accelerazione , sdwan ed utm next generation firewall;
- numero variabile di Access Point Wireless in tecnologia Fortinet wifi6 per interni ed esterni
- adeguato gruppo di continuità per alimentazione del rack network e del rack centrale telefonica voip esterno.



6 OSSERVATORIO SISMICO DELLE STRUTTURE (OSS)

Attraverso la rete nazionale dell'OSS, il Dipartimento monitora le oscillazioni causate dal terremoto in 156 costruzioni di proprietà pubblica: 143 edifici, oltre a 7 ponti e 6 dighe.

Queste costruzioni si trovano in comuni classificati per lo più in zona sismica 1 (33%) e 2 (60%).

Quando una costruzione dell'OSS è colpita da un terremoto significativo, il sistema di monitoraggio registra il movimento del terreno e quello della struttura, inviando immediatamente i dati registrati al server centrale OSS di Roma.

Il server, immediatamente dopo l'evento, elabora le misure in automatico e produce una scheda di sintesi dei principali parametri di risposta dinamica di tutte le strutture interessate dal terremoto.

Inoltre, nelle ore subito successive ad un sisma grave, viene installata in area epicentrale una rete temporanea di almeno 4 sistemi di monitoraggio semplificati, subito integrati nell'OSS.

In questo caso le strutture monitorate sono prevalentemente gli edifici adibiti al coordinamento degli interventi per la gestione dell'emergenza, come le sedi dei Centri Operativi Misti e della DiComaC.

Le strutture dell'OSS vengono monitorate mediante accelerometri di tipo force balance, posizionati ai vari piani ed a terra; i sensori sono collegati via cavo o Wi-Fi ad una centralina situata nell'edificio, collegata via Internet al server centrale di Roma.

Un sistema di monitoraggio "dettagliato" dell'OSS si compone di sensori distribuiti su tutti i piani dell'edificio ed a terra, per una media di 20 misure di accelerazione, in modo da ricostruire adeguatamente i modi di vibrare della struttura e stimare il danno.

I sensori sono collegati via cavo ad una centralina sismica, connessa via ADSL con il server OSS di Roma.

Nell'OSS si hanno 132 sistemi OSS di questo tipo.

24 ulteriori sistemi permanenti dell'OSS sono invece di tipo "semplificato", simili a quelli della rete temporanea installata in emergenza.

In questo caso ci sono soltanto sensori a terra e sull'ultimo piano dell'edificio, indipendenti e collegati tra loro in rete WiFi.



7 RETE ACCELEROMETRICA NAZIONALE (RAN)

La RAN è una rete di monitoraggio che registra la risposta del territorio italiano al terremoto, in termini di accelerazioni del suolo.

I dati prodotti permettono di descrivere nel dettaglio lo scuotimento sismico nell'area dell'epicentro, consentono di stimare gli effetti attesi sulle costruzioni e sulle infrastrutture, sono utili per gli studi di sismologia e di ingegneria sismica e possono contribuire a definire l'azione sismica da applicare nei calcoli strutturali per la ricostruzione.

La RAN è distribuita sull'intero territorio nazionale, con maggiore densità nelle zone ad alta sismicità, ed è attualmente costituita da 647 postazioni digitali provviste di un accelerometro, un digitalizzatore, un modem/router con un'antenna per trasmettere i dati digitalizzati via GPRS ed un ricevitore GPS per associare al dato il tempo universale UTC e per misurare la latitudine e longitudine della postazione.

Di queste 647 postazioni, 234 sono inserite all'interno di cabine di trasformazione elettrica di Enel Distribuzione e 413 sono posizionate su terreni di proprietà pubblica.

I dati affluiscono al server centrale della RAN nella sede del Dipartimento, dove vengono acquisiti ed elaborati in maniera automatica per ottenere una stima dei principali parametri descrittivi della scossa sismica.

Al database della RAN affluiscono in tempo quasi reale i dati provenienti da altre reti accelerometriche di proprietà pubblica, in base a intese programmatiche e a convenzioni.

I parametri e le forme d'onda sono archiviati automaticamente nel database centrale e sono poi resi disponibili su questo sito: ran.protezionecivile.it.



8 RETE DEI CENTRI FUNZIONALI

La gestione del sistema di allertamento nazionale è assicurata dal Dipartimento e dalle Regioni e Province Autonome con 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 dipartimentale 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.