Priamo
FONDO PENSIONE COMPLEMENTARE A CAPITALIZZAZIONE PER I LAVORATORI ADDETTI AI SERVIZI DI TRASPORTO PUBBLICO E PER I LAVORATORI DEI SETTORI AFFINI

Allegato 1

Descrizione servizi

Il servizio prevede l'erogazione dei Vostri sistemi dalla nostra infrastruttura Cloud in replica comprensivo di gestione e supporto dei vari sistemi. Inoltre, il servizio include anche gestione e manutenzione dei server e client dislocati presso le vostre sedi.

Risorse Cloud dedicate

All'interno della nostra infrastruttura cloud verranno dedicate le seguenti risorse atte ad ospitare i vostri servizi all'interno di una VLAN dedicata e protetta da firewall anch'esso dedicato

Q.tà	Descrizione
21	1 vCPU Intel Xeon
62	1 Gb RAM
24	100 GB Storage alte prestazioni
1	Connettività 500Mbps
8	IP pubblici

Su questa struttura verranno erogati i seguenti server

- Firewall
- Domain Controller (*)
- Server Exchange (**)
- Server Reverse Proxy
- Server Web
- Next Cloud
- Sistema SIEM Wazuh
- Server Presenze
- server OCS-NG per tracciamento Hardware

Tutti i sistemi girano su ambienti ridondati multinodo al fine di garantire la massima affidabilità, su sistemi di virtualizzazione VmWare.

I nostri server sono ospitati nella webfarm Wind di via di Tor Cervara, Roma e replicabili nella webfarm Aruba Gobetti.

L'infrastruttura è connessa con la sede del Fondo per mezzo di una connessione VPN di tipo LAN-to-LAN in grado di garantire la sicurezza del canale trasmissivo pubblico (Internet) tramite avanzati sistemi di crittografia. In questo modo non sarà necessario sostenere costi aggiuntivi per la creazione di un collegamento punto-punto fisico.

Sarà reso disponibile l'accesso ai dati anche ai Client Remoti, che dovranno utilizzare un sistema di connessione VPN di tipo "Road Warrior". La connessione instaurerà un canale trasmissivo sicuro tra il client e l'infrastruttura server utilizzando un sistema di crittografia a due fattori, in cui l'accesso al servizio richiederà quindi il possesso di un certificato creato appositamente e una password. I client che accederanno da remoto potranno non essere in dominio, e potranno essere preventivamente configurati per facilitare le operazioni di connessione al servizio.

(*) Le licenze dei sistemi Microsoft Windows, Exchange e relative CAL sono già proprietà del Fondo.
(**) Le licenze dei sistemi Microsoft Windows, Exchange e relative CAL sono già proprietà del Fondo, il sistema è in fase di migrazione a Microsoft 365.

Backup dei sistemi cloud

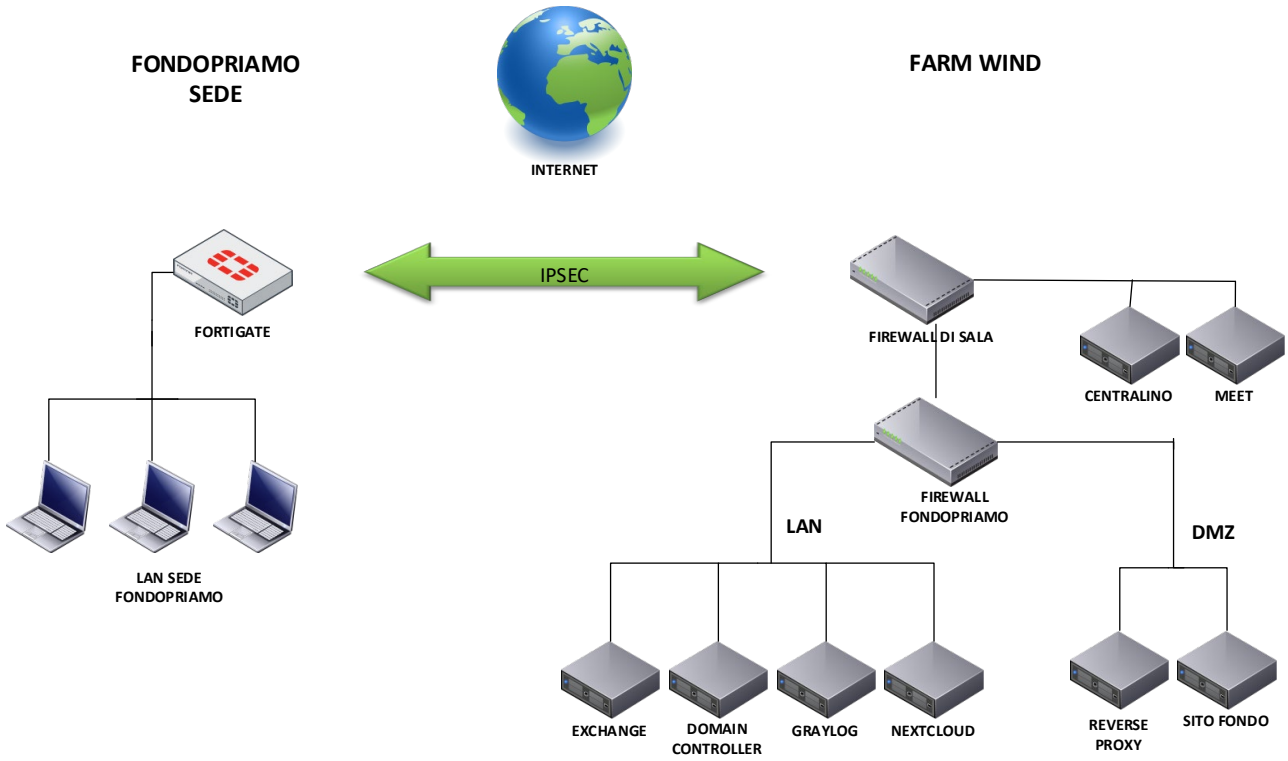
Tutti i sistemi sono posti sotto backup giornaliero con retention di 30 giorni. Il sistema di backup effettuerà una copia dell'intero server e dei suoi componenti permettendo poi il ripristino capillare dei suoi dati come ad esempio una singola e-mail.
Sono previsti, durante l'arco dell'anno, almeno due test di ripristino dei dati.

Replica dei sistemi cloud

Tutti i sistemi sono posti sotto replica giornaliera nella web farm di Arezzo, sempre su infrastruttura Cloud di proprietà della società di IT.
Le due farm sono interconnesse tra di loro mediante connessione VPN LAN-to-LAN.
Durante l'anno è previsto un test di DR, comprensivo di verifica del funzionamento. Il test consiste nell'accensione dei sistemi in replica in un ambiente isolato. Tali sistemi verranno mantenuti attivi per tutti il tempo necessario e verranno distrutti a fine verifica.

Durante il test il personale del Fondo sarà messo in condizione di effettuare i vari test tra cui:

- login con le credenziali di domino (*verifica del dialogo con AD*)
- verifica della raggiungibilità dei documenti condivisi (*verifica del servizio di file sharing*)
- verifica della presenza delle e-mail sulla casella personale (*verifica del servizio di posta elettronica*)
- verifica della raggiungibilità della copia privata di cui sopra del sito web del fondo


FONDOPRIAMO
SEDE
INTERNET
FARM WIND
FORTIGATE
IPSEC
FIREWALL DI SALA
CENTRALINO
MEET
FIREWALL
FONDOPRIAMO
LAN
DMZ
LAN SEDE
FONDOPRIAMO
EXCHANGE
DOMAIN
CONTROLLER
GRAYLOG
NEXTCLOUD
REVERSE
PROXY
SITO FONDO

Sistema Antispam LIBRA ESVA E-mail Security

Verrà fornito in modalità SAAS, il servizio antispam LIBRA ESVA E-mail Security.

L'Email Security Virtual Appliance di LibraEsva è un sistema di difesa proattiva contro phishing, 0-day malware, impersonificazione, spoofing e altri attacchi. È la soluzione italiana nominata da Virus Bulletin come la miglior soluzione al mondo di sicurezza per e-mail. Rileva il 99,96% dello spam e azzera il numero dei falsi positivi.

Le caratteristiche principale del servizio sono

- Fino a 3 motori di scansione antivirus
- 14 livelli di analisi e protezione Sandbox
- UrlSand protection
- Protezione e-mail in uscita
- QuickSand protection e filtraggio degli allegati
- Rilevazione multilivello di spam e minacce e-mail
- Alta Affidabilità in setup distribuito
- Modulo di gestione delle quote SMTP
- Immediatezza dei dettagli su mail ricevute e inviate
- Protezione da Phishing, Malware e Whaling
- Threats Analysis Portal

Ogni utente avrà la possibilità di segnalare e-mail come spam o come valide in completa autonomia, seguendo i link posti in calce ad ogni e-mail.

Il costo del servizio è calcolato a casella

Assistenza sistemistica e monitoraggio

Tutti i sistemi sono posti sotto monitoraggio h24 con generazione di alert in caso di anomalie.

È inoltre previsto supporto ai sistemi dove nello specifico le attività erogate saranno le seguenti:

- analisi giornaliera dei dati di monitoraggio del Software di base, nei diversi ambienti, con finalità predittiva rispetto a situazioni di possibile instabilità/blocco di sistema, e rispetto dei tempi di risposta del sistema (costanza delle prestazioni nel tempo);
- analisi giornaliera dei dati di monitoraggio del backup dei server virtuali
- analisi giornaliera dei dati fornitici dalla piattaforma di monitoraggio
- intervento a seguito di malfunzionamento e successivo ripristino di una o più delle unità hardware facenti parte del sistema;
- aggiornamento periodico del sistema operativo, delle librerie e dei componenti.

Analisi log, vulnerabilità e notifica al Fondo pensione Priamo

All’interno dell’ambiente cloud è installato un sistema SIEM completo e dedicato. Un sistema SIEM (Security Information and Event Management) è una soluzione software utilizzata per raccogliere, analizzare e monitorare in tempo reale i dati di sicurezza di un'azienda. I sistemi SIEM raccolgono informazioni da diversi dispositivi di sicurezza, come firewall, IDS/IPS e sistemi di autenticazione, e le utilizzano per generare report e avvisi in caso di minacce potenziali o violazioni di sicurezza.
I vantaggi di un sistema SIEM includono:

- Monitoraggio in tempo reale dei sistemi
- Rilevamento e risposta alle minacce in corso
- Analisi dei log per individuare attività sospette
- Generazione di report di sicurezza per la conformità normativa.
- Aiuta a identificare le vulnerabilità e i punti deboli del sistema.
- Rilevamento modifiche al sistema, come installazione software o modifiche chiavi di registro

Sono posti sotto monitoraggio tutti i server e, se richiesto, anche i client del fondo.
La nostra attività prevede l’analisi dei log e delle vulnerabilità rilevate e la notifica al fondo nel caso venga evidenziata una vulnerabilità potenzialmente pericolosa o in caso di anomalie sui log.

Antivirus BitDefender

Il sistema antivirus Bit Defender fornisce una piattaforma Cluod che permette ad i client connessi di aggiornare ed essere protetti anche fuori dalla sede di lavoro. Questa soluzione garantisce un’ottima copertura di difesa anche durante lo Smart Working.

Il Supporto e SLA

Le attività di supporto e gli SLA saranno svolti secondo le tabelle di seguito riportate:

Servizio attivo nei giorni feriali dalle 09.00 alle 18.00 (lunedì-venerdì).	
Altissima urgenza	Situazione di fermo sistema. Il sistema è completamente fermo, o non riesce a eseguire la normale operatività, e comunque l'operatività (o lo svolgimento di azioni mission critical) è severamente impattata dal problema e il lavoro non può essere portato avanti. Non ci sono modi di aggirare il problema.
Media urgenza	Funzionamento limitato del sistema. Il sistema può essere utilizzato esclusivamente con limitazioni, funzioni in parte disponibili. Il sistema in produzione è soggetto a periodiche interruzioni di servizio ed è da considerarsi instabile anche dopo un riavvio dei servizi.
Bassa urgenza	Per problematiche che non causano l'inoperatività del software/unità o la inaccessibilità e la mancata funzionalità del sistema. Per richieste di Change.

Livelli di servizio	SLA
Tempo di risposta per gli interventi	• entro al max 2 ore lavorative per i casi di Altissima urgenza; • entro al max 8 ore lavorative per i casi di Media urgenza;
Tempo di risposta convocazione al team di risposta incidenti ICT	• entro al max 12 ore dalla convocazione da parte del Fondo*.

* Qualora il termine cada in un giorno non lavorativo, esso si intende automaticamente posticipato al primo giorno lavorativo successivo, comunque entro e non oltre le ore 10, senza che ciò costituisca inadempimento.

La risoluzione dei problemi nell'80% delle segnalazioni di intervento viene svolta entro 8 ore lavorative, il restante 20% entro 2 giorni lavorativi.
In ogni caso, Società IT notificherà entro 1 giorno lavorativo qualsiasi sviluppo che possa avere un impatto significativo sulla capacità di prestare i servizi oggetto del presente Contratto.
In caso di evento informatico rilevante, Società IT informa senza indebito ritardo il Fondo e fornisce tempestivamente le informazioni necessarie in tempo utile a consentire al Fondo di rispettare i termini e i contenuti di notifica previsti dalla normativa applicabile, inclusi quelli di cui all'art. 5 del Reg. (UE) 2025/301 e ai relativi modelli/procedure stabiliti dal Reg. (UE) 2025/302. Società IT mantiene aggiornato il Fondo fino alla risoluzione e collabora alla predisposizione della documentazione verso l'Autorità.
Per problematiche non standard (criticità delle connessioni, danno grave alla Farm, etc.) sarà necessaria una analisi ad hoc e verrà comunicato il tempo di risoluzione.
Per problematiche extra orario lavorativo si procederà secondo lo schema riportato sotto la valutazione economica, in modalità Best Effort. Lo SLA sarà quindi concordato nella fase di presa in carico.

Adempimenti Normativi

Il Fondo per sua natura è obbligato ad aderire alla normativa del Regolamento (UE) 2022/2554 ("DORA"), piano di adeguamento normativo ad oggi in corso.