GARA PER L'AFFIDAMENTO DEL SERVIZIO DI SVILUPPO, GESTIONE E MANUTENZIONE DEL SISTEMA INFORMATICO E DELLE LINEE DATI DI EUREGIO PLUS SGR S.P.A. - AOV/SUA-SF 02/2021 - CODICE CIG 8950213D68

CAPITOLATO TECNICO

Indice

1. Contesto organizzativo

1.1 Introduzione

Euregio Plus SGR S.p.A./A.G. (di seguito la “SGR”, la “Stazione appaltante” o la “SA”) è una società di gestione del risparmio controllata da Pensplan Centrum S.p.A. ed operante come società in-house della Regione Trentino-Alto Adige e della Provincia Autonoma di Bolzano. Opera nel comparto finanziario, nella gestione dei fondi pensione, nel settore immobiliare, nel private debts, nel private equity e nel venture capital. La SA ha sede legale e principale a Bolzano in via della Mostra 11/13 ed una secondaria a Trento in via Romano Guardini 17.

1.2 Contesto normativo

La SA è sottoposta alla vigilanza di Banca d’Italia, Consob e Covip e ricade nella definizione di soggetto pubblico.
L’affidamento degli incarichi a terzi per l’esecuzione delle attività previste nel presente documento configura una ipotesi di “esternalizzazione di funzione aziendale operativa essenziale o importante” (di seguito “Outsourcing”) e deve avvenire nel rispetto delle norme in materia di delega di funzioni di cui a:

- il Regolamento Delegato (UE) n. 231/2013 della Commissione del 19 dicembre 2012 (di seguito “Regolamento 231/2013”), che integra la direttiva 2011/61/UE del Parlamento europeo e del Consiglio;
- il Regolamento Delegato (UE) n. 565/2017 della Commissione del 25 aprile 2016(di seguito “Regolamento 565/2017”), che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio;
- il Regolamento di attuazione degli articoli 4-unidecies e 6, comma 1, lettere b) e c-bis) del TUF adottato da Banca d’Italia con Provvedimento numero 1470228/19 del 5 dicembre 2019 (di seguito “Regolamento Banca d’Italia”);
- l’eventuale ulteriore normativa di settore.

All'oggetto del bando inoltre sono applicate le indicazioni del:

- Regolamento UE 2016/679 (c.d. GDPR) in materia di Privacy, con collegate linee guida dell'EDPB (Comitato Europeo per la Protezione dei Dati), in particolare sui temi correlati all'attribuzione di incarichi esterni e alla gestione di servizi informatici;
- D.Lgs 81/08 e s.m.e i. in tema di sicurezza del lavoro, in particolare sui temi riferibili ai fornitori per gli aspetti legati alla regolarità contributiva e ai rischi da interferenza;
- D.Lgs 231/01 e s.m.e i. (responsabilità amministrativa) in tema di reati informatici.

1.3 Profilo informatico

All’infrastruttura informatica devono accedere un minimo di 30 ed un massimo di 50 utenti informatici.

Attualmente la memoria di massa utilizzata per il salvataggio di dati è pari a 5 Tbyte (Sistema PACS e vari file server esclusi) e negli ultimi tre anni è aumentata di circa 1 Tbyte.

L'accesso alla infrastruttura informatica avviene tramite pc fissi, portatili e think client prevalentemente dalla sede principale e, in caso di necessità o emergenza, tramite VPN. Nella sede principale è disponibile una sala server.
Il sistema informatico nella configurazione attuale è costituito da:

- postazioni di lavoro (PC desktop con sistema operativo Windows 10 (PRO e HOME), Notebook con sistema operativo Windows 10 (PRO e HOME), ThinkClient della PRAIM con sistema operativo proprietario basato su Linux, periferiche (stampanti, scanner, etc.) agganciati al dominio della SA;
- dispositivi multifunzione di rete (stampanti, fotocopiatrici, scanner e fax);
- infrastruttura tecnologica (server, server virtuali, storage, software di base e di ambiente, software applicativi, database, ecc.) installata presso il datacenter dell'attuale outsourcer informatico della SGR e altri apparati siti nella sala server della SA;
- rete LAN comprensiva di apparati attivi, componenti passive e sistemi di sicurezza;
- rete WIFI nella sede di Bolzano e di Trento con accesso internet;
- apparati di rete per la connessione nei vari piani dello stabile (switch);
- apparati di sicurezza (firewall primario e secondario);
- apparati di connessione ADSL, VDSL

Il dimensionamento attuale del sistema è riportato nel punto 4 "Attuale consistenza del sistema informatico della SA hardware-software e linee"
La Ditta Appaltatrice (di seguito "DA") dovrà garantire i servizi descritti nei successivi paragrafi sull'intero sistema informatico come descritto in questo documento..
La DA dovrà creare una struttura informatica vendendo alla SA l'hardware richiesto, supportare gli eventuali hardware che risultano ancora idonei, affittare e vendere software.
La sede principale della SA è disposta su più piani; la SGR ha facoltà di utilizzare una stanza sita al piano -1 nel palazzo di via Mostra 11/13 a Bolzano adibita a sala server, conforme agli standard di sicurezza, dotata di sistemi anti-intrusione ed anti-allagamento, aria condizionata, linee di corrente sotto UPS e punto di accesso alla rete internet. Allo stato attuale tale sala viene utilizzata solo per apparati di rete e centralino telefonico, ma dovrà essere attrezzata dalla DA come sala server della SA.

La certificazione ISO27001 è richiesta ai fini della stipula del contratto.

2. Oggetto ed obiettivi dell'Appalto

L'oggetto del bando è dato da:

- Fornitura hardware ad esecuzione istantanea in conto vendita
- Manutenzione periodica Hardware ad esecuzione istantanea in conto vendita
- Fornitura software ad esecuzione istantanea in conto vendita
- Fornitura software ad esecuzione continuativa in canone di servizio
- Fornitura linee dati ad esecuzione istantanea e in canone di servizio
- Progettazione e implementazione dell'infrastruttura informatica ad esecuzione istantanea

- Gestione e manutenzione dell'Infrastruttura Tecnologica del Data Center ad esecuzione continuativa
- Help Desk di assistenza tecnica "all inclusive" ad esecuzione continuativa
- Monitoraggio di sistemi e servizi delle linee dati ad esecuzione continuativa

Per le modalità di esecuzione delle forniture e dei servizi richieste/i (p.es. pagamento, SLA) si rinvia a quanto disposto nel documento “SLA.pdf”.

La DA prende atto che le Autorità di Vigilanza, la SGR, Audit EDP e i suoi revisori contabili potranno svolgere l’attività di supervisione e controllo attraverso l’accesso, anche presso i locali della DA, alle informazioni, ai dati e a tutta la documentazione relativa allo svolgimento dell’attività oggetto del bando.

2.1 Fornitura dell’infrastruttura informatica

Si specifica che in questo capitolo si richiedono forniture ad esecuzione istantanea (salvo il punto 2.1.2) - per le modalità di pagamento si rinvia a quanto nel documento disposto “Capitolato speciale d'appalto per servizi”. La DA dovrà utilizzare la sala server a disposizione della SA e mettere a disposizione un locale adibito a sala server per il sito di Disaster Recovery (di seguito “DR”), come definito nel paragrafo 2.2.10 “Business Continuity e Disaster Recovery”.
La DA dovrà proporre un progetto di infrastruttura server e infrastruttura di rete, dimensionando i sistemi offerti sulla base dei seguenti requisiti minimi:

- un minimo di 30 accessi informatici alla infrastruttura informatica;
- la corretta distribuzione memoria RAM e CPU dedicata ad ogni server della infrastruttura e la possibilità di aumentare in qualsiasi momento in caso di necessità;
- prevedere almeno 50 Giga di spazio dedicato ad ogni macchina virtuale presente nell’infrastruttura informatica, il numero di server virtuali sono come minimo gli stessi che attualmente utilizziamo;
- conformità alle caratteristiche richieste all’interno della presente documentazione;
- la possibilità di attivare un nuovo server virtuale con qualsiasi sistema operativo e renderlo operativo in caso di necessità;
- almeno 6 terabyte di spazio dedicato ai dati della SA replicati in ambiente DR.

La DA sarà responsabile della pianificazione e del coordinamento di tutte le attività necessarie per il trasferimento delle applicazioni software e delle basi di dati in esercizio dall’infrastruttura attuale alla nuova infrastruttura.
La DA concorderà con la SA e successivamente metterà in atto il passaggio tra l’esercizio della vecchia infrastruttura e la nuova, in modo che la SA non abbia interruzioni di servizio.
La SA potrà, durante la durata del contratto, installare nuovi sistemi nell’infrastruttura di rete e nella sala server. La DA dovrà contribuire al processo di selezione di nuovo software da parte della SA,

anche al fine di assicurare che i requisiti tecnici dello stesso siano compatibili con l'infrastruttura della SGR.

2.1.1. Fornitura hardware

La DA deve fornire, come minimo:

- Numero 1 Firewall in cluster da fornire, installare, configurare, gestire e mantenere da posizionare nella sala server della SA con le seguenti caratteristiche:
  8 x 10/100/1000 Porte Ethernet attive ed indipendenti con due Poe+, 1,32 Gbps velocita' Firewall, 1,4 Gbps velocita' VPN, 1,32 Gbps velocita' UTM;

- Numero 1 Firewall in cluster da fornire, installare, configurare, gestire e mantenere da posizionare nella sala server della SA con le seguenti caratteristiche:
  8 x 10/100/1000 Porte Ethernet attive ed indipendenti con due Poe+, 1,32 Gbps velocita' Firewall, 1,4 Gbps velocita' VPN, 1,32 Gbps velocita' UTM;

- Numero 1 Firewall da fornire, installare, configurare, gestire e mantenere da posizionare nella sala DR della DA con le seguenti caratteristiche:
  8 x 10/100/1000 Porte Ethernet attive ed indipendenti con due Poe+, 1,32 Gbps velocita' Firewall, 1,4 Gbps velocita' VPN, 1,32 Gbps velocita' UTM;

- Numero 1 Firewall da fornire, installare, configurare, gestire e mantenere da posizionare nella sede principale a Milano presso un cliente della SA con le seguenti caratteristiche:
  5 x 10/100/1000 Porte Ethernet attive ed indipendenti con una Poe+, 1 Gbps velocita' Firewall, 880 Mbps velocita' VPN, 300 Mbps velocita' UTM;

- Numero 1 Firewall da fornire, installare, configurare, gestire e mantenere da posizionare nella sede principale a Milano presso un cliente della SA con le seguenti caratteristiche:
  5 x 10/100/1000 Porte Ethernet attive ed indipendenti con una Poe+, 1 Gbps velocita' Firewall, 880 Mbps velocita' VPN, 300 Mbps velocita' UTM;

- Numero 1 SAN fibre channel unità dischi fc, 16 gb, con 6 Hard Disk da 1,0 tb installati in RAID 5, comprensivi di cavi e alloggiamenti per Rack;

- Numero 2 Switch SAN in fibra 16 gb, sftp e cavi in fibra, comprensivi di cavi e alloggiamenti per Rack;

- Numero 2 Server in cluster da fornire, installare, configurare, gestire e mantenere da posizionare nella sala server della SA con le seguenti caratteristiche minime: 2 X Xeon Gold 6134 o di un modello equivalente di un altro produttore(8 Core, Clock 3.0GHz, Cache 24,75 MB L3) 32GB 2933MHz (128GB, rDIMM), No Backplane, RAID, 2x1100W, XCC Enterprise, Tooless Rails, 2 Hard Disk interni per boot del sistema,1 Scheda Fibre Channel 16 Gigabit a 2 porte, Scheda controller a 4 porte a 1 gigabit, scheda di rete, comprensivi di cavi e alloggiamenti per Rack;

- Numero 1 Server da fornire, installare, configurare, gestire e mantenere da posizionare nella sala server di DR della DA con le seguenti caratteristiche minime: 2 X Xeon Gold 6134 o di un modello equivalente di un altro produttore (8 Core, Clock 3.0GHz, Cache 24,75 MB L3) 32GB 2933MHz (128GB, rDIMM), No Backplane, RAID, 2x1100W, XCC Enterprise, Tooless Rails, 2 Hard Disk

interni per boot del sistema, 1 Scheda Fibre Channel 16 Gigabit a 2 porte, Scheda controller a 4 porte a 1 gigabit, 1 controller RAID interno, 6 dischi 2.5" da 1.8 TB da 8000 rpm per il backup in caso di DR, comprensivi di cavi e alloggiamenti per Rack;

- Numero 1 Sistema NAS iscsi 10 gb, proc Intel Xeon D-1521 o di un modello equivalente di un altro produttore, da 12 alloggiamenti disponiblii da fornire, installare, configurare, gestire e mantenere da posizionare nella sala server della SA. Nel NAS devono essere presenti 8 dischi SATA (SATA/600) da 1.8 Tb in RAID 5, comprensivi di cavi e alloggiamenti per Rack;

- Numero 2 switch, da 24 alloggiamenti da 1Gb, 2 SFP+ Ports, 19inch Rackmountable, internal PSU

2.1.2. Fornitura software

Si specifica che in questo punto si richiedono forniture ad esecuzione istantanea e ad esecuzione continuativa - per le modalità di pagamento e rispettivi SLA si rinvia a quanto disposto nel documento "SLA.pdf".

La DA dovrà fornire per tutta la durata del contratto il software necessario per l'utilizzo dell'infrastruttura informatica. Al momento dell'avvio del contratto, la struttura informatica dovrà prevedere come minimo la fornitura del seguente software:

Ad esecuzione istantanea e in conto vendita:

- Numero 30 licenze WinSvrCAL 2019 SNGL OLP NL UsrCAL - R18-05768; (non serve la manutenzione)
- Numero 30 licenze WinRmtDsktpSrvcsCAL 2019 SNGL OLP NL UsrCAL - 6VC-03748; (non serve la manutenzione)
- Numero 3 Windows Server 2019 Datacenter edition 16Core, Secondary OS, No Media, Unlimited VMs
- Numero 12 Windows Server 2019 Datacenter Additional License (2 core) (No Media/Key) (Reseller POS Only)
- Numero 1 licenza software di virtualizzazione for 3 Host (MAX 2 PROCESSORS PER HOST) con 3 anni di manutenzione e aggiornamento
- Numero 1 licenza Software di backup e Replication per virtualizzazione con 3 anni di manutenzione;

Manutenzione periodica hardware

- Garanzia e Manutenzione onsite 24x7 dei 3 Server e di tutte lo componentistiche interne, NAS, SAN, Dischi NAS, Dischi SAN e 2 Switch SAN, Fiber Channel e dei 5 firewall.

Ad esecuzione continuativa e in canone di servizio:

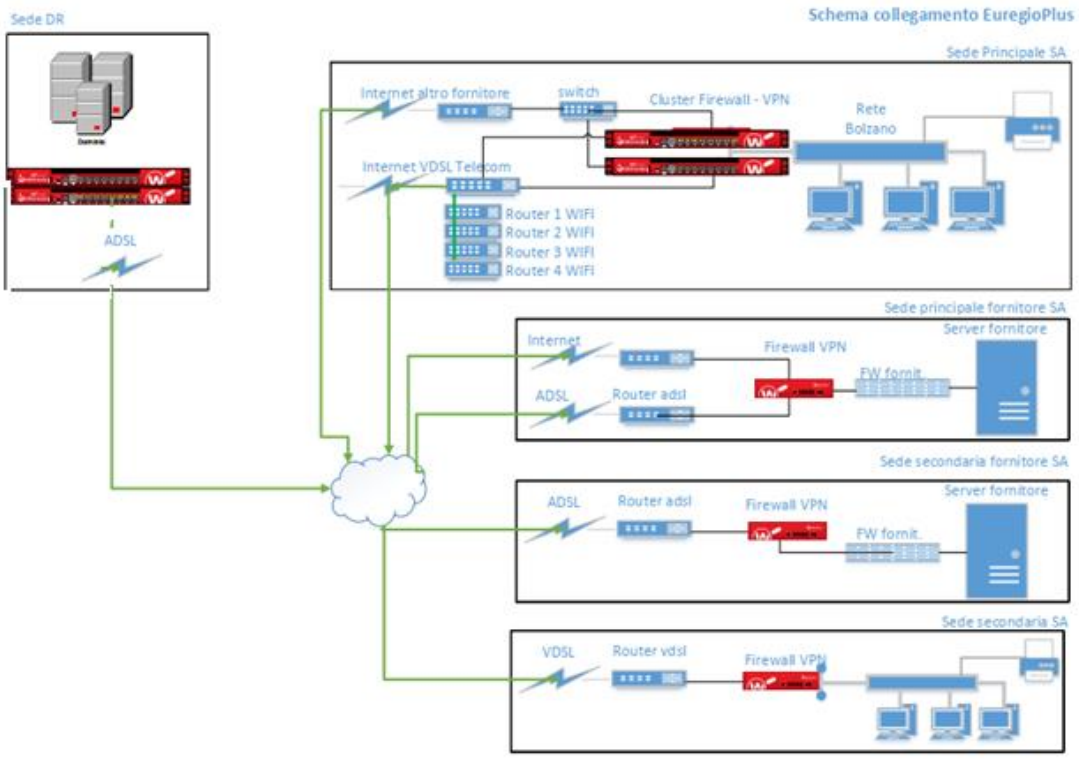
- Numero 1 licenza antispam antivirus Mail server;
- Numero 30 licenze software di connessione VPN tramite software;
- Numero 15 licenze software di connessione VPN tramite software e in aggiunta autenticazione token o app;
- Numero 30 licenze Antivirus (Client, portatili e server) con servizio log e inventario software e hardware;
- Numero 30 licenze di HCL Domino 11 Complete Collaboration (CCB) TERM;

2.1.3. Fornitura linee dati

Si specifica che in questo capitolo si richiedono forniture ad esecuzione istantanea - per le modalità di pagamento si rinvia a quanto disposto nel “Capitolato speciale d'appalto per servizi”.

La DA dovrà fornire e gestire le linee dati della SA e garantire la massima sicurezza tramite firewall.
Il sito di DR dovrà essere predisposto per ricevere da linee dati e internet.
Sono richieste 5 linee VDSL con le seguenti caratteristiche:
Download 100 Mega – Upload 20 Mega:

- 2 linee dati a Bolzano sede SA + 8 ip pubblici
- 2 linee dati a Milano da installare nella sede principale e secondaria a Milano di Objectway
- 1 linea dati presso la sede secondaria della SA a Trento per sincro



2.1.4. Manutenzione periodica Hardware

La DA deve provvedere ad attivare, gestire e rinnovare per tutta la durata del contratto la manutenzione hardware ed estensione di garanzia di tutti i componenti hardware oggetto del bando.
Le garanzie e assistenze devono essere per tutti i componenti hardware di 24 ore su 24, 7 giorni su 7 con un supporto “onsite” in 4 ore.
La DA deve consegnare alla SA tutte le garanzie e manutenzioni attivate a nome della SA.

2.2 Progettazione e implementazione dell'infrastruttura informatica

Si specifica che in questo capitolo si richiedono servizi ad esecuzione istantanea - per le modalità di pagamento e SLA si rinvia a quanto disposto nel documento "SLA.pdf".

La progettazione ed implementazione dell'infrastruttura informatica software e hardware della SA, comprensiva della fornitura e configurazione dell'hardware di nuova generazione per le sedi e per il sito di DR della DA;

La DA dovrà:

- Installare fisicamente tutti i firewall e collegarli all'infrastruttura, configurarli e attivare tutte le policy di sicurezza nelle sedi della SA, nella sala Disaster Recovery della DA e nelle sedi di clienti a Milano e rendere sicure le linee dati;

- Installare fisicamente il NAS e tutti gli Hard Disk a corredo, collegarlo all'infrastruttura della SA, creare il RAID 5 e configurarlo per gestire i backup;

- Installare fisicamente la SAN e tutti gli Hard Disk a corredo, collegarlo all'infrastruttura della SA, creare il RAID 5 e configurarlo per creare le Virtual Machine e i dati della SA;

- Installare fisicamente il primo server in cluster completo di CPU, RAM, processori, Hard Disk, scheda madre, Scheda Fibre Channel, Scheda controller SCSI 4 porte 1 Giga, scheda di rete, alimentatori e di tutti i componenti nella sede della SA:
    - Creare il RAID in mirroring dei due Hard Disk per il boot;
    - Installare, configurare e aggiornare il Sistema operativo;
    - Installare e configurare il programma VwWare e l'ambiente in replica;
    - Installare, creare e configurare Farm Citrix su ambiente virtuale;
    - Installare e configurare tutti server virtuali;
    - Creare replica con il secondo server;

  Vedasi documento Capitolato Tecnico paragrafo 4.2 Attuali Server virtuali

  Si specifica che tutti i server virtuali devono avere installata l'ultima versione di SO e anche tutte le ultime versioni di software devono essere installate con le ultime versioni disponibili.
- Installare fisicamente il secondo server in cluster completo di CPU, RAM, processori, Hard Disk, scheda madre, Scheda Fibre Channel, Scheda controller SCSI 4 porte 1 Giga, scheda di rete, alimentatori e di tutti i componenti nella sede della SA.
    - Creare il RAID in mirroring dei due Hard Disk per il boot;
    - Installare, configurare e aggiornare il Sistema operativo;
    - Installare e configurare il programma VwWare e l'ambiente in replica;
    - Installare, creare e configurare Farm Citrix su ambiente virtuale;
    - Installare e configurare tutti server virtuali;
    - Creare il dominio e tutte le policy necessarie per il funzionamento;
    - Creare replica con il primo server;

  Vedasi documento Capitolato Tecnico paragrafo 4.2 Attuali Server virtuali

Si specifica che tutti i server virtuali devono avere installata l'ultima versione di SO e anche tutte le ultime versioni di software devono essere installate con le ultime versioni disponibili.

- Installare fisicamente il server di DR completo di CPU, RAM, processori, 2 Hard Disk di avvio, , Scheda controller SCSI 4 porte 1 Giga, alimentatori, Scheda Fibre Channel, Scheda controller RAID e 8 Hard Disk, scheda madre e tutti i componenti nelle sede della DA
    - Creare il RAID in mirroring dei due Hard Disk di avvio;
    - Installare, configurare e aggiornare il Sistema operativo ultima versione;
    - Installare e configurare il programma VwWare e tutto l'ambiente;
    - Installare, creare e configurare Farm Citrix su ambiente virtuale;
    - Installare e configurare tutti server virtuali;
    - Creare il RAID 5 dei 8 dischi per la replica dei dati con la SAN;
    - Configurare Replica schedulata dati con SAN

    Vedasi documento Capitolato Tecnico paragrafo 4.2 Attuali Server virtuali
    Si specifica che tutti i server virtuali devono avere installata l'ultima versione di SO e anche tutte le ultime versioni di software devono essere installate le ultime versioni disponibili.
- Installare, configurare le linee dati e testare il funzionamento e predisporre il WIFI interno;
- Creare dominio, regole, policy, e connessioni FTPS;
- Creare politica di backup;
- Predisporre il piano di Business Continuity e Disaster Recovery;
- Creare il dominio e tutte le policy necessarie per il funzionamento dell'infrastruttura;
- Migrare tutti i dati.

La DA in fase di analisi si impegna a stimare eventuali apparecchiature e componenti di sostituzione che si dovessero rendere necessari e che quindi saranno a carico della DA; le eventuali sostituzioni hardware sono parte integrante dell'offerta e dovranno essere indicati i criteri utilizzati per la stima.

2.2.1. Creazione Server Farm Citrix

la SA è proprietaria di 45 licenze Citrix. La DA dovrà creare la farm Citrix in ambiente virtuale da inserire nel dominio della SA. In generale dovranno essere installati almeno i seguenti server:

- 1 server dedicato al servizio Management Citrix:
- Minimo 3 server Provisioning Citrix;
- 1 server Console Citrix;
- 1 server SQL Citrix;
- 1 server Master Citrix (immagine Citrix);
- 2 server dedicato al portale web Citrix (distribuzione Applicazioni);
- Almeno 7 server farm idonei a supportare fino a 50 utenze di accesso con la possibilità di attivarne su richiesta della SA;
- 1 server farm Citrix di test per testare aggiornamenti o distribuzioni;
- 1 server farm Citrix in stand-bye da attivare in caso di necessità
- 1 server Console Citrix

Tutti i server della farm Citrix dovranno essere replicati in ambiente DR e nel server di replica.

L'accesso all'app center, a tutti i server virtuali e fisici, Active Directory etc, dovrà essere consentito alla SA in modalità di amministratore di rete e dovranno essere attivi tutti i log di accesso.Tutti i server della farm Citrix dovranno essere replicati in ambiente DR e nel server di replica..

2.2.2. Creazione server Domain Controller

La DA dovrà installare 1 server virtuale dedicato al servizio Domain Controller. L'installazione e la configurazione dei server devono seguire le linee guide della casa produttrice del software.
I server dovranno essere replicati in ambiente DR e nel server di replica.
I server virtuali dovranno essere configurati in modo da non avere latenze o rallentamenti e la distribuzione del carico di risorse è in capo alla DA.
La DA deve seguire le istruzioni della SA durante la configurazione del dominio

2.2.3. Creazione Server dedicati alla posta HCL Domino 11 e annessi

La SA utilizza il sistema di posta Domino 8.5.3 in quanto è l'unico programma nel quale è stato sviluppato un'interfaccia personalizzata che si collega direttamente al software per la gestione documentale. La DA deve vendere alla SA il software HCL Domino Complete Collaboration (CCB) TERM versione 11 o superiore, installarlo, configurarlo, importare le attuali impostazioni, personalizzazioni e database. Inoltre la DA deve rendere operativa la posta di tutti i dipendenti della SA utilizzando l'attuale dominio euregioplus.com, configurare i cellulari di tutta la SA tramite il software Traveler e attivare la chat interna tramite il software Sametime.
La DA deve installare:

- 2 server virtuali da inserire nel dominio della SA dedicato al servizio Domino (server di posta aziendale del dominio euregioplus.com) e la relativa configurazione e gestione del programma.
- 1 server virtuale da inserire nel dominio della SA dedicato al servizio Traveler (server di posta su cellulare) e la relativa configurazione e gestione del programma.
- 1 server virtuale da inserire nel dominio della SA dedicato al servizio Sametime (server di chat interna del programma Lotus) e la relativa configurazione e gestione del programma.
- 1 server virtuale da inserire nel dominio della SA dedicato al servizio Proxy (server proxy di filtraggio antispam e antivirus) e la relativa configurazione e gestione del programma.
- 1 server virtuale da inserire nel dominio della SA dedicato al portale web la relativa configurazione e gestione del programma.

Allo stato attuale sono presenti circa 200 db di posta associati a vari utenti comprensivi di archivi personali e relativa associazione agli utenti.
I server dovranno essere replicati in ambiente DR e nel server di replica.

2.2.4. Creazione politica di backup

La DA deve creare una politica di backup tramite il software che la DA dovrà vendere alla SA, installare e configurare.
La politica di backup deve avere obbligatoriamente avere 4 tipi di backup:

- Il backup giornaliero notturno prevede dalla domenica al venerdi il salvataggio su nastro o Hard Disk esterno staccato dalla rete o cloud solamente i dati modificati presenti nel NAS e

sulle partizioni “D:” di tutti i server virtuali (backup incrementale). Il backup giornaliero deve essere mantenuto 1 mese.

- Il backup settimanale notturno prevede ogni sabato il salvataggio su nastro o Hard Disk esterno staccato dalla rete o cloud di tutti i dati presenti nel NAS e i dati delle partizioni “D:” di tutti i server virtuali. Il backup settimanale deve essere mantenuto 1 mese.

- Il backup mensile notturno prevede ogni ultimo sabato del mese il salvataggio su nastro o Hard Disk esterno staccato dalla rete o cloud di tutti i dati presenti nel NAS e i dati delle partizioni “D:” e le immagini virtuali di tutti i server. Il backup mensile deve essere mantenuto 1 anno.

- Il Backup annuale notturno prevede ogni ultimo sabato dell’anno il salvataggio su nastro o Hard Disk esterno staccato dalla rete o cloud di tutti i dati presenti nel NAS, i dati delle partizioni “D:” e le immagini virtuali di tutti i server. Il backup annuale deve essere mantenuto 10 anni.

Il supporto di registrazione nastro o unità disco esterna o cloud è in carico alla DA che provvederà al mantenimento dei dati nel tempo.
In qualsiasi momento la SA potrà chiedere alla DA uno specifico restore o un backup intero.

2.2.5. Desktop virtuali

Per ciascun dipendente della SA deve essere messo a disposizione un Virtual Desktop in ambiente citrix avente, a pena di esclusione, le seguenti caratteristiche minime:

- CPU equivalente ad un Intel Core i5 di 7a generazione o un modello equivalente di un altro produttore;
- 6Gb di RAM
- Non è necessaria una scheda dedicata

I virtual desktop devono funzionare con i nuovi sistemi di videocomunicazione

La DA dovrà gestire, mantenere e aggiornare i desktop virtuali per tutta la durata del contratto.

2.2.6. Server con programmi gestiti da terzi fornitori

La DA dovrà predisporre e configurare tutti i server virtuali che attualmente vengono utilizzati dalla SA per i software di terze parti che necessitano di un server dedicato.
La DA dovrà anche creare minimo 7 server virtuali con Sistema Operativo Windows Server u.v. da inserire nel dominio della SA e la relativa installazione del programma in collaborazione con l’azienda fornitrice e la SA del software e importare le impostazioni presenti nella vecchia infrastruttura.
La DA deve installare:

- Server Ms Windows per software di archiviazione documentale;

- Server Ms Windows per software MySQL;
- Server Linux per software Registro Ordini;
- Server Ms Windows per elaborazione di prospetti;
- Server Ms Windows per software presenze
- Server Ms Windows per software Antivirus
- Server Ms Windows da utilizzare in caso di necessità

La SA in caso di necessità potrà chiedere alla DA di attivare in qualsiasi momento il Server Ms Windows da utilizzare in caso di necessità.
Tutti i server devono avere la partizione C: dedicata al SO e la partizione D: dedicata ai programmi e ai dati programmi.

2.2.7. Server di servizi

La DA dovrà predisporre e configurare 4 server virtuali con Sistema Operativo Windows Server u.v. da inserire nel dominio della SA e le relative configurazioni dei servizi e programmi e importare le impostazioni presenti nella vecchia infrastruttura.

- Server Ms Windows dedicato ai servizi di flussi SFTP;
- Server Ms Windows per programma del servizio di VPN;
- Server Ms Windows dedicato al servizio delle stampanti.
- Server Ms da utilizzare in caso di necessità

La SA in caso di necessità potrà chiedere alla DA di attivare in qualsiasi momento il Server Ms Windows da utilizzare in caso di necessità.
Tutti i server devono avere la partizione C: dedicata al SO e la partizione D: dedicata ai programmi e ai dati programmi.

2.2.8. Server Active Directory

La DA dovrà predisporre e configurare 1 server virtuale dedicato al servizio Active Directory e importare le impostazioni presenti nella vecchia infrastruttura, quindi la DA dovrà:

- Progettazione della foresta;
- Progettazione del dominio;
- Progettazione radice della foresta;
- Pianificazione dello spazio dei nomi di Active Directory;
- Infrastruttura DNS per supportare Active Directory;
- Creazione della progettazione di un’unità organizzativa:
- Configurazioni policy aziendali

Il server dovrà essere replicato in ambiente DR e nel server di replica.
Il server deve avere la partizione C: dedicata al SO e la partizione D: dedicata ai programmi e ai dati programmi.

2.2.9. Migrazione dati

La DA dovrà effettuare la migrazione di tutti dati della SA nella nuova infrastruttura. I dati copiati dovranno ereditare le stesse a policy di accesso e la DA dovrà dimostrare alla SA tramite log o report la congruenza dei dati spostati dalla vecchia alla nuova infrastruttura.
La DA prima della migrazione dovrà sottoporre i dati a un controllo completo, verificare che i dati da copiare non abbiano problemi e nel caso risolverli tramite strumenti informatici ed infine effettuare il monitoraggio e il reporting sulla qualità dei dati.
La DA potrà spostare i dati o tramite una migrazione “Big Bang” (ossia in una volta durante un fine settimana) o tramite una migrazione “trickle” (il vecchio sistema ed il nuovo sistema vengono eseguiti in parallelo).
Si specifica che tutti i dati e database di posta dovranno essere leggibili compresi archivi tenendo presente che i files devono ereditare le stesse autorizzazioni di accesso.
Obbligo della DA anche di migrare tutte le policy della Active Directory e ricreare la stessa mappatura di rete. Inoltre la DA dovrà anche ricreare tutti flussi SFTP attualmente attivi.
Si specifica che tutti i dati sono attualmente posizionati nel NAS e nelle partizioni D: di tutti i server virtuali.

2.2.10. Business Continuity e Disaster Recovery

Conformemente a quanto previsto dalla normativa vigente, la SA si è dotata di un piano di emergenza e di continuità operativa (di seguito “Business Continuity Plan”, o “BCP”) e DR al fine di garantire di poter reagire in maniera adeguata alle emergenze e di mantenere le attività operative critiche in caso di interruzione delle proprie procedure operative ordinarie.

Il BCP documentato racchiude tutte le informazioni e procedure necessarie per la gestione di eventi straordinari che compromettano l’ordinaria attività lavorativa della SA. Il BCP prevede al suo interno una sezione appositamente dedicata del Piano di DR che definisce i possibili disastri e gli scenari di rischio, individua i processi critici e le figure di riferimento, interne ed esterne alla SA, in caso di gravi problemi oltre che le modalità di risoluzione degli stessi.
La DA deve prevedere sistemi software e hardware che garantiscano la continuità lavorativa dell’azienda ed una accurata gestione del rischio. Si chiede pertanto alla DA una spiccata sensibilità sulle minacce (Analisi delle minacce) e la comprensione dell’impatto di una loro indisponibilità (Business Impact Analysis).
Oggetto del bando è anche la creazione e gestione della BCP e DR di tutta infrastruttura informatica della SA.

La DA deve effettuare almeno una prova annuale di DR; i tempi di ripartenza dei processi dovranno risultare compatibili con i parametri utilizzati dalla SA per il proprio piano di BC genericamente contenute entro un massimo di 4 ore e comunque entro i tempi di invio dei dati all'esterno della SA (quali ad esempio le comunicazioni verso Authority); la DA dovrà inoltre creare un piano di DR funzionante che preveda un Backup “a caldo” di tutti dati della SA nel sito di DR fornito dalla DA contenente i server e unità dischi dell’oggetto del bando; con periodicità almeno annuale deve essere svolto un test dell’intera sala server con l’attivazione del sito di DR; i tempi di ripartenza dei macchinari dovranno risultare compatibili con i parametri utilizzati dalla SA per il proprio piano di BC genericamente contenute entro un massimo di 8 ore e comunque entro i tempi di invio dei dati all'esterno della SA (quali ad esempio le comunicazioni verso Authority);La DA dovrà mettere a

disposizione della SA un locale adibito a Sala Server per il sito di DR (Sala Server DR), che dovrà essere distante almeno 50 chilometri dalla Sala Server della SA.
L'accesso alla Sala Server DR dovrà essere garantito alle Autorità di Vigilanza, alla SGR ed ai suoi revisori contabili al fine dello svolgimento delle attività di supervisione e controllo.
Requisiti essenziali per la BCP sono:

- doppi sistemi hardware almeno dei seguenti hardware
    - Firewall sede principale SA: come da richiesta di fornitura si deve prevedere il cluster dei firewall, relativa configurazione e gestione;
    - Server sede principale SA: come da richiesta di fornitura si deve prevedere il cluster dei server e relativa configurazione e gestione;
    - Hard Disk (HD) sede principale SA: come da richiesta di fornitura si deve prevedere di creare la corretta gestione dei dischi dei server e della NAS.
- linee doppie delle seguenti località:
    - Sede principale SA:
    - Sede principale fornitore esterno finanziario

n caso di caduta delle due linee prevedere di attivare la linea di D.R.

- Servizi software essenziali della infrastruttura informatica:
    - sede principale SA: prevedere di configurare doppi servizi.

Requisito fondamentale che i dati della SA vengano salvati nel sito di DR tramite Backup a caldo.
i server virtuali possono essere salvati nel sito DR tramite backup a freddo.
Inoltre si deve prevedere l'accesso ai servizi aziendali tramite sistemi di Smart Working, avendo cura che siano implementati nel rispetto dei principi di sicurezza e protezione dei dati e accompagnati da una adeguata attività di formazione e aggiornamento delle risorse.

Con periodicità minima annuale dovrà essere effettuato un test di DR della sala server e relativa attivazione della sala server di DR. Il test dovrà essere concordato tra le parti e dovrà essere effettuato preferibilmente nel fine settimana. Al test DR potrà partecipare la SA e/o un incaricato esterno.
È obbligatorio ricevere una guida step by step sulle varie operazioni che verranno eseguite il giorno del test ed in ultimo, a fine lavori, eseguire un rapporto dettagliato che verrà portato nella documentazione del CDA dell'azienda. In caso di esito negativo o di risultato non soddisfacente dovrà essere riprogrammato un altro test entro 45 giorni dal primo test.
La DA deve quindi prevedere un test DR funzionale e realistico che preveda inagibilità della sala server e attivazione del piano DR della sala server per le seguenti cause:

- interruzione della connettività internet;
- interruzione di uno o di tutti i path di un server;
- guasto di uno o più server che pregiudicano il funzionamento della infrastruttura;
- guasto dello storage;
- disastro della sede.

2.2.11. Sala Server di Disaster Recovery

La DA deve mettere a disposizione tutta la durata del contratto un locale adibito a Sala Server di DR comprensivo di impianto di condizionamento, Armadio Rack, Illuminazione, Corrente elettrica, UPS, una Linea Internet e uno spazio di archiviazione di 8 TB per poter effettuare gli eventuali backup in caso di DR e i test di DR.

<u>Sala Server di DR:</u>

La Sala Server di DR di proprietà della DA deve essere dotata di UPS, impianto di condizionamento, illuminazione e relativa corrente elettrica. La Sala Server di DR deve essere messa a diposizione della SA per ospitare un Server e un Firewall di proprietà della SA.
L'accesso alla Sala Server di DR deve avere la tracciatura degli accessi e solamente il team del progetto della DA deve poter accedere alle apparecchiature della SA.
La sala di D.R. deve essere ad una distanza minima di 50 km dalla sede principale della SGR di Bolzano.

Armadio Rack di DR:
La DA deve mettere a disposizione un armadio Rack per poter inserire le apparecchiature della SA, il montaggio del server e firewall e relative configurazioni devono essere fatte dalla DA.

Corrente elettrica, illuminazione e UPS:
La DA deve mettere a disposizione un UPS, corrente elettrica e illuminazione sono a carico della DA.

Linea Internet
La DA deve fornire una linea Internet con le seguenti caratteristiche: 100/20

Spazio dati
La DA deve fornire uno spazio di archiviazione dati digitali di 8 Tb da collegare al server di proprietà della SA

2.3 Gestione e manutenzione dell'Infrastruttura Tecnologica del Data Center

Si specifica che in questo capitolo si richiedono servizi ad esecuzione continuativa, per le modalità di pagamento e rispettivi SLA si rinvia a quanto disposto nel documento "SLA.pdf".

Gli obiettivi del presente servizio sono quelli di fornire il supporto tecnico necessario per mantenere operativa ed efficiente l'infrastruttura tecnologica per tutto il periodo di vigenza contrattuale, consentendo una corretta operatività delle piattaforme tecnologiche informatiche e del relativo software di base e di ambiente su cui sono ospitati gli attuali applicativi e database del Sistema Informativo dell'Azienda nonché di quanto sarà aggiunto durante il periodo di vigenza contrattuale.
Alla DA è richiesto di gestire detta infrastruttura nel rispetto delle policy e dei livelli di servizio definiti nei paragrafi successivi, impiegando i mezzi e le modalità più idonei per prestare il servizio nel rispetto dei requisiti contrattuali.
Il servizio dovrà comprendere la gestione della sicurezza logica e fisica, tesa a garantire l'integrità, la disponibilità e la riservatezza dei dati siti sui sistemi server e storage.
Dovrà essere garantita la gestione completa del sistema centrale (inteso con tutti i sistemi server storage e tutte le periferiche ad essi collegate), e pertanto la presa in carico, la conduzione operativa ed il monitoraggio, gli interventi manutentivi schedulati, la risoluzione di guasti e di malfunzionamenti, la gestione dello storage, ecc..
Tutti i costi per la manutenzione ed estensione di garanzia saranno a carico della DA. L'organizzazione del servizio proposta dovrà prevedere una struttura che consentirà l'espletamento delle attività descritte nei seguenti paragrafi.

2.3.1. Gestione tecnica ed operativa dell'infrastruttura hardware e software di base e d'ambiente

Il servizio dovrà comprendere almeno le seguenti operazioni:

- manutenzione dei sistemi centrali sia correttiva che preventiva con relativa gestione operativa e risoluzione dei malfunzionamenti;
- gestione, conduzione e monitoraggio delle attività di backup, restore e recovery, degli applicativi e delle basi di dati presenti, gestione operativa storage, dei media e dei supporti utilizzati secondo le modalità previste dalle procedure dei sistemi e dalle basi dati;
- gestione delle performance dei sistemi;
- gestione dello spazio su disco;
- esecuzione delle procedure batch;
- gestione della virtualizzazione dei server;
- gestione della farm citrix
- gestione di tutto l'ambiente di posta
- configurazione ed amministrazione dei server;
- gestione operativa delle prestazioni dei server;
- gestione e monitoraggio dei parametri ambientali della sala macchine;
- gestione delle code di stampa e delle stampe centralizzate;
- gestione del file sharing;
- gestione delle problematiche relative alla sicurezza logica dell'infrastruttura curando la conformità alla normativa e applicazione delle policy di sicurezza;
- supporto alla definizione ed all'attuazione di politiche di DR eBusinessContinuity;
- gestione replica dei server
- gestione sicurezza
- supporto per la definizione di ampliamento/consolidamento del data Center;
- definizione e formalizzazione di tutte le procedure operative;
- gestione log di accesso di amministratori di sistema.

2.3.2. Gestione dei Server

Il Servizio di Gestione dei Server include tutte le attività necessarie per condurre e mantenere sempre efficiente l'infrastruttura server utilizzata per l'erogazione dei servizi informatici
L'infrastruttura include:

- Garantire il perfetto funzionamento dei sistemi server hardware e software e gli apparati ad essi connessi (firewall, storage, library, router…) della sala server della SA e della sala server di DR della DA messa a disposizione alla SA;
- Garantire il perfetto funzionamento di tutta l'infrastruttura di rete della sala server della SA (firewall, switch e apparati di rete);

L'attuale configurazione delle infrastrutture server presenti presso le sedi della SA al di fuori della sala server è definita nel documento del Capitolato Tecnico capitolo "4 Attuale consistenza del sistema informatico della SA hardware-software e linee", nel quale sono indicati gli attuali server, che saranno inclusi nella nuova sala server come server virtualizzati.
Il servizio dovrà essere fornito, senza oneri aggiuntivi e senza alcun vincolo, rispettando gli SLA contrattuali, relativamente alle configurazioni ed ai volumi che potranno risultare dalle evoluzioni che la SA richiederà alla DA, nel corso del periodo contrattuale, per il proprio Sistema Informativo (ad esempio modifiche ed incremento dei server).

In tale contesto si definisce “Sistema” o “Server” l’insieme di più componenti hardware e software (Sistema Operativo e componenti software come ad esempio Domino o MS Office), assimilabili ad una unità elaborativa autonoma a supporto dello sviluppo, del test e dell’esercizio di uno o più servizi.

In tale contesto anche l’infrastruttura di rete della sala server è considerata come un “Sistema”.

Il servizio coprirà l’intero ciclo di vita dei Sistemi, ed includerà quindi, tra gli altri:

- conduzione operativa dei Sistemi e misurazione delle prestazioni;
- change management locale o remoto (gestione ed esecuzione di modifiche riguardanti software di base, d’ambiente e di rete ed eventuale assistenza a software applicativo di terze parti);
- IMAC (movimentazione, aggiunta e cambiamento di componenti HW e periferiche);
- asset Management (gestione e controllo delle configurazioni installate);
- gestione degli incidenti, assistenza tecnica e manutenzione Hardware e Software;
- rendicontazione.

La DA si impegna a garantire il corretto funzionamento e la disponibilità richiesta dei servizi di elaborazione centrale, tramite adeguati servizi di assistenza sistemistica sui diversi ambiti che impattano l’operatività dei sistemi. Sarà a carico della DA la gestione software e hardware delle apparecchiature di tutte le attrezzature, inoltre si fa presente che la DA dovrà avere un ruolo primario con le aziende che dovranno eseguire la manutenzione e aiutare la SA nella gestione delle chiamate di assistenza con i vari fornitori hardware e software (ad esempio, aprire chiamate di assistenza, telefonare, essere disponibili per eventuali test).

2.3.3. Server Applicativi

I server applicativi dovranno essere monitorati e gestiti lato sistema operativo, il supporto alle applicazioni di terze parti ed i relativi obiettivi di disponibilità sono di responsabilità della SA.
Per quanto riguarda i server che forniscono servizi applicativi non gestiti direttamente, la DA provvederà:

- all’eventuale installazione, configurazione ed ottimizzazione del sistema operativo e del software d’ambiente (es. Application Server, Oracle Application, software di virtualizzazione);
- alla configurazione dei parametri di sistema (partizioni, istanze, storage, RAM, CPU, etc.) per l’ambiente di test e di produzione degli applicativi;
- al supporto nell’installazione degli applicativi ed alla definizione di script di gestione (startup, shutdown, etc.) in collaborazione con il fornitore esterno dell’applicativo;
- alla connettività alla rete e ai servizi a valore aggiunto quali: il monitoraggio, la sicurezza (firewall), il backup centralizzato;
- alla gestione delle code di stampa;
- al supporto infrastrutturale, inclusa la consulenza sistemistica per l’ottimizzazione delle prestazioni;
- alla gestione dei malfunzionamenti, a partire dal supporto Service Desk fino alla manutenzione tramite i contratti già in essere;
- alla prevenzione di idonee misure di sicurezza per garantire l’integrità delle applicazioni in esercizio.
- agli aggiornamenti di Windows e di sicurezza;
- all’installazione e gestione antivirus.

2.3.4. Gestione Server Farm Citrix

La DA deve gestire e mantenere l'intera farm citrix, prevedere di effettuare aggiornamenti e risoluzione di eventuali anomalie. Obbligo della DA di creare nuovi accessi citrix e di ripartizionare in modo corretto la gestione delle risorse e nel caso aumentare il numero di server virtuali in base alle necessità.

2.3.5. Server Domain Controller

La DA dovrà 'installare un server virtuale dedicato al servizio Domain Controller. L'installazione e la configurazione dei server devono seguire le linee guide della casa produttrice del software.
I server dovranno essere replicati in ambiente DR e nel server di replica.
I server virtuali dovranno essere configurati in modo da non avere latenze o rallentamenti e la distribuzione del carico di risorse è in capo alla DA.

2.3.6. Gestione Server dedicati alla posta HCL Domino 11 e annessi

La DA deve gestire il server di posta, nonché tutti i database di posta e applicativi associati ad esso.
La DA deve verificare il corretto funzionamento della posta e delle policy di autorizzazione di accesso secondo organigramma aziendale. Gestire gli archivi di posta, le regole di SPAM e
La DA ha il dovere di creare nuove utenze su richiesta della SA tramite apposita richiesta su Help Desk

2.3.7. Server Active Directory

La DA dovrà gestire le Active Directory con i seguenti servizi configurati:

- Gestione dellaforesta;
- gestione del dominio;
- Gestione Infrastruttura DNS per supportare Active Directory;
- Gestioni diunità organizzative:
- Gestioni policy aziendali

Il server dovrà essere replicato in ambiente DR e nel server di replica.

2.3.8. Server con programmi gestiti da terzi fornitori

La DA dovrà tenere sempre aggiornati server virtuali e tenerli costantemente monitorati e sotto controllo, garantire la completa compatibilità dei software di altri fornitori e lavorare con loro in caso di necessità.
Compito della DA di eseguire regolarmente una pulizia del computer, correggere bug.
In caso di problematica la DA dovrà collaborare con i fornitori e seguire le indicazioni per migliorare le performance.
La SA e le aziende fornitrici dei software dovranno poter accedere al server dedicati per la manutenzione del programma.

Tutti i server dovranno essere replicati in ambiente DR e nel server di replica.

2.3.9. Server di servizi

Compito della DA sarà di aggiornare e rendere performanti i server virtuali inoltre gestire, implementare, modificare e cancellare su richiesta della SA i servizi di VPN, flussi SFTP e stampanti.
Tutti i server dovranno essere replicati in ambiente DR e nel server di replica.

2.3.10. Gestione VmWare

La DA dovrà gestire tutto l'ambiente virtualizzato tramite il software VmWare installato nei 3 server fisici oggetto del bando,
Per quanto riguarda l'installazione la DA dovrà attenersi alle linee guida del programma VmWare disponibili direttamente nel sito del produttore o all'assistenza del prodotto.
Tutti i server dovranno essere replicati in ambiente DR e nel server di replica.

2.3.11. Gestione dei servizi

La DA dovràdovrà configurare, gestire e aggiungere e modificare per tutta la durata del contratto i servizi DNS, NAT, SFTP, Domini, certificati vari, domain controller, active directory, file server, driver di stampanti, policy ed in generale tutti i servizi necessari per il funzionamento della infrastruttura.
Tutti i server dovranno essere replicati in ambiente DR e nel server di replica.

La DA dovrà gestire, mantenere e aggiornare la gestione dei servizi.

2.3.12. Gestione sistemistica del software

La DA dovrà eseguire le seguenti operazioni per tutta la durata del contratto

- installazione dei prodotti software (es. fix, hot patch e/o service pack, patch, driver, aggiornamento del software standard e dei sistemi/ambienti operativi, ecc …), sia a titolo preventivo che come soluzione di malfunzionamenti riscontrati;
- configurazione dei prodotti hardware, software di base e di ambiente;
- attività di gestione dei sistemi operativi, dei prodotti software e delle basi dati;
- gestione utenze (utenti e gruppi) e controllo accessi/autorizzazioni (MS Active Directory);
- supporto ottimizzazione politiche di backup;
- servizi per la rete;
- definizione e formalizzazione di tutte le procedure operative;
- eventuale installazione, configurazione ed ottimizzazione del sistema operativo e del software d'ambiente (es. DB Server, software di virtualizzazione);
- configurazione dei parametri di sistema (partizioni, istanze, storage, RAM, CPU, etc.) per l'ambiente di test e di produzione dei DB Server;
- realizzazione della connettività alla rete ed erogazione di servizi a valore aggiunto, quali il monitoraggio ed il backup centralizzato;
- supporto infrastrutturale, inclusa la consulenza sistemistica per l'ottimizzazione dei sistemi software installati (MySQLServer);

- gestione dei malfunzionamenti, dal supporto Service Desk fino alla manutenzione tramite i contratti già in essere;

2.3.13. Realizzazione di idonee misure di sicurezza per garantire l'integrità dei dati in esercizio.Supporto specialistico

La DA dovrà farsi carico di tutte le attività volte a garantire la massima efficienza e disponibilità delle infrastrutture di elaborazione, garantendo il supporto specialistico sui server a fronte di problematiche hardware e software. Il supporto ha l'obiettivo di analizzare e risolvere problemi di particolare rilevanza. Il servizio dovrà essere organizzato in modalità tale da prevedere come minimo la seguente lista di attività:

- installazione e configurazione dei componenti hardware necessari all'espletamento dei servizi;
- installazione e configurazione di sistemi operativi (di seguito anche "SO");
- installare di software database (di seguito anche "DB") (ad esempio Oracle, Sql Server);
- analisi dell'utilizzo dei server e fornitura di report per permettere interventi di bilanciamento dei carichi e/o di incremento delle componenti;
- ottimizzazione di SO e DB per migliorarne le prestazioni;
- gestione e manutenzione ordinaria e straordinaria di SO e DB;
- gestione di modifiche temporanee alle schedulazioni elaborative seguendo le indicazioni comunicate da SA di volta in volta;
- ottimizzazione dello spazio su memoria di massa e ripristino dei dati in caso di guasto;
- definizione e preparazione di procedure e standard d'allocazione degli archivi;
- monitoraggio costante di parametri significativi e fornitura di informazioni alla SA sullo stato dei sistemi tramite rapporti periodici, al fine di garantire la qualità del Servizio.

2.3.14. Gestione Antivirus e tecnologie di sicurezza

Si richiede la fornitura, gestione e manutenzione dell'Antivirus fornito dalla DA e altro software utilizzato ai fine della sicurezza logica, sia per la gestione centralizzata che nell'installazione, gestione, manutenzione sui client e sui server. Inoltre, l'attività riguarderà gli aggiornamenti ed adeguamenti all'eventuale mutato e crescente numero delle postazioni di lavoro. La DA dovrà collaborare con i fornitori di software per la sicurezza, per quanto riguarda necessità di upgrade, migrazioni a nuovi sistemi (installazione su server e client, etc.), nonché configurando ad hoc gli strumenti di prevenzione, dovrà esaminare proattivamente eventuali minacce e rischi in corso, anche analizzando le statistiche fornite dai software sulla sicurezza.
L'antivirus deve essere capace di fare da inventario info

2.3.15. Attivazione, gestione, conservazione e manutenzione della documentazione e del database dei componenti e degli interventi

La DA dovrà definire il processo per garantire il costante mantenimento ed aggiornamento delle informazioni relative all'installato, gestire le garanzie relative ai componenti hardware e gestire le licenze relative al software.
L'Azienda si riserva il diritto di effettuare verifiche a campione in merito all'attendibilità e all'aggiornamento del DB, dell'infrastruttura tecnologica/sistema centrale: server, periferiche, software di base e di ambiente, software applicativo ed in generale di tutte le apparecchiature ed i prodotti utilizzati dalla DA per l'erogazione dei servizi oggetto del contratto; gli utenti autorizzati dall'Azienda dovranno poter accedere a queste informazioni con modalità in linea e con la possibilità di prelevare le informazioni

contenute per un eventuale operazione fuori linea. Il CMDB (Configuration Management Data Base) ed eventuali licenze, al termine dell'appalto, dovranno essere trasferiti alla SA in un formato leggibile.

2.3.16. Conduzione operativa dei server

La gestione operativa dei Server consiste nel presidio e controllo continuativo dei sistemi al fine di garantirne il funzionamento secondo quanto previsto nei livelli di servizio, ed include il supporto nella risoluzione di eventuali problemi operativi, con attività tra cui:

- installazione/sostituzione dei componenti hardware, software e firmware, assicurandone il corretto funzionamento;
- interazione con il servizio di manutenzione hardware;
- personalizzazione ed aggiornamento della configurazione dei server quando opportuno mediante manutenzione ordinaria e straordinaria programmata, installando le modifiche e gli aggiornamenti necessari o richiesti, e mantenendoli allineati con gli aggiornamenti di sicurezza consigliati dai costruttori;
- definizione e realizzazione delle modifiche all'architettura delle risorse hardware e software e delle personalizzazioni necessarie all'integrazione di altri prodotti software e per l'esercizio delle applicazioni;
- installazione, personalizzazione, distribuzione, manutenzione e test del sistema operativo, dei sottosistemi e dei prodotti middleware (Application Server, sw virtualizzazione,ecc.);
- definizione ed attuazione delle procedure di automazione operativa (accensione e spegnimento, produzione di stampe, start-up dei collegamenti, ecc.);
- configurazione, erogazione e monitoraggio dei servizi secondo le modalità e regole indicate da SA;
- gestione dei carichi di lavoro in termini di caratterizzazione delle componenti ed assegnazione delle priorità;
- pianificazione, esecuzione e controllo degli interventi di manutenzione sul software e sull'hardware (per esempio l'introduzione di patch);
- implementazione di regole (policy) all'interno degli ambienti operativi ed applicativi, atte a definire le modalità di erogazione dei Servizi;
- attività di manutenzione e di controllo associate ai database aziendali, che sono tipicamente quelle di seguito elencate:
    - Shutdown & Startup (schedulato e on demand);
    - Backup & Restore (schedulato e on demand);
    - Import & Export (schedulato e on demand);
    - attività di monitoraggio delle performance;
    - attività di ripristino in caso di errore;
    - attività per l'upgrade a nuove release;
    - gestione delle attività schedulate (pianificazione di job e lettura dei log di esecuzione).

2.3.17. Monitoraggio automatico dei sistemi e dei servizi applicativi

La DA dovrà mettere in atto un sistema di monitoraggio, anche automatico dei sistemi server ed anche dei servizi applicativi installati sui sistemi server (fisici e virtuali).
Il monitoraggio dovrà operare da remoto ed essere in grado di chiamare un servizio di reperibilità su urgenza della DA e della SA in modo da garantire la continuità operativa.
Il monitoraggio, a fronte di situazioni critiche dovrà essere in grado di avvisare (via sms e/o chiamata telefonica su cellulare e/o mail) il responsabile del Presidio EDP della SA.

Il monitoraggio terrà sotto controllo:

- i principali parametri operativi dei sistemi server;
- la disponibilità delle risorse (ad esempio lo spazio disponibile per i DB e per il File System con diversi livelli di soglia);
- la disponibilità di istanze di DB;
- la funzionalità dei servizi applicativi sulla base di parametri (processi, informazioni di log, …) documentati dai fornitori del software applicativo;
- anomalie hardware dei server;
- spazio disco in esaurimento.

Il monitoraggio innescherà l'emissione e la gestione di allarmi:

- derivanti dalla rilevazione di anomalie;
- derivanti dal superamento di soglie di indicatori rappresentativi del servizio (monitoraggio delle prestazioni).

La SA valuta come **caratteristica migliorativa** la fornitura di un applicativo che consenta alla SGR il monitoraggio dei servizi principali dei server, delle linee dati e internet e dell'hardware in generale, con possibilità di implementare anche autonomamente altri servizi.

2.3.18. Analisi del carico dei Sistemi e monitoraggio delle prestazioni

la DA dovrà mantenere le prestazioni dei sistemi, controllando, misurando ed analizzando le prestazioni dei server (ad esempio in termini di occupazione di RAM, di occupazione di spazio disco a diverse soglie, di consumo di CPU, di swap su disco, etc.) e fornendo rapporti per la determinazione di eventuali interventi preventivi al fine di garantire i livelli di servizio.
La DA dovrà comunicare per tempo ai referenti SA del servizio eventuali necessità di adeguamento/aggiornamento HW e/o SW dei Sistemi tali da consentire la corretta continuità dei servizi erogati, come ad esempio in presenza di ampliamenti applicativi o di incremento delle utenze che potrebbero comportare anche adeguamenti HW.

2.3.19. Gestione degli incidenti, assistenza tecnica e manutenzione correttiva

La DA, a seguito della rilevazione di malfunzionamenti hardware o software o incidenti di sicurezza, dovrà operare per la risoluzione delle problematiche riscontrate.
Le attività comprendono gli interventi su tutti i componenti hardware e software (di base e d'ambiente) dei sistemi e relativi accessori che per qualsivoglia ragione dovessero guastarsi o presentare anomalie di funzionamento.
Più in dettaglio le attività possono riassumersi in:

- risoluzione della causa del guasto tramite sostituzione di parti sulla base dello scambio e/o tarature elettroniche, meccaniche o software finalizzate al recupero delle prestazioni iniziali dell'apparecchiatura;
- ripristino del servizio sui livelli preesistenti al guasto/anomalia;
- collaudo del sistema in tutte le sue funzionalità per verificare l'avvenuta eliminazione della causa del guasto/anomalia;
- ripristino della funzionalità del sistema attraverso sostituzione momentanea con un proprio apparato equivalente, in caso d'impossibilità a garantire la riparazione/manutenzione (ad esempio per indisponibilità delle parti di ricambio);
- attivazione, se necessario, delle ditte fornitrici con le quali la DA ha in atto contratti di manutenzione;

- attivazione, se necessario, e gestione delle ditte fornitrici con le quali la DA ha in essere clausole contrattuali di garanzia o d'intervento;
- attivazione, se il caso, delle ditte fornitrici con le quali SA la ha in essere clausole contrattuali di garanzia o di intervento. La DA opera in collaborazione con le suddette ditte fornendo tutto il supporto necessario al fine di risolvere prontamente il problema.

La gestione degli incidenti è tracciata attraverso le modalità e lo strumento di trouble ticketing messo a disposizione dal servizio di Help Desk (vedere il file Capitolato Tecnico paragrafo 2.4 Help Desk di assistenza tecnica "all inclusive".

2.3.20. Servizio di Distribuzione del Software

Al fine di garantire la corretta gestione del parco software installato, sia esso software di base che di ambiente, quando necessario la DA dovrà provvedere alla distribuzione o all'aggiornamento dei programmi (compreso l'aggiornamento di patch e firmware).
Si specifica che per tutta la durata contratto la DA dovrà su richiesta della SA installare, aggiornare e disinstallare anche tutti i programmi rilasciati in ambiente citrix e dei programmi installati nei "Server Applicativi" e "Server di servizi". Inoltre, la DA deve descrivere come intende:

- effettuare un'analisi delle patch presenti sulla postazione di lavoro e indicare la presenza di patch datate nonché l'opportunità di installare patch di aggiornamento;
- acquisire da remoto il controllo della postazione di lavoro sulla quale è necessario intervenire;
- installare e configurare da remoto sulla postazione di lavoro sistemi operativi (upgrade di release, service pack, ecc …) e applicazioni software (es. antivirus, hotfix, security patch, virus pattern...);
- effettuare la distribuzione di applicazioni e pacchetti software attraverso l'infrastruttura di rete;
- aggiornare periodicamente o su richiesta della SA i vari applicativi/software installati con le nuove release.

In caso di acquisto di nuovo software da parte della SA, la DA dovrà innanzitutto verificarne la compatibilità con l'infrastruttura informatica e una volta verificata la fattibilità la DA dovrà installare il software in ambiente citrix o in un server virtuale in base alle esigenze della SA. Questo servizio di installazione, aggiornamento o disinstallazione sarà richiesto dalla SA tramite apposita richiesta di Help Desk (vedere il file Capitolato Tecnico paragrafo 2.4 Help Desk di assistenza tecnica "all inclusive"=.

2.3.21. Manutenzione ed estensione garanzia hardware

La DA dovrà per tutta la durata del contratto estendere la garanzia e la relativa manutenzione in modalità 7x24 su tutte le apparecchiature hardware del bando. In caso di guasto la DA sarà parte attiva con l'assistenza tecnica.
Per Manutenzione ed estensione di garanzia hardware si intendono i rinnovi della manutenzione da parte dei produttori e la relativa sostituzione in caso di guasto con reperibilità 7 giorni / 24 ore.
La DA dovrà fornire l'assistenza al produttore e rendersi parte attiva nel processo di ripristino della anomalia.

2.3.22. Gestione politica di backup

La DA deve gestire i backup in autonomia e predisporre il metodo di salvataggio.
In caso di fallimento del backup la DA è tenuta ad inviare una email di spiegazione del problema e della sistemazione dell'anomalia e nel caso in cui il fallimento del backup fosse quello relativo al

backup settimanale o backup mensile o backup annuale, il backup deve essere schedulato per il giorno successivo.
La SA potrà in qualsiasi momento chiedere alla DA, tramite l'apposito strumento di Help Desk di effettuare i restore.
La DA deve inoltre consegnare alla SA un rapporto quotidiano degli esiti del backup e restore tramite email e a fine anno la DA fornire alla SA un file di log complessivo di tutti backup e restore per poterlo consegnare alle autorità di Vigilanza.
In qualsiasi momento i backup possono essere visionati dalla SA e dalle autorità di Vigilanza.

2.3.23. Gestione Sala Server di Disaster Recovery

Per tutta la durata del contratto la DA deve garantire e gestire la messa disposizione della Sala Server di DR, con condizionatore, UPS, un armadio Rack, linea dati e spazio di archiviazione per backup. La DA deve garantire la sicurezza degli accessi alla sala server tenendo traccia degli accessi alla sala. è richiesto il presidio on-site di almeno una persona del team di progetto, vedasi capitolo 2.6 Team di progetto.
La Sala Server di DR deve avere sempre una temperatura costante e controllata automaticamente da un condizionatore.
La DA deve provvedere per tutta la durata del contratto alla messa disposizione di una linea internet 100/20, all'impianto di illuminazione e alla corrente elettrica.
La DA deve provvedere alla gestione dei backup del server di DR posizionato all'interno della sala Server di DR, la DA deve mettere a disposizione uno spazio di 8 Tb dedicato ai backup.
A richiesta la SA, Audit esterno e Organi di Vigilanza hanno il diritto di accedere alla sala Server della DA.
Si specifica che tutti costi di gestione della sala, contratto luce, linea internet, messa disposizione di un armadio Rack, aria condizionata, UPS e spazio per backup in caso di DR sono a carico della DA per tutta la durata del contratto, rinnovo e proroga.

2.4 Help Desk di assistenza tecnica "all inclusive"

Si specifica che in questo capitolo si richiedono servizi di esecuzione continuativa - per le modalità di pagamento si rinvia a quanto disposto nel "Capitolato speciale d'appalto per servizi".

Per servizio di Help Desk si intende la disponibilità di un punto di accesso unico per raccogliere richieste di intervento dell'utenza finale, in merito a qualsiasi elemento facente parte del perimetro oggetto del servizio. Dovrà essere fornito a tutti gli utenti interni del sistema informatico dell'Azienda, un supporto per la soluzione dei problemi relativi all'utilizzo delle postazioni di lavoro (hardware, software di base e software applicativo), dell'infrastruttura informatica (LAN, Server, ecc …), del portale e della intranet dei servizi aziendali.

Il servizio di Help Desk ha l'obiettivo di accogliere richieste sia in merito a segnalazioni di problemi sistemistici che in merito a richieste per il supporto all'utilizzo di una componente applicativa del Sistema Informativo Aziendale.
La DA dovrà a tal fine assicurare un servizio di Help Desk, logicamente distinto tra primo e secondo livello, che costituisca per gli utenti, un unico punto di accesso ed un insieme di funzioni di assistenza riguardanti l'uso delle piattaforme tecnologiche informatiche.
Con Help Desk di primo livello si intende il front-end del servizio organizzato dalla DA che opererà come punto di contatto centralizzato per le chiamate degli utenti, mentre quello di secondo livello avrà funzione di back office.
L'organizzazione proposta dalla DA dovrà prevedere una struttura che riceverà tutte le richieste di supporto secondo le modalità di seguito descritte:

- ricezione delle segnalazioni presso un unico punto di contatto; le segnalazioni richieste potranno pervenire attraverso un accesso telefonico, e-mail, web, intranet, ecc.; potranno essere attivati interventi anche a seguito di comunicazione diretta da parte del personale interno referente per il servizio;
- apertura di un ticket a fronte della chiamata ricevuta ed inserimento in un apposito strumento di trouble ticketing management con assegnazione in automatico di un codice identificativo univoco di tipo numerico/alfanumerico e contenente almeno le seguenti informazioni:
    - data (anno, giorno, ora, minuti) di ricezione della richiesta;
    - unità operativa (centro di costo) e soggetto che ha richiesto l'intervento;
    - modalità di ricezione;
    - azione avviata (risoluzione, smistamento ad altra struttura o rigettato perché non di competenza);
    - nel caso di presa in carico della richiesta verranno indicate una descrizione del problema, la gravità, e la priorità assegnata all'intervento;
    - una breve descrizione della modalità d'intervento;
    - una stima del tempo di chiusura.
- diagnosi della richiesta di supporto pervenuta ed identificazione del problema;
- risoluzione del problema in sede di prima chiamata oppure gestione della procedura di escalation con attivazione e coordinamento di risorse di secondo livello idonee alla soluzione del problema, al fine di fornire la soluzione all'utente nel più breve tempo possibile e comunque nei livelli di servizio stabiliti;
- controllo dell'avanzamento delle azioni necessarie alla chiusura del ticket, anche quando l'intervento sia stato eventualmente effettuato da strutture diverse da quelle della DA;
- verifica con chi ha emesso la segnalazione della risoluzione di quanto segnalato e conseguente notifica della chiusura del ticket, riportando almeno le seguenti informazioni:
    - descrizione dell'intervento attivato;
    - data (anno, giorno, ora, minuti) di chiusura dell'intervento;
    - impegno speso in ore / uomo per gli interventi effettuati.

L'organizzazione proposta dalla DAdovrà prevedere:

- la completa responsabilità della gestione e della chiusura dei ticket, nei confronti dell'utente, da parte dell'Help Desk di primo livello;
- la gestione di tutto ciò che riguarda le richieste di intervento per modifiche all'assetto dei sistemi informatici di un qualunque tipo e natura (ad esempio l'installazione di un nuovo posto di lavoro o di un suo componente, modifica della configurazione di rete, etc.);
- lo strumento di trouble ticketing sarà a carico dell'aggiudicatario e dovrà essere accessibile tramite web;

- il servizio di Help Desk dovrà essere dislocato in termini di risorse professionali ed infrastrutture presso locali e strutture della DA;
- il personale dell'Help Desk di primo livello è tenuto alla risoluzione delle problematiche più comuni e quelle di non elevata complessità, riguardanti gli applicativi aziendali maggiormente diffusi (office automation, posta, internet, etc …); perciò il personale per il servizio di Help Desk dovrà possedere le conoscenze necessarie al funzionamento delle postazioni di lavoro in uso presso l'Azienda e dei prodotti software installati su tali postazioni di lavoro, nonché dell'ambiente applicativo dell'Azienda;
- il controllo della qualità del servizio fornito, attraverso l'analisi delle chiamate gestite nel periodo di riferimento, al fine di identificare i fabbisogni e definire azioni di prevenzione dei problemi;
- la produzione di reportistica su base periodica da definire con l'Azienda relativa ai servizi resi ed ai relativi livelli di servizio conseguiti (es. numero di interventi nel periodo di osservazione per centro di costo, durata degli interventi per centro di costo, distribuzione dei problemi per gravità e priorità d'intervento, per modalità d'intervento, durata media degli interventi);
- i referenti della DA ' dovranno essere in grado, in qualsiasi momento, di verificare lo stato di qualsiasi chiamata, e di garantirne la gestione secondo le modalità sopra descritte.

La SA valuta come **caratteristica migliorativa** la possibilità da parte della SA di utilizzare un software per la gestione di ticket interni al fine di raccogliere internamente le richieste da inoltrare alla DA.

È onere della DA rendicontare le attività di Help Desk con periodicità semestrale mediante una Relazione sul Servizio descrittiva delle attività gestite e dei livelli di servizio garantiti.

Le attività di help desk dovranno essere garantite secondo le modalità suddette dal lunedì al venerdì dalle ore 8:30 alle 17:30.

2.5 Monitoraggio di sistemi e servizi e delle linee dati

Si specifica che in questo capitolo si richiedono servizi di esecuzione continuativa - per le modalità di pagamento si rinvia a quanto disposto nel Capitolato speciale d'appalto per servizi".
Nei giorni dal lunedì al venerdì nella fascia orario 8:30 – 17:30 la DA dovrà garantire un servizio di monitoraggio dei sistemi e servizi, di teleassistenza per estendere la copertura oraria dei servizi di Presidio on site.
Dovrà, inoltre, essere garantito un servizio di reperibilità anche nei giorni festivi, per qualunque urgenza che si dovesse verificare sui sistemi del Data Center e/o sulla rete e che potrebbero compromettere i servizi critici comprensivo di intervento on site entro 2 ore dalla chiamata. L'intervento potrà, se la situazione lo permette, essere effettuato anche da remoto ove risolutivo.
Per ciascuno dei servizi la DA deve specificare gli elementi caratteristici al fine di una loro valutazione.

Il servizio deve permettere, inoltre, il monitoraggio delle performance dell'intera infrastruttura di rete e delle linee dati, con lo scopo di individuare e segnalare tempestivamente i malfunzionamenti e di identificare preventivamente gli eventi che possono rappresentare una causa di potenziale malfunzionamento.
Il servizio dovrà prevedere l'impiego di un sistema di monitoraggio di tutte le componenti di rete a carico della DA e dovrà essere messa a diposizione internamente all'unità aziendale competente della SGR.
La piattaforma di monitoraggio e gestione dovrà garantire funzionalità minimali per:

- interrogare ciclicamente gli elementi gestiti per verificarne lo stato di funzionamento;

- ricevere allarmi generati a seguito di malfunzionamenti hardware e/o software;
- permettere la classificazione degli allarmi ricevuti in funzione della gravità;
- effettuare attività predefinite a seguito del verificarsi di eventi codificati.

La piattaforma di monitoraggio e gestione dovrà essere in grado di:

- raccogliere periodicamente le informazioni sul traffico di rete (rete locale e connessioni geografiche);
- rendere disponibili sotto forma di grafico su periodi selezionabili (ore, giorni, settimane, mesi) le informazioni del traffico di rete raccolte.

È onere della DA rendicontare le prestazioni della rete con periodicità annuale mediante un Relazione sulle Performance di Rete descrittiva delle prestazioni delle risorse monitorate, descrivendo gli interventi di ottimizzazione effettuati o che si propone di effettuare per il miglioramento complessivo delle prestazioni.
Il set di indicatori oggetto del monitoraggio deve essere definito nell'offerta tecnica e potrà essere integrato con ulteriori indicatori su richiesta della stazione appaltante.

In occasione di interventi di manutenzione straordinaria del sistema informatico le attività dovranno essere garantite anche di sabato e nei giorni festivi, in orari da concordare con la SA.

Le attività di monitoraggio dovranno essere garantite secondo le modalità suddette dal lunedì al venerdì dalle ore 8:30 alle 17:30.

2.6 Team di progetto

in riferimento all'oggetto e agli obbiettivi dell'appalto cosi come specificati nei paragrafi che precedono, la scrivente SA ha individuato nelle seguenti figure professionali ila composizione del team di progetto che dovrà assicurare il corretto svolgimento del servizio e della fornitura dell'infrastruttura informatica richiesta.
In particolare si richiede la seguente composizione minima di collaboratori/trici assegnati/e alla corretta esecuzione dell'appalto:

n. 1 Project Manager esperto in sicurezza e firewall
n. 1 Sistemista Senior esperto in citrix, virtualizzazioni e windows
n. 1 Sistemista Senior esperto in sistemi operativi
n. 1 Sistemista Senior esperto in networking
n. 1 Sistemista Junior networking

3. Opzione dell'appalto (assistenza sistemistica o analisi a richiesta)

Sono richieste totale massimo di 150 ore di assistenza tecnica a richiesta.
Il servizio di assistenza sistemistica, analisi programmazione SQL, java a richiesta ha la principale funzione di integrare e di specializzare quanto previsto per mezzo dell'attività di conduzione

sistemistica a presidio. L'integrazione si rende utile per lo svolgimento delle seguenti tipologie di attività:
attività non continuative, sporadiche ed in emergenza che richiedo un "effort" lavorativo superiore alle oggettive possibilità del gruppo che effettua il Presidio on site; attività di tipo specialistico inerenti all'attuazione di nuovi progetti o evoluzione di servizi esistenti; inserimento di linee di attività che prevedano l'utilizzo di prodotti per i quali allo stato attuale non siano previste le relative professionalità; analisi di efficientamento per migliorare i processi o l'operatività della SA; lavori a richiesta in sala server sviluppo software.
Per questo servizio le risorse verranno attivate su specifica richiesta dell'Azienda entro i 7 giorni solari successivi dalla data della comunicazione alla DA.
Nella comunicazione di cui sopra verranno indicati di volta in volta i profili necessari e il loro impegno temporale.
Si precisa che la SA sarà tenuta al pagamento dell'importo relativo alle sole ore utilizzate all'interno del pacchetto di ore.

4. Attuale consistenza del sistema informatico della SA hardware-software e linee

La consistenza del Sistema Informatico della SA è descritta nei paragrafi successivi. L'aggiudicatario dovrà garantire i servizi dettagliati nei paragrafi precedenti sull'intero sistema informatico nell'attuale configurazione e sulle sue evoluzioni durante il periodo contrattuale.
Si richiede in generale di installare le ultime versioni di software e di tenerle per la durata del contratto aggiornate

4.1 Postazioni di lavoro

Per postazioni di lavoro si intendono i personal computer (nella tipologia desktop, notebook, tablet e Thinkclient) completi delle periferiche quali video, stampante, scanner.

SISTEMA OPERATIVO	PC (Desktop)	Portatili
Windows 10 Pro	8	8
Windows 7 Pro	1	0
ThinkClient Praim	28	0
Totale	**37**	**5**

4.2 Attuali Server virtuali

Nome server	Sistema Operativo	Servizio
PPI-Artica	Other 2.6.x Linux (64-bit)	
PPI-Artica1	Other 2.6.x Linux (64-bit)	
PPI-CTXPVS01	Microsoft Windows Server 2008 R2 (64-bit)	Server Provisioning

Nome server	Sistema Operativo	Servizio
PPI-CTXPVS02	Microsoft Windows Server 2008 R2 (64-bit)	Server Provisioning
PPI-CTXPVS03	Microsoft Windows Server 2008 R2 (64-bit)	Server Provisioning
PPI-CTXWEB01	Microsoft Windows Server 2008 R2 (64-bit)	Portale Web citrix
PPI-CTXWEB02	Microsoft Windows Server 2008 R2 (64-bit)	Portale Web citrix
PPI-DC01	Microsoft Windows Server 2008 R2 (64-bit)	Server Domain Controller
PPI-DC02	Microsoft Windows Server 2008 R2 (64-bit)	Server Domain Controller
PPI-DOMINO01	Microsoft Windows Server 2008 R2 (64-bit)	Server Domino (posta) e servizi SFTP
PPI-DOMINO02	SUSE Linux Enterprise 11 (64-bit)	Server Domino (posta)
PPI-FS00	Microsoft Windows Server 2008 R2 (64-bit)	Server Active Directory
PPI-FS01	Microsoft Windows Server 2008 R2 (64-bit)	Server Active Directory
PPI-FS02	Microsoft Windows Server 2008 R2 (64-bit)	Server Active Directory
PPI-JDOC	Microsoft Windows Server 2008 R2 (64-bit)	Server sw Documentale fornitore esterno
PPI-Master	Microsoft Windows Server 2008 R2 (64-bit)	Server immagine Citrix
PPI-PRESENZE	Microsoft Windows Server 2008 R2 (64-bit)	Server SW cartellino presenze
PPI-PRINT01	Microsoft Windows Server 2008 R2 (64-bit)	Server Stampanti
PPI-AUTHPOINT	Microsoft Windows Server 2018 R2 (64-bit)	Server autenticazione VPN
PPI-Proxy	Other 2.6.x Linux (64-bit)	Server Proxy
PPI-PSQL	Debian GNU/Linux 6 (64-bit)	Server farm Citrix
PPI-RENDICONTO	Microsoft Windows Server 2008 R2 (64-bit)	Server SW Rendiconto.NET con SQL
PPI-SAMETIME	Microsoft Windows Server 2008 R2 (64-bit)	Server chat Domino
PPI-SQL01	Microsoft Windows Server 2008 R2 (64-bit)	Server SQL citrix
PPI-traveler	SUSE Linux Enterprise 11 (64-bit)	Server posta App dispositivi
PPI-XENAPP0	Microsoft Windows Server 2008 R2 (64-bit)	Server Console farm citrix
PPI-XENAPP18	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix

Nome server	Sistema Operativo	Servizio
PPI-XENAPP20-Mnt	Microsoft Windows Server 2008 R2 (64-bit)	Server management citrix
PPI-XENAPP21-Test	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix di test
PPI-XENAPP22	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix
PPI-XENAPP23	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix
PPI-XENAPP24	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix
PPI-XENAPP25	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix
PPI-XENAPP26	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix
PPI-XENAPP27	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix
PPI-XENAPP28	Microsoft Windows Server 2008 R2 (64-bit)	Server farm citrix

4.3 Software distribuito in Citrix tramite Active Directory

Software	Descrizione	Di proprietà	Installati	In affitto
Adobe Writer	10	X		
Adobe cloud	Ultima versione			X
Ms Office 2019 Professional Plus 2019 OLP government	Excel, Word, PowerPoint, Access X64 U.V.	X		X
IBM Lotus Notes	Lotus versione 8.5.3			X
7 ZIP	7-ZIP 18.05 X64		X	
BASECAMP 3	Ultima versione			X
DIKE 6	Ultima versione		X	
ACROBAT READER DC	Ultima versione		X	
ARUBA SIGN	Ultima versione		X	
FILEZILLA FTP	Ultima versione		X	
FIREFOX	Ultima versione		X	
FIRMA OK	Ultima versione		X	
FOXIT READER	Ultima versione		X	
GANTT PROJECT	Ultima versione		X	
GOOGLE CHROME	Ultima versione		X	
IDLE PHYTON	3.5 X64		X	
LibreOfficePortable_6.2.2_MultilingualAll			X	

Software	Descrizione	Di proprietà	Installati	In affitto
NOTEPAD ++	Ultima versione		X	
Ms Office 2019 Professional Plus	2019	X		
OCTAVE	Ultima versione		X	
PDF SPLIT AND MERGE	2.2.4		X	
PDF CREATOR	1.6.1		X	
PSAICK	Ultima versione		X	
R	Ultima versione		X	
RAP.NET	4.3.48	X		
RENDICONTO		X		
R-STUDIO	Ultima versione		X	
SAFEGUARD PRIVATCRYPTO			X	
STATPRO REVOLUTION				X
THINKCELL componente in MS Excel	Ultima versione			X
TRADEWEB			X	
TRELLO	Ultima versione		X	
TREND OFFICESCAN				X
ULTRA VNC			X	
WINSCP	Ultima versione		X	

U.V.: Ultima versione

4.4 Attuali dispositivi di rete

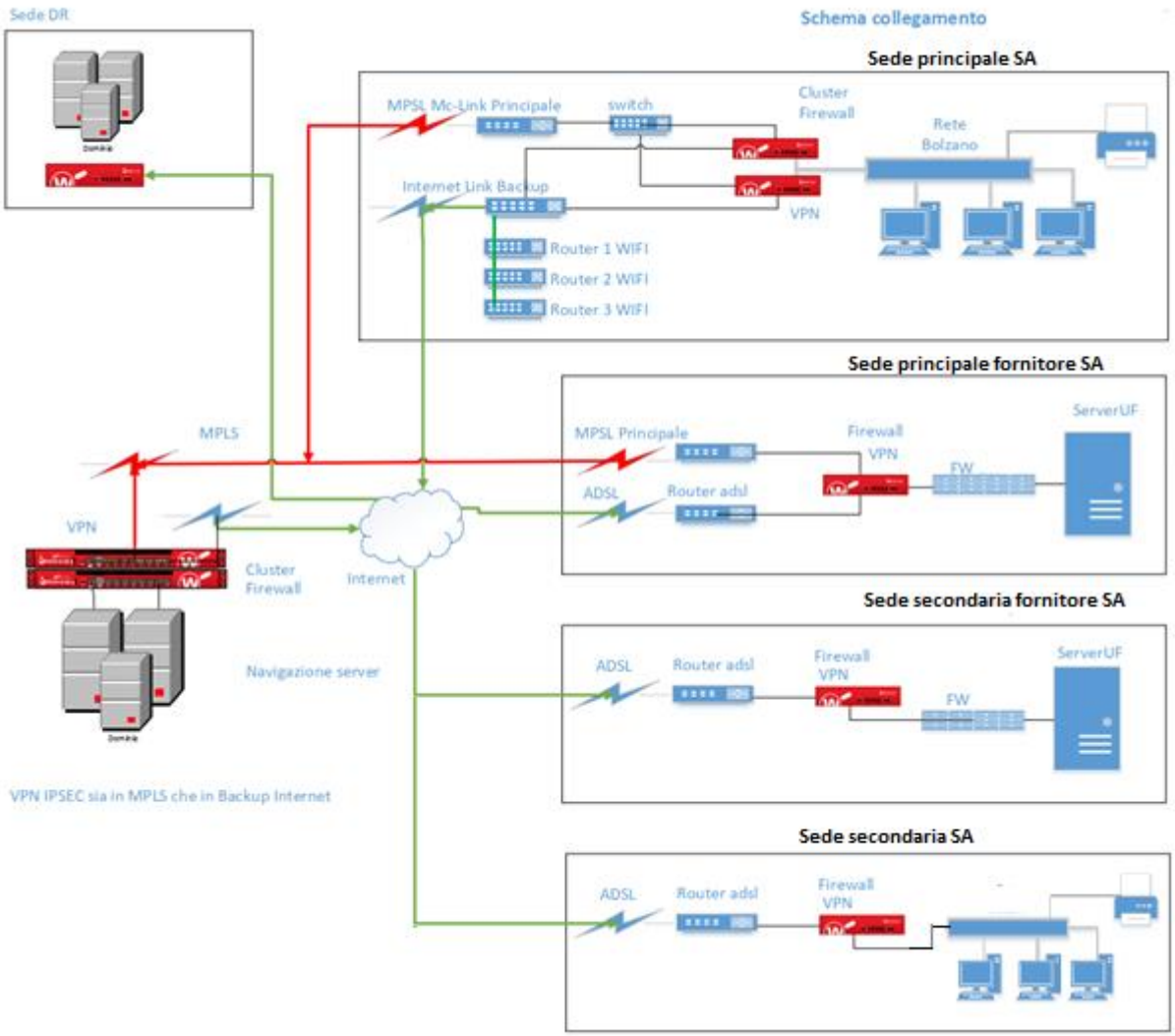
Marca e modello	Ubicazione
STAMPANTE XEROX 3330	4° Piano
STAMPANTE XEROX 3330	3° Piano
STAMPANTE XEROX 3330	3° Piano
STAMPANTE XEROX C8055	1° Piano
STAMPANTE RICOH C3001	1° Piano
STAMPANTE ZDESIGNER	3° Piano
STAMPANTE ZDESIGNER	3° Piano
SWITCH 48	Sala server SA
SWITCH 48	Sala server SA
FIREWALL	Sala server SA
FIREWALL	Sala server SA
ROUTER WIFI	Sala server SA
2 RIPETITORI WIFI	1° Piano
2 RIPETITORE WIFI	2° Piano
2 RIPETITORE WIFI	3° Piano
1 RIPETITORE WIFI	4° Piano
CENTRALINO TELEFONICO	Sala server SA
LAMA BLADE	Sala Server attuale fornitore servizi EDP
LAMA BLADE	Sala Server attuale fornitore servizi EDP
LAMA BLADE	Sala Server attuale fornitore servizi EDP

Marca e modello	Ubicazione
SAN	Sala Server attuale fornitore servizi EDP

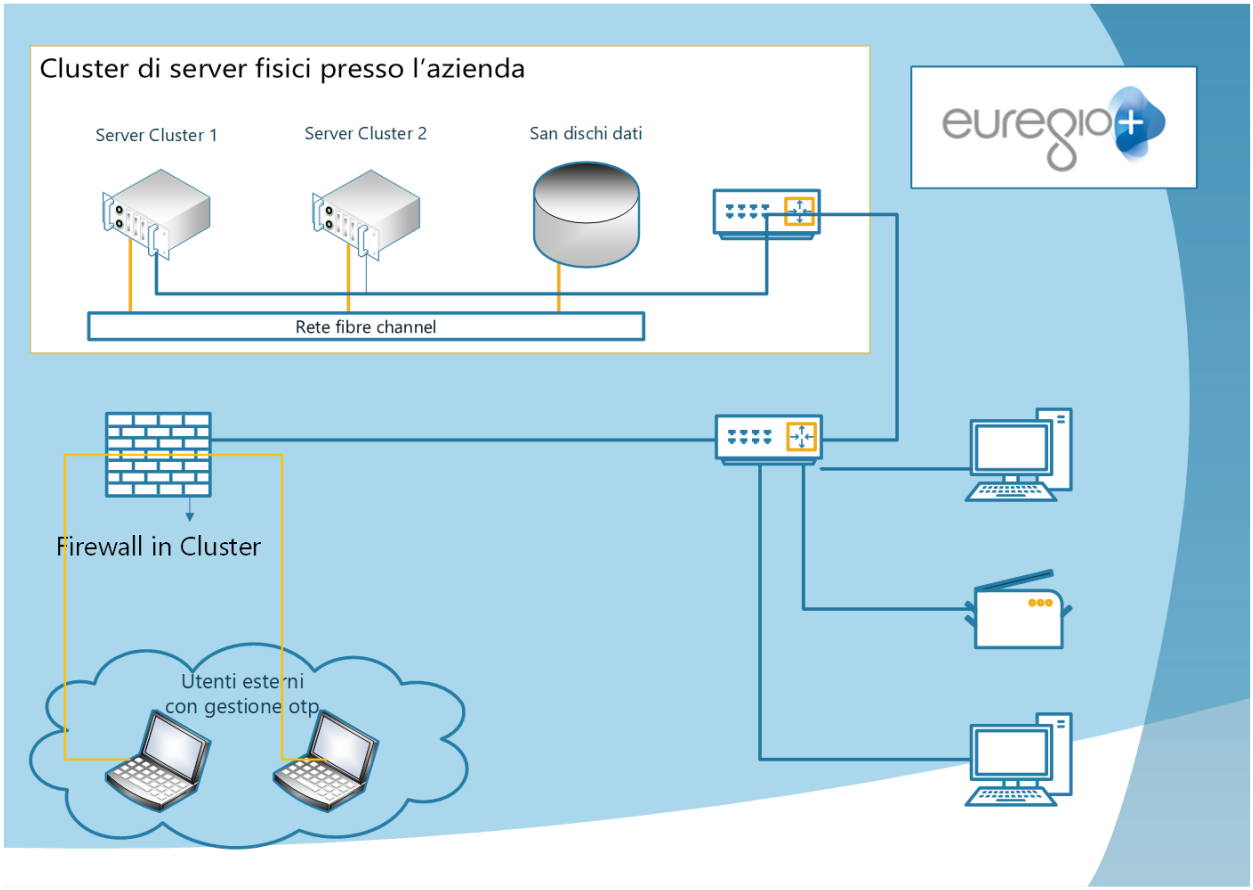
4.5 Attuali linee dati

UBICAZIONE	DESTINAZIONE	DESCRIZIONE	FORN.	TIPO	VELOCITÀ
Euregio Plus: via della Mostra 11/–3 – 39100 Bolzano	INTERNET	Accesso Internet e backup D.R. e utilizzo per accessi VPN	Fornitore 1	VDSL	Download 100 Mega – Upload 20 Mega
Euregio Plus: via della Mostra 11/–3 – 39100 Bolzano	Sala Server presso attuale outsourcer informatico	Collegamento sala server – sede SA	Fornitore 2	MPLS	Download 8 Mega – Upload 8 Mega
Sala Server presso attuale outsourcer informatico		Chiusura circuito MPLS	Fornitore 2	Consegna MPLS	Download 100 Mega – Upload 100
Sala Server presso attuale outsourcer informatico	Fornitore finanziario: via Savona 1–5 – 20144 Milano	Collegamento sala server – fornitore di servizi finanziari linea principale	Fornitore 2	MPLS	Download 4 Mega – Upload 4 Mega
Sala Server presso attuale outsourcer informatico	Fornitore finanziario: via Savona 1–5 – 20144 Milano	Collegamento sala server – fornitore di servizi finanziari linea backup	Fornitore 1	ADSL	Download 20 Mega – Upload 1 Mega
Sala Server presso attuale outsourcer informatico	Fornitore finanziario: via Darwin –5 – 20019 Settimo Milanese	Collegamento sala server – fornitore di servizi finanziari linea D.R.	Fornitore 1	ADSL	Download 20 Mega – Upload 1 Mega
INTERNET		Linea internet per backup	Fornitore 2	FIBRA	1 gigabit simmetrico
Sala Server presso attuale outsourcer informatico	INTERNET	Linea navigazione server	Fornitore 2	FIBRA	Download 100 Mega – Upload 100
Sede secondaria attuale outsourcer informatico	Sala Server presso attuale outsourcer informatico	Collegamento sala server e sede D.R.	Fornitore 2	FIBRA	Fibra Spenta 10 giga bit

4.6 Attuale schema collegamento



4.7 Schema base struttura server



WETTBEWERB ZUR VERGABE DES DIENSTES FÜR DIE ENTWICKLUNG, DEN BETRIEB UND DIE WARTUNG DES IT-SYSTEMS UND DER DATENLEITUNGEN- TECHNISCHES LEISTUNGSVERZEICHNIS VON EUREGIO PLUS SGR S.P.A. - AOV/SUA-SF 02/2021 - CODICE CIG 8950213D68

Inhaltsverzeichnis

1. Organisatorischer Kontext

1.1 Einführung

Euregio Plus SGR S.p.A./A.G. (nachstehend „SGR“, „Vergabestelle“ oder die „VS“) ist eine von Pensplan Centrum S.p.A/AG kontrollierte Kapitalanlagegesellschaft, die als In-house-Gesellschaft der Region Trentino-Südtirol und der Autonomen Provinz Bozen tätig ist. Die Gesellschaft ist im Finanzbereich, in der Verwaltung von Rentenfonds, im Immobiliensektor, in den Bereichen Private Debt, Private Equity und Venture Capital tätig. Die VS hat ihren Rechts- und Hauptsitz in Bozen, Mustergasse 11/13 und einen Zweitsitz in Trient, Via Romano Guardini 17.

1.2 Gesetzlicher Rahmen

Die VS untersteht der Aufsicht von Banca d’Italia, Consob und Covip und fällt unter die Definition eines öffentlichen Rechtssubjekts.
Die Vergabe von Aufträgen an Dritte zur Ausführung der in diesem Dokument vorgesehenen Tätigkeiten stellt eine „Auslagerung von wesentlichen oder wichtigen operativen Unternehmensfunktionen (nachstehend „Outsourcing“) dar und muss unter Einhaltung der einschlägigen Bestimmungen erfolgen, die die Übertragung von Funktionen regeln. Dazu gehören:

- die Delegierte Verordnung (EU) Nr. 231/2013 der Kommission vom 19. Dezember 2012 (nachstehend „Verordnung 2013/231“) zur Ergänzung der Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates
- die Delegierte Verordnung (EU) Nr. 565/2017 der Kommission vom 25. April 2016 (nachstehend „Verordnung 2017/565“) zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates;
- die Durchführungsverordnung zu den Artikeln 4-unidecies und 6, Abs.1, lit. b) und c-bis) des Finanzmarktgesetzes (TUF), die von der Banca d‘Italia mit der Maßnahme Nummer 1470228/19 vom 5. Dezember 2019 verabschiedet wurde (nachstehend Verordnung Banca d‘Italia);
- etwaige weitere einschlägige Gesetze.

Für den Gegenstand der Bekanntmachung gelten weiters die Vorgaben folgender Rechtsvorschriften:

- Datenschutz-Verordnung EU 2016/679 (so genannte DSGVO) mit den damit verbundenen Leitlinien des Europäischen Datenschutzausschusses (EDPB), insbesondere was Aspekte in Zusammenhang mit der Vergabe von externen Aufträgen und der Erbringung von IT-Dienstleistungen anbelangt;
- GvD Nr. 81/08 in geltender Fassung hinsichtlich Arbeitssicherheit, insbesondere in Zusammenhang mit Aspekten, die die Lieferanten betreffen (ordnungsgemäße Entrichtung der Sozialbeiträge und Risiken durch Interferenzen bei der Ausführung von Arbeiten);
- GvD Nr. 231/01 in geltender Fassung (Managementhaftung) im Bereich IT-Kriminalität.

1.3 Anforderungen an die IT-Infrastruktur

Mindestens 30 und höchstens 50 Nutzer müssen Zugang zur IT-Infrastruktur erhalten.

Derzeit beträgt der für die Datenspeicherung verwendete Massenspeicher 5 TByte (ohne PACS-System und verschiedene Dateiserver); in den letzten drei Jahren wurde eine Zunahme um etwa 1 TByte verzeichnet.

Der Zugang zur IT-Infrastruktur erfolgt über Desktop PCs, Laptops und Think Clients hauptsächlich am Hauptsitz und bei Bedarf oder im Notfall auch über VPN. Am Hauptsitz steht ein Serverraum zur Verfügung. Das IT-System weist in der aktuellen Konfiguration folgende Zusammensetzung auf:

- Arbeitsstationen (Desktop PC mit Betriebssystem Windows 10 PRO und HOME), Notebook mit Betriebssystem Windows 10 (PRO und HOME), ThinkClient von PRAIM mit Linux-basiertem, proprietärem Betriebssystem, Peripheriegeräte (Drucker, Scanner usw..), die mit der Domäne der VS verbunden sind;
- vernetzte Multifunktionsgeräte (Drucker, Kopierer, Scanner und Fax);
- technologische Infrastruktur (Server, virtuelle Server, Speicher, Basis- und Umgebungssoftware, Anwendungssoftware, Datenbanken usw.), die im Datenzentrum des aktuellen externen IT-Dienstleisters der SGR installiert ist, und andere Geräte, die im Serverraum der VS untergebracht sind;
- LAN-Netzwerk, einschließlich aktiver Geräte, passiver Komponenten und Sicherheitssysteme;
- WiFi-Netzwerk am Sitz in Bozen und in Trient mit Internetanschluss;
- Netzwerkausrüstung für die Verbindung der verschiedenen Etagen des Gebäudes (Switches);
- Sicherheitseinrichtungen (primäre und sekundäre Firewall);
- ADSL-, VDSL-Anschlussgeräte.

Die aktuelle Dimensionierung des Systems ist unter Punkt 4 “Derzeitiger Bestand des IT-Systems der VS - Hardware - Software und Datenleitungen " angegeben.
Der Auftragnehmer (nachstehend „AN“) muss die in den folgenden Absätzen beschriebenen Dienste für das gesamte IT-System, so wie es in diesem Dokument beschrieben ist, gewährleisten.
Der AN muss eine IT-Struktur einrichten, indem er die benötigte Hardware an die VS verkauft, die noch geeignete Hardware betreut, Software vermietet und verkauft.
Der Hauptsitz der VS ist über mehrere Stockwerke verteilt; die SGR hat das Recht, einen Raum im ersten Stock im Gebäude in der Mustergasse 11/13 in Bozen als Serverraum zu nutzen; dieser Raum entspricht den Sicherheitsstandards, ist mit Einbruch- und Überflutungsschutz, Klimaanlage, Leitungen, die eine unterbrechungsfreie Stromversorgung (USV) sichern, und mit einem Internet-Zugangspunkt ausgestattet. Dieser Raum wird zurzeit nur für die Netzwerktechnik und Telefonzentrale genutzt, soll aber vom Auftragnehmer als Serverraum für die VS ausgestattet werden.

Voraussetzung für den Vertragsabschluss ist die Zertifizierung nach ISO/IEC 27001:2013 – UNI CEI EN ISO/IEC 27001:2017

2. Gegenstand und Ziele der Ausschreibung

Der Gegenstand der Ausschreibung umfasst folgende Leistungen:

- Hardware-Lieferung - sofort auszuführen (in Konsignation)
- Periodische Hardwarewartung - sofort auszuführen (in Konsignation)
- Software- Lieferung - sofort auszuführen (in Konsignation)
- Software-Lieferung - kontinuierlich auszuführende Leistung gegen Servicegebühren
- Lieferung von Datenleitungen - sofort auszuführende Leistung gegen Servicegebühr
- Planung und Implementierung der IT-Infrastruktur - sofort auszuführen

- Betrieb und Wartung der technologischen Infrastruktur des Datenzentrums - kontinuierlich auszuführen

- Helpdesk für den „All-inclusive-Support - kontinuierlich auszuführen

- Überwachung der Systeme und Dienste für die Datenleitungen - kontinuierlich auszuführen

Hinsichtlich der Modalitäten der zu erbringenden Lieferungen und Leistungen (z.B. Zahlung, SLA-Vereinbarungen), wird auf das Dokument "SLA.pdf“ verwiesen.

Der Auftragnehmer (nachstehend „AN“) nimmt zur Kenntnis, dass die Aufsichtsbehörden, die Kapitalverwaltungsgesellschaft SGR, Audit EDP und ihre Rechnungsprüfer ihre Überwachungs- und Kontrolltätigkeiten durchführen können, indem sie - auch in den Räumlichkeiten des Auftragnehmers selbst - auf Informationen, Daten und alle Unterlagen zugreifen, die die Ausübung der vergabegegenständlichen Tätigkeit betreffen.

2.1 Lieferung der IT-Infrastruktur

Es wird darauf hingewiesen, dass in diesem Kapitel sofort auszuführende Lieferungen (außer unter Punkt 2.1.2) gefordert werden. Hinsichtlich der Zahlungsmodalitäten wird auf das Dokument "Sonderleistungsverzeichnis für Dienstleistungen“ verwiesen. Der Auftragnehmer muss den der VS zur Verfügung stehenden Serverraum nutzen und muss einen als Serverraum ausgestatteten Raum als Disaster-Recovery-Standort (nachstehend „DR“) zur Verfügung stellen, wie in Abschnitt 2.2.10 "Business Continuity und Disaster Recovery" festgelegt.
Der Auftragnehmer muss ein Projekt für die Server- und Netzwerkinfrastruktur vorschlagen, wobei die Dimensionierung der angebotenen Systeme auf der Grundlage der folgenden Mindestanforderungen erfolgen soll:

- Zugriff auf die IT-Infrastruktur für mindestens 30 Nutzer;
- korrekte Verteilung des RAM- und CPU-Speichers, der jedem Server in der Infrastruktur zugewiesen ist, mit der Möglichkeit, diesen bei Bedarf zu erhöhen;
- für jede virtuelle Maschine in der IT-Infrastruktur sind mindestens 50 Giga Speicherplatz vorzusehen, die Anzahl der virtuellen Server muss mindestens der Zahl der derzeit verwendeten Server entsprechen;
- Einhaltung der in dieser Dokumentation geforderten Merkmale;
- Möglichkeit, einen neuen virtuellen Server mit einem beliebigen Betriebssystem zu aktivieren und ihn bei Bedarf in Betrieb zu nehmen;
- mindestens 6 Terabyte Speicherplatz für die Replikation der Daten der VS in die DR-Umgebung.

Der Auftragnehmer ist für die Planung und Koordinierung aller Abläufe verantwortlich, die für die Übertragung der in Betrieb befindlichen Softwareanwendungen und Datenbanken von der derzeitigen Infrastruktur auf die neue Infrastruktur erforderlich sind.

Der AN stimmt sich mit der VS ab und führt dann den Transfer von der alten zur neuen Infrastruktur so durch, so dass die VS keinen Serviceausfall hat.
Die VS kann während der Vertragsdauer neue Systeme in der Netzwerkinfrastruktur und im Serverraum installieren. Der AN muss am Auswahlverfahren der VS für neue Software mitwirken, auch um sicherzustellen, dass die technischen Anforderungen der Software mit der Infrastruktur der SGR kompatibel sind.

2.1.1. Lieferung der Hardware

Der Auftragnehmer muss mindestens Folgendes bereitstellen:

- 1 Firewall Cluster: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung im Serverraum der VS. Gefordert werden folgende Merkmale:
  8 x 10/100/1000 aktive und unabhängige Ethernet-Ports mit zwei PoE+, 1,32 Gbps Firewall-Durchsatz, 1,4 Gbps VPN-Durchsatz, 1,32 Gbps UTM-Durchsatz;

- 1 Firewall Cluster: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung im Serverraum der VS. Gefordert werden folgende Merkmale:
  8 x 10/100/1000 aktive und unabhängige Ethernet-Ports mit zwei PoE+, 1,32 Gbps Firewall-Durchsatz, 1,4 Gbps VPN-Durchsatz, 1,32 Gbps UTM-Durchsatz;

- 1 Firewall: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung im DR-Raum des AN. Gefordert werden folgende Merkmale:
  8 x 10/100/1000 aktive und unabhängige Ethernet-Ports mit zwei PoE+, 1,32 Gbps Firewall-Durchsatz, 1,4 Gbps VPN-Durchsatz, 1,32 Gbps UTM-Durchsatz;

- 1 Firewall: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung am Hauptsitz eines Kunden der VS in Mailand. Gefordert werden folgende Merkmale:
  5 x 10/100/1000 aktive und unabhängige Ethernet-Ports mit einem PoE+, 1 Gbps Firewall-Durchsatz, 880 Mbps VPN-Durchsatz, 300 Mbps UTM-Durchsatz;

- 1 Firewall: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung am Hauptsitz eines Kunden der VS in Mailand. Gefordert werden folgende Merkmale:
  5 x 10/100/1000 aktive und unabhängige Ethernet-Ports mit einem PoE+, 1 Gbps Firewall-Durchsatz, 880 Mbps VPN-Durchsatz, 300 Mbps UTM-Durchsatz;

- 1 Fibre Channel SAN FC Laufwerk, 16 gb, mit 6 x 1,0 tb Festplatten als RAID 5 installiert, einschließlich Kabel und Rack-Gehäuse;

- 2 glasfaserbasierte SAN Switches 16 gb, sftp und Glasfaserkabel, einschließlich Kabel und Rack-Gehäuse;

- 2 Server-Cluster: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung im Serverraum der VS. Gefordert werden folgende Mindestmerkmale: 2 X Xeon Gold 6134 oder ein vergleichbares Modell eines anderen Herstellers (8 Core, Clock 3.0GHz, Cache 24,75 MB L3) 32GB 2933MHz (128GB, rDIMM), keine Rückwandplatine, RAID, 2x1100W, XCC Enterprise, Toolless Rails, 2 interne Festplatten für Systemstart, 1 x 2 Port 16 Gigabit Fibre Channel Card, 4 Port 1 Gigabit Controller Card, Netzwerkkarte, einschließlich Kabel und Rack-Gehäuse;

- 1 Server: Lieferung, Installation, Konfiguration, Verwaltung und Wartung, Unterbringung im DR-Serverraum des Auftragnehmers.Gefordert werden folgende Mindestmerkmale: 2 X Xeon Gold 6134 oder ein vergleichbares Modell eines anderen Herstellers (8 Core, Clock 3.0GHz, Cache 24,75 MB L3) 32GB 2933MHz (128GB, rDIMM), keine Rückwandplatine, RAID, 2x1100W, XCC Enterprise, Toolless Rails, 2 interne Festplatten für den Systemstart, 1 x 2-Port 16 Gigabit Fibre Channel Card, 4-Port 1 Gigabit Controller Card, 1 x interner RAID Controller, 6 x 2.5" 1.8TB 8000rpm Festplatten für die Datensicherung im Notfall (DR), inklusive Kabel und Rack-Gehäuse;

- 1 NAS System iscsi 10 gb, proc Intel Xeon D-1521 oder ein vergleichbares Modell eines anderen Herstellers mit 12 Bays: Lieferung, Installation Konfiguration, Verwaltung und Wartung, Unterbringung im Serverraum der VS. Im NAS müssen 8 SATA-Festplatten (SATA/600) 1,8 TB im RAID 5 installiert sein, samt Kabel und Rackgehäuse;

- 2 Switch, mit 12 Bays 1Gb, 2 SFP+ Ports, 19inch Rackmountable, internal PSU

2.1.2. Lieferung der Software

Man beachte, dass unter diesem Punkt sofort und kontinuierlich auszuführende Lieferungen gefordert werden. Hinsichtlich der Zahlungsmodalitäten und der jeweiligen SLA-Vereinbarungen wird auf das Dokument "SLA.pdf“ verwiesen.

Der Auftragnehmer muss für die gesamte Vertragsdauer die für die Nutzung der IT-Infrastruktur nötige Software liefern. Bei Vertragsbeginn ist für die IT-Infrastruktur mindestens die folgende Software bereitzustellen:

Sofortige Ausführung und auf Konsignation:
- 30 Lizenzen WinSvrCAL 2019 SNGL OLP NL UsrCAL - R18-05768; (keine Wartung erforderlich)
- 30 Lizenzen WinRmtDsktpSrvcsCAL 2019 SNGL OLP NL UsrCAL - 6VC-03748; (keine Wartung erforderlich)
- 3 Windows Server 2019 Datacenter Edition 16Core, sekundäres Betriebssystem, No Media, unbegrenzte VMs
- 12 Windows Server 2019 Datacenter Zusatzlizenz (2 Core) (No Media/Key) (Reseller POS Only)
- 1 Lizenz Virtualisierungssoftware für 3 Host (MAX 2 PROZESSOREN PRO HOST) mit 3 Jahren Wartung und Update
- 1 Lizenz für Backup und Replikation für die Virtualisierung mit 3 Jahren Wartung

Regelmäßige Wartung der Hardware
- 24x7-Garantie und Vor-Ort-Wartung der 3 Server und aller internen Komponenten, NAS, SAN, NAS-Festplatten, SAN-Festplatten und 2 SAN-Switches, Fiber Channel und der 5 Firewalls.

Auf kontinuierlicher Basis und gegen Servicegebühr:
- 1 Antispam-Antivirus-Lizenz für den Mail-Server;
- 30 Softwarelizenzen für die softwarebasierte VPN-Verbindung;
- 15 Softwarelizenzen für die softwarebasierte VPN-Verbindung und zusätzlich mit Token- oder App-Authentifizierung;
- 30 Antivirus-Lizenzen (Clients, Laptops und Server) mit Protokolldienst und Software- und Hardware-Inventar;

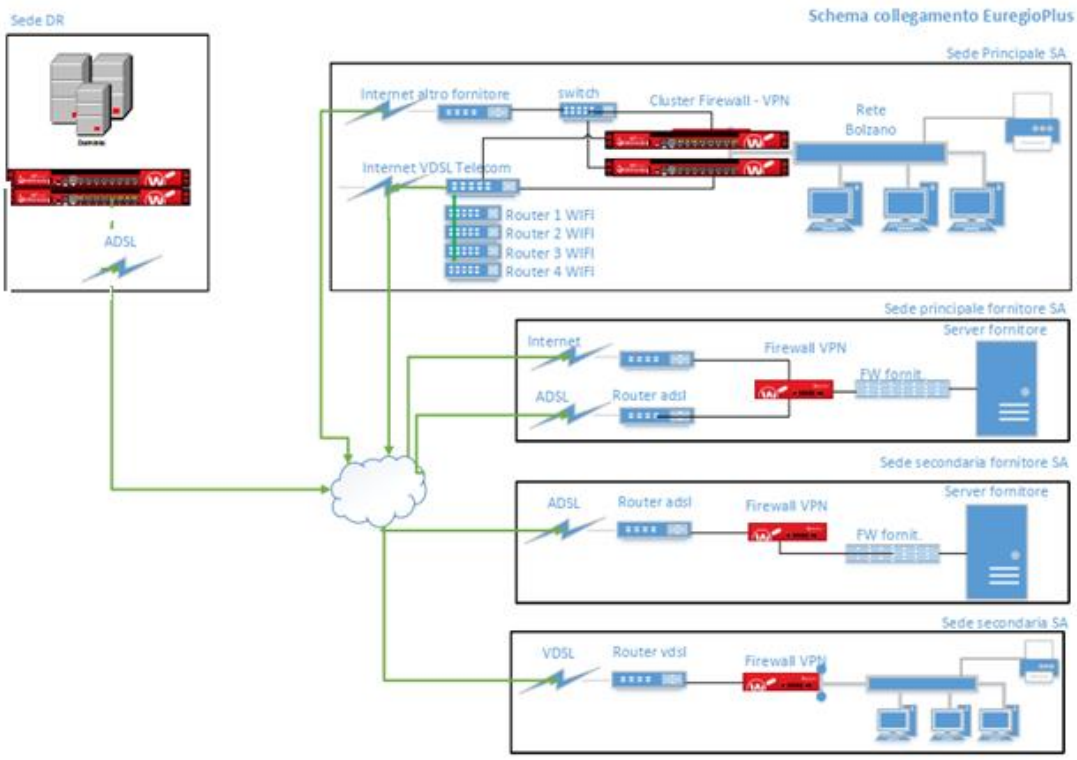
- 30 Lizenzen für HCL Domino 11 Complete Collaboration (CCB) TERM.

2.1.3. Lieferung von Datenleitungen

Man beachte, dass in diesem Kapitel sofort auszuführende Lieferungen gefordert werden. Hinsichtlich der Zahlungsmodalitäten wird auf das Dokument "Sonderleistungsverzeichnis für Dienstleistungen“ verwiesen.

Der Auftragnehmer muss die Datenleitungen der VS bereitstellen und betreiben und über Firewalls maximale Sicherheit gewährleisten.
Der DR-Standort muss für den Empfang über Datenleitungen und über das Internet eingerichtet werden.
Gefordert werden 5 VDSL-Leitungen mit folgenden Merkmalen:
Download 100 Mega - Upload 20 Mega:

- 2 Datenleitungen am Sitz der VS in Bozen + 8 öffentliche IPs
- 2 Datenleitungen in Mailand, die am Hauptsitz und in der Zweitniederlassung von Objectway in Mailand zu installieren sind.
- 1 Datenleitung am Zweitsitz der VS in Trient zur Synchronisation



2.1.4. Periodische Hardwarewartung

Der AN muss während der gesamten Vertragslaufzeit die Hardware-Wartung und die erweiterte Garantie für alle Hardware-Komponenten, die Gegenstand der Ausschreibung sind, aktivieren, verwalten und erneuern.

Die Garantien und der Support-Dienst müssen für alle Hardwarekomponenten rund um die Uhr, 7 Tage die Woche (24h/7T) und mit "Vor-Ort"-Support innerhalb von 4 Stunden gelten.
Der AN muss der VS alle in ihrem Namen aktivierten Garantien und Wartungsverträge aushändigen. La DA deve consegnare alla SA tutte le garanzie e manutenzioni attivate a nome della SA.

2.2 Projektierung und Umsetzung der IT-Infrastruktur

Man beachte, dass in diesem Kapitel sofort auszuführende Leistungen gefordert werden. Hinsichtlich der Zahlungsmodalitäten und der jeweiligen SLA-Vereinbarungen wird auf das Dokument "SLA.pdf " verwiesen.

Projektierung und Umsetzung der IT-Infrastruktur, der Software und Hardware der VS, einschließlich der Lieferung und Konfiguration von Hardware der neuen Generation für den Haupt- und den Zweitsitz und für den DR-Standort des AN.

Der AN hat folgende Leistungen zu erbringen:

- Physische Installation aller Firewalls und deren Anschluss an die Infrastruktur, Konfiguration und Aktivierung aller Sicherheitsrichtlinien am Haupt- und am Zweitsitz der VS, im Disaster-Recovery-Raum des AN und in den Räumlichkeiten des Kunden in Mailand sowie Bereitstellung sicherer Datenleitungen

- Physische Installation des NAS und aller dazugehörigen Festplatten, Anschluss an die Infrastruktur der VS, Erstellen des RAID 5 und Konfiguration für das Backup-Management

- Physische Installation des SAN und aller dazugehörigen Festplatten, Anschluss an die Infrastruktur der VS, Erstellen des RAID 5 und Konfiguration zum Erstellen der virtuellen Maschinen und der Daten der VS

- Physische Installation des ersten Server Clusters mit CPU, RAM, Prozessoren, Festplatte, Hauptplatine, Fibre-Channel-Karte, 4-Port-SCSI-Controllerkarte 1 Giga, Netzwerkkarte, Netzteilen und allen Komponenten am Sitz der VS:
    - RAID-Spiegelung der beiden Boot-Festplatten;
    - Installation, Konfiguration und Update des Betriebssystems;
    - Installation und Konfiguration des Programms VwWare und der Replikationsumgebung;
    - Installation, Erstellung und Konfiguration der Citrix-Farm in einer virtuellen Umgebung;
    - Installation und Konfiguration aller virtuellen Server;
    - Replikat erstellen mit dem zweiten Server.

  Siehe Dokument Technisches Leistungsverzeichnis, Abschnitt 4.2 Aktuelle virtuelle Server.
  Es wird darauf hingewiesen, dass auf allen virtuellen Servern die neueste Betriebssystemversion installiert sein muss und dass für alle Softwareversionen ebenfalls die neueste verfügbare Version zu installieren ist.

- Physische Installation des zweiten Servers im Cluster mit CPU, RAM, Prozessoren, Festplatte, Hauptplatine, Fibre-Channel-Karte, 4-Port-SCSI-Controllerkarte 1 Giga, Netzwerkkarte, Netzteilen und allen Komponenten in den Räumlichkeiten der VS.
    - RAID-Spiegelung der beiden Boot-Festplatten;
    - Installation, Konfiguration und Update des Betriebssystems;
    - Installation und Konfiguration des Programms VwWare und der Replikationsumgebung;
    - Installation, Erstellung und Konfiguration der Citrix-Farm in einer virtuellen Umgebung;
    - Installation und Konfiguration aller virtuellen Server;
    - Domäne und alle für den Betrieb erforderlichen Richtlinien erstellen;
    - Replikat erstellen mit dem ersten Server;

  Siehe Dokument Technisches Leistungsverzeichnis, Abschnitt 4.2 Aktuelle virtuelle Server.

  Es wird darauf hingewiesen, dass auf allen virtuellen Servern die neueste Betriebssystemversion installiert sein muss und dass für alle Softwareversionen ebenfalls die neueste verfügbare Version zu installieren ist.

- Physische Installation des DR-Servers samt CPU, RAM, Prozessoren, 2 Boot-Festplatten, 4-Port SCSI-Controllerkarte 1 Giga, Netzteilen, Fibre-Channel-Karte, RAID-Controllerkarte und 8 Festplatten, Hauptplatine und allen Komponenten in den Räumlichkeiten des AN
    - RAID-Spiegelung der beiden Boot-Festplatten;
    - Installation, Konfiguration und Update der neuesten Version des Betriebssystems;
    - Installation und Konfiguration des Programms VwWare und der gesamten Umgebung;
    - Installation, Erstellung und Konfiguration der Citrix-Farm in einer virtuellen Umgebung;
    - Installation und Konfiguration aller virtuellen Server;
    - RAID 5 aus 8 Festplatten für die SAN-Daten-Replikation erstellen;
    - Geplante SAN-Daten-Replikation konfigurieren.

  Siehe Dokument Technisches Leistungsverzeichnis, Abschnitt 4.2 Aktuelle virtuelle Server.

  Es wird darauf hingewiesen, dass auf allen virtuellen Servern die neueste Betriebssystemversion installiert sein muss und dass für alle Softwareprogramme ebenfalls die neueste verfügbare Version zu installieren ist.
- Installation, Konfiguration der Datenleitungen, Testen des Betriebs, Einrichtung des internen WIFI;
- Erstellen der Domäne, von Regeln, Richtlinien und FTPS-Verbindungen;
- Erstellen der Backup-Richtlinien;
- Ausarbeitung des Business Continuity und Disaster Recovery Plans;
- Erstellen der Domäne und aller für den Betrieb der Infrastruktur erforderlichen Richtlinien;
- Migration aller Daten.

Der AN verpflichtet sich, in der Analysephase eine Schätzung vorzunehmen für die Geräte und Komponenten, die eventuell zu ersetzen sind und deren Kosten vom AN zu tragen sind. Der etwaige Austausch von Hardware ist integrierender Bestandteil des Angebots, in dem auch die Kriterien anzugeben sind, auf deren Basis die Schätzung erfolgt.

2.2.1. Aufbau einer Citrix Server Farm

Die VS besitzt bereits 45 Citrix-Lizenzen. Der AN muss die Citrix-Farm in virtualisierter Umgebung bereitstellen, die in die Domäne der VS aufgenommen werden soll. Generell sind mindestens die folgenden Server zu installieren:

- 1 Citrix Management Server:

- Mindestens 3 Citrix Provisioning-Server;
- 1 Citrix Konsolenserver;
- 1 Citrix SQL-Server;
- 1 Citrix Masterserver (Citrix-Image);
- 2 Server für das Citrix-Webportal (Verteilung von Anwendungen);
- Mindestens 7 Serverfarmen für die Unterstützung von bis zu 50 zugriffsberechtigten Benutzern, mit der Möglichkeit, diese auf Anfrage der VS zu aktivieren;
- 1 Citrix-Test-Serverfarm zum Testen von Updates oder Verteilungen;
- 1 Citrix-Serverfarm im Standby-Modus, die bei Bedarf aktiviert werden kann;
- 1 Citrix Konsolenserver.

Alle Server in der Citrix-Farm müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

Der Zugriff auf das App Center, auf alle virtuellen und physischen Server, auf Active Directory usw. muss der VS im Administrator-Modus gewährt werden; alle Zugriffsprotokolle müssen aktiv sein. Alle Server in der Citrix-Farm müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

2.2.2. Erstellung eines Domänencontroller-Servers

Der AN muss einen virtuellen Server für die Funktion des Domänencontrollers installieren. Die Installation und Konfiguration der Server muss nach den Richtlinien des Softwareherstellers erfolgen.
Die Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.
Die virtuellen Server müssen so konfiguriert werden, dass es keine Latenz oder Verlangsamung gibt; die Verteilung der Ressourcenlast liegt in der Verantwortung des AN.
Der AN muss bei der Konfiguration der Domäne die Anweisungen der VS befolgen.

2.2.3. Erstellen von dedizierten Mailservern für HCL Domino 11 und Zubehör

Die VS verwendet das Mailsystem Domino 8.5.3, da es das einzige Programm ist, in dem eine benutzerdefinierte Schnittstelle entwickelt wurde, die sich direkt mit der Software der Dokumentenverwaltung verbindet. Der AN muss der VS die Software HCL Domino Complete Collaboration (CCB) TERM Version 11 oder höher verkaufen, sie installieren, konfigurieren, die aktuellen Einstellungen, benutzerdefinierten Anpassungen und Datenbanken importieren. Darüber hinaus muss der AN die elektronische Post für alle Beschäftigten der VS über die derzeitige Domäne euregioplus.com in Betrieb nehmen, die Mobiltelefone der gesamten VS über die Software Traveler konfigurieren und den internen Chat über die Software Sametime aktivieren.
Der AN muss folgende Installationsleistungen erbringen:

- 2 virtuelle Domino-Server, die in die Domäne der VS aufgenommen werden sollen (betrieblicher Mailserver der Domäne euregioplus.com), und die damit verbundene Konfiguration und Verwaltung des Programms.
- 1 virtueller Traveler-Server, der in die Domäne der VS aufgenommen werden soll (Mailserver für Mobiltelefone), und die damit verbundene Konfiguration und Verwaltung des Programms.
- 1 virtueller Sametime-Server, der in die Domäne der VS aufgenommen werden soll (Server für die interne Chatfunktion im Lotus-Programm), und die damit verbundene Konfiguration und Verwaltung des Programms.

- 1 virtueller Proxy-Server, der in die Domäne der VS aufgenommen werden soll (Antispam + Antivirus Proxy) und die damit verbundene Konfiguration und Verwaltung des Programms.
- 1 virtueller Server für das Webportal, der in die Domäne der VS aufgenommen werden soll, und die damit verbundene Konfiguration und Verwaltung des Programms.

Derzeit gibt es ca. 200 db von Mails, die verschiedenen Benutzern zugeordnet sind, einschließlich persönlicher Archive und deren Verknüpfung mit den Benutzern.
Die Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

2.2.4. Erstellung von Sicherungsrichtlinien

Der AN muss eine softwarebasierte Backup-Richtlinie erstellen; nach dem Verkauf der Software an die VS muss der AN die Installation und Konfiguration vornehmen.
Die Sicherungsrichtlinie muss 4 Arten von Sicherungen vorsehen:

- Die tägliche nächtliche Sicherung von Sonntag bis Freitag sieht vor, dass nur die geänderten Daten auf dem NAS und auf den Partitionen "D:“ aller virtuellen Server auf Band oder auf einer externen, vom Netzwerk getrennten Festplatte oder in der Cloud gespeichert werden (inkrementelle Sicherung). Das tägliche Backup muss einen Monat lang aufbewahrt werden.

- Bei der wöchentlichen nächtlichen Sicherung werden jeweils am Samstag alle Daten auf dem NAS sowie die Daten auf den Partitionen "D:“ aller virtuellen Server auf Band oder auf einer externen, vom Netzwerk getrennten Festplatte oder in der Cloud gespeichert. Das wöchentliche Backup muss 1 Monat lang aufbewahrt werden.

- Bei der monatlichen nächtlichen Sicherung werden alle Daten auf dem NAS und die Daten auf den Partitionen „D:“ und die virtuellen Abbilder aller Server jeden Monat jeweils am letzten Samstag auf Band oder auf einer externen, vom Netzwerk getrennten Festplatte oder in der Cloud gespeichert. Das monatliche Backup muss 1 Jahr lang aufbewahrt werden.

- Bei der jährlichen nächtlichen Sicherung werden jeweils am letzten Samstag des Jahres alle Daten auf dem NAS, auf den Partitionen „D:“ und die virtuellen Abbilder aller Server auf einem Band oder auf einer externen, vom Netzwerk getrennten externen Festplatte oder in der Cloud gespeichert. Das jährliche Backup muss 10 Jahre lang aufbewahrt werden.

Das Speichermedium Band, externes Festplattenlaufwerk oder Cloud liegen in der Verantwortung des AN, der für den langfristigen Erhalt der Daten sorgen muss.
Die VS kann vom AN jederzeit eine bestimmte Wiederherstellung oder eine vollständige Sicherung verlangen.

2.2.5. Virtuelle Desktops

Für jeden Mitarbeiter der VS muss ein virtueller Desktop in einer Citrix-Umgebung zur Verfügung gestellt werden, der folgende Mindestmerkmale aufweisen muss:

- CPU, die gleichwertig ist mit einem Intel Core i5 der 7. Generation oder einem anderen gleichwertigen Modell eines anderen Herstellers entspricht;
- 6Gb RAM;
- keine dedizierte Karte erforderlich

Die virtuellen Desktops müssen mit den neuen Videokommunikationssystemen funktionieren.

Der AN muss die virtuellen Desktops während der gesamten Vertragsdauer verwalten, betreuen und aktualisieren.

2.2.6. Server mit Programmen, die von Drittanbietern verwaltet werden

Der AN muss alle virtuellen Server einrichten und konfigurieren, die derzeit von der VS für die Software von Drittanbietern verwendet werden, für die ein dedizierter Server erforderlich ist.
Der AN muss außerdem mindestens 7 virtuelle Server mit dem Betriebssystem Windows Server u.v. erstellen, die in die Domäne der VS aufgenommen werden sollen, und das Programm in Zusammenarbeit mit dem Software-Lieferanten und der VS installieren und die Einstellungen aus der alten Infrastruktur importieren.
Der AN muss folgende Installationsleistungen erbringen:

- Ms Windows Server für die Dokumentenarchivierungssoftware;
- Ms Windows Server für die MySQL-Software;
- Linux Server für die Software des Börsenorderregisters
- Ms Windows Server für die Ausarbeitung von Buchhaltungsübersichten;
- Ms Windows Server für die Anwesenheitssoftware
- Ms Windows Server für die Antivirus-Software
- Ms Windows Server, der im Bedarfsfall genutzt werden kann

Die VS kann den AN jederzeit auffordern, den Ms Windows Server zu aktivieren, damit er im Bedarfsfall jederzeit genutzt werden kann.
Alle Server müssen eine Partition C: für das Betriebssystem und eine Partition D: für Programme und Programmdaten haben.

2.2.7. Dienst-Server

Der AN muss 4 virtuelle Server mit dem Betriebssystem Windows Server u.v., die in die Domäne der VS aufgenommen werden sollen, bereitstellen und konfigurieren, und für die Konfiguration der Dienste und Programme und den Import der Einstellungen aus der alten Infrastruktur sorgen.

- Ms Windows-Server für die SFTP-Verbindungen
- Ms Windows Server für das Programm des VPN-Dienstes
- Ms Windows Druckerserver
- Ms-Server für den Bedarfsfall

Die VS kann den AN jederzeit auffordern, den Ms Windows Server zu aktivieren, damit er im Bedarfsfall jederzeit genutzt werden kann.

Alle Server müssen eine Partition C: für das Betriebssystem und eine Partition D: für Programme und Programmdaten haben.

2.2.8. Active Directory Server

Der AN muss einen virtuellen Server für den Active Directory-Dienst einrichten und konfigurieren und die Einstellungen aus der alten Infrastruktur importieren. Der AN muss folgende Leistungen erbringen:

- Forest Design
- Domain Design
- Forest root design
- Active Directory Namespace-Planung
- DNS-Infrastruktur zur Unterstützung von Active Directory
- Erstellen des Designs einer Organisationseinheit
- Konfiguration der Unternehmensrichtlinien

Der Server muss in die DR-Umgebung und auf den Replikationsserver repliziert werden.
Der Server muss eine Partition C: für das Betriebssystem und eine Partition D: für Programme und Programmdaten haben.

2.2.9. Datenmigration

Der AN muss für die Migration aller Daten der VS auf die neue Infrastruktur sorgen. Für die kopierten Daten müssen dieselben Zugriffsrichtlinien gelten, und der AN muss der VS anhand von Protokollen oder Berichten die Kongruenz der von der alten in die neue Infrastruktur migrierten Daten nachweisen.
Der AN muss vor der Migration eine gründliche Überprüfung der Daten vornehmen, sich vergewissern, dass die zu kopierenden Daten keine Probleme aufweisen, und diese gegebenenfalls mit Hilfe von IT-Tools lösen, und schließlich die Qualität der Daten überwachen und darüber Bericht erstatten.
Der AN kann die Daten entweder durch eine "Big Bang"-Migration (d.h. an einem Wochenende auf einmal) oder durch eine "Trickle"-Migration (das alte und das neue System werden parallel betrieben) transferieren.
Es wird darauf hingewiesen, dass alle Mail-Daten und Mail-Datenbanken einschließlich der Archive lesbar sein müssen, wobei zu berücksichtigen ist, dass für die Dateien dieselben Zugriffsberechtigungen vorzusehen sind.
Der AN ist verpflichtet, auch alle Active Directory-Richtlinien zu migrieren und die gleiche Netzwerkzuordnung neu zu erstellen. Der AN muss auch alle derzeit aktiven SFTP-Verbindungen neu erstellen.
Es wird darauf hingewiesen, dass sich alle Daten derzeit auf dem NAS und auf den Partitionen D: aller virtuellen Server befinden.

2.2.10. Business Continuity und Disaster Recovery

In Übereinstimmung mit den geltenden Rechtsvorschriften hat die VS einen Notfallplan und einen Plan zur Aufrechterhaltung der Geschäftskontinuität (nachstehend Business Continuity Plan - "BCP“ genannt) und

einen DR-Plan ausgearbeitet, um sicherzustellen, dass sie bei einem Ausfall angemessen reagieren und die geschäftskritischen Tätigkeiten im Falle einer Unterbrechung der normalen Betriebsabläufe angemessen aufrechterhalten kann.

Im dokumentierten Business Continuity Plan werden alle Informationen und Verfahren dargelegt, die zur Bewältigung von außergewöhnlichen Ereignissen nötig sind, die die normale Arbeitstätigkeit der VS beeinträchtigen könnten. Der BCP enthält in einem eigenen Kapitel auch den Disaster-Recovery-Plan: Darin werden mögliche Katastrophen und Risikoszenarien beschrieben und die geschäftskritischen Prozesse und die internen und externen Ansprechpersonen der VS für den Ernstfall genannt; weiters werden die Prozesse zur Lösung der Probleme bestimmt.

Der AN muss Software- und Hardwaresysteme bereitstellen, die die Ausfallsicherheit des Unternehmens und ein sorgfältiges Risikomanagement gewährleisten. Vom AN wird daher gefordert, dass er in verstärktem Maß das Augenmerk auf Bedrohungen (Bedrohungsanalyse) und auf das Erkennen der Folgeschäden eines Notfalls (Business Impact Analysis) richtet.

Gegenstand der Ausschreibung sind auch die Erstellung des BCP und des DR sowie das BC- und DR-Management für die gesamte IT-Infrastruktur der VS.

Der AN muss mindestens einen jährlichen DR-Test durchführen; die Wiederanlaufzeiten der Prozesse müssen mit den im BC-Plan der VS verwendeten Parametern kompatibel sein, die in der Regel maximal 4 Stunden vorsehen, und müssen auf jeden Fall innerhalb der Frist für die Übermittlung von Daten der VS an externe Stellen (z. B. Mitteilungen an Aufsichtsbehörden) liegen. Der AN muss außerdem einen funktionierenden Disaster-Recovery-Plan erstellen, der ein Hot Backup aller Daten der VS am vom AN bereitgestellten DR-Standort vorsieht, an dem sich die vergabegegenständlichen Server und Laufwerke befinden. Mindestens einmal jährlich muss ein Test des gesamten Serverraums mit Aktivierung des DR-Standorts durchgeführt werden; die Wiederanlaufzeiten der Maschinen müssen mit den im Business Continuity Plan der VS verwendeten Parametern kompatibel sein, die in der Regel maximal 8 Stunden vorsehen, und müssen auf jeden Fall innerhalb der Frist für die Übermittlung von Daten der VS an externe Stellen (z. B. Mitteilungen an Aufsichtsbehörden) liegen. Der AN muss der VS einen Raum als Serverraum für den DR-Standort (DR-Serverraum) zur Verfügung stellen, der mindestens 50 Kilometer vom Serverraum der VS entfernt sein muss.

Der Zugang zum DR-Serverraum für Aufsichts- und Kontrolltätigkeiten ist den Aufsichtsbehörden, der SGR und ihren Rechnungsprüfern zu gewähren.

Wesentliche Anforderung an den BCP sind:

- Doppelte Auslegung mindestens der folgenden Hardware:
    - Firewall am Hauptsitz der VS: wie in der Lieferanfrage beschrieben, sind die Bereitstellung, Konfiguration und Verwaltung des Firewall-Clusters vorzusehen:
    - Server am Hauptsitz der VS: wie in der Lieferanfrage beschrieben, sind die Bereitstellung, Konfiguration und Verwaltung des Server-Clusters vorzusehen;
    - Festplatten (HD) am Hauptsitz der VS: wie in der Lieferanfrage beschrieben, ist für den korrekten Betrieb der Festplatten der Server und des NAS-Systems zu sorgen.
- Doppelte Leitungen an folgenden Orten:
    - Hauptsitz VS:
    - Hauptsitz externer Finanzdienstleister

Bei einem Ausfall der beiden Leitungen ist die Aktivierung der DR-Leitung vorzusehen.

- Wesentliche Software-Dienste der IT-Infrastruktur:
    - Hauptsitz der VS: Dienste doppelt konfigurieren.

Es wird auf jeden Fall vorausgesetzt, dass die Daten der VS am DR-Standort per Hot Backup gesichert werden.

Die virtuellen Server können per Cold Backup am DR-Standort gesichert werden.

Darüber hinaus ist der Zugang zu den Unternehmensdiensten über Smart-Working-Systeme vorzusehen; dabei ist darauf zu achten, dass diese nach den Grundsätzen der Sicherheit und des Datenschutzes zu implementieren sind, außerdem muss für eine angemessene Schulung und für die regelmäßige Aktualisierung der Ressourcen gesorgt werden.

Mindestens einmal im Jahr ist ein DR-Test des Serverraums mit dazugehöriger Aktivierung des DR-Serverraums durchzuführen. Der Test muss von den Parteien vereinbart werden und soll vorzugsweise an Wochenenden durchgeführt werden. Am DR-Test kann die VS und/oder ein externer Beauftragter teilnehmen.
Dafür sind detaillierte Anweisungen zu den verschiedenen Vorgängen bereitzustellen, die am Testtag durchgeführt werden; nach Abschluss ist ein detaillierter Bericht zu erstellen, der in die Dokumentation des Verwaltungsrats des Unternehmens aufgenommen wird. Im Falle eines negativen oder unbefriedigenden Ergebnisses muss ein weiterer Test innerhalb von 45 Tagen nach dem ersten Test angesetzt werden.
Der AN muss also einen realistischen funktionalen DR-Test ausarbeiten, der die Unzugänglichkeit des Serverraums und die Aktivierung des DR-Plans für den Serverraum infolge der nachstehenden Ursachen vorsieht.

- Unterbrechung der Internet-Verbindung;
- Unterbrechung eines oder aller Serverpfade;
- Ausfall eines oder mehrerer Server, wodurch der Betrieb der Infrastruktur beeinträchtigt ist;
- Speicherausfall;
- Katastrophe am Sitz.

2.2.11. Disaster Recovery Serverraum

Der AN muss für die gesamte Vertragslaufzeit einen Raum zur Verfügung stellen, der als DR-Serverraum genutzt werden soll, um im Notfall die eventuell nötigen Datensicherungen und die DR-Tests durchzuführen. Der Raum muss folgende Ausstattung aufweisen: Klimaanlage, Rack-Schrank, Beleuchtung, Strom, USV, Internetleitung, Speicherplatz von 8 TB.

<u>DR-Serverraum:</u>
Der DR-Serverraum im Eigentum des AN muss folgende Ausstattung aufweisen: USV, Klimaanlage, Beleuchtung und Stromversorgung. Der DR-Serverraum muss der VS für die Unterbringung ihres Servers und ihrer Firewall zur Verfügung gestellt werden.
Der Zugang zum DR-Serverraum muss überwacht werden, nur das Projektteam des AN darf Zugang zu den Geräten der VS haben.
Der Disaster Recovery Saal muss zwischen mindestens 50 km vom Sitz der Gesellschaft in Bozen entfernt sein

<u>RACK-SCHRANK IM DR-RAUM:</u>
Der AN muss einen Rack-Schrank zur Verfügung stellen, in dem die Geräte der VS untergebracht werden können; es ist Aufgabe des AN, für die Montage des Servers und der Firewall sowie deren Konfiguration zu sorgen.

<u>Strom, Beleuchtung und USV:</u>
Der AN muss eine USV bereitstellen, Strom und Beleuchtung gehen zu Lasten des AN.

<u>Internetleitung</u>

Der AN muss eine Internetleitung mit folgenden Merkmalen bereitstellen: 100/20

Speicherplatz
Der AN muss einen 8 TB Speicher für digitale Daten zur Verfügung stellen, der an den Server der VS angeschlossen wird.

2.3 Betrieb und Wartung der technologischen Infrastruktur des Datenzentrums

Man beachte, dass in diesem Kapitel kontinuierlich auszuführende Leistungen gefordert werden. Hinsichtlich der Zahlungsmodalitäten und der jeweiligen SLA-Vereinbarungen wird auf das Dokument "SLA.pdf“ verwiesen.

Ziel dieses Dienstes ist die Bereitstellung des nötigen technischen Supports, um die technologische Infrastruktur während der gesamten Vertragslaufzeit funktionsfähig und effizient zu halten, wodurch der korrekte Betrieb der technologischen IT-Plattformen und der dazugehörigen Basis- und Umgebungssoftware ermöglicht werden soll, auf denen sich die aktuellen Anwendungen und Datenbanken des IT-Systems des Unternehmens befinden, sowie aller Geräte, die während der Vertragslaufzeit hinzugefügt werden.
Der AN ist verpflichtet, diese Infrastruktur unter Einhaltung der in den folgenden Absätzen definierten Richtlinien und Service-Levels zu betreiben; dafür sind die jeweils am besten geeigneten Mittel und Methoden einzusetzen, um den Dienst entsprechend den vertraglichen Anforderungen zu erbringen.
Der Dienst umfasst auch das Logical und Physical Security Management mit dem Ziel, die Integrität, Verfügbarkeit und Vertraulichkeit der in den Server- und Speichersystemen befindlichen Daten zu gewährleisten.
Das komplette Management des Zentralsystems (inklusive aller Server-Storage-Systeme und aller daran angeschlossenen Peripheriegeräte) muss gewährleistet sein, dazu gehören auch die Betreuung, der operative Betrieb und die Überwachung, die planmäßigen Wartungsarbeiten, die Fehlersuche und -behebung, das Storage-Management usw.

Die Kosten für die Wartung und die erweiterte Garantie gehen zu Lasten des AN.

Die vorgeschlagene Organisation des Wartungsdienstes muss eine Struktur vorsehen, die die Durchführung der in den folgenden Abschnitten beschriebenen Tätigkeiten ermöglicht.

2.3.1. Technisches und operatives Management der Hardware-Infrastruktur und der Basis- und Umgebungssoftware

Der Dienst muss mindestens folgende Tätigkeiten umfassen:

- korrektive und präventive Wartung der zentralen Systeme mit entsprechender operativer Abwicklung und Behebung von Störungen;
- Verwaltung, Durchführung und Überwachung von Backup-, Restore- und Recovery-Aktivitäten, der bestehenden Anwendungen und Datenbanken, operative Verwaltung der Speicher, Medien und Datenträger, die entsprechend den Vorgaben eingesetzt werden, die von den Systemverfahren und von den Datenbanken vorgesehen werden;

- Leistungsmanagement der Systeme;
- Speicherplatzverwaltung;
- Ausführung von Batch-Verfahren;
- Verwaltung der Server-Virtualisierung;
- Citrix-Farm-Management
- Verwaltung der gesamten E-Mail-Umgebung
- Serverkonfiguration und -verwaltung;
- operative Verwaltung der Serverleistung;
- Verwaltung und Überwachung der Umgebungsparameter des Maschinenraums;
- Verwaltung von Druckwarteschlangen und von zentralen Druckvorgängen;
- Verwaltung des File-Sharing;
- Lösung von Problemen in Zusammenhang mit der logischen Sicherheit der Infrastruktur, wobei auf die Einhaltung von Rechtsvorschriften und die Anwendung der Sicherheitsrichtlinien zu achten ist;
- Unterstützung bei der Definition und Umsetzung von DR- und Business-Continuity-Richtlinien;
- Verwaltung der Serverreplikation;
- Sicherheitsmanagement;
- Unterstützung bei der Definition der Erweiterung/Konsolidierung des Datenzentrums;
- Definition und Formalisierung aller betrieblichen Prozeduren;
- Verwaltung der Zugriffsprotokolle der Systemadministratoren.

2.3.2. Server-Management

Das Server Management umfasst alle nötigen Aktivitäten, um die Server-Infrastruktur, die für die Bereitstellung der IT-Dienste der VS verwendet wird, zu betreiben und stets effizient zu halten.
Die Infrastruktur umfasst:

- Sicherstellung der einwandfreien Funktionsweise der Hardware- und Software-Server und der dazu zugehörigen Geräte (Firewall, Speicher, Bibliothek, Router usw.) im Serverraum der VS und im DR-Serverraums des AN, der der VS zur Verfügung gestellt wird
- Sicherstellung der einwandfreien Funktionsweise der gesamten Netzwerkinfrastruktur des Serverraums der VS (Firewall, Switches und Netzwerkgeräte)

Die aktuelle Konfiguration der Serverinfrastrukturen, die sich in den Büros der VS außerhalb des Serverraums befinden, ist im Dokument „Technisches Leistungsverzeichnis“, Kapitel 4 „Derzeitiger Bestand des IT-Systems der VS - Hardware - Software und Datenleitungen“ dargelegt. Hier finden sich auch die Angaben zu den derzeitigen Servern, die als virtualisierte Server in den neuen Serverraum aufgenommen werden sollen.
Die Dienstleistung ist ohne zusätzliche Kosten und ohne jegliche Einschränkung unter Einhaltung der vertraglichen SLA-Vereinbarungen zu erbringen, und zwar in Bezug auf die Konfigurationen und Volumina, die sich aus der Weiterentwicklung ergeben können, die die VS während der Vertragslaufzeit für ihr IT-System beim AN anfordert (z. B. Änderungen und Erweiterung der Server).
In diesem Zusammenhang werden die Begriffe "System" oder "Server" definiert als eine Reihe von Hardware- und Softwarekomponenten (Betriebssystem und Softwarekomponenten wie z.B. Domino oder MS Office), die zu einer autonomen Verarbeitungseinheit zusammengefasst werden können, die die Entwicklung, das Testen und den Betrieb eines oder mehrerer Dienste unterstützt.

In diesem Zusammenhang wird auch die Netzwerkinfrastruktur des Serverraums als "System" angesehen.

Das Dienstleistungsangebot muss den gesamten Lebenszyklus der Systeme abdecken. Dazu gehören daher u.a:

- der operative Betrieb der Systeme und die Leistungsmessung;

- Änderungsmanagement (vor Ort oder remote) (Verwaltung und Durchführung von Änderungen an der Basis-, Umgebungs- und Netzwerksoftware und eventuell Support für die Anwendungssoftware von Drittanbietern);
- IMAC (Handhabung, Hinzufügen und Ändern von HW-Komponenten und Peripheriegeräten);
- Asset Management (Verwaltung und Kontrolle der installierten Konfigurationen);
- Incident Management, technischer Support und Wartung von Hardware und Software;
- Berichterstattung.

Der AN verpflichtet sich, das ordnungsgemäße Funktionieren und die geforderte Verfügbarkeit der zentralen Verarbeitungsdienste durch einen angemessenen Systemsupport in den verschiedenen Bereichen sicherzustellen, die für die Funktionsfähigkeit der Systeme relevant sind. Es wird in der Verantwortung des AN liegen, die Soft- und Hardware aller Geräte zu verwalten. Darüber hinaus ist zu beachten, dass der AN eine zentrale Rolle für den Kontakt zu den Unternehmen innehat, die die Wartung ausführen müssen. Der AN muss weiters die VS bei der Abwicklung der Supportanrufe an die verschiedenen Hardware- und Softwarelieferanten unterstützen (z.B. Supportanfragen eröffnen, Telefonanrufe tätigen, für etwaige Tests zur Verfügung stehen).

2.3.3. Anwendungsserver

Die Anwendungsserver sind betriebssystemseitig zu überwachen und zu verwalten, der Support für Drittanwendungen und die entsprechenden Verfügbarkeitsziele fallen in die Zuständigkeit der VS.
Hinsichtlich der Server, die nicht direkt verwaltete Anwendungsdienste bereitstellen, muss der AN für Folgendes sorgen:

- etwaige Installation, Konfiguration und Optimierung des Betriebssystems und der Umgebungssoftware (z.B. Application Server, Oracle Application, Virtualisierungssoftware);
- Konfiguration der Systemparameter (Partitionen, Instanzen, Speicher, RAM, CPU usw.) für die Test- und Produktionsumgebung der Anwendungen;
- Unterstützung bei der Installation von Anwendungen und der Definition von Management-Skripten (Startup, Shutdown usw.) in Zusammenarbeit mit dem externen Lieferanten der Anwendung;
- Netzwerkkonnektivität und Mehrwertdienste wie: Überwachung, Sicherheit (Firewall), zentralisiertes Backup;
- Verwaltung der Druckwarteschlangen;
- Infrastruktur-Support, einschließlich Systemberatung zur Leistungsoptimierung;
- Störungsmanagement, vom Service Desk-Support bis zur Wartung über bereits bestehende Verträge;
- Prävention durch geeignete Sicherheitsmaßnahmen, um die Integrität der in Betrieb befindlichen Anwendungen zu gewährleisten.
- Windows- und Sicherheitsupdates;
- Installation und Verwaltung von Antivirenprogrammen.

2.3.4. Citrix Server Farm Management

Der AN muss die gesamte Citrix-Farm verwalten und pflegen, für Upgrades und gegebenenfalls für die Fehlerbehebung sorgen. Der AN ist verpflichtet, neue Citrix-Zugänge einzurichten und die Ressourcen korrekt zuzuweisen und gegebenenfalls die Anzahl der virtuellen Server nach Bedarf zu erhöhen.

2.3.5. Domänencontroller-Server

Der AN muss einen virtuellen Server für die Funktion des Domänencontrollers installieren. Die Installation und Konfiguration der Server muss nach den Richtlinien des Softwareherstellers erfolgen.
Die Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

Die virtuellen Server müssen so konfiguriert werden, dass es keine Latenz oder Verlangsamung gibt; die Verteilung der Ressourcenlast liegt in der Verantwortung des AN.

2.3.6. Verwaltung von dedizierten Mailservern für HCL Domino 11 und Zubehör

Der AN muss den Mailserver und alle damit verbundenen Mail- und Anwendungsdatenbanken verwalten.
Der AN muss das ordnungsgemäße Funktionieren der elektronischen Post und der Regelung der Zugangsberechtigung gemäß dem Organigramm des Unternehmens überprüfen. Verwalten von E-Mail-Archiven, SPAM-Regeln
Der AN hat die Aufgabe, auf Anfrage der VS (über einen eigenen Antrag beim Helpdesk) neue Nutzer anzulegen.

2.3.7. Active Directory Server

Der AN muss Active Directory mit folgenden konfigurierten Diensten verwalten:

- Active Directory Forest Management
- Domänenverwaltung
- Verwaltung der DNS-Infrastruktur zur Unterstützung von Active Directory
- Verwaltung von Organisationseinheiten
- Verwaltung von Unternehmensrichtlinien

Der Server muss in die DR-Umgebung und auf den Replikationsserver repliziert werden.

2.3.8. Server mit Programmen, die von Drittanbietern verwaltet werden

Der AN muss die virtuellen Server regelmäßig aktualisieren, sie überwachen und unter Kontrolle halten und die vollständige Kompatibilität mit der Software anderer Hersteller sicherstellen und bei Bedarf mit diesen zusammenarbeiten.
Aufgabe des AN ist es, den Computer regelmäßig zu reinigen und Bugs korrigieren.
Bei Problemen muss der AN mit den Lieferanten zusammenarbeiten und die Anweisungen zur Verbesserung der Performance befolgen.
.
Der AN und die Software-Lieferanten müssen für die Wartung der Programme Zugang zu den dedizierten Servern erhalten.

Alle Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

2.3.9. Dienst-Server

Die Aufgabe des AN wird es sein, die virtuellen Server zu aktualisieren und leistungsfähig zu machen, VPN-Dienste, SFTP-Verbindungen und Drucker zu verwalten, zu erstellen, zu modifizieren und auf Anfrage der VS zu löschen.
Alle Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

2.3.10. VmWare-Verwaltung

Der AN muss die gesamte virtualisierte Umgebung mit der Software VmWare verwalten, die auf den drei physischen Servern installiert ist, die Gegenstand der Ausschreibung sind.
Bei der Installation muss der AN die Anweisungen des Programms VmWare befolgen, die direkt auf der Website des Herstellers oder beim Produktsupport erhältlich sind.
Alle Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

2.3.11. Service-Management

Der AN muss während der gesamten Vertragslaufzeit folgende Dienste konfigurieren, verwalten, hinzufügen und ändern: DNS, NAT, SFTP, Domänen, verschiedene Zertifikate, Domänencontroller, Active Directory, Dateiserver, Druckertreiber, Richtlinien und generell alle für den Betrieb der Infrastruktur erforderlichen Dienste.
Alle Server müssen in die DR-Umgebung und auf den Replikationsserver repliziert werden.

Der AN muss für die Umsetzung, Pflege und Aktualisierung des Servicemanagements sorgen.

2.3.12. Systematisches Software-Management

Der AN muss während der gesamten Vertragslaufzeit folgende Maßnahmen ausführen:

- Installation von Softwareprodukten (z. B. Fixes, Hot Patches und/oder Service Packs, Patches, Treiber, Aktualisierung von Standardsoftware und von Betriebssystemen/Betriebsumgebungen usw.), sowohl präventiv als auch zur Behebung von aufgetretenen Fehlfunktionen;
- Konfiguration von Hardwareprodukten, der Basissoftware und Umgebungssoftware;
- Verwaltung von Betriebssystemen, Softwareprodukten und Datenbanken;
- Benutzerverwaltung (Benutzer und Gruppen) und Zugriffs-/Berechtigungssteuerung (MS Active Directory);
- Unterstützung bei der Optimierung von Backup-Richtlinien;
- Netzwerkdienste;
- Definition und Formalisierung aller betrieblichen Prozeduren;
- eventuell Installation, Konfiguration und Optimierung des Betriebssystems und der Umgebungssoftware (z.B. DB Server, Virtualisierungssoftware);
- Konfiguration der Systemparameter (Partitionen, Instanzen, Speicher, RAM, CPU usw.) für die Test- und Produktionsumgebung der DB-Server
- Herstellung der Netzwerkkonnektivität und Bereitstellung von Mehrwertdiensten wie z.B. Überwachung und zentralisiertes Backup;
- Infrastruktur-Support, einschließlich Systemberatung zur Optimierung der installierten Softwaresysteme (MySQLServer);
- Störungsmanagement, vom Support über das Service-Desk bis zur Wartung im Rahmen bestehender Verträge.

2.3.13. Umsetzung geeigneter Sicherheitsmaßnahmen, um die Integrität der Daten im Betrieb zu gewährleisten. Fachspezifischer Support

Der AN ist für alle Aktivitäten verantwortlich, mit denen die maximale Effizienz und Verfügbarkeit der Rechnerinfrastruktur gewährleistet werden soll; dazu garantiert er den fachspezifischen Support für die Server bei Hardware- und Softwareproblemen. Ziel des Supports ist die Analyse und Lösung von besonders relevanten Problemen.
Diese Leistungen müssen muss so organisiert sein, dass mindestens folgende Liste von Aktivitäten vorgesehen wird:

- Installation und Konfiguration der für die Erbringung der Dienste erforderlichen Hardwarekomponenten;
- Installation und Konfiguration von Betriebssystemen (nachstehend auch als "BS" bezeichnet);
- Installation von Datenbanksoftware (nachstehend auch "DB") (z. B. Oracle, Sql Server);
- Analyse der Serverauslastung und Bereitstellung von Berichten, um Maßnahmen zur Lastverteilung und/oder Vergrößerung der Komponenten zu ermöglichen;
- BS- und DB-Optimierung zur Leistungsverbesserung;
- Verwaltung sowie ordentliche und außerordentliche Wartung von BS und DB;
- Verwaltung von vorübergehenden Änderungen der Verarbeitungspläne nach den von der VS jeweils mitgeteilten Angaben;
- Optimierung des Massenspeicherplatzes und Datenwiederherstellung im Störungsfall;
- Definition und Vorbereitung von Verfahren und Standards für die Archivzuordnung;
- ständige Überwachung wichtiger Parameter und Bereitstellung von Informationen an die VS über den Status der Systeme anhand periodischer Berichte, um die Servicequalität zu gewährleisten.

2.3.14. Antivirus-Management und Sicherheitstechnologien

Gefordert werden die Lieferung, Verwaltung und Wartung der vom AN bereitgestellten Antivirensoftware und anderer Softwareprogramme, die für Zwecke der logischen Sicherheit verwendet werden, und zwar sowohl für das zentrale Management als auch in der Installation, Verwaltung und Wartung von Clients und Servern. Darüber hinaus umfasst die Tätigkeit Aktualisierungen und Anpassungen bei einer etwaigen Änderung und Erhöhung der Anzahl der Arbeitsstationen. Der AN muss mit den Lieferanten der Sicherheitssoftware zusammenarbeiten, sollten Upgrades oder Migrationen auf neue Systeme nötig sein (Installation auf Servern und Clients usw.); durch das Ad-hoc-Konfigurieren von Präventionsinstrumenten muss er proaktiv etwaige Bedrohungen und laufende Risiken überprüfen, auch durch Analyse der von der Sicherheitssoftware bereitgestellten Statistiken.

2.3.15. Aktivierung, Verwaltung, Speicherung und Pflege der Dokumentation und der Datenbank der Komponenten und der Interventionen

Der AN muss den Prozess definieren, mit dem sichergestellt werden soll, dass die Informationen zu den installierten Geräten ständig gepflegt und aktualisiert werden, weiters muss er die Garantien für die Hardwarekomponenten und die Softwarelizenzen verwalten.
Das Unternehmen behält sich das Recht vor, stichprobenartig die Zuverlässigkeit und Aktualisierung der DB, der technologischen Infrastruktur/des zentralen Systems (Server, Peripheriegeräte, Basis- und Umgebungssoftware, Anwendungssoftware) und ganz allgemein aller Geräte und Produkte zu überprüfen, die vom AN für die Erbringung der vertragsgegenständlichen Leistungen eingesetzt werden. Die vom Unternehmen berechtigten Benutzer müssen online Zugriff zu diesen Informationen erhalten und die Möglichkeit haben, die enthaltenen Informationen für eventuelle Offline-Bearbeitungen abzurufen. Die CMDB (Configuration Management Data Base) und etwaige Lizenzen sind bei Vertragsende in einem lesbaren Format an die VS zu übergeben.

2.3.16. Operativer Betrieb der Server

Das Servermanagement besteht in der kontinuierlichen Überwachung und Kontrolle der Systeme, um deren Betrieb gemäß den vorgesehenen Service-Levels zu gewährleisten; inbegriffen ist auch die Hilfe bei der Lösung von Betriebsproblemen, wobei diese Tätigkeiten Folgendes umfassen:

- Installation/Austausch von Hardware-, Software- und Firmware-Komponenten und Sicherstellung ihrer ordnungsgemäßen Funktion;
- Interaktion mit dem Hardware-Wartungsdienst;
- benutzerdefinierte Anpassung und Aktualisierung der Serverkonfiguration bei Bedarf durch planmäßige ordentliche und außerordentliche Wartungsarbeiten, durch die Installation notwendiger oder geforderter Änderungen und Updates sowie Anpassung an die von den Herstellern empfohlenen Sicherheitsupdates;
- Definition und Durchführung von Änderungen an der Architektur der Hard- und Softwareressourcen sowie der benutzerdefinierten Anpassungen, die für die Integration anderer Softwareprodukte und den Betrieb der Anwendungen notwendig sind;
- Installation, benutzerdefinierte Anpassung, Verteilung, Wartung und Test des Betriebssystems, der Subsysteme und der Middleware-Produkte (Application Server, Virtualisierungssoftware usw.);
- Definition und Durchführung von Automatisierungsabläufen (Ein- und Ausschalten, Erstellung von Ausdrucken, Verbindungsaufbau, usw.;)
- Konfiguration, Bereitstellung und Überwachung der Dienste nach den von der VS vorgegebenen Methoden und Regeln;
- Workload-Management im Sinne einer Charakterisierung von Komponenten und Priorisierung;
- Planung, Durchführung und Kontrolle von Wartungsarbeiten an Software und Hardware (z. B. Einspielen von Patches);
- Implementierung von Regeln (Policy) innerhalb der Betriebs- und Anwendungsumgebungen, anhand deren die Modalitäten der Erbringung der Dienste festgelegt werden;
- Wartungs- und Kontrollaktivitäten im Zusammenhang mit Unternehmensdatenbanken. Dazu gehören typischerweise:
    - Herunterfahren und Hochfahren (geplant und auf Anfrage);
    - Backup & Restore (geplant und auf Anfrage);
    - Import & Export (geplant und auf Anfrage);
    - Aktivitäten zur Leistungsüberwachung;
    - Wiederherstellungsaktivitäten im Falle eines Fehlers;
    - Aktivitäten zum Upgrade auf neue Versionen;
    - Verwaltung geplanter Aktivitäten (Planen von Jobs und Lesen von Ausführungsprotokollen).

2.3.17. Automatisierte Überwachung von Anwendungssystemen und -diensten

Der AN muss ein System zur - auch automatischen - Überwachung der Serversysteme und auch der auf den Serversystemen (physisch und virtuell) installierten Anwendungsdienste einrichten.
Die Überwachung muss aus der Ferne erfolgen und muss so eingerichtet sein, dass der Bereitschaftsdienst des AN und der VS bei Dringlichkeit angerufen wird, damit der durchgehende Betrieb gewährleistet bleibt. Der Überwachungsdienst muss bei kritischen Situationen in der Lage sein, den Verantwortlichen des IT-Departments der VS zu benachrichtigen (per SMS und/oder Mobiltelefonanruf und/oder E-Mail).

Im Rahmen der Überwachung werden folgende Aspekte kontrolliert:

- die wichtigsten Betriebsparameter der Serversysteme;
- die Ressourcenverfügbarkeit (z. B. verfügbarer Speicherplatz für die DB und für das Dateisystem mit unterschiedlichen Schwellenwerten);

- die Verfügbarkeit von DB-Instanzen;
- die Funktionalität der Anwendungsdienste auf der Basis von Parametern (Prozesse, Log-Informationen ...), die von den Lieferanten der Anwendungssoftware dokumentiert werden;
- Unregelmäßigkeiten der Server-Hardware;
- Speicherplatz-Knappheit auf der Festplatte.

Die Überwachung sorgt für die Auslösung und Verwaltung von Alarmen:

- bei Erkennung von Unregelmäßigkeiten;
- bei Überschreitung von Schwellenwerten von Indikatoren, die für den Dienst repräsentativ sind (Leistungsüberwachung).

Als **Verbesserungsmerkmal** bewertet die VS die Bereitstellung einer Anwendung, die es der SGR erlaubt, die wichtigsten Dienste der Server, der Daten- und Internetleitungen und der Hardware im Allgemeinen zu überwachen, und die Möglichkeit zur autonomen Implementierung weiterer Dienste bietet.

2.3.18. Analyse der Systemauslastung und Leistungsüberwachung

Der AN muss die Systemleistung aufrechterhalten, indem er die Serverleistung kontrolliert, misst und analysiert (z. B. hinsichtlich RAM-Belegung, Belegung des Festplattenplatzes bei verschiedenen Schwellenwerten, CPU-Auslastung, Auslagerung auf die Festplatte usw.) und Berichte erstellt, damit vorbeugende Maßnahmen zur Sicherstellung der Servicelevels festgelegt werden können.
Der AN muss die Dienstverantwortlichen der VS rechtzeitig informieren, wenn eine Anpassung/Aufrüstung der HW und/oder SW der Systeme vorzunehmen ist, um die Servicekontinuität zu gewährleisten, wie z. B. im Falle von Anwendungserweiterungen oder bei einer Erhöhung der Nutzerzahl, was auch HW-Anpassungen erfordern könnte.

2.3.19. Störungsmanagement, technische Unterstützung und korrektive Wartung

Der AN muss nach der Feststellung von Hardware- oder Software-Fehlfunktionen oder Sicherheitsvorfällen für die Behebung der festgestellten Probleme sorgen.
Die Tätigkeiten umfassen Eingriffe an allen Hardware- und Software-Komponenten (Basis- und Umgebungssoftware) der Systeme und des damit verbundenen Zubehörs, die aus irgendeinem Grund ausfallen oder Funktionsfehler aufweisen sollten.
Im Detail können die Aktivitäten wie folgt zusammengefasst werden:

- Behebung der Fehlerursache durch die Ersetzung von Teilen (Austausch) und/oder durch elektronische, mechanische oder Software-Kalibrierungen zur Wiederherstellung der ursprünglichen Leistung des Geräts;
- Wiederherstellung des Dienstes auf dem Niveau vor dem Ausfall/der Störung;
- Testen des Systems in all seinen Funktionalitäten, um die Behebung der Ursache des Fehlers/der Störung zu verifizieren;
- Wiederherstellung der Systemfunktionalität durch die vorübergehende Ersetzung mit einem eigenen gleichwertigen Gerät, falls die Reparatur/Wartung nicht gewährleistet werden kann (z. B. wegen Nichtverfügbarkeit von Ersatzteilen);
- Einschaltung, falls erforderlich, der Lieferanten, mit denen der AN Wartungsverträge hat;
- bei Bedarf Einschaltung und Koordinierung der Lieferanten, mit denen der AN Verträge mit entsprechenden Garantie- oder Interventionsklauseln abgeschlossen hat;
- ggf. Aktivierung der Lieferfirmen, mit denen die VS Verträge mit entsprechenden Garantie- oder Interventionsklauseln abgeschlossen hat. Der AN arbeitet mit diesen Unternehmen zusammen und bietet die nötige Unterstützung für die rasche Lösung des Problems.

Das Nachverfolgen des Incident-Prozesses erfolgt nach den Modalitäten und mit Hilfe des Trouble-Ticketing-Tool, das vom Helpdesk-Dienst zur Verfügung gestellt wird (siehe Technisches Leistungsverzeichnis - Abschnitt 2.4. Helpdesk für den „All-inclusive-Support“)

2.3.20. Software-Verteilung

Um die ordnungsgemäße Verwaltung des installierten Softwarebestands (Basis- und Umgebungssoftware) zu gewährleisten, muss der AN bei Bedarf für die Verteilung oder Aktualisierung der Programme (einschließlich Patch- und Firmware-Updates) sorgen.
Es wird festgelegt, dass der AN während der gesamten Vertragsdauer auf Verlangen der VS auch alle in der Citrix-Umgebung freigegebenen Programme und die auf den "Anwendungsservern" und "Dienstservern" installierten Programme installieren, aktualisieren und deinstallieren soll. Darüber hinaus muss der AN beschreiben, wie er folgende Leistungen erbringen will:

- Durchführen einer Analyse der auf der Arbeitsstation vorhandenen Patches; Hinweisen auf das Vorhandensein von veralteten Patches sowie auf die Zweckmäßigkeit, Update-Patches zu installieren;
- Remote-Übernahme der Kontrolle der Arbeitsstation, an der ein Eingriff erforderlich ist;
- Ferninstallation und Fernkonfiguration der Betriebssysteme (Release-Upgrades, Service Packs usw. ...) und Software-Anwendungen (z.B. Antivirus, Hotfixes, Security Patches, Virus Patterns ...) auf den Arbeitsstationen;
- Verteilung der Anwendungen und Softwarepakete über die Netzwerkinfrastruktur;
- Aktualisierung - periodisch oder auf Anfrage der VS - der verschiedenen installierten Anwendungen/Software mit den neuen Versionen.

Beim Erwerb neuer Software durch die VS muss der AN zunächst deren Kompatibilität mit der IT-Infrastruktur prüfen. Sobald diese bestätigt ist, installiert der AN die Software in einer Citrix-Umgebung oder auf einem virtuellen Server entsprechend den Anforderungen der VS. Die Installation, Aktualisierung oder Deinstallation wird von der VS über eine entsprechende Anfrage an das Helpdesk angefordert (siehe Technisches Leistungsverzeichnis - Abschnitt 2.4. Helpdesk für den „All-inclusive-Support“).

2.3.21. Hardware-Wartung und erweiterte Hardware- Garantie

Der AN muss für die gesamte Vertragslaufzeit die Garantie und die damit verbundene Wartung im 7x24-Modus auf alle Hardware-Geräte der Ausschreibung erweitern. Bei einem Defekt ist der AN zur aktiven Mitwirkung mit dem technischen Support verpflichtet.
Unter Wartung und erweiterter Hardware-Garantie versteht man Erneuerung der Wartung durch die Hersteller und Ersatz im Falle eines Ausfalls mit Rund-um-die-Uhr-Erreichbarkeit (24h - 7/7).
Der AN unterstützt den Hersteller und beteiligt sich aktiv an der Fehlerbehebung.

2.3.22. Verwaltung von Sicherungsrichtlinien

Der AN muss die Sicherungen selbständig abwickeln und die Sicherungsmethode einrichten.
Im Falle einer fehlgeschlagenen Datensicherung muss der AN eine E-Mail senden, in der das Problem und dessen Behebung erläutert wird. Wenn die wöchentliche, monatliche oder jährliche Datensicherung fehlschlägt, muss die Datensicherung für den nächsten Tag geplant werden.
Die VS kann den AN jederzeit über das Helpdesk-Tool auffordern, Wiederherstellungen vorzunehmen.
Außerdem muss der AN der VS täglich einen Bericht über die Ergebnisse der Sicherungs- und Wiederherstellungsvorgänge per E-Mail übermitteln; am Jahresende muss der AN der VS eine

Gesamtprotokolldatei aller Sicherungs- und Wiederherstellungsvorgänge zur Vorlage bei den Aufsichtsbehörden übermitteln.
Die Backups können von der VS und den Aufsichtsbehörden jederzeit eingesehen werden.

2.3.23. Organisation des Disaster Recovery Serverraums

Während der Vertragslaufzeit muss der AN die Bereitstellung des DR-Serverraums mit Klimaanlage, USV, Rack-Schrank, Datenleitung und Speicherplatz für Backups gewährleisten und verwalten. Der AN muss die Sicherheit des Zugangs zum Serverraum gewährleisten, indem er den Zugang zum Raum überwacht. Gefordert wird die Überwachung vor Ort durch mindestens eine Person aus dem Projektteam (siehe Kapitel 2.6 Projektteam)
Der DR-Serverraum muss immer eine konstante, automatisch durch eine Klimaanlage geregelte Temperatur haben.
Der AN muss für die gesamte Vertragslaufzeit eine 100/20-Internetleitung, einen Anschluss an das Beleuchtungssystem und einen Stromanschluss zur Verfügung stellen.
Der AN ist für das Backup-Management des DR-Servers zuständig, der sich im DR-Serverraum befindet; weiters muss er 8 TB Speicherplatz für Backups bereitstellen.
Auf Anfrage sind die VS, die externen Auditoren und die Aufsichtsorgane berechtigt, den Serverraum des AN zu betreten.
Es wird darauf hingewiesen, dass alle Kosten für das DR-Raummanagement (Stromvertrag, Internetleitung, Bereitstellung eines Rack-Schranks, Klimaanlage, USV und Backup-Speicherplatz im Falle eines Notfalls) während der gesamten Vertragsdauer sowie bei Vertragserneuerung und -verlängerung vom AN zu tragen sind.

2.4 Helpdesk für den „All-inclusive-Support“

Man beachte, dass in diesem Kapitel kontinuierlich auszuführende Leistungen gefordert werden. Hinsichtlich der Zahlungsmodalitäten wird auf das Dokument "Sonderleistungsverzeichnis für Dienstleistungen“ verwiesen.

Vom Help Desk-Service wird die Bereitstellung eines einzigen Zugangspunkts erwartet, wo Interventionsanfragen von Endbenutzern gesammelt werden, die alle servicerelevanten Aspekte betreffen können. Allen internen Benutzern des IT-Systems des Unternehmens muss Hilfe bei der Lösung von Problemen in Zusammenhang mit der Nutzung der Arbeitsstationen (Hardware, Basissoftware und Anwendungssoftware), der IT-Infrastruktur (LAN, Server usw. ...), des Portals und des Intranets der Unternehmensdienste angeboten werden.
Der Helpdesk-Service hat den Zweck, sowohl Anfragen zu Meldungen über Systemprobleme als auch Support-Anfragen betreffend die Nutzung einer Anwendungskomponente des betrieblichen IT-Systems entgegenzunehmen.

Zu diesem Zweck muss der AN logisch getrennt einen First-Level- und einen Second-Level-Helpdesk bereitstellen, so dass den Anwendern eine einzige Anlaufstelle und eine Reihe von Help-Funktionen für die Nutzung der IT-Technologieplattformen zur Verfügung stehen.
Als First-Level-Helpdesk wird das Frontend des vom AN organisierten Dienstes bezeichnet, das als zentrale Anlaufstelle für Benutzeranfragen fungiert, während der Second-Level-Helpdesk als Back-Office tätig ist.
Das vom AN vorgeschlagene Organisationsmodell muss eine Einrichtung vorsehen, die alle Supportanfragen in der unten beschriebenen Weise entgegennimmt:

- Entgegennahme der Meldung an einer einzigen Anlaufstelle; die angeforderten Meldungen können per Telefon, E-Mail, Web, Intranet usw. eingehen; Eingriffe können auch nach direkter Kommunikation durch das für den Dienst zuständige interne Personal aktiviert werden;
- Eröffnung eines Tickets für den eingegangenen Anruf und Eintragung in ein spezielles Trouble Ticket Management Tool mit automatischer Zuweisung eines eindeutigen numerischen/alphanumerischen Identifikationscodes, der mindestens die folgenden Informationen enthält:
    - Datum (Jahr, Tag, Stunde, Minute) des Eingangs der Anfrage;
    - Betriebsstätte (Kostenstelle) und Person, die den Eingriff beantragt;
    - Modalitäten des Anfrageeingangs;
    - eingeleitete Maßnahme (Lösung, Weiterleiten an eine andere Einrichtung oder Ablehnung wegen fehlender Zuständigkeit);
    - wird die Anfrage angenommen, sind folgende Angaben zu machen: Beschreibung des Problems, Schweregrad und Priorität, die dem Eingriff zugeordnet wird;
    - kurze Beschreibung der Art des Eingriffs;
    - Schätzung des Zeitaufwands bis zur Schließung des Tickets;
- Diagnose der eingegangenen Support-Anfrage und Identifizierung des Problems;
- Lösung des Problems im Rahmen des ersten Anrufs oder Bearbeitung des Eskalationsverfahrens mit Aktivierung und Koordination von zur Problemlösung geeigneten Ressourcen der zweiten Ebene, um dem Benutzer in möglichst kurzer Zeit, auf jeden Fall aber innerhalb der festgelegten Service-Levels, die Lösung bereitzustellen;
- Kontrolle des Fortschritts der Maßnahmen, die zum Schließen des Tickets erforderlich sind, auch wenn der Eingriff eventuell von anderen Organisationen und nicht vom AN selbst durchgeführt wird;
- Überprüfung mit der Person, die den Bericht ausgestellt hat, dass das gemeldete Problem behoben wurde, und anschließende Benachrichtigung über die Schließung des Tickets, wobei mindestens die folgenden Informationen anzugeben sind:
    - Beschreibung des aktivierten Eingriffs;
    - Datum (Jahr, Tag, Stunde, Minute), an dem der Eingriff beendet wurde;
    - Zeitaufwand für die durchgeführten Eingriffe in Mannstunden.

Die vom AN vorgeschlagene Organisation sollte Folgendes umfassen:

- die vollständige Verantwortung für die Bearbeitung und Schließung der Tickets gegenüber dem Benutzer durch den First-Level-Helpdesk;
- Abwicklung aller Schritte in Zusammenhang mit Interventionsanfragen zu Änderungen im Aufbau der IT-Systeme jeglicher Art und Natur (z. B. Installation eines neuen Arbeitsplatzes oder einer seiner Komponenten, Änderung der Netzwerkkonfiguration usw.);
- das Trouble-Ticketing-Tool liegt in der Verantwortung des Zuschlagsempfängers und muss über das Web zugänglich sein;
- der Helpdesk-Service muss - was die Fachkräfte und Infrastruktur anbelangt - in den Räumlichkeiten und Einrichtungen des AN angesiedelt sein;

- das Personal des First-Level-Helpdesk ist verpflichtet, die häufigsten Probleme und solche von geringer Komplexität zu lösen, die die gängigsten betrieblichen Anwendungen (Office Automation, E-Mail, Internet usw. ...) betreffen; daher muss das Helpdesk-Personal das notwendige Wissen über die Funktionsweise der im Unternehmen eingesetzten Arbeitsstationen und über die darauf installierten Softwareprodukte sowie über die Anwendungsumgebung des Unternehmens besitzen;
- die Überwachung der Servicequalität durch die Analyse der im Bezugszeitraum bearbeiteten Anrufe, um den Bedarf zu erkennen und Maßnahmen zur Vermeidung von Problemen zu definieren;
- die Erstellung von periodischen, mit dem Unternehmen festzulegenden Berichten über die erbrachten Leistungen und die erreichten Servicelevels (z.B. Anzahl der Eingriffe im Beobachtungszeitraum pro Kostenstelle, Dauer der Eingriffe pro Kostenstelle, Verteilung der Probleme nach Schwere und Priorität des Einsatzes, nach den Modalitäten des Eingriffs, durchschnittliche Dauer der Eingriffe);
- die Verantwortlichen des AN müssen jederzeit in der Lage sein, den Status jeder beliebigen Anfrage zu überprüfen und deren Bearbeitung nach den oben beschriebenen Modalitäten zu gewährleisten.

Als **Verbesserungsmerkmal** bewertet wird die Möglichkeit für die VS, eine interne Ticket-Management-Software zu verwenden, um intern die für den AN bestimmten Anfragen zu sammeln.

Es liegt in der Verantwortung des AN, halbjährlich über die Arbeit des Helpdesks in Form eines Service-Reports zu berichten, in dem die ausgeführten Tätigkeiten und die garantierten Servicelevels beschrieben werden.

Der Helpdesk-Service muss nach den oben genannten Modalitäten von Montag bis Freitag von 8:30 bis 17:30 Uhr gewährleistet werden.

2.5 Überwachung von Systemen, Diensten und Datenleitungen

Man beachte, dass in diesem Kapitel kontinuierlich auszuführende Leistungen gefordert werden. Hinsichtlich der Zahlungsmodalitäten wird auf das Dokument "Sonderleistungsverzeichnis für Dienstleistungen “ verwiesen.
Der AN muss von Montag bis Freitag von 8:30 bis 17:30 Uhr die Überwachung der Systeme und Dienste sowie die Fernbetreuung in Ergänzung zu den vom Vor-Ort-Service abgedeckten Stunden garantieren.
Darüber hinaus muss - auch an Feiertagen - ein Bereitschaftsdienst garantiert werden für alle Notfälle, die in den Systemen des Datenzentrums und/oder im Netzwerk auftreten und geschäftskritische Dienste gefährden könnten; weiters muss der Vor-Ort-Eingriff innerhalb von 2 Stunden nach dem Anruf garantiert werden. Der Eingriff kann, wenn die Situation es zulässt, auch aus der Ferne erfolgen, wenn damit der Fehler erfolgreich behoben wird.
Für alle Dienste muss der AN zur Bewertung des Angebots die charakteristischen Merkmale angeben.

Der Dienst muss auch die Überwachung der Leistung der gesamten Netzwerkinfrastruktur und der Datenleitungen ermöglichen, damit Störungen rechtzeitig erkannt und gemeldet und Ereignisse im Voraus festgestellt werden können, welche die Ursache für eine mögliche Störung sein könnten.
Der Dienst muss den Einsatz eines Überwachungssystems für alle in den Verantwortungsbereich des AN fallenden Netzkomponenten vorsehen; dieses System muss intern der zuständigen Abteilung der SGR zur Verfügung gestellt werden.
Die Überwachungs- und Verwaltungsplattform muss folgende Mindestfunktionalitäten gewährleisten:

- zyklische Abfrage der verwalteten Elemente, um deren Funktionsstatus zu überprüfen;
- Empfang von Alarmen, die aufgrund von Hardware- und/oder Software-Fehlfunktionen erzeugt wurden;
- Klassifizierung der empfangenen Alarme nach Schweregrad;

- Ausführung von vordefinierten Aktivitäten nach dem Auftreten von codierten Ereignissen.

Die Überwachungs- und Verwaltungsplattform muss in der Lage sein:

- in regelmäßigen Abständen Informationen über den Netzwerkverkehr (lokales Netzwerk und geografische Verbindungen) zu sammeln;
- die gesammelten Informationen über den Netzwerkverkehr für auswählbare Zeiträume (Stunden, Tage, Wochen, Monate) in Form einer Grafik zur Verfügung zu stellen.

Es ist Aufgabe des AN jährlich über die Netzwerkleistung zu berichten, und zwar in Form eines Berichts über die Netzwerkleistung, in dem die Leistungen der überwachten Ressourcen beschrieben und die durchgeführten oder zur allgemeinen Leistungsverbesserung vorgeschlagenen Optimierungsmaßnahmen dargelegt werden.
Das zu überwachende Indikatorenset muss im technischen Angebot festgelegt werden und kann auf Antrag der VS um zusätzliche Indikatoren ergänzt werden.

Bei außerordentlichen Wartungsarbeiten am IT-System muss deren Ausführung auch an Samstagen und Feiertagen zu mit der VS zu vereinbarenden Zeiten garantiert werden.

Die Überwachung muss nach den oben genannten Modalitäten von Montag bis Freitag von 8:30 bis 17:30 Uhr gewährleistet werden.

2.6 Projektteam

Unter Bezugnahme auf den Gegenstand und die Ziele der Ausschreibung, wie sie in den vorstehenden Absätzen beschrieben sind, hat die unterzeichnende VS die folgenden Fachkräfte für die Zusammensetzung des Projektteams bestimmt, das die ordnungsgemäße Ausführung der Dienstleistung und die Bereitstellung der erforderlichen IT-Infrastruktur gewährleisten soll.
Für die ordnungsgemäße Auftragsausführung wird die folgende personelle Mindestbesetzung gefordert:

1 Projektmanager mit Erfahrung in den Bereichen Sicherheit und Firewall
1 Senior IT-Systemtechniker, Experte für Citrix, Virtualisierung und Windows
1Senior IT-Systemtechniker mit Erfahrung im Bereich Betriebssysteme
1 Senior IT-Systemtechniker mit Erfahrung im Bereich Netzwerke
1 Junior Netzwerk-Systemtechniker

3. Derzeitiger Bestand des IT-Systems der VS - Hardware - Software und Datenleitungen

Der Bestand des IT-Systems der VS wird in den folgenden Abschnitten beschrieben. Der Zuschlagsempfänger muss die in den vorstehenden Absätzen beschriebenen Leistungen für das gesamte IT-System in seiner aktuellen Konfiguration und für die Weiterentwicklungen des Systems während der Vertragslaufzeit gewährleisten.

Generell wird verlangt, die neuesten Softwareversionen zu installieren und sie für die Dauer des Vertrages auf dem neuesten Stand zu halten.

3.1 Arbeitsstationen

Darunter versteht man Personal Computer (Desktops, Notebooks, Tablets und Thinkclients) samt Peripheriegeräten wie Bildschirm, Drucker und Scanner.

BETRIEBSSYSTEM	PC (Desktop)	Laptops
Windows 10 Pro	8	8
Windows 7 Pro	1	0
ThinkClient Praim	28	0
Insgesamt	**37**	**5**

3.2 Aktuelle virtuelle Server

Name des Servers	Betriebssystem	Dienst
PPI-Artica	Other 2.6.x Linux (64-bit)	
PPI-Artica1	Other 2.6.x Linux (64-bit)	
PPI-CTXPVS01	Microsoft Windows Server 2008 R2 (64-Bit)	Server Provisioning
PPI-CTXPVS02	Microsoft Windows Server 2008 R2 (64-Bit)	Server Provisioning
PPI-CTXPVS03	Microsoft Windows Server 2008 R2 (64-Bit)	Server Provisioning
PPI-CTXWEB01	Microsoft Windows Server 2008 R2 (64-Bit)	Portal Web Citrix
PPI-CTXWEB02	Microsoft Windows Server 2008 R2 (64-Bit)	Portal Web Citrix
PPI-DC01	Microsoft Windows Server 2008 R2 (64-Bit)	Domänencontroller-Server
PPI-DC02	Microsoft Windows Server 2008 R2 (64-Bit)	Domänencontroller-Server
PPI-DOMINO01	Microsoft Windows Server 2008 R2 (64-Bit)	Domänenserver (Mail) und SFTP-Dienste
PPI-DOMINO02	SUSE Linux Enterprise 11 (64-bit)	Domänenserver (E-Mail)
PPI-FS00	Microsoft Windows Server 2008 R2 (64-Bit)	Active Directory Server
PPI-FS01	Microsoft Windows Server 2008 R2 (64-Bit)	Active Directory Server
PPI-FS02	Microsoft Windows Server 2008 R2 (64-Bit)	Active Directory Server
PPI-JDOC	Microsoft Windows Server 2008 R2 (64-Bit)	Dokumentenserver externer Lieferant
PPI-Master	Microsoft Windows Server 2008 R2 (64-Bit)	Citrix-Image-Server
PPI-PRÄSENZEN	Microsoft Windows Server 2008 R2 (64-Bit)	Server SW Stempelkarte
PPI-PRINT01	Microsoft Windows Server 2008 R2 (64-Bit)	Druckerserver
PPI-AUTHPOINT	Microsoft Windows Server 2018 R2 (64-Bit)	VPN-Authentifizierungsserver
PPI-Proxy	Other 2.6.x Linux (64-bit)	Proxy-Server
PPI-PSQL	Debian GNU/Linux 6 (64-bit)	Citrix-Server-Farm
PPI-REPORT	Microsoft Windows Server 2008 R2 (64-Bit)	Server SW Rendiconto.NET mit SQL
PPI-SAMETIME	Microsoft Windows Server 2008 R2 (64-Bit)	Domino Chat Server
PPI-SQL01	Microsoft Windows Server 2008 R2 (64-Bit)	Citrix SQL-Server

Name des Servers	Betriebssystem	Dienst
PPI-traveler	SUSE Linux Enterprise 11 (64-bit)	Mailserver App für Endgeräte
PPI-XENAPP0	Microsoft Windows Server 2008 R2 (64-Bit)	Konsolenserver Citrix Farm
PPI-XENAPP18	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP20-Mnt	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Management
PPI-XENAPP21-Test	Microsoft Windows Server 2008 R2 (64-Bit)	Testserver Citrix Farm
PPI-XENAPP22	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP23	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP24	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP25	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP26	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP27	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm
PPI-XENAPP28	Microsoft Windows Server 2008 R2 (64-Bit)	Server Citrix Farm

3.3 In Citrix mit Active Directory verteilte Software

Software	Beschreibung	Eigentum	Installiert	Gemietet
Adobe Writer	10	X		
Adobe Cloud	Neueste Version			X
Ms Office 2019 Professional Plus 2019 OLP government	Excel, Word, PowerPoint, Access X64 U.V.	X		X
IBM Lotus Notes	Lotus Version 8.5.3			X
7 ZIP	7-ZIP 18.05 X64		X	
BASECAMP 3	Neueste Version			X
DIKE 6	Neueste Version		X	
ACROBAT READER DC	Neueste Version		X	
ARUBA-SIGN	Neueste Version		X	
FILEZILLA FTP	Neueste Version		X	
FIREFOX	Neueste Version		X	
FIRMA OK	Neueste Version		X	
FOXIT-LESER	Neueste Version		X	
GANTT PROJECT	Neueste Version		X	
GOOGLE CHROME	Neueste Version		X	
IDLE PHYTON	3.5 X64		X	
LibreOfficePortable_6.2.2_MultilingualAll			X	
NOTEPAD ++	Neueste Version		X	
Ms Office 2019 Professional Plus	2019	X		
OCTAVE	Neueste Version		X	
PDF SPLIT AND MERGE	2.2.4		X	
PDF CREATOR	1.6.1		X	
PSAICK	Neueste Version		X	
R	Neueste Version		X	
RAP.NET	4.3.48	X		

Software	Beschreibung	Eigentum	Installiert	Gemietet
RENDICONTO		X		
R-STUDIO	Neueste Version		X	
SAFEGUARD PRIVATCRYPTO			X	
STATPRO REVOLUTION				X
THINKCELL-Komponente in MS Excel	Neueste Version			X
TRADEWEB			X	
TRELLO	Neueste Version		X	
TREND OFFICESCAN				X
ULTRA VNC			X	
WINSCP	Neueste Version		X	

U.V.: Ultima versione / Neueste Version

3.4 Aktuelle Netzwerkgeräte

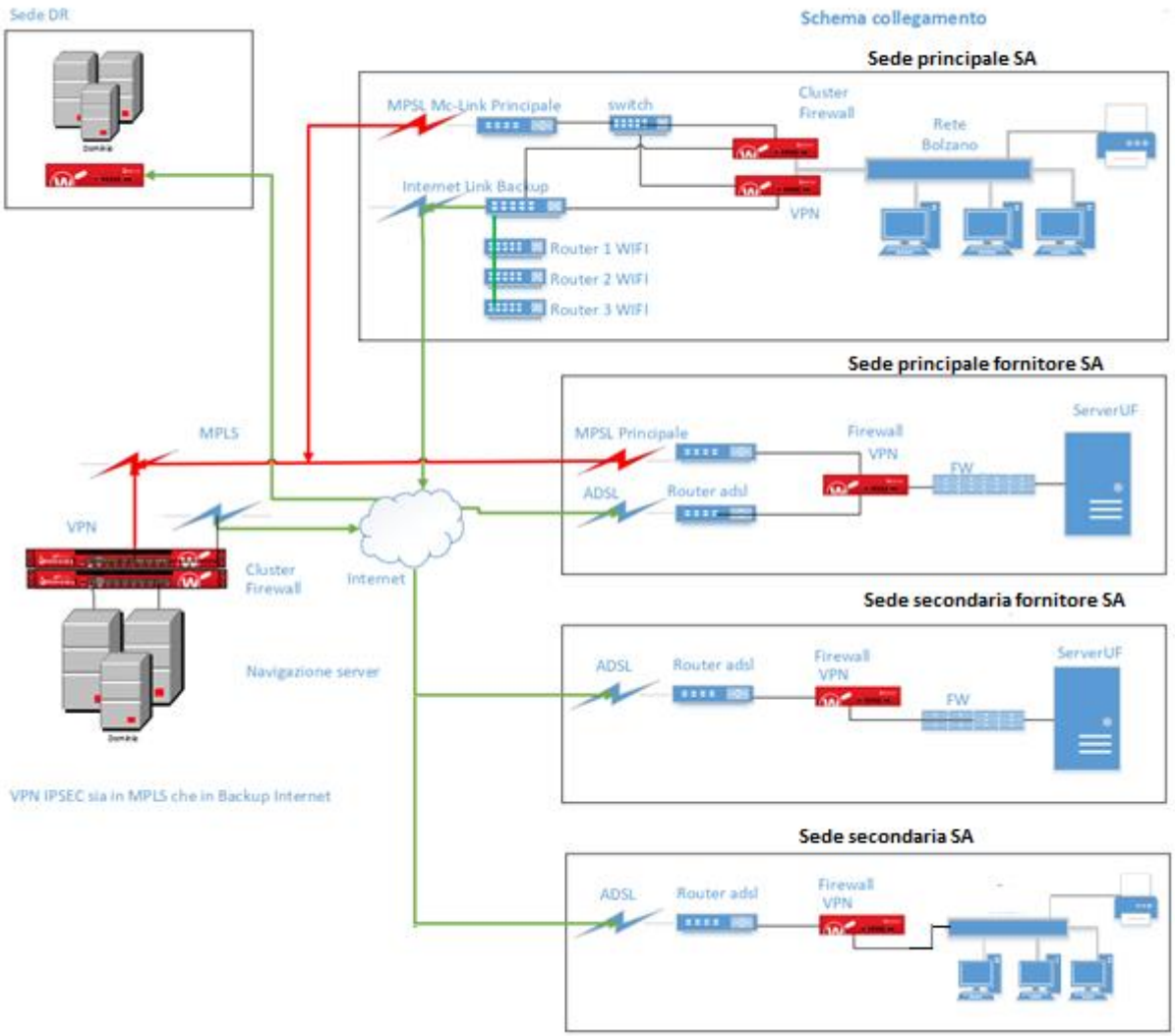
Marke und Modell	Standort
XEROX 3330 DRUCKER	4. Stockwerk
XEROX 3330 DRUCKER	3. Stockwerk
XEROX 3330 DRUCKER	3. Stockwerk
XEROX C8055 Drucker	1. Stockwerk
RICOH C3001 DRUCKER	1. Stockwerk
ZDESIGNER-DRUCKER.	3. Stockwerk
ZDESIGNER-DRUCKER.	3. Stockwerk
SWITCH 48	Serverraum VS
SWITCH 48	Serverraum VS
FIREWALL	Serverraum VS
FIREWALL	Serverraum VS
WIFI-ROUTER	Serverraum VS
2 WIFI-REPEATER	1. Stockwerk
2 WIFI-REPEATER	2. Stockwerk
2 WIFI-REPEATER	3. Stockwerk
1 WIFI-REPEATER	4. Stockwerk
TELEFONZENTRALE	Serverraum VS
BLADE	Serverraum des derzeitigen IT-Dienstleisters
BLADE	Serverraum des derzeitigen IT-Dienstleisters
BLADE	Serverraum des derzeitigen IT-Dienstleisters
SAN	Serverraum des derzeitigen IT-Dienstleisters

3.5 Aktuelle Datenleitungen

STANDORT	BESTIMMUNG	BESCHREIBUNG	LIEFERANT	TYP	SPEED
Euregio Plus: Mustergasse	INTERNET	Internetzugang und D.R.-Backup und	Anbieter 1	VDSL	Download 100 Mega -

STANDORT	BESTIMMUNG	BESCHREIBUNG	LIEFERANT	TYP	SPEED
11/-3 - 39100 Bozen		Nutzung für VPN-Zugänge			Upload 20 Mega
Euregio Plus: Mustergasse 11/-3 - 39100 Bozen	Serverraum beim derzeitigen externen IT-Dienstleister	Verbindung Serverraum - Sitz der VS	Anbieter 2	MPLS	Download 8 Mega - Upload 8 Mega
Serverraum beim derzeitigen externen IT-Dienstleister		MPLS-Schliessung	Anbieter 2	Lieferung MPLS	Download 100 Mega – Upload 100
Serverraum beim derzeitigen externen IT-Dienstleister	Finanzdienstleister: via Savona 1-5 - 20144 Milano	Verbindung Serverraum - Finanzdienstleister - Hauptleitung	Anbieter 2	MPLS	Download 4 Mega - Upload 4 Mega
Serverraum beim derzeitigen externen IT-Dienstleister	Finanzdienstleister: via Savona 1-5 - 20144 Milano	Verbindung Serverraum - Finanzdienstleister - Backup-Leitung	Anbieter 1	ADSL	Download 20 Mega - Upload 1 Mega
Serverraum beim derzeitigen externen IT-Dienstleister	Finanzdienstleister: via Darwin -5 - 20019 Settimo Milanese	Verbindung Serverraum - Finanzdienstleister D.R.-Leitung.	Anbieter 1	ADSL	Download 20 Mega - Upload 1 Mega
INTERNET		Internetleitung für Backup	Anbieter 2	Glasfaser	1Gbit symmetrisch
Serverraum beim derzeitigen externen IT-Dienstleister	INTERNET	Internetleitung Server	Anbieter 2	Glasfaser	Download 100 Mega – Upload 100
Zweitsitz des aktuellen externen IT-Dienstleisters	Serverraum beim derzeitigen externen IT-Dienstleister	Verbindung zwischen dem Serverraum und dem DR-Standort	Anbieter 2	Glasfaser	Dark Fiber 10 Gigabit

3.6 Derzeitiges Anschlussschema



3.7 Schema der Serverstruktur