

Allegato A – Capitolato tecnico

Sommario

Allegato A – Capitolato tecnico.....	1
1. PREMESSA	3
1.1 Introduzione al sistema informativo	3
1.2 Obiettivi e benefici attesi	3
2. OGGETTO DEL CAPITOLATO	3
3. RESPONSABILE DI PROGETTO E REFERENTE TECNICO	4
4. REQUISITI DEL FORNITORE E DEL CENTRO SERVIZI.....	4
5. DESCRIZIONE DEL SISTEMA INFORMATIVO (AS-IS).....	5
5.1. Area 1 [AS-IS] – “Private Cloud” Aruba	6
5.2. AREA 2 [AS-IS] – “O.CLOUD” Irideos	10
6. INFRASTRUTTURA CLOUD [TO-BE].....	13
6.1. AREA 1 [TO-BE].....	15
6.2. AREA 2 [TO-BE].....	15
6.3. Riepilogo risorse complessive richieste e requisiti	18
6.4. Requisiti non funzionali.....	19
7. SERVIZI DI GESTIONE E MANUTENZIONE.....	21
7.1. Monitoraggio ed assistenza	21
7.2. Servizi gestione e manutenzione infrastruttura	22
7.3. Servizi di manutenzione e gestione ordinaria dell’ambiente applicativo	23
7.4 Riservatezza e Protezione dei dati	24
7.5 Presa in carico e migrazione dell'infrastruttura.....	25
7.6 Rilascio al termine del servizio.....	25
8. SERVIZIO DI HELP-DESK.....	26
8.1 Help-Desk di primo livello	26
8.2 Help desk di secondo livello.....	27

Acronimi

API:	Application Programming Interface
BI:	Business Intelligence
DMZ:	DeMilitarized Zone
F/OSS:	Free and Open Source Software
IaaS:	Infrastructure as a Service
ICT:	Information and Communication Technology
IDS:	Intrusion Detection Systems
IE:	Internet Explorer
IPS:	Intrusion Prevention Systems
IT:	Information Technology
KPI:	Key Performance Indicator
PaaS:	Platform as a Service
HTTP:	Hyper Text Transport Protocol
HTTPS:	Secure HyperText Markup Language
IMAP:	Internet Mail Access Protocol
SMTP:	Simple Mail Transfer Protocol
SAL:	Stato Avanzamento Lavori
SAN:	Storage Area Network
SLA:	Service Level Agreement
SSD:	Solid State Drive
VDC:	Virtual Data Center
VLB:	Virtual Load Balancer
VM:	Virtual Machine
VNetwork:	Virtual Network
VF:	Virtual Firewall
VPN:	Virtual Private Network

1. PREMESSA

1.1 Introduzione al sistema informativo

Allo scopo di aumentare l'efficienza dell'infrastruttura informatica, di garantire la migliore affidabilità delle comunicazioni da e verso le aziende aderenti, di perseguire un attento contenimento dei costi e di garantire un servizio di supporto ed assistenza con elevate garanzie e performance, il Fondo ha proceduto dal 2014 alla migrazione dei server fisici su una infrastruttura cloud.

L'infrastruttura informatica è strategica, per la delicatezza e la quantità dei dati gestiti ai fini dell'erogazione dei finanziamenti, nonché per gli obblighi derivanti dalla normativa nel rapporto con l'Ente vigilante - Ministero del Lavoro e delle Politiche Sociali - INPS – ed aziende aderenti. Inoltre, dal 2010, il Fondo ha adottato un software di *business process management*, che ha consentito il progressivo superamento della gestione documentale e relativa archiviazione in formato cartaceo.

Nel triennio 2015-2017, il sistema informativo si è evoluto con importanti modifiche alla Piattaforma adottata per la gestione delle fasi di presentazione, monitoraggio e rendicontazione dei Piani formativi finanziati a valere sugli Avvisi emanati dal Fondo (di seguito "Piattaforma di Gestione degli Avvisi"). La soluzione adottata è costituita da un front-office basato su una web application su piattaforma LAMP ed un back-office basato su Filemaker.

Si sottolinea che è attualmente in fase di completamento l'implementazione di una nuova Piattaforma di Gestione Avvisi (NSI), che sostituirà la precedente ed integrerà altre parti del sistema informativo in essere, secondo quanto, di seguito, meglio dettagliato. Parallelamente, è in fase di sviluppo la nuova piattaforma di Business Intelligence.

1.2 Obiettivi e benefici attesi

Nell'ottica di garantire un continuo miglioramento ed aggiornamento tecnologico del Sistema Informativo, il Fondo si propone di:

- Integrare in un unico ambiente cloud l'intera infrastruttura di server componenti il Sistema Informativo;
- Dotarsi di un sistema sicuro ed ad alta affidabilità per far fronte alla crescente mole di informazioni gestite;
- Gestire, in maniera elastica, i picchi di richiesta, consentendo una scalabilità (verticale ed orizzontale), facilmente gestibile ed attivabile in tempi rapidi;
- Garantire l'affidabilità di utilizzo della nuova Piattaforma di Gestione Avvisi e dei dati nella stessa gestiti nonché l'integrazione delle diverse componenti, ad oggi, distribuite su diversi sistemi.

2. OGGETTO DEL CAPITOLATO

Il Fondo, con la presente procedura di gara, intende affidare, per la **durata di 18 (diciotto) mesi**, la fornitura ed i servizi di seguito descritti:

- Servizi in modalità cloud computing di tipo:
 - Infrastructure as a Service (IaaS) per la fruizione di risorse remote virtuali;

- Platform as a Service (PaaS) per l'erogazione di servizi DBMS (ad esempio MySQL) e middleware per lo sviluppo, collaudo, manutenzione ed esercizio di applicazioni "container-based";
- Disaster Recovery as a Service (DraaS) per la protezione da interruzioni dei servizi e per garantire la continuità operativa di parte dell'infrastruttura.

I servizi sono corredati da strumenti di gestione e configurazione che includono funzionalità di networking tra cui virtual load balancer, virtual firewall, virtual lan;

- Progettazione ed esecuzione delle operazioni di migrazione e presa in carico dell'attuale infrastruttura;
- Servizi di gestione sistemistica, monitoraggio e controllo dell'infrastruttura, di manutenzione e gestione ordinaria dell'ambiente applicativo;
- Servizio di Help Desk.

3. RESPONSABILE DI PROGETTO E REFERENTE TECNICO

L'Affidataria dovrà nominare un proprio Responsabile di Progetto, al quale saranno affidate le mansioni di supervisione e coordinamento delle attività svolte nell'esecuzione del Contratto.

Il Responsabile di Progetto (Capo Progetto) rappresenterà il referente unico del Direttore dell'Esecuzione del Contratto nominato dal Fondo ed assicurerà, tra l'altro, la necessaria assistenza consulenziale al Fondo, anche al fine di definire le interazioni, a livello di infrastruttura, tra i servizi offerti e quelli resi disponibili attraverso sistemi informativi di Enti ed Istituzioni.

L'Affidataria dovrà, inoltre, nominare un Referente Tecnico, che sarà responsabile della conduzione ed amministrazione dell'infrastruttura fornita e si renderà sempre disponibile, anche telefonicamente, per acquisire le segnalazioni di anomalia, per la relativa gestione e per l'esecuzione delle attività aventi carattere di urgenza.

4. REQUISITI DEL FORNITORE E DEL CENTRO SERVIZI

L'erogazione dei servizi in modalità "as a service", richiede che l'Affidataria dovrà disporre obbligatoriamente di Centri Servizi, che devono rispondere a quanto di seguito indicato e garantire i requisiti definiti al Capitolo 6:

- i Centri Servizi in cui l'Affidataria erogherà i servizi di cui al presente Capitolato dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio comunitario ed ottemperare alla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio (*Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*). È fatto obbligo, inoltre, all'Affidataria di trattare, trasferire e conservare le eventuali repliche dei dati conservati dai suddetti Centri Servizi sempre all'interno del territorio comunitario;
- l'infrastruttura tecnologica dei Centri Servizi dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza. Dovrà essere garantita la continuità di servizio, anche in presenza di guasti, prevedendo le necessarie ridondanze dei componenti e dei collegamenti sia interni che verso la rete Internet. In caso di eventi di disastro che rendono indisponibile l'intero sito preposto all'erogazione dei servizi, l'Affidataria dovrà garantirne la ripartenza, anche su un diverso sito;

- l’Affidataria dovrà garantire la sicurezza delle strutture, dei collegamenti, la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l’applicazione di procedure e politiche di sicurezza da adottare al proprio interno. In particolare, è responsabilità dell’Affidataria assicurare che i Centri Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni siano protette mediante l’adozione di adeguati sistemi e metodologie, oltre che gestite in piena conformità con la normativa cogente;
- devono essere adottate tutte le necessarie misure, volte a limitare il rischio di attacchi informatici ed eliminare eventuali vulnerabilità della rete, causate dalla violazione e dall’utilizzo illecito di sistemi o delle infrastrutture fornite.

Per i Data Center che erogano i servizi sono richieste le certificazioni ISO 9001:2015 (Sistema di gestione per la qualità) e ISO/IEC 27001:2013 (Sistema di gestione per la sicurezza dei dati) o successive.

Le suddette certificazioni devono essere valide alla data di presentazione dell’offerta e devono essere mantenute tali per l’intera durata contrattuale.

5. DESCRIZIONE DEL SISTEMA INFORMATIVO (AS-IS)

In questo capitolo viene fornita una descrizione del sistema informativo del Fondo.

Sono attualmente utilizzate due distinte infrastrutture cloud, fornite da operatori diversi e collegate direttamente con gli uffici del Fondo tramite connessioni VPN, che dovranno essere migrate sulla nuova infrastruttura cloud dell’Affidataria:

- nella prima, caratterizzata da una virtualizzazione di tipo “*Virtual-Machine based*” ed implementata sul servizio “Private Cloud” di Aruba basato su VMware, sono implementati i principali applicativi in uso al Fondo (es. gestione contabilità, mail server, piattaforma documentale, etc) e sono pubblicate su Internet diverse web application sviluppate sia su piattaforma MS-Windows che su piattaforma LAMP; nella stessa area è, inoltre, pubblicato il sito web istituzionale del Fondo realizzato con il CMS Wordpress;
- nella seconda, caratterizzata da una virtualizzazione di tipo “*Container based*” ed implementata sul servizio OpenStack “O.Cloud” di Irideos, è in corso l’implementazione della nuova piattaforma di gestione degli Avvisi (NSI) ed i servizi di Business Intelligence ed Analytics. La stessa offre, tramite un servizio PaaS, l’accesso e la gestione ad un cluster DBMS (MySQL8.0).

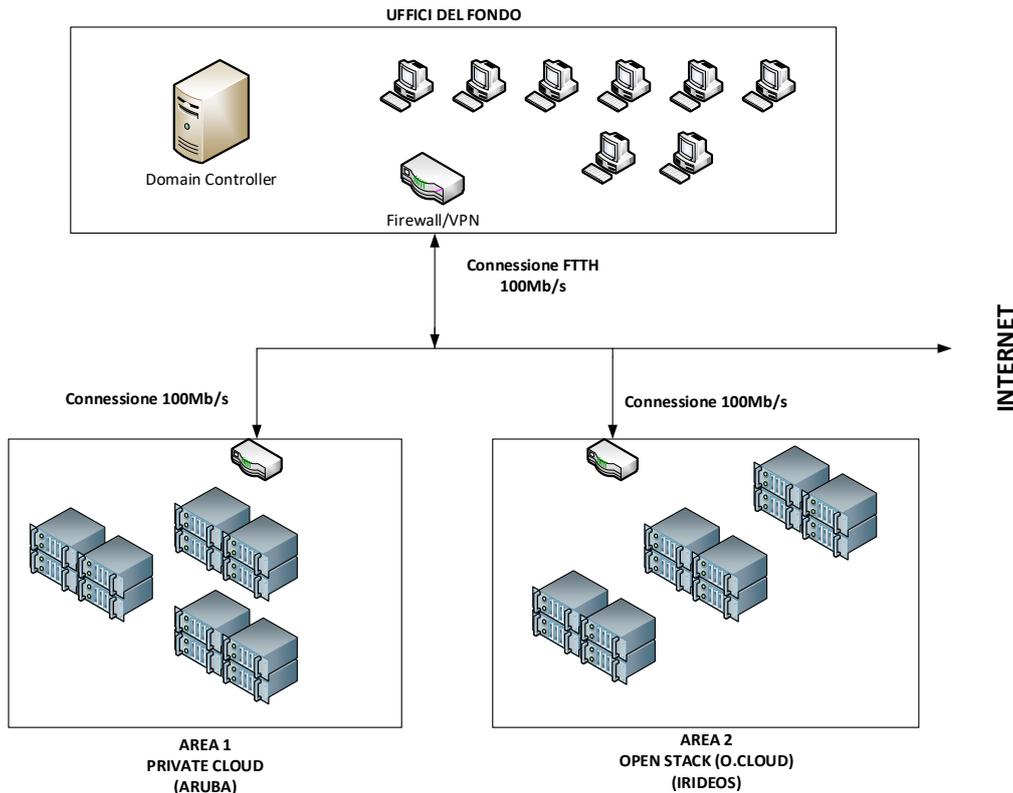


Figura 5.1

5.1. Area 1 [AS-IS] – “Private Cloud” Aruba

L’intera infrastruttura, realizzata con un servizio IaaS di cloud computing (“Private Cloud” fornito da Aruba S.p.A.), implementa un Virtual Data Center dimensionato con le seguenti caratteristiche:

- VM implementate 19;
- vCPU: 110;
- RAM: 175 GB;
- Spazio su disco: 5.415GB (SSD+SAS);
- Rete dedicata con 16 IP pubblici;
- Piattaforma di virtualizzazione: VMware vSphere 6.5 (hypervisor: ESXi 6.5).

La rete interna al VDC è suddivisa in due subnet: una in DMZ in cui sono pubblicate le applicazioni web accessibili da Internet ed una privata accessibile dagli uffici del Fondo. Il flusso di ingresso verso i web server collocati in DMZ è filtrato da un appliance virtuale (pfSense).

Il collegamento tra gli uffici del Fondo e l’infrastruttura cloud è realizzato con una linea VPN (tunnel IPsec in configurazione lan-to-lan e roadwarrior) implementata su una connessione in fibra ottica FTTH (punto-punto e dedicata), con una banda simmetrica garantita di 100 Mb/s.

Esistono altre configurazioni IPsec in modalità roadwarrior che permettono la connessione al VDC alle aziende e/o ai consulenti, che collaborano con il Fondo e che devono avere accesso ai server. Per ognuno di loro è stata predisposta una coppia di dati che rappresentano le credenziali di accesso alla rete privata.

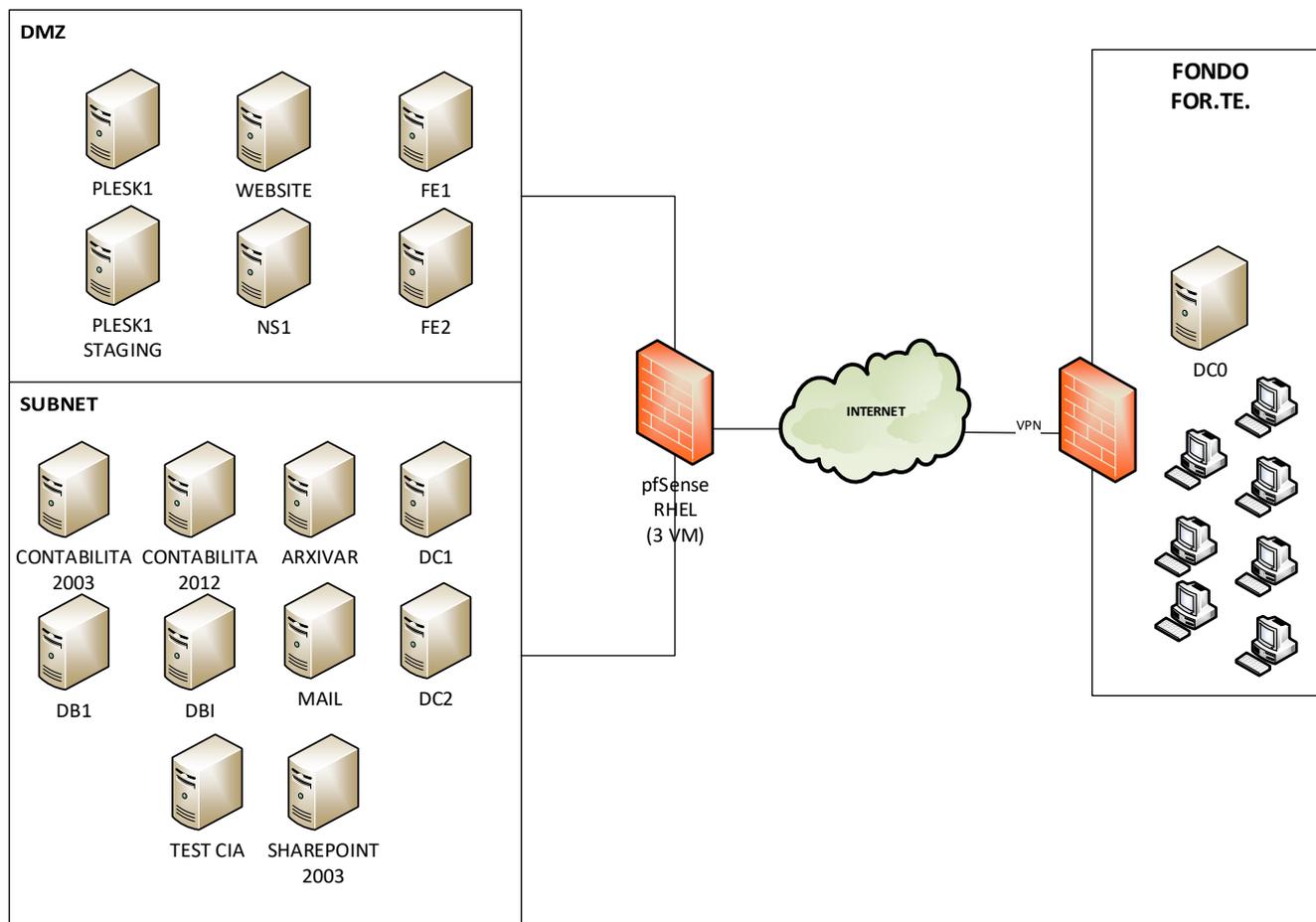


Figura 5.2

Di seguito, l'elenco delle VM implementate con le relative caratteristiche:

AREA 1 -AMBIENTE PRIMARIO

ID	Nome Server	Ambiente / Sistema Operativo	Ruolo	vCPU	RAM GB	NIC	Nm. dischi	Totale spazio disco (GB)	Incremento annuale	Disaster Recovery
1-A	Firewall	FreeBSD(64-bit)	Firewall	2	2	3	1	8		
1-B	Firewall-copy	FreeBSD(64-bit)	Firewall	2	2	3	1	8		
1-C	Check_MK	RHEL 7	Check-MK	2	2	1	1	40		
2	ARXIVAR	LAN - Windows 2012R2 Standard	Applicazione Documentale Arxivar	8	16	1	2	620	+70 GB/anno	S
3	CONTABILITA-2012	LAN - Windows 2012R2 Standard	Nuovo Server contabilità	4	8	1	3	270		S
4	CONTABILITA-	LAN - Windows	Applicazioni	4	8	1	3	270		

	2003	2003 Enterprise Edition	Contabilità							
5	DB1	DMZ - Windows 2012R2 Standard	Database server	8	16	1	2	800	+10 GB/anno	S
6	DBI	LAN - Windows 2012R2 Standard	Database server	4	8	1	3	340		
7	DC1	LAN - Windows 2012R2 Standard	Domain Controller	2	4	1	1	40		
8	DC2	LAN - Windows 2012R2 Standard	Domain Controller	2	4	1	1	40		
9	FE1	DMZ - Windows 2012R2 Standard	SERVIZI WEB SU IIS	8	16	1	1	40		
10	FE2	DMZ - Windows 2012R2 Standard	SERVIZI WEB SU IIS	8	16	1	1	40		
11	MAIL1	DMZ - CentOS	Server di posta	1	2	2	4	820	+120 GB/anno	S
12	NS1	DMZ - Windows 2012R2 Standard	Share folder dei web server	4	8	1	2	240		
13	PLESK1	DMZ - CentOS	Web server basato su plesk Linux	28	24	1	2	700		
14	PLESK1-STAGING	DMZ - CentOS	Web server di staging basato su plesk Linux	2	4	1	1	300		
15	TEST-CIA	LAN - Windows 2012R2 Standard	Test e staging CIA	2	8	1	2	190		
16	SHAREPOINT-2003	LAN - Windows 2003 Enterprise Edition	Vecchio SharePoint	1	3	1	3	390	+50 GB/anno	
17	LPIT1-FFTWEB01	CentOS	WEBSITE	18	24	1	5	59		S
				110	175	24		5.215		

(*) Indica se è richiesto il servizio di Disaster Recovery descritto al par. 6.4.2

Per i server, dove è stato possibile determinare un incremento, è stata indicata la proiezione annuale basata sui dati storici degli ultimi 5 anni.

L'incremento di spazio su disco per gli altri server, che non presentano particolari attività o interazioni con gli utenti, è da considerare trascurabile.

LICENZE COMMERCIALI

Nell'AREA 1 sono presenti VM basate su piattaforma MS Windows per le quali sono previste licenze commerciali del sistema operativo e del DBMS, MS Sql Server. Si precisa che il costo di tali licenze deve essere compreso nella fornitura:

- n. 10 VM (50 vCPU) con Windows Server 2012 R2 64 bit
- di cui n. 5 VM (26 vCPU) con Sql Server 2012 Web Edition

Pr quanto riguarda le VM con Windows Server 2003 e SharePoint, sono utilizzate licenze legacy di proprietà del Fondo.

SERVER DI POSTA

Il server di posta (MAIL1), raggiungibile con indirizzo IP pubblico, è su distribuzione Linux CentOS 6 ed utilizza un software opensource tra i quali:

- Dovecot, per i servizi POP3 ed IMAP4
- Postfix v. 2.6.6, per la gestione dell'invio delle email (SMTP)
- Roundcube, per la consultazione della posta utilizzando il web browser.
- PostfixAdmin, per la gestione degli account di posta.

Il numero di caselle mail gestite sul dominio "fondoforte.it" è pari a 389 di cui 70 attive, lo spazio di storage occupato è di 535 GB, pari al 69% del totale (820GB).

DOCUMENTALE E CONTABILITA'

La soluzione documentale utilizzata dal Fondo è Arxivar. Tale soluzione è implementata su piattaforma Windows su una VM dedicata (ARXIVAR), che gestisce integralmente le funzioni di repository dei file fisici, il DBMS (MS Sql Server) ed i servizi applicativi accessibili dai client, utilizzando diverse interfacce e canali di comunicazione (RPC, SOAP).

La soluzione di contabilità è GAMMA ENTERPRISE di Team System, anch'essa implementata su piattaforma Windows su una VM dedicata, che utilizza MS Sql Server come DBMS.

Sono due componenti fondamentali del sistema informativo, per le quali è previsto un incremento delle risorse dedicate, computazionali e di storage, per far fronte al crescente aumento della mole di dati gestita dal Fondo. Le due VM sono funzionalmente connesse con i componenti sviluppati in AREA 2, che costituiscono la nuova piattaforma NSI.

STORAGE E BACKUP

Lo spazio di storage allocato è erogato tramite SAN di ultima generazione che prevede due livelli di tier in SSD ed un terzo tier basato su dischi SAS ad alte prestazioni. L'intera infrastruttura cloud è sottoposta ad un backup quotidiano, con una retention di 7 giorni.

Nell'infrastruttura viene trasferito quotidianamente un backup differenziale di una macchina fisica presente negli uffici del Fondo, che funge da Domain Controller e File Server, contenente le cartelle con i dati degli utenti interni (dimensione complessiva di circa 600GB), che è soggetto, quindi, alla stessa retention-policy. Lo spazio complessivo di storage riservato è pari a 5.815 GB.

GESTIONE DOMINIO

Le macchine della rete interna del Fondo e le VM Windows presenti in AREA 1 sono gestite con 3 server di dominio (Windows Server 2012 R2 Standard):

- DC0, (master) macchina fisica ospitata presso gli uffici del Fondo: *DC-UFFICI.forte.it*
- DC1, VM implementate nel VDC: *DC1-forte.it*
- DC2, VM implementate nel VDC: *DC2-forte.it*

Di seguito, alcuni dettagli relativi alla configurazione.

Livello Funzionalità

<i>Domain functional level:</i>	Windows Server 2003
<i>Forest functional level:</i>	Windows Server 2003

Ruoli

<i>Schema master:</i>	DC-UFFICI.forte.it
<i>Domain naming master:</i>	DC-UFFICI.forte.it
<i>PDC:</i>	DC1..forte.it
<i>RID pool manager:</i>	DC1..forte.it
<i>Infrastructure master:</i>	DC1..forte.it

Workstation and User

AD Computer count:	70
AD User Count:	108

Macchine a dominio per S.O.

Windows Server 2003	10
Windows Server 2012 Standard	1
Windows Server 2012 R2 Standard	5
Windows 7 Ultimate	2
Windows 10 Pro	29
Windows 7 Professional	23

5.2. AREA 2 [AS-IS] – “O.CLOUD” Irideos

In quest'area, basata sulla soluzione OpenStack (O.Cloud) di Irideos, sono implementate le seguenti soluzioni:

- Nuova piattaforma per la gestione degli Avvisi (NIS)
- Piattaforma di Business Intelligence

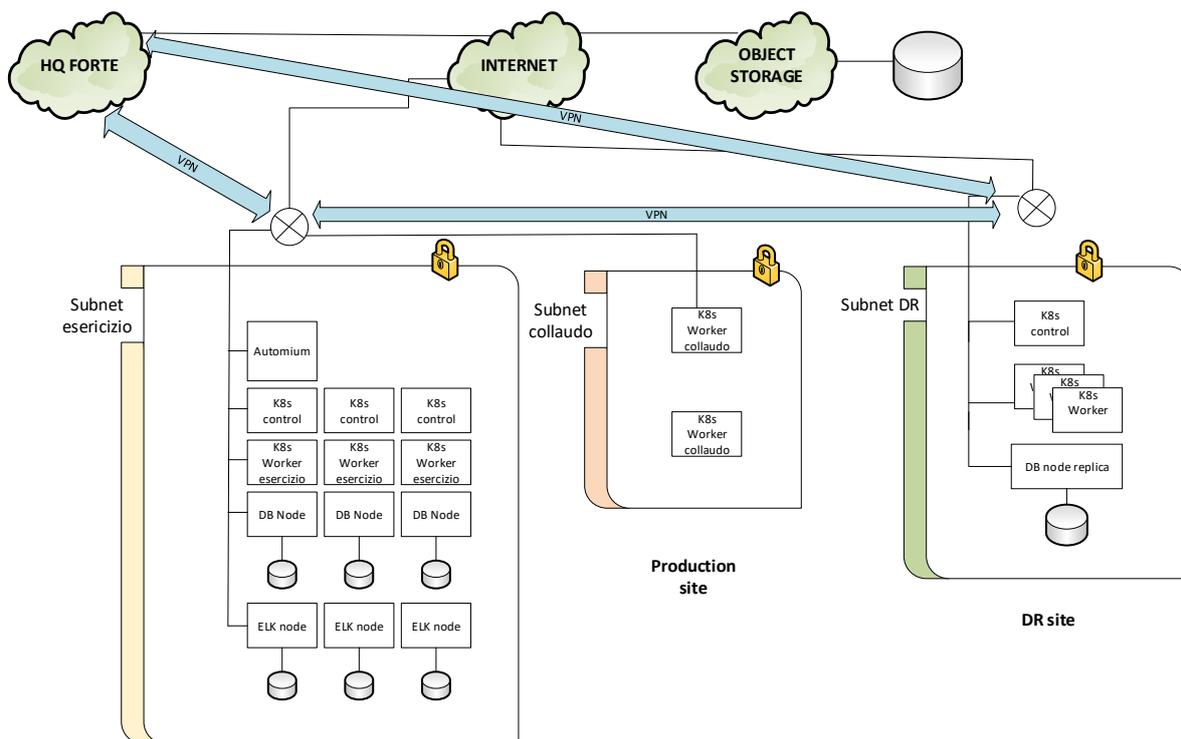


Figura 5.3

L'architettura è costituita da cluster Kubernetes (versione 1.15), con nodi dedicati alla parte di Control Plane ed engine secondari per il monitoraggio della telemetria e la gestione del cluster applicativo.

A supporto dei nodi di controllo, sono predisposti due "worker node pool", uno dedicato alla rete di produzione (esercizio) ed uno dedicato alla rete di staging (collaudo): questi pool sono gestiti indipendentemente l'uno dall'altro e scalati orizzontalmente in base alle esigenze, sia in modo manuale che in modo automatico (scalabilità elastica).

È possibile, quindi, flessibilmente aggiungere o rimuovere istanze delle singole componenti in maniera indipendente tra i due ambienti.

I dati stateful sono gestiti all'interno di un cluster database MySQL di 3 nodi con tecnologia di replica sincrona tramite la soluzione Percona XtraDB Cluster. È, inoltre, presente un cluster ELK (Elasticsearch, Logstash e Kibana) per la gestione centralizzata dei log applicativi e infrastrutturali.

Ulteriori risorse sono riservate a 4 VM dedicate all'implementazione di un sistema di Business Intelligence e relativa Data Warehouse.

I backup dell'intera infrastruttura sono conservati nel Cloud Storage della soluzione O.Cloud con almeno una replica su territorio europeo; i backup sono incrementali con una retention di 7 giorni.

L'architettura applicativa, implementata sull'infrastruttura appena descritta, realizzata con componenti organizzati in container Docker ed orchestrati tramite cluster Kubernetes, viene descritta con maggior dettaglio nel capitolo 6.2.

Di seguito, viene riportato il riepilogo delle risorse computazionali e di storage attualmente riservate a quest'area:

AREA 2 [AS-IS] - AMBIENTE PRIMARIO

Descrizione servizio	Q.tà VM	vCPU	RAM GB	Note
Monitoring-0	1	2	2	
Atomium (Automation Service OCloud)	1	4	8	
Kubernetes Control Plane	3	2	4	
Kubernetes Worker Esercizio	3	8	16	Solo applicativo
Kubernetes Worker Collaudo	2	8	16	Applicativo + DB
Node database (Cluster)	3	4	8	
Node Logging (Cluster)	3	2	4	
TOTALE	16	30	58	

Storage	Q.tà (GB)	Note
Block Storage TOP HDD	1.500	Ambiente DB (data base)
Block Storage TOP HDD	300	Logging
Object Storage	3.000	Backup dati + eventuale docker registry storage
TOTALE	4.800	

AREA 2 [AS-IS] - AMBIENTE DISASTER RECOVERY

Descrizione servizio	Q.tà VM	vCPU	RAM GB	Note
Node database	1	4	8	

Storage	Q.tà (GB)	Note
Block Storage TOP HDD	500	Replica DB (data base)

AREA 2 – [AS-IS] - AMBIENTE BI e DWH

Descrizione servizio	Q.tà VM	vCPU	RAM GB	Note
Ambiente BI	2	8	16	
Ambiente DWH	2	8	16	

Storage	Q.tà (GB)	Note
Block Storage TOP HDD	3.000	BI-DWH

Risorse complessive AREA 2 [AS-IS]

- VM implementate: 21
- vCPU: 50
- RAM: 98 GB
- Spazio disco: 8.300 GB

DISASTER RECOVERY

La soluzione prevede un servizio di Disaster Recovery dell'Ambiente Primario su un DC differente rispetto a quello di esercizio, localizzato in un'altra area geografica. I dati sono costantemente sincronizzati sui due differenti DC, permettendo l'attivazione automatica del secondo ambiente.

CONNETTIVITÀ

L'accesso ad Internet è garantito con una banda di 100Mb/s; è, inoltre, implementato un Tunnel VPN Ipsec tra DC primario e DC Disaster Recovery.

6. INFRASTRUTTURA CLOUD [TO-BE]

All'Affidataria è richiesto di importare integralmente il sistema informativo costituito dalle due aree cloud descritte nel precedente capitolo 5. Dove non diversamente indicato, vengono mantenuti, come requisiti richiesti, quelli degli attuali servizi e configurazioni.

Data la natura eterogenea delle soluzioni implementate nelle due aree, è richiesto uno strumento "multi-cloud" che implementi sia una virtualizzazione "Virtual-Machine Based" (per le VM definite in AREA 1 e parte di quelle definite in AREA 2) sia una virtualizzazione "Container Based", che fornisca i servizi di orchestrazione necessari al funzionamento dei componenti definiti in AREA 2.

Sono richiesti, inoltre, servizi erogati in modalità PaaS, tra cui lo stesso DBMS (MySQL 8.0) definito in AREA 2.

Devono essere garantite:

- l'applicazione delle best practices utili ad implementare una valida sicurezza perimetrale prevedendo, a protezione dell'intera infrastruttura, uno o più firewall;
- la prevenzione e la protezione da attacchi informatici od attacchi causati da virus (es. attacchi DoS, Ransomware...);
- le connessioni protette (VPN) con gli uffici del Fondo e con gli ambienti di Disaster Recovery che saranno implementati.

In vista dei futuri sviluppi della piattaforma NSI e del sistema informativo in generale, sarà richiesto un incremento delle risorse computazionali, secondo quanto di seguito indicato. Nello schema seguente, viene rappresentato il sistema informativo completo [TO-BE] in cui viene mostrata l'integrazione tra quello che, oggi, è implementato nelle due aree descritte precedentemente.

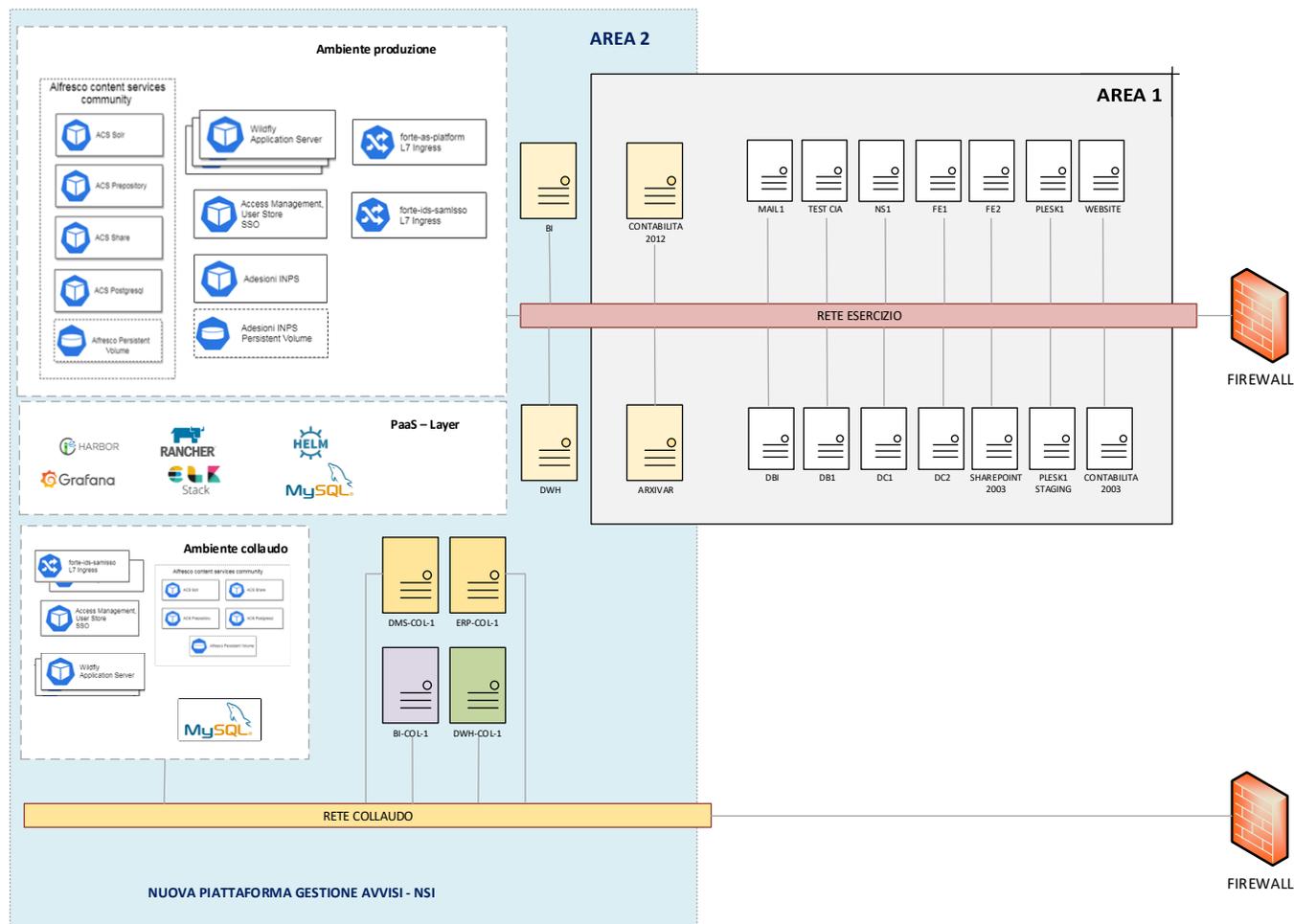


Figura 6.1

Si evidenzia l'esistenza di 2 reti distinte, una di esercizio ed una di collaudo. Sulla rete di esercizio sono connesse le VM definite in AREA 1, le VM e le implementazioni "Container Based", dedicate alla pubblicazione della nuova piattaforma NSI. Su entrambe le reti, è prevista la creazione di diverse subnet e la possibilità di definire specifiche policy di accesso. Per l'ambiente di produzione dell'AREA 2 collegato alla rete di esercizio, ad esclusione delle macchine dedicate alla BI (DWH-1 e BI-1), è richiesto un servizio di Disaster Recovery con i requisiti indicati al capitolo 6.4.2.

6.1. AREA 1 [TO-BE]

Con riferimento all'infrastruttura definita in AREA 1, è richiesto un incremento delle risorse computazionali utile ad ottimizzare le prestazioni ed aumentare lo storage delle VM a più intenso utilizzo (ARXIVAR, CONTABILITA, DB1, MAIL1, WEBSITE), precisamente:

- vCPU: 110 +10 → 120
- RAM: 175 GB + 25 GB → 200 GB
- Spazio disco: 5.815 GB (SSD+SAS) + 1.685 GB → 7.500 GB

Per le sopra elencate 5 VM dell'AREA 1 è richiesto un servizio di Disaster Recovery con i requisiti indicati al capitolo 6.4.2.

Come già descritto, in quest'area sono presenti VM basate su piattaforma MS Windows: si precisa che il costo delle licenze commerciali del sistema operativo e di Microsoft Sql Server deve essere compreso nella fornitura.

Dovrà, inoltre, essere prevista una replica delle VM ARXIVAR e CONTABILITA (entrambe su piattaforma Windows con istanze di MS Sql Server) destinate all'ambiente di collaudo (Tab. A2-2) della piattaforma NSI.

6.2. AREA 2 [TO-BE]

L'architettura è basata su Openstack e cluster Kubernetes: una volta importato il sistema [AS-IS] descritto al capitolo 5.2, la stessa sarà estesa, sviluppando ed integrando gli ambienti di collaudo ed esercizio, destinati alle piattaforme pubblicate in quest'area (NSI e la piattaforma di Business Intelligence). L'implementazione dei due ambienti di esercizio e di collaudo dovrà essere effettuata su cluster distinti e non connessi.

L'architettura applicativa di quest'area, rappresentata in fig.6.1, è prevalentemente realizzata con componenti organizzati in container Docker ed orchestrati tramite cluster Kubernetes. Ciò consente di:

- controllare e automatizzare i deployment e gli aggiornamenti;
- risparmiare ottimizzando le risorse infrastrutturali grazie all'utilizzo dell'hardware in modo più efficiente;
- orchestrare container su host multipli;
- risolvere problemi comuni dovuti alla proliferazione dei container organizzandoli in "pod";
- scalare in tempo reale risorse e applicazioni;
- testare e correggere automaticamente le applicazioni.

Lo strato superiore è composto dall'insieme dei container che costituiscono l'applicazione in esecuzione su pod Kubernetes:

- Forte-as - Application Server Wildfly: contiene le componenti da distribuire, forte-web (pacchetto WAR di frontend) e forte-services (pacchetto EAR di backend);
- Forte-ids - Access Management, User Store e Single-Sign On (il container dispiega un'istanza dell'Identity Server WSO2);
- Adesioni INPS – batch che gestisce i flussi dati proveniente dall'INPS (il container implementa una Java Virtual Machine ed un server FTP);
- Alfresco Content Service Community – è l'insieme delle componenti della suite documentale Alfresco, formata da 4 container e installata e configurata tramite gestore di pacchetti HELM.

Sono, inoltre, presenti le seguenti componenti nello strato PaaS:

- Harbor: docker private registry;
- Rancher: Kubernetes Management;
- Elk: cluster Elasticsearch+Logstash+Kibana per raccolta log e visualizzazione;
- Grafana: sistema di monitoraggio risorse e dashboard;
- Helm: packaging tool kubernetes (utilizzato per installare Alfresco e MySQL);
- MySQL DB: cluster MySQL 8.0 con gli schemi applicativi e dell'identity server.

Di seguito, l'elenco delle risorse richieste per i componenti e le VM indicate nei due ambienti:

AREA 2 – [TO-BE] - AMBIENTE ESERCIZIO (Tab. A2-1)

VM - CONTAINER NAME	RUOLO	ISTANZE / NODI / POD / SERVIZIO	SERVER	vCPU	RAM (GB)	DISCO (GB)	DISASTER RECOVERY (*)
Access Management	Identity Access Management	1 nodo	WSO2 Identity Server 5.6	2	4	20	S
Wildfly Application Server	Application Server JEE	3 nodi in cluster	RedHat Wildfly 16	12	48	60	S
Forte-as-platform Forte-ids-samlSso	Load Balancer + Reverse Proxy + HTTPS	2 ingressi diversi	Kubernetes Cluster (Servizio di bilanciamento erogato nativamente dalla piattaforma Kubernetes del Cloud Provider)	6	12	150	S

Alfresco	Documentale applicativo interno	4 pod diversi (1 istanza Alfresco)	Alfresco Community Edition 6.0.5	8	16	2000	S
Servizi PaaS	DB - Servizio di persistenza erogato come managed service	Previsti fino ad un massimo di 3 nodi	MySQL 8.0	12	24	2100	S
	Servizi di gestione			8	16	3000	S
VM-BI	Piattaforma Business Intelligence	-	Linux	8	16	50	N
VM-DWH	Data Warehouse	-	Linux	8	16	1400	N
				64	152	8.780	

(*) Indica se è richiesto il servizio di Disaster Recovery descritto al par. 6.4.2

AREA 2 – [TO-BE] - AMBIENTE COLLAUDO (Tab. A2-2)

VM - CONTAINER NAME	RUOLO	ISTANZE / NODI / POD / SERVIZIO	SERVER	vCPU	RAM (GB)	DISCO (GB)
Access Management	Identity Access Management	1 nodo	WSO2 Identity Server 5.6	1	2	20
Wildfly Application Server	Application Server JEE	2 nodi in cluster	RedHat Wildfly 16	4	16	50
Forte-as-platform Forte-ids-samlSso	Load Balancer + Reverse Proxy + HTTPS	2 ingressi diversi	Kubernetes Cluster (Servizio di bilanciamento erogato nativamente dalla piattaforma Kubernetes del Cloud Provider)	1	2	50
Alfresco	Documentale applicativo interno	4 pod diversi (1 istanza Alfresco)	Alfresco Community Edition 6.0.5	8	16	2000
DB	DBMS	2 pod	MySql 8.0	4	8	1400
VM-BI	Piattaforma Business Intelligence	1 VM	Linux	4	8	50
VM-DWH	Data Warehouse	1 VM	Linux	4	8	1400
ERP-COL-1 (*)	Contabilità	1 VM	Windows 2012.R2 Std + MS Sql Server	4	8	300
DMS-COL-1 (*)	Documentale	1 VM	Windows 2012.R2 Std + MS Sql Server	8	16	630
				38	84	5.900

(*) Come indicato al capitolo 6-1, le VM ERP-COL-1 e DMS-COL-1 sono repliche delle macchine descritte in AREA 1, rispettivamente il server per CONTABILITA e ARXIVAR, utilizzate per l'ambiente di collaudo della nuova piattaforma NSI.

Le risorse computazionali complessive massime che saranno richieste per l'AREA 2, quindi, sono:

AMBIENTE	vCPU	RAM	DISCO (GB)
ESERCIZIO	64	152	8.780
COLLAUDO	38	84	5.900
TOTALE AREA 2	102	236	14.680

6.3. Riepilogo risorse complessive richieste e requisiti

Le risorse computazionali complessive richieste per entrambe le aree, quindi, sono:

Riepilogo risorse (Tab. RT-1)

	AREA	Licenze commerciali	vCPU	RAM (GB)	STORAGE (GB)
AS-IS Risorse minime necessarie per la migrazione dell'attuale infrastruttura	AREA 1	10 VM (50 vCPU) con Windows Server 2012 di cui: 5 VM (26 vCPU) con Sql Server 2012 Web Edition	110	175	5.215
	AREA 2 (*)	Nessuna	50	98	8.300
	TOTALE [AS-IS]		160	273	14.115
TO-BE Risorse massime previste	AREA 1	10 VM con Windows Server 2012 di cui: 5 VM con Sql Server 2012 Web Edition	120	200	7.500
	AREA 2 (*)	Nessuna	102	236	14.680
	TOTALE [TO-BE]		222	436	22.180

L'infrastruttura cloud proposta dovrà assicurare, fin dall'inizio della fornitura, le risorse computazionali necessarie all'implementazione stimata con il dimensionamento massimo previsto (TOTALE [TO-BE]).

Di seguito, un elenco delle caratteristiche minime richieste all'infrastruttura cloud:

Caratteristiche infrastruttura

La piattaforma di virtualizzazione deve prevedere un sistema DRS (Distributed Resource Scheduling) che ridistribuisce dinamicamente i carichi di lavoro, al fine di massimizzare le prestazioni per le VM/Container a più intenso utilizzo. Di seguito, il dimensionamento richiesto:

Potenza computazionale complessiva garantita:	200 GHz
Numero di vCPU x Core:	<=3
Frequenza minima garantita alla singola vCPU:	>= 0.6 GHz
Velocità network interna (VM, SAN, ...):	>= 10 Gbit/s
Velocità network esterna (Internet):	>= 100 Mb/s
Numero indirizzi IP pubblici:	16
vCPU massime per singola VM:	>= 32
RAM assegnata alla singola VM:	esclusiva senza condivisione
RAM massima per singola VM:	>= 256 GB
Numero dischi massimo per VM:	>= 128
Dimensione massima disco per VM:	>= 1 TB
Numero massimo reti per VM:	>= 10
Unità componente storage:	MultiTier: Tier SSD SLC / Tier SAS

6.4. Requisiti non funzionali

6.4.1 - ALTA AFFIDABILITA'

L'uptime dell'infrastruttura fisica deve essere maggiore od uguale al 99,95% del tempo totale, calcolato in minuti su base annuale. Sarà considerata condizione di indisponibilità il verificarsi di almeno una delle seguenti condizioni:

- indisponibilità delle risorse di rete, sia pubbliche che private, alle VM o ai servizi PaaS;
- indisponibilità delle risorse computazionali alle VM o dei servizi PaaS;
- indisponibilità dello storage su cui sono istanziate le VM o utilizzato dalle VM;

6.4.2 - DISASTER RECOVERY

È richiesto un servizio di Disaster Recovery (DraaS), attivo sulle seguenti risorse connesse alla RETE IN ESERCIZIO:

- Parte dell'ambiente produzione NSI (Tab. A2-2) → vCPU:48 | RAM:120 GB | STG: 7.330 GB
- Parte delle VM definite in AREA 1
(ARXIVAR, CONTABILITA, MAIL1, DB1, WEBSITE) → vCPU:39 | RAM:66 GB | STG: 2.600 GB

Il servizio gestito dall'Affidataria deve consentire il ripristino dell'ambiente primario o di parte di questo (VM, Storage, Rete) da un Data Center, dislocato in un'area geografica differente. I requisiti richiesti sono:

- ridondanza su un DC localizzato in territorio europeo ad una distanza di almeno 200 Km da quello su cui è implementata l'infrastruttura primaria;
- ridondanza dell'infrastruttura di rete alla quale sono collegati gli host che ospitano le VM;
- passaggio del workload di produzione nel sito di disaster recovery (RTO) inferiore a 5 minuti;
- garanzia di un disallineamento (RPO) inferiore a 5 minuti;
- possibilità di monitorare il RPO;
- possibilità di creare snapshot.

6.4.3 – SCALABILITA' ELASTICA

È richiesta la disponibilità di una scalabilità sia orizzontale (scale out - aggiunta di istanze) che verticale (scale up - aggiunta di VM assegnando le risorse nei limiti di quelle massime dimensionate).

Soprattutto per la parte di infrastruttura, caratterizzata da una virtualizzazione "Container Based", è richiesta la possibilità di definire policy di autoscaling automatiche, capaci di incrementare le risorse allocate per fronteggiare eventuali picchi di utilizzo e garantire efficienza ed affidabilità delle applicazioni implementate in quest'area.

Tale funzionalità diventa maggiormente rilevante in corrispondenza di particolari eventi (Click Day), ripetibili più volte durante l'anno, durante i quali, per un periodo di tempo limitato, dell'ordine delle 12 - 24 hh, la parte di sistema dedicata alla NSI (AREA 2 – Esercizio) deve poter gestire numerose sessioni contemporanee (dell'ordine di 1.500 utenti).

6.4.4 - REPORT E MONITORAGGIO RISORSE

Deve essere resa disponibile un'area, accessibile via web, attraverso la quale visualizzare l'intera infrastruttura, le VM utilizzate e le relative risorse, l'utilizzo dello storage e delle risorse di rete. Nella stessa area è richiesto di ricevere notifiche relative a situazioni critiche, ad errori e/o eccessivo consumo delle risorse.

6.4.5 - BACKUP E RETENTION POLICY

È richiesto un backup quotidiano dell'intera infrastruttura cloud con una retention di almeno 7 giorni, prevedendo almeno una replica su una sede diversa in territorio europeo.

Deve essere, inoltre, previsto, in un'area di storage dell'ambiente cloud, un backup della macchina fisica presente negli uffici del Fondo (DC0), che funge da Domain Controller e File Server, contenente le cartelle con i dati degli utenti interni (dimensione complessiva di circa 600GB), che sarà soggetto, quindi, alla stessa retention-policy.

Le operazioni di backup quotidiano devono essere effettuate a partire dalle ore 20.00 e, comunque, al di fuori dell'orario di normale operatività degli uffici del Fondo (ore 9.00 – 18.00).

6.4.6 - PROTEZIONE DEI DATI E RISPETTO DEL REGOLAMENTO UE

L'infrastruttura proposta deve essere dotata degli strumenti ed apparati utili a garantire la sicurezza perimetrale, la prevenzione e la protezione da attacchi informatici od attacchi causati da virus. I servizi devono essere svolti nel rispetto del REGOLAMENTO (UE) 2016/679 e delle eventuali normative e/o regolamenti nazionali che dovessero essere emanati in materia di privacy e protezione dei dati.

7. SERVIZI DI GESTIONE E MANUTENZIONE

I servizi richiesti di gestione dell'infrastruttura consistono nella gestione ordinaria, manutenzione programmata ed esecuzione dei controlli periodici per verificare il permanere delle condizioni di alta affidabilità della infrastruttura, i livelli di performance e le possibili criticità di carico.

L'Affidataria dovrà eseguire tutti gli aggiornamenti software (minor e major release) delle diverse componenti architeturali (sistemi operativi, web server, application server, database, componenti network, ecc.), garantendo la compatibilità con gli applicativi.

Sono, inoltre, comprese nella gestione ordinaria le attività di patching e di migrazione alle nuove release dei prodotti, comprensive delle attività di test, degli aggiornamenti delle configurazioni applicative e degli adeguamenti dei programmi di interfaccia con gli altri sistemi. In caso di disservizio, l'Affidataria dovrà porre in essere tutti gli interventi correttivi sia a livello architeturale, sia a livello di configurazione sistemistica ed applicativa.

Sono, inoltre, incluse le attività di manutenzione straordinaria ed evolutiva e tutte le attività necessarie a supportare nuovi progetti applicativi ed infrastrutturali: l'Affidataria dovrà attivare processi di presa in carico e rilascio dei nuovi servizi (es. autenticazione tramite single sign on di una nuova applicazione) per verificarne il corretto funzionamento, i livelli di performance, la sicurezza e la compatibilità con l'architettura.

L'Affidataria dovrà farsi carico di tutti i costi di accesso (hardware, licenze software, servizi, connessioni dati, ecc.) e relativi aggiornamenti. Si ribadisce che i costi e gli oneri connessi alle attività di migrazione dei dati dall'attuale infrastruttura a quella oggetto della proposta, rimarranno ad esclusivo carico dell'Affidataria stessa.

7.1. Monitoraggio ed assistenza

È richiesto un servizio di monitoraggio e assistenza, 24 ore su 24 per 7 giorni su 7, dei servizi in produzione. Esso dovrà comprendere la gestione sistemistica ed il monitoraggio hardware e software di tutti i server. Eventuali guasti hardware o la mancata raggiungibilità dei server (ping IP, servizio http, servizio smtp etc.) comporteranno l'intervento proattivo del personale tecnico.

Il sistema di monitoraggio proposto dovrà effettuare il controllo di disponibilità dell'infrastruttura, la verifica puntuale e tracciata della disponibilità dei servizi e delle performance delle principali applicazioni indicate dal Fondo, attraverso simulazioni di accesso e di effettivo utilizzo lato utente. È, inoltre, richiesto il monitoraggio del sistema di firewalling, atto a rilevare eventi di intrusione e la conseguente tempestiva gestione degli eventuali incidenti di sicurezza.

L'Affidataria sarà tenuta a presentare trimestralmente una relazione sull'andamento dei servizi ed un registro delle operazioni svolte.

7.2. Servizi gestione e manutenzione infrastruttura

Di seguito, un elenco dei servizi minimi richiesti per la gestione dell'infrastruttura:

- gestione sistemistica comprensiva delle operazioni di ottimizzazione delle risorse e di configurazione della sicurezza nonché del monitoraggio delle prestazioni generali dei sistemi;
- gestione sistemistica ed amministrativa dei profili utente su posta documentali e Domain Controller;
- gestione degli ambienti virtualizzati;
- gestione del servizio di Disaster Recovery;
- gestione dei domini attivi e dei servizi ad essi correlati (es: DNS, spool, wins, proxy ecc.);
- gestione policy per l'accesso alle risorse (es. spazio disco condiviso, ecc.);
- gestione dei backup ridondato;
- installazione e disinstallazione di server;
- gestione completa dei sistemi antivirus, antispamming in linea con le politiche di sicurezza e di controllo definite dal Fondo;
- gestione completa del patch management;
- gestione degli ambienti database esistenti e futuri, comprese le operazioni di ottimizzazione delle risorse, la configurazione della sicurezza ed i permessi sugli oggetti dei database;
- gestione completa e monitoraggio delle Infrastrutture e Sistemi SAN e NAS;
- ottimizzazione degli ambienti database in funzione delle esigenze dei servizi applicativi e delle interfacce;
- monitoraggio delle prestazioni generali dei sistemi;
- monitoraggio delle prestazioni generali degli ambienti database;
- risoluzione di tutti i problemi di funzionalità e disponibilità degli ambienti server e database, ivi comprese le azioni correttive finalizzate a prevenire malfunzionamenti o disservizi;
- preparazione, esecuzione e controllo della produzione batch e delle schedulazioni;
- garantire l'adozione delle adeguate misure di sicurezza logica ovvero sicurezza dei dati, programmi e procedure dal rischio di perdita, alterazione o distruzione o dall'accesso non autorizzato da parte di terzi ai dati di proprietà del Fondo;
- gestione fisica dei file di dati e delle librerie (protezione, recupero, riorganizzazione, gestione spazio, ottimizzazione, etc.);
- interazione con il Fondo al fine di verificare l'impatto delle caratteristiche dell'hardware e del software di sistema sulle sue applicazioni;
- aggiornamenti periodici delle release del software in uso e dei sottosistemi, anche nel caso di prodotti software di proprietà del Fondo;

- supporto consulenziale per attività di progetto ed evoluzione dei servizi;
- tutte le attività sistemistiche necessarie ad implementare nuovi progetti applicativi ed infrastrutturali, nonché l'evoluzione dei vari servizi e dei sistemi;
- gestione dei Log dell'ambiente al fine di individuare eventuali anomalie determinate da errori e/o accessi non autorizzati.

7.3. Servizi di manutenzione e gestione ordinaria dell'ambiente applicativo

Posta elettronica/antispamming

Il Fondo mette a disposizione dei propri utenti un servizio di posta elettronica con un server di posta, implementato nell'attuale su una specifica VM (MAIL1), al quale è abbinato il sistema di antispamming.

L'Affidataria, oltre alle disponibilità degli ambienti, così come previsto dai livelli di servizio, dovrà garantire l'esecuzione di tutte le attività di normale gestione legate alla creazione e manutenzione delle caselle di posta (ad es: attività di creazione, eliminazione, modifica delle cassette postali, gestione delle liste di distribuzione, ecc.); inoltre, in accordo con il Fondo, l'Affidataria dovrà gestire le policy relative all'ambiente antispamming.

Microsoft Active Directory

Il Fondo ha implementato il sistema di Microsoft Active Directory, attraverso il quale esegue la gestione e la verifica delle credenziali di accesso, nel rispetto della normativa e l'assegnazione dei profili autorizzativi in base alle diverse tipologie di utenti, rispetto al ruolo all'interno dell'organizzazione aziendale.

L'Affidataria, attraverso la gestione delle infrastrutture descritte nei capitoli precedenti, dovrà garantire la corretta configurazione ed ottimizzazione dell'intera architettura applicativa, la diagnostica delle performance e la verifica delle componenti applicative; dovrà, inoltre, garantire il funzionamento del servizio di autenticazione e di provisioning delle identità.

Servizio Antivirus

Nell'esecuzione di tutti i servizi descritti nel presente documento, l'Affidataria dovrà porre la massima attenzione alle problematiche di sicurezza degli ambienti e degli utenti. In particolare, dovrà farsi carico, per tutta la durata del Contratto, di installare e gestire un sistema antivirus per garantire la protezione dei server e delle postazioni di lavoro. A titolo esemplificativo, si segnalano le seguenti attività:

- garantire la disponibilità dell'ambiente antivirus;
- garantire l'aggiornamento delle impronte virali, motori di scansione e programmi come da specifiche del Fornitore del prodotto (anche per i singoli client);
- intervenire tempestivamente in caso di diffusione di virus con lo scopo di ripristinare la normale funzionalità di tutto l'ambiente;
- eseguire l'aggiornamento delle release di prodotto.

Nel caso in cui l'ambiente antivirus installato non sia in grado di intercettare/bloccare una specifica infezione virale dovranno essere, comunque, messe in atto tempestivamente procedure alternative per limitarne la diffusione e garantire, comunque, un'operatività seppur limitata.

7.4 Riservatezza e Protezione dei dati

L’Affidataria dovrà, senza alcun aggravio di costi, garantire al Fondo il rispetto dei medesimi livelli di protezione dei dati da parte dei soggetti coinvolti nell'erogazione dei servizi ed, in particolare, dovrà:

- assicurare la riservatezza dei dati personali di cui il Fondo è titolare ed il loro trattamento nel rispetto delle normative in materia di protezione dei dati personali, applicabili relativamente ad ogni territorio nel quale vengano localizzati i servizi;
- assicurare che i backup effettuati non vengano eliminati, ma che siano conservati per tutta la durata del servizio e restituiti al Fondo alla scadenza contrattuale;
- garantire il rispetto di adeguate misure di sicurezza volte alla protezione dei dati personali, nel rispetto della normativa di riferimento (Reg. UE 2016/679 – GDPR in primis), prestando, in particolar modo, adeguate garanzie in merito alla distruzione, alla perdita ed alla prevenzione di accessi non autorizzati ai dati del Fondo da parte di terzi, prevedendo idonee procedure di notificazione al Fondo da parte dei soggetti coinvolti nell'erogazione dei servizi, in caso di accesso abusivo, sottrazione e perdita dei dati, così come per qualsiasi richiesta giuridicamente vincolante presentata da autorità giudiziarie e/o di polizia, ai fini della comunicazione dei dati personali;
- garantire che i soggetti coinvolti nell'erogazione dei servizi accettino la nomina a "responsabile esterno del trattamento", ottemperino alle istruzioni ivi previste dal Fondo e rispondano prontamente ed adeguatamente a tutte le richieste relative al trattamento dei dati personali;
- garantire l’adempimento delle disposizioni in materia di amministrazione di sistema da parte dei soggetti coinvolti nell'erogazione dei servizi, ove applicabili;
- garantire al Fondo la possibilità di effettuare adeguate procedure di audit e svolgere per conto dello stesso le medesime procedure di controllo nei confronti dei soggetti coinvolti nell'erogazione dei servizi;
- assicurare un livello adeguato di formazione del personale chiamato ad interagire o, comunque, coinvolto nei processi di erogazione dei servizi.

L’Affidataria risponderà verso il Fondo anche per la violazione degli obblighi relativi al trattamento dei dati personali ad opera dei soggetti terzi coinvolti nell'erogazione dei servizi e dovrà tenere indenne il Fondo da qualsiasi sanzione e/o danno ad esso provocato per effetto del trattamento di dati personali eseguito dall’Affidataria stessa o dai soggetti terzi da essa coinvolti nell'erogazione dei servizi, ivi inclusi, a titolo esemplificativo: danni arrecati al Fondo, e/o a soggetti terzi e/o agli interessati al trattamento dei dati personali di cui il Fondo è titolare e per i quali sia tenuto a rispondere, per trattamento illegittimo, sottrazione e/o perdita dei dati personali medesimi, per ordini di cessazione del trattamento e/o adozione di misure da parte delle autorità competenti.

7.5 Presa in carico e migrazione dell'infrastruttura

A partire dalla data di stipula del Contratto Esecutivo, l'Affidataria dovrà predisporre una procedura, condivisa ed approvata dai Referenti Tecnici del Fondo, per la presa in carico e migrazione dei servizi attualmente erogati.

Le relative attività svolte da personale esperto, che non costituiranno alcun onere aggiuntivo per il Fondo, potranno consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. elenco degli asset informatici, catalogo dei sistemi e delle applicazioni, documentazione relativa agli sviluppi in corso, etc.) fornita dal Fornitore uscente, affiancamento al Fornitore uscente nell'operatività quotidiana condotta.

Le suddette attività dovranno essere descritte in modo dettagliato in un verbale attestante il completamento del passaggio di consegne.

Tutti gli interventi eseguiti sulle piattaforme in esercizio, che potrebbero compromettere il normale utilizzo dei servizi, dovranno obbligatoriamente essere effettuati al di fuori dell'orario di lavoro del personale del Fondo e, comunque, in intervalli orari definiti dal Fondo, coerentemente con le proprie esigenze di operatività.

Pur nel rispetto della continuità del servizio, l'Affidataria deve consentire il massimo parallelismo delle attività al fine di minimizzare i tempi di attivazione. Il processo deve prevedere, ove applicabile, una fase di "parallelo operativo" che garantisca, in una determinata finestra temporale, la coesistenza dei servizi erogati dagli attuali Fornitori.

Il parallelo operativo deve essere tenuto attivo per il tempo necessario a completare le attività di migrazione e verificare la corretta operatività dei nuovi servizi. Il pagamento dei corrispettivi per la fornitura dei servizi oggetto di migrazione decorrerà dalla data di collaudo positivo (verbale di collaudo) dei servizi ovvero dalla data di accettazione da parte del Fondo.

Si precisa che le operazioni di migrazione dell'attuale infrastruttura nella nuova dovranno concludersi entro 14 (quattordici) giorni solari a partire dalla data di stipula del Contratto.

7.6 Rilascio al termine del servizio

Il Rilascio al termine del servizio comprende tutte le attività necessarie per trasmettere al personale del Fondo (o al personale di altro Fornitore subentrante) le informazioni acquisite nel corso dell'esecuzione dei servizi, nonché quant'altro, anche a livello documentale, risulti necessario per garantire la regolare prosecuzione dei servizi. L'Affidataria si impegna a prestare il massimo supporto e collaborazione per consentire al Fondo e/o a terzi di subentrare alla stessa nell'erogazione dei servizi.

Tutte le attività che saranno svolte in questa fase non dovranno in alcun modo gravare sull'operatività delle risorse umane e tecnologiche impiegate, né sui livelli di servizio. Inoltre, tale fase non comporterà ulteriori oneri economici per il Fondo.

Al rilascio o transizione in uscita devono essere garantite le seguenti attività, da considerarsi come requisiti minimi:

- "passaggio di consegne" in caso di servizi on premise e servizi as a service;

- “consegna dei dati”, negli altri casi (es. consegna dell'immagine delle macchine virtuali, configurazione degli ambienti di virtualizzazione, backup dei database);
- “consegna della documentazione tecnica” completa ed aggiornata allo stato dell'arte dei servizi.

L'Affidataria dovrà garantire, al personale del Fondo e/o a terzi da esso designati, un periodo di supporto alla transizione, almeno pari ad **un mese**, al fine di consentire il trasferimento del know-how sulle attività condotte e rendere l'eventuale prosecuzione delle attività quanto più efficace possibile.

Al fine di facilitare il trasferimento del know-how, **2 mesi** prima della scadenza contrattuale, l'Affidataria dovrà predisporre il Piano di Trasferimento, articolato in attività con l'indicazione di scadenze di inizio e fine, di responsabilità, di contenuti e risultati tali da rendere controllabile l'effettivo svolgimento del trasferimento di know-how; il piano, che dovrà essere formalizzato nei tempi richiesti dal Fondo, dovrà essere prodotto dall'Affidataria (operatore uscente) e condiviso con il nuovo Operatore Economico individuato dal Fondo (nuovo operatore entrante) e mantenuto aggiornato per tutto il periodo di vigenza contrattuale.

In particolare, la transizione in uscita dovrà avere durata massima pari ad **un mese** e svolgersi, indicativamente, nell'ultimo mese antecedente la scadenza del Contratto Esecutivo.

8. SERVIZIO DI HELP-DESK

È richiesto un servizio di Help Desk e di assistenza sistemistica su tutto il sistema messo a disposizione strutturato su due livelli:

- Help Desk di primo livello;
- Help Desk di secondo livello.

Il servizio dovrà essere disponibile H24, 7 giorni su 7.

L'Affidataria dovrà implementare un sistema di Trouble Ticketing, riservando specifiche credenziali di accesso al personale del Fondo, destinato a ricevere le richieste di assistenza e le segnalazioni di eventuali problematiche inerenti ai servizi offerti.

8.1 Help-Desk di primo livello

L'HD di primo livello è responsabile della ricezione della segnalazione (che, oltre al suddetto sistema di Trouble Ticketing, potrà essere inoltrata anche via mail o telefono), della registrazione, classificazione ed inoltro delle richieste di intervento provenienti dal Fondo e/o dalle segnalazioni dai sistemi di monitoraggio; svolgerà, nell'arco temporale di un'ora dalla segnalazione, con le opportune competenze, le seguenti funzioni (a titolo indicativo e non esaustivo):

- risposta ad eventuali richieste di informazioni tecniche di base sul servizio;
- prima analisi e risoluzione delle problematiche più semplici;
- controllo dello stato di avanzamento dei ticket, la relativa chiusura e la comunicazione al Fondo.

Il personale dell'HD di primo livello gestirà i contatti, fornirà le informazioni richieste, prenderà in carico segnalazioni di problematiche e deciderà l'eventuale inoltro all'HD di secondo livello, qualora non possa intervenire direttamente.

Nel caso di risoluzione delle problematiche direttamente da parte del primo livello di assistenza, questo provvederà ad aggiornare il ticket con le informazioni sul contatto ed a chiuderlo.

Le funzioni richieste all'HD di primo livello sono:

- creazione e Presa in carico delle richieste;
- analisi della richiesta;
- gestione di Incident e Request;
- eventuale riclassificazione delle richieste (in caso di erronea classificazione);
- eventuali approfondimenti con l'utente Finale che ha generato la richiesta;
- individuazione della soluzione definitiva o di un workaround;
- innesco delle procedure di escalation (nel caso di impossibilità a chiudere la richiesta);
- tracciatura della richiesta;
- inoltro della Risposta/Soluzione per la chiusura del Ticket (Resolved).

Oltre all'attività di supporto all'utente finale, l'HD di primo livello si occupa anche di:

- monitoraggio H24;
- gestione degli allarmi, qualificazione e, in caso di escalation, creazione del Ticket con assegnazione al gruppo competente di 2° livello;
- attivare i reperibili per i problemi critici ed urgenti durante la notte, nei fine settimana e nei festivi.

8.2 Help desk di secondo livello

L'attività di supporto di 2° Livello viene erogata dagli specialisti ai quali il l'HD di primo livello inoltra gli Incident ed i Problem che non hanno trovato una soluzione.

Le funzioni e garanzie richieste all'Help Desk di secondo livello sono:

- garantire il livello di servizio concordato;
- gestire i processi di Incident e Problem Management sino alla definitiva soluzione;
- gestire le attività di ripristino dell'infrastruttura del Fondo;
- analizzare, pianificare e realizzare i Change autorizzati;
- disporre di risorse con skill specialistici per ambito tecnologico;
- condurre e amministrare l'infrastruttura fornita;

- effettuare la revisione periodica del Capacity Planning per le varie risorse infrastrutturali e, in caso di necessità gestire il deploy delle migliorie d'applicare;
- garantire la System Administration degli apparati di rete e dei sistemi;
- garantire il Servizio di Reperibilità;
- effettuare le attività di Change dopo averle pianificate e concordate con il Fondo.