Sede amministrativa - Verwaltungssitz:
Via Zuegg Str. 40 I - 39012 Merano-Meran
Tel. +39 0473 498 300 - Fax +39 0473 498 303

Sede legale – Rechtssitz:
Via A.-Ammon Str. 24 I - 39042 Bressanone – Brixen
Tel. +39 0472 823 636 - Fax +39 0472 823 666
CF P.IVA St./MwSt.Nr IT / 02298140217

Capitolato Tecnico

Indice

1. Introduzione - Natura giuridica, oggetto sociale e ambito dell'attività svolta da ITS S.r.l. 2
2. Perimetro del servizio 3
2.1. Descrizione dell'infrastruttura attuale 3
2.2. Risorse attualmente allocate ed utilizzate 3
2.3. Requisiti per il Datacenter che ospita l'infrastruttura di virtualizzazione 4
2.4. Requisiti dell'infrastruttura di virtualizzazione 6
2.5. Licensing dei sistemi nel datacenter 6
2.6. Requisiti per la gestione del Backup 7
2.7. Requisiti per la gestione del Disaster Recovery 9
2.8. Disastro che interessi una sede di ITS 9
2.9. Disastro che interessi il Datacenter 10
2.10. Requisiti per la protezione antivirus/antimalware 11
2.11. Requisiti per la gestione della virtualizzazione delle postazioni di lavoro 11
2.12. Requisiti per la gestione della sicurezza perimetrale del Datacenter e delle sedi ITS 12
2.13. Auditing di sicurezza dei sistemi 15
2.14. Gestione dei sistemi di ITS nel datacenter 15
2.15. Gestione dei dispositivi client nelle sedi ITS 16
2.16. Gestione licenze di proprietà ITS 17
2.17. Gestione dei dispositivi di rete attivi nelle sedi ITS 17
2.18. Migrazione dei sistemi al nuovo fornitore 18
2.19. Organizzazione del servizio post migrazione 20
3. Time & Material 21
4. Livelli di servizio 22
5. Ampliamenti 23

1. Introduzione - Natura giuridica, oggetto sociale e ambito dell'attività svolta da ITS S.r.l.

ITS S.r.l. è una società a integrale partecipazione pubblica, che opera secondo il modello del "in house providing", come disciplinato dall'ordinamento dall'Unione Europea e dall'ordinamento interno, a norma degli artt. 5 e 192 del d.lgs. n. 50/2016 e s.m.i., 4 e 16 del d.lgs. n. 175/2016 e s.m.i. e della L.P. Bolzano n. 12/2007 e s.m.i..

In qualità di società in house, ITS svolge attività di produzione di beni e servizi necessari per il perseguimento delle finalità istituzionali delle Società Socie in via diretta e, loro tramite, delle Amministrazioni indirettamente partecipanti (art. 4, comma 1, d.lgs. n. 175/2016 e s.m.i.; art. 1, comma 4, L.P. Bolzano n. 12/2007 e s.m.i.), vale a dire, attività di autoproduzione di beni o servizi strumentali alle Socie in via diretta e alle Amministrazioni indirettamente partecipanti, o strumentali allo svolgimento delle loro funzioni (servizi informatici strumentali), nel rispetto delle condizioni stabilite dalle direttive europee in materia di contratti pubblici e della relativa disciplina nazionale di recepimento (art. 4, commi 2, lett. "d", e 4, d.lgs. n. 175/2016 e s.m.i.; art. 1, comma 4 bis, L.P. Bolzano n. 12/2007 e s.m.i.).

In ragione di quanto sopra, le prestazioni e le specifiche tecniche descritte nel presente capitolato tecnico devono intendersi riferite al fabbisogno di ITS complessivamente inteso, ricomprendente le attività strumentali dalla medesima svolte in favore dei propri enti Soci, tenendo altresì conto che le sedi di esecuzione dei servizi sono localizzate sia presso ITS, sia presso gli enti Soci della stessa ITS. In particolare, le sedi di esecuzione del servizio saranno le seguenti:

- ITS: Via Peter Anich 24, 39011, Lana (BZ)
- ITS: Via A.Ammon 24A, 39042, Bressanone (BZ)
- ITS: Via A. Brogliati civici 8 10 12 14, 39012 Merano (BZ) – NUOVA SEDE
- ASM Merano: Viale Europa 4, 39012, Merano (BZ)
- ASM Merano: Via L.Zuegg 68c, 39012, Merano (BZ)
- ASM Merano: Via Peter Anich 24, 39011, Lana (BZ)
- ASM Merano: Via A. Brogliati civici 8 10 12 14, 39012 Merano (BZ) – NUOVA SEDE
- ASM Bressanone: via Alfred Ammon 24, 39042 Bressanone (BZ)
- ASM Bressanone: c/o Acquarena, Via Mercato Vecchio 28/b, 39042 Bressanone (BZ)
- ASM Bressanone: Via Roma 9, 39042 Bressanone (BZ)
- SEAB: via Lancia, 4/A, 39100 Bolzano (BZ)

In tutto il documento, salvo dove diversamente specificato, il riferimento alle sedi di ITS dovrà intendersi come sedi di ITS e Società Socie; analogamente, salvo dove diversamente specificato, l'erogazione dei servizi ad ITS sarà da intendersi come servizi per ITS e Società Socie.

La nuova sede di ITS e ASM Merano di Via Brogliati a Merano diverrà operativa verosimilmente durante l'anno 2022, e comporterà il trasferimento di personale e materiali da altre sedi delle rispettive aziende. Non si prevede che l'apertura della nuova sede comporti variazioni nel numero di postazioni complessive e nel numero dei sistemi gestiti che ricadono sotto il presente bando. L'azienda aggiudicataria sarà coinvolta nelle attività di trasferimento degli apparati per quanto concerne lo spostamento e riconfigurazione dei dispositivi di sicurezza perimetrale e riconfigurazione delle

postazioni di lavoro, attingendo alle risorse già previste nel **Errore. L'origine riferimento non è stata trovata.**.

2. Perimetro del servizio

Il perimetro del servizio oggetto di gara si compone delle seguenti componenti:

- fornitura e gestione dell'infrastruttura di virtualizzazione per i server applicativi ed infrastrutturali di ITS;
- fornitura e gestione dell'infrastruttura di virtualizzazione per i desktop virtuali (VDI) delle postazioni di lavoro (PDL);
- gestione e manutenzione dei sistemi operativi dei server infrastrutturali ed applicativi;
- gestione e manutenzione centralizzata dei sistemi client presenti nelle diverse sedi di ITS;
- fornitura e gestione della sicurezza perimetrale del datacenter;
- fornitura e gestione della sicurezza perimetrale delle sedi ITS indicate nell'apposito paragrafo;
- gestione degli apparati di rete attivi delle sedi ITS (switch, router, access-point, ecc.) indicate nell'apposito paragrafo;
- supporto sistemistico per le attività svolte da altri fornitori sugli applicativi e sui sistemi presenti nell'infrastruttura di ITS;
- gestione della sicurezza dei dati ospitati nel datacenter, con particolare riferimento alle procedure di backup;
- gestione delle procedure di attivazione del servizio di Disaster Recovery in caso di disastro del datacenter o di una o più sedi di ITS;
- documentazione del servizio;
- supporto per l'implementazione e successiva presa in carico di eventuali nuovi servizi ed applicativi che verranno implementati successivamente all'aggiudicazione.

Nei capitoli seguenti si andranno ad esporre nel dettaglio le succitate componenti.

2.1. Descrizione dell'infrastruttura attuale

L'infrastruttura di ITS è attualmente ospitata nei datacenter di Konverto S.p.A., con sede in Bolzano, Via Bruno Buozzi, 8, appaltatore uscente del servizio, ed è composta di:

- 30 server virtuali dedicati ad ospitare gli applicativi infrastrutturali e gestionali di ITS;
- un'infrastruttura di virtualizzazione delle postazioni di lavoro (PDL) basata su Citrix XenApp con 4 VDA server dedicati ad ITS (di cui 3 generici ed 1 dedicato ad una specifica funzione);
- un server fisico (di proprietà di ITS) utilizzato per il database Oracle.

I servizi erogati dal Datacenter sono utilizzati dagli utenti dislocati nelle sedi di ITS e società socie indicate nel paragrafo **Errore. L'origine riferimento non è stata trovata.** attraverso connettività MPLS e dagli utenti mobili ed in Smart Working attraverso Internet utilizzando i servizi di VPN erogati dall'attuale gestore.

2.2. Risorse attualmente allocate ed utilizzate

Nell'allegato A è riportato il dettaglio delle macchine virtuali e fisiche attualmente presenti nel sistema informativo di ITS con le risorse ad esse allocate ed una spiegazione della funzione di ciascun server.

In totale l'attuale occupazione di risorse virtuali per i server di ITS (esclusi i server VDA di Citrix) è pari a:

- Numero server: 30 server attivi
- CPU: 85 vCPU assegnate
- RAM: 274 GB allocati
- Disco: 8290 GB effettivi distribuiti su 61 dischi virtuali

Oltre ai sistemi succitati, già operativi nel datacenter attuale, è previsto di spostare in datacenter anche l'applicativo SAP attualmente installato a Bressanone, la cui migrazione è già in corso e che si prevede sia portata a compimento prima che sia completata la gara di cui al presente bando. I sistemi SAP richiederanno le seguenti risorse aggiuntive:

- Numero server: 3 server aggiuntivi
- CPU: 8 vCPU assegnate
- RAM: 48 GB allocati
- Disco: 1500 GB effettivi distribuiti su 36 dischi virtuali

Come successivamente descritto in modo più approfondito nel capitolo dedicato, le risorse impiegate per i server VDA Citrix sono da considerare escluse dal computo delle risorse di ITS in quanto considerate come parte del servizio e quindi da contemplare nel canone mensile per postazione.

Per consentire le opportune valutazioni di seguito sono indicate le risorse computazionali attualmente dedicate ai server Citrix VDA:

- Numero server: 4 server attivi
- CPU: 32 vCPU assegnate
- RAM: 146 GB allocati
- Disco: 430 GB effettivi distribuiti su 4 dischi virtuali

Considerando i tassi standard di crescita del volume dei dati trattati e dell'utilizzo delle risorse computazionali, si stima che le risorse da allocare complessivamente nei prossimi due anni, a parità di numero di server, includendo i nuovi server SAP ed escludendo le risorse dedicate a Citrix, siano indicativamente:

- CPU: 100 vCPU
- RAM: 360GB
- Disco: 12 TB

L'aggiudicatario si impegna a mettere a disposizione sin da subito, o entro 8 ore lavorative dalla richiesta, le risorse stimate nel paragrafo precedente nel reso40urce pool dedicato ad ITS. L'utilizzo delle risorse fino ai limiti precedentemente indicati, salvo variazione del numero di server virtuali, dovrà essere contemplato nel canone mensile e non dovrà comportare alcun costo aggiuntivo per ITS (al netto di eventuali costi di licenza aggiuntivi necessari per fare uso delle suddette risorse).

2.3. Requisiti per il Datacenter che ospita l'infrastruttura di virtualizzazione

Il Datacenter che ospiterà i sistemi di ITS di produzione, virtuali e fisici, dovrà essere di proprietà dell'azienda aggiudicataria o in alternativa potrà essere ospitato in un Datacenter di altra azienda purché in rack dedicati ai sistemi dell'azienda aggiudicataria ed il cui accesso sia sotto il controllo e la responsabilità dell'impresa partecipante.

Il datacenter dovrà avere i seguenti requisiti minimi:

- essere dotato di almeno due linee di alimentazione elettrica indipendenti;
- essere dotato di un gruppo di continuità (UPS, Uninterruptible Power Supply) su ciascuna linea per la prevenzione delle interruzioni di energia elettrica (è indifferente la tecnologia purché opportunamente dimensionato) e per la stabilizzazione dell'alimentazione;
- essere dotato di generatori ausiliari che possano garantire almeno 72 ore continuative di autonomia in caso di problemi di fornitura dell'energia elettrica;
- essere dotato di un sistema di controllo della temperatura ed umidità ridondato della sala che dovrà ospitare i sistemi con cui verranno erogati i servizi del presente bando;
- essere dotato di un sistema antincendio, basato su rilevatori di fumo e/o rilevatori di calore, che funzioni utilizzando gas inerte o aerosol o tecnologia equivalente che non danneggi le apparecchiature non direttamente interessate dal fuoco;
- essere dotato di almeno due connessioni ad internet indipendenti su percorsi fisici differenziati e/o su tecnologie differenti ed afferenti ad almeno due diversi fornitori di connettività;
- essere dotato di un controllo di accesso che consenta la tracciabilità degli accessi fisici delle persone alla sala che ospita i sistemi e che conservi il log degli accessi per almeno 30 giorni;
- essere dotato di un sistema di videosorveglianza che registri gli accessi alla sala che ospita i sistemi di ITS e che conservi i filmati per almeno 24 ore;
- essere dotato di un sistema di allarme anti intrusione;
- essere dotato di rack con chiusura a chiave o elettronica; l'azienda si impegna a garantire che tutti i rack ospitanti i sistemi di ITS siano chiusi a chiave salvo durante lo svolgimento di operazioni di manutenzione;
- essere presidiato localmente o remotamente 24 ore al giorno, 7 giorni su 7, con possibilità di accedere ai sistemi a qualsiasi ora ed in qualsiasi giorno entro 4 ore dalla richiesta di accesso; le modalità con cui effettuare la richiesta dovranno essere indicate dall'azienda aggiudicatrice;
- essere provvisto di un'analisi dei rischi che consideri tutti i principali rischi di disastro e le eventuali contromisure adottate per evitarli e/o mitigarli.

Oltre al datacenter principale per i sistemi di produzione, dovrà essere nella disponibilità dell'azienda aggiudicataria **- sempre per la fase di esecuzione del servizio, al momento della stipulazione del contratto d'appalto -** un secondo datacenter per la gestione del disaster recovery (DR). Il datacenter di DR potrà essere di proprietà o di aziende terze, purché siano rispettati tutti i requisiti enunciati precedentemente per il datacenter di produzione.
Il datacenter di DR dovrà inoltre rispettare i seguenti requisiti aggiuntivi:

- essere in un luogo geografico differente dal datacenter di produzione e distante dallo stesso almeno 40km in linea d'aria;
- essere esposto a rischio idrogeologico differente dal datacenter di produzione, per esempio per collocazione in un bacino idrogeologico differente o per diverse misure di mitigazione del rischio (p.es. sopraelevazione);
- essere esposto a rischio sismico differente dal datacenter di produzione, per esempio per localizzazione in un'area sismica differente o per l'adozione di sistemi di isolamento sismico.

Il datacenter di produzione dovrà essere ospitato sul territorio italiano entro un raggio di 140km dalla città di Bolzano, questo per permettere eventuali interventi sui server di proprietà entro tempi ragionevoli, mentre il datacenter di DR potrà essere localizzato in qualsiasi paese dell'Unione Europea. In nessun caso i sistemi ed i dati di ITS potranno essere salvati o copiati su sistemi in stati esterni all'Unione Europea se non in forma crittografata con crittografia AES e chiave a 256bit o superiore.

2.4. Requisiti dell'infrastruttura di virtualizzazione

L'infrastruttura di virtualizzazione per i server applicativi ed infrastrutturali di ITS dovrà essere basata sulla piattaforma vSphere 6.7 o superiore di VMware. Tale piattaforma è requisito necessario per la certificazione dei sitemi utilizzati da alcune applicazioni in uso da ITS.
I server fisici che ospitano le macchine virtuali di ITS dovranno essere configurati in modo tale che non siano vulnerabili ad attacchi basati su side-channels (Spectre, Meldown, ecc.), per esempio disabilitando le funzionalità di Hyper Threading o con le apposite confiugrazioni previste dal vendor. In alternativa, se preferito dal fornitore, i server fisici potranno essere dedicati ad ITS, ovvero durante il funzionamento ordinario sui medesimi host fisici non dovranno essere presenti sistemi di altri clienti, fatta eccezione per i sistemi del fornitore stesso necessari per la corretta erogazione dei servizi (p.es. antivirus centralizzato, appliance VMware di gestione, sistemi di backup, ecc.). Questa regola potrà essere derogata solo durante le fasi di manutenzione o in caso di malfunzionamento di un host fisico o in accordo con ITS per specifiche virtual machine.
Le macchine virtuali, le reti ed i Datastore utilizzati dai sistemi di ITS, con l'esclusione dei sistemi per l'erogazione dei servizi di virtualizzazione dei desktop, dovranno essere associati ad un insieme di risorse dedicato (Resource Pool) e dovrà essere fornito ad ITS un accesso al sistema di gestione dell'infrastruttura di virtualizzazione (p.es. Vcenter o vCloud Director) che consenta di amministrare le risorse nel Resource Pool assegnato senza necessariamente interessare il fornitore per l'esecuzione delle attività ordinarie (accesso console alle VM, accensione e spegnimento delle macchine, variazioni di RAM, CPU o disco nei limiti delle risorse del Resource Pool, spostamento di rete di una VM, ecc.).
I sistemi implicati nell'erogazione dei servizi di virtual desktop non dovranno far parte del Resource Pool di cui al paragrafo precedente ma potranno essere messi in un diverso Resource Pool, dedicato o condiviso tra i clienti dell'azienda aggiudicataria. Per i server dell'infrastruttura di virtualizzazione delle postazioni di lavoro non è richiesto l'accesso gestionale da parte di ITS (VCenter, vCloud Director, ecc.).

2.5. Licensing dei sistemi nel datacenter

Tutte le licenze per l'infrastruttura di virtualizzazione vSphere dovranno essere gestite secondo i criteri del VMware Service Provider Program (VSPP). Le licenze per i sistemi operativi Microsoft dovranno essere incluse nel costo delle virtual machine; è indifferente il modello di licensing scelto dall'azienda per i sistemi operativi, purché tutte le macchine virtuali siano correttamente licenziate; il costo del licenziamento Microsoft per il sistema operativo dovrà essere considerato come costo mensile ricorrente per il committente.

Il licenziamento per la soluzione di backup varia in funzione della soluzione proposta e del software utilizzato. L'aggiudicatario è tenuto a garantire che tutti i sistemi siano correttamente licenziati secondo quanto previsto dal produttore del prodotto offerto.

Il licenziamento per la soluzione antivirus/antimalware varia in funzione della soluzione proposta e del software utilizzato. L'aggiudicatario è tenuto a garantire che tutti i sistemi siano correttamente licenziati secondo quanto previsto dal produttore del prodotto offerto.

I costi di licenza per i server virtuali, per i sistemi operativi Microsoft, per il backup dei sistemi e per la soluzione antivirus/antimalware dovranno essere mantenuti invariati durante l'intera durata del contratto, a meno che non intervengano modifiche da parte dei rispettivi vendor sul modello di licensing dei sistemi o variazioni di costo maggiori del 15% sul listino di riferimento del vendor. Nel caso in cui l'aggiudicatario, durante il periodo di validità del contratto, intenda cambiare i prodotti utilizzati per la gestione dei servizi accessori (antivirus, backup, sicurezza perimetrale, ecc.), sarà sua responsabilità garantire il rispetto dei requisiti del presente capitolato da parte dei nuovi prodotti e da tale attività non potranno derivare disservizi o maggiori oneri per la stazione appaltante.

2.6. Requisiti per la gestione del Backup

Per garantire l'integrità e la disponibilità dei dati, dovranno essere effettuate delle copie di sicurezza (backup) di tutti i sistemi di ITS che includano sia il sistema operativo che le applicazioni ed i relativi dati. Il sistema di backup implementato dovrà rispettare i seguenti requisiti:

- la soluzione di backup dovrà garantire la possibilità di eseguire il restore di interi sistemi o di singoli files interni ai sistemi, sia per i sistemi Microsoft Windows, sia per i sistemi GNU/Linux. Dovrà inoltre garantire l'integrità applicativa nel salvataggio di database Active Directory, Oracle e Microsoft SQL Server e consentire il restore di singoli oggetti per i database Active Directory, Oracle e Microsoft SQL Server. Per tutti gli altri applicativi è sufficiente che sia garantita la crash consistency;
- i salvataggi dovranno essere effettuati per tutti i servizi con cadenza almeno giornaliera (compresi sabato, domenica e festivi); per i servizi critici potrà essere definita una frequenza di salvataggio dei dati maggiore ma non inferiore ad 1 ora;
- l'esito dei backup dovrà essere verificato giornalmente e dovrà essere segnalata al referente di ITS ogni anomalia che abbia comportato il fallimento del salvataggio di uno o più sistemi e/o servizi (o in alternativa inviare giornalmente la notifica dell'esito dei backup al referente di ITS);

- in caso di fallimento di un backup dovrà esserne verificata la causa e dovranno essere adottate le opportune misure correttive che garantiscano il successo del salvataggio di sicurezza entro le 24 ore successive, eventualmente provvedendo all'esecuzione di un backup estemporaneo od adottando temporaneamente un'altra soluzione di salvataggio, anche manuale, che garantisca di non superare le 48 ore di indisponibilità delle copie di sicurezza di tutti sistemi di ITS. In tale circostanza dovrà essere tempestivamente avvisato il referente di ITS riportando l'evento, le cause che l'hanno determinato e le misure correttive adottate;
- i backup di tutti i sistemi dovranno essere conservati utilizzando uno schema GFS (Grandfather, Father and Son) per i seguenti intervalli di tempo:
  - 1 giorno per i salvataggi ad intervalli di tempo inferiori alle 24 ore;
  - 30 giorni per i salvataggi con granularità di 1 giorno;
  - 1 anno per i salvataggi con granularità di 1 mese;
  - 5 anni con granularità di 1 anno;
- le copie di backup dei sistemi di ITS degli ultimi 7 giorni dovranno essere ospitate su sistemi online che garantiscano il restore dei dati dell'ultimo salvataggio in tempi rapidi e possibilmente che consentano di far ripartire eventuali virtual machine critiche direttamente dal repository di backup (p.es. NAS, Storage Appliance dedicate, ecc.);
- con cadenza non superiore a 3 giorni, le copie di backup dovranno essere copiate o trasferite su un sistema di salvataggio offline rispetto al sistema principale (p.es. librerie di nastri LTO, VTL con gestione automatica della retention, Storage Appliance con funzionalità di Snapshot automatizzato, soluzioni di gestione del backup in cloud, ecc.) in modo tale da garantire che anche in caso di minacce informatiche che prendano di mira i sistemi di produzione e i sistemi di backup online (p.es. furto di credenziali del sistema di backup, ransomware, ecc.), del committente e/o del fornitore, non ci possa essere una perdita di dati superiore a 4 giorni solari;
- la soluzione di backup proposta deve prevedere la verifica automatica dell'integrità delle copie di salvataggio con cadenza almeno settimanale. In accordo con ITS dovranno essere condotte delle prove di ripristino dei salvataggi di backup:
  - con cadenza semestrale dovrà essere effettuata una prova di restore di una o più macchine virtuali nella loro interezza;
  - con cadenza mensile dovrà essere effettuata una prova di restore di uno o più files e/o oggetti applicativi;
  - con cadenza annuale dovrà essere effettuata una prova di restore del server fisico con Oracle su altro server fisico o su macchina virtuale, verificando che i dati e le applicazioni funzionino correttamente sul sistema ripristinato.

  Qualora si verifichi la reale necessità di un restore di interi sistemi e/o di singoli files, si considererà effettuata la prova per il periodo corrispondente.

Allo stato attuale per il backup dei sistemi sono utilizzati complessivamente 21,5TB di spazio. Si richiede pertanto che sia incluso nel canone del servizio l'occupazione di massimo 30TB entro il termine del contratto. Eventuali esigenze di aumento dello spazio per i salvataggi oltre i 30TB

potranno essere richiesti in tagli di 100GB e comporteranno un adeguamento del canone come da offerta economica.
Oltre ai backup dei sistemi di ITS presso il datacenter del fornitore, è richiesto l'approntamento di una soluzione di backup che gestisca i salvataggi dei dati ospitati sulla piattaforma in cloud di Microsoft Office365. In particolare la soluzione di backup proposta dovrà salvare tutti i documenti ed i files degli applicativi per la gesione delle mail (Outlook), Microsoft Teams, Microsoft OneDrive e Microsoft Sharepoint ospitati sui tenant di ITS e delle Società Socie in gestione all'azienda aggiudicataria e dovrà garantire la retention di almeno un anno con granularità di un giorno. Attualmente per i salvataggi di Office365 sono utilizzati circa 780GB di spazio di archiviazione; è pertanto richiesto di includere nel canone del servizio uno spazio dedicato al salvataggio di Office365 di 1,5TB; eventuali esigenze di aumento dello spazio per i salvataggi oltre gli 1,5TB potranno essere richiesti in tagli di 100GB e comporteranno un adeguamento del canone come da offerta economica.
Per quanto riguarda il sistema di gestione dei backup offline, la proposta di soluzioni con media rimovibili (p.es. nastri LTO) o non sovrascrivibili (p.es. Appliance con gestione automatica della retention) sono preferite rispetto a soluzioni di storage tradizionali.
Si richiede di allegare all'offerta la documentazione tecnica che descriva la soluzione di backup proposta evidenziandone il rispetto dei requisiti sopra indicati.

2.7. Requisiti per la gestione del Disaster Recovery

Al fine di garantire l'erogazione dei servizi anche nell'eventualità che si verifichi un disastro, dovrà essere predisposto un piano di disaster recovery per tutti i servizi inclusi nel perimetro.
Per disastro si intende qualsiasi incidente che determini l'indisponibilità totale o parziale dei sistemi informatici del datacenter e/o che determini l'indisponibilità totale o parziale di una delle sedi di ITS inclusa nel perimetro del servizio per un tempo prolungato.

2.8. Disastro che interessi una sede di ITS

Nel caso ad essere interessata da disastro sia una sede di ITS, e ciò comporti la perdita totale o parziale dei dispositivi informatici presenti nel sito interessato e coperti dal servizio, l'azienda aggiudicataria, entro un massimo di 72 ore dalla comunicazione della dichiarazione di disastro da parte di ITS, dovrà mettere a disposizione:

- fino ad un massimo di 15 postazioni di lavoro presso una o più sale, in un'unico sito, distante non più di 40km dalla città di Bolzano;
- adeguata connettività tra il sito con le postazioni di lavoro ed il datacenter;
- fino ad un massimo di 10 postazioni di lavoro per smart-working.

Ciascuna postazione di lavoro dovrà essere dotata di:

- una scrivania;
- una sedia ergonomica;
- un PC con monitor da almeno 15 pollici, indifferentemente portatile o desktop con tastiera e mouse;
- connettività ethernet o WiFi con accesso ad Internet, al Datacenter ed alle altre sedi ITS;

- gestione della sicurezza perimetrale con caratteristiche analoghe a quelle delle altre sedi ITS anche in configurazione non ridondante

Le postazioni di lavoro per smart-working dovranno essere costituite da:

- un sistema portatile con monitor da almeno 14 pollici, preconfigurato per accedere ai servizi di ITS mediante VPN.

Il servizio potrà avere una durata massima di 60 giorni solari.

2.9. Disastro che interessi il Datacenter

L'azienda aggiudicataria deve allegare all'offerta il Piano di Disaster Recovery (DRP – Disaster Recovery Plan) per i servizi di datacenter inerente il datacenter di produzione deputato ad ospitare i sistemi di ITS. Nel DRP dovranno essere individuate le figure coinvolte nella gestione del disaster recovery e le modalità di attivazione delle procedure di gestione del disastro.

Le procedure di disaster recovery (DR) potranno essere attivate qualora i servizi di ITS erogati presso il datacenter di produzione siano indisponibili per un tempo stimato superiore alle 4 ore lavorative ed in accordo con il personale di ITS. Il DRP dovrà esplicitare le procedure che verranno adottate nel caso di indisponibilità dei servizi erogati ad ITS per eventi che coinvolgano il datacenter o parte del datacenter; nell'Allegato A, unitamente all'elenco dei sistemi di ITS, sono indicati i valori di RTO (Return To Operation) ed RPO (Recovery Point Objective) massimi richiesti per ciascun sistema parte del perimetro del servizio.

Per quanto concerne i server virtuali, il disaster recovery dovrà essere effettuato utilizzando una diversa infrastruttura di virtualizzazione basata sulla medesima versione di VMware vSphere presente in produzione. I sistemi sul sito di disastro dovranno mantenere inalterato lo spazio disco allocato, mentre potranno essere ridotte le risorse in termini di RAM e di CPU nella misura massima del 25% e 50% rispettivamente, a condizione che la perdita di performance complessiva stimata dei sistemi non sia superiore al 20% in condizioni operative standard.

Per quanto concerne il server fisico Oracle, vitsdb01, è lasciata a discrezione dell'offerente l'implementazione della soluzione di disaster recovery su altro server fisico o su server virtuale che offra analoghe risorse e prestazioni. E' compito dell'aggiudicatario verificare e garantire che siano rispettati i termini di licenza di Oracle per quanto concerne il Disaster Recovery del server fisico, dotando i sistemi di destinazione della necessaria licenza oppure approntando una procedura di backup e restore rapidi che consentano di ripristinare il sistema rispettando i tempi di RPO ed RTO massimi indicati nell'Allegato A.

Qualora la situazione di disastro si protragga oltre i 15 giorni, l'azienda aggiudicataria dovrà integrare le risorse hardware presso il sito di DR per garantire la disponibilità delle risorse riservate ad ITS presenti sui precedenti sistemi di produzione.

Qualora la situazione di disastro si protragga oltre i 30 giorni, l'azienda aggiudicataria dovrà predisporre un nuovo piano di disaster recovery che consideri la possibilità di un disastro nel datacenter di DR; in questo caso i tempi di RTO ed RPO da rispettare per i sistemi di ITS si considereranno triplicati rispetto ai dati riportati nell'Allegato A.

Entro 60 giorni dall'attivazione del DR il fornitore dovrà predisporre un piano di "rientro da disastro" in cui siano esplicitate le attività necessarie per la riattivazione del datacenter di produzione (ove

possibile) o per il ripristino del datacenter di produzione in altro sito, rispettando i criteri indicati nel capitolo "**Errore. L'origine riferimento non è stata trovata.**". Le attività di rientro da disastro dovranno essere portate a termine entro 120 giorni solari dalla data di attivazione delle procedure di DR. Nel caso in cui il datacenter di DR rispetti le caratteristiche richieste per il datacenter di produzione come enunciate nel capitolo ad esso dedicato, è facoltà dell'azienda aggiudicataria, in accordo con ITS, promuovere il sito di DR in sito di produzione, con il contestuale approntamento di un nuovo datacenter di DR che rispetti tutte le prescrizioni previste nel presente capitolato ed il ripristino delle risorse richieste dai sistemi di produzione.
I costi associati all'attivazione del Disaster Recovery ed al rientro da disastro da parte del fornitore saranno interamente a suo carico e nulla potrà essere imputato ad ITS in tale evenienza.

2.10. Requisiti per la protezione antivirus/antimalware

Tutti i server oggetto del servizio, salvo diversamente indicato da ITS in fase di esecuzione, dovranno essere provvisti di protezione antivirus/antimalware. La protezione antivirus potrà essere erogata sia mediante un software installato in ogni server virtuale (agent), sia integrata nel sistema di virtualizzazione (agentless), a discrezione dell'azienda offerente. Per il server fisico Oracle dovrà necessariamente essere scelta una soluzione basata su agente. Il prodotto antivirus scelto dovrà essere provvisto di una gestione centralizzata che consenta un controllo di accesso basato sui ruoli. Dovrà inoltre essere fornito ad ITS un set di credenziali che consenta al personale preposto di verificare in autonomia lo stato della protezione antivirus sui singoli sistemi e le eventuali minacce intercettate.
Oltre alla soluzione antivirus per i server virtuali, il fornitore dovrà predisporre una soluzione antivirus e antimalware anche per il server fisico Oracle e per tutte le postazioni di lavoro fisiche, siano esse desktop, portatili o dispositivi mobili, per le postazioni di ITS e di ASM Merano. In questa prima fase i sistemi di ASM Bressanone e SEAB non saranno inclusi nella gestione della protezione antivirus/antimalware centralizzata, ma potrebbero essere aggiunte in un futuro prossimo. Analogamente a quanto scritto per i server virtuali, il prodotto scelto deve offrire una console di gestione centralizzata con controllo di accesso basato sui ruoli. Anche per questa console, se differente da quella utilizzata per i server virtuali, dovrà essere fornito ad ITS un set di credenziali che consenta al personale preposto di verificare in autonomia lo stato della protezione antivirus sui singoli sistemi e le eventuali minacce intercettate.
Il prodotto antivirus proposto per i server virtuali potrà essere diverso da quello previsto per le postazioni di lavoro fisiche degli utenti. Se ritenuto opportuno il prodotto antivirus per le postazioni client fisiche potrà essere integrato con il prodotto di gestione della sicurezza perimetrale per un controllo integrato della sicurezza delle reti ITS.
Il licenziamento dei sistemi server dovrà essere gestito dal fornitore secondo il modello di licensing del vendor del prodotto. Il costo della licenza del prodotto antivirus/antimalware per i server, ove previsto, dovrà essere considerato come costo mensile per ciascuna macchina.
Il licenziamento delle postazioni client fisiche dovrà essere gestito dal fornitore secondo il modello di licensing del vendor del prodotto. Nell'offerta dovrà essere considerato come costo mensile per ciascuna macchina.

2.11. Requisiti per la gestione della virtualizzazione delle postazioni di lavoro

Per la gestione delle postazioni di lavoro virtualizzate attualmente è utilizzata la piattaforma di Citrix dell'attuale fornitore. Sono attualmente presenti 4 server virtuali dedicati per ITS che utilizzano il prodotto XenApp per l'erogazione di un totale di 66 postazioni di lavoro virtuali; di queste circa 40-45 sono normalmente attive contemporaneamente. Dei 4 server VDA presenti, 3 server sono generici e offrono tutti gli applicativi di base agli utenti, mentre uno è dedicato per l'applicazione WinSmart in uso al centro di riciclaggio per la pesa.

La soluzione di virtualizzazione delle postazioni di lavoro proposta dovrà essere basata sulla piattaforma di Citrix, indifferentemente nella versione XenApp o XenDesktop o una combinazione delle due soluzioni. I server infrastrutturali di supporto per la soluzione (p.es. Access Gateway, Storefront, Delivery Controller, License server, SQL Server, ecc.) potranno essere dedicati ad ITS oppure condivisi con altri clienti, mentre i server VDA (Virtual Delivery Agent) dovranno essere dedicati ad ITS. L'accesso ai sistemi da parte degli utenti dovrà essere basato sul database utenti Active Directory di ITS; tutti i dati degli utenti, compresi i profili utente e le home directory degli stessi, dovranno essere ospitati sul file server di ITS (vitsfs01) in modo tale che, indipendentemente dal server cui si collega, ciascun utente abbia a disposizione il proprio ambiente e l'accesso ai propri dati.

I prodotti software da rendere disponibili all'interno delle postazioni di lavoro sono indicati nell'Allegato B. Per quanto concerne il licensing degli applicativi utilizzati nelle postazioni di lavoro, le licenze sono attualmente di proprietà di ITS e potranno essere utilizzate anche sulla nuova infrastruttura. Anche le licenze di eventuali nuovi prodotti di cui dovesse essere richiesta l'installazione durante il periodo di valitità del contratto, saranno acquistate da ITS (salvo indicazioni diverse previste dal modello di licensing del software adottato) e messe a disposizione del fornitore del servizio.

Per quanto concerne il licensing delle postazioni di lavoro virtuali, con l'esclusione delle licenze dei software di cui al paragrafo precedente, tutto il licenziamento dell'infrastruttura dovrà essere effettuato secondo i modelli previsti da Citrix e dovrà comprendere anche il licensing delle virtual machine, dei sistemi operativi e le licenze Microsoft RDS.

Il costo delle postazioni di lavoro virtualizzato dovrà essere considerano come costo mensile omnicomprensivo delle risorse computazionali e di licensin, indipendentemente dal numero di virtual desktop richiesti, dal numero di virtual machine impiegate per erogare il servizio e dalle risorse ad esse allocate. In particolare, i costi associati all'erogazione del servizio di virtual desktop, compresi i costi delle risorse virtuali utilizzate, i costi di licensing dei server virtuali VDA, del sistema operativo, delle connessioni remote desktop, del backup, dell'antivirus, dell'ordinaria manutenzione dei sistemi, dovranno essere inclusi nel canone mensile unitario per ciascuna postazione virtualizzata.

2.12. Requisiti per la gestione della sicurezza perimetrale del Datacenter e delle sedi ITS

Per la gestione della sicurezza perimetrale del datacenter e delle sedi di ITS, l'aggiudicatario dovrà implementare una soluzione basata su prodotti di firewalling di tipo NGFW (Next Generation Firewall) che prevedano le funzionalità UTM (Unified Threat Protection) sia per il datacenter che per le sedi di ITS, con la possibilità di implementare una soluzione di SD-WAN nativamente supportata dai dispositivi proposti.

La soluzione da implementare dovrà essere basata su una o più istanze fisiche o virtuali dedicate ai sistemi di ITS nel datacenter e su una o più istanze fisiche o virtuali per le sedi in cui sono presenti le postazioni di lavoro di ITS. Tutte le istanze dovranno essere fornite in configurazione ridondante per garantire la disponibilità dei servizi di sicurezza anche in caso di guasto hardware di un dispositivo o del sistema di virtualizzazione a supporto dell'istanza virtuale. La gestione di tutte le istanze fisiche e/o virtuali dovrà essere unica, centralizzata ed accedibile via Web utilizzando un browser e dovrà essere fornito ad ITS, a fini di auditing, almeno un set di credenziali che consentano l'autonoma verifica delle policy implementate e dei log, sia per i firewall del datacenter che per i firewall delle sedi periferiche.

I firewall proposti dovranno prevedere funzionalità di firewalling classiche e funzionalità avanzate NGFW e UTM tra cui costituiscono requisito indispensabile:

- SSL inspection per la verifica dei contenuti protetti da crittografia applicabile almeno ai servizi di navigazione web (HTTP), posta elettronica (SMTP, IMAP, POP3) e di secure shell (SSH);
- antivirus perimetrale che analizzi i contenuti per la navigazione web (HTTP) ed i servizi di posta elettronica (SMTP, IMAP e POP3), sia in chiaro che protetti da crittografia SSL/TLS;
- Application Control che consenta di definire policy basate sul riconoscimento delle principali applicazioni in uso da ITS (p.es. Microsoft Office365, Microsoft Teams, Citrix ICA, Autodesk 360, Adobe Creative, ecc.) indipendentemente dai protocolli o dalle porte utilizzate;
- funzionalità di IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) che consentano di rilevare e prevenire minacce legate a vulnerabilità dei sistemi protetti ed eventuali attacchi provenienti da internet o dalle reti di ITS o dei partner;
- integrazione con Microsoft Active Directory per il riconoscimento degli utenti e possibilità di definire policy dedicate per specifici utenti o gruppi di utenti, sia per i client fisici che per l'ambiente di virtualizzazione del desktop. Possibilità di utilizzare la base utenti Active Directory anche per l'autenticazione delle VPN;
- filtraggio della navigazione web basato su categorie che permetta di bloccare la navigazione verso siti web ospitanti specifiche categorie di contenuti (p.es. contenuti pornografici, insicuri, gioco d'azzardo, ecc.) con la possibilità di definire politiche di filtering differenti in base ai gruppi di appartenenza dell'utente;
- Content Filtering per poter bloccare o autorizzare specifiche tipologie di contenuti (per esempio identificazione dei file eseguibili) e opzionalmente DLP (Data Leakage Prevention)

per identificare e/o impedire eventuali tentativi di far uscire dall'azienda dati riservati e/o protetti;

- supporto della definizione di FQDN (Fully Qualified Domain Name) come source o destination delle policy di filtering;
- supporto per la gestione della Quality of Service (QoS) e del Traffic Shaping che consentano di dare priorità o di limitare specifiche tipologie di traffico e/o specifici gruppi di utenti;
- supporto dell'accesso remoto via VPN degli utenti e dei fornitori di ITS. Il servizio VPN dovrà essere disponibile, almeno per le funzionalità principali, anche in modalità clientless, ovvero basato sull'utilizzo di un browser Web senza necessità di installare un client VPN specifico sul dispositivo che si connette e/o in modalità portale con supporto almeno ai protocolli RDP, VNC, SSH e TELNET;
- supporto per VPN Site to Site di tipo IPSEC con supporto ai protocolli IKEv1 ed IKEv2;
- supporto delle funzionalità di SD-Wan per la gestione dinamica (quality based, reliability based ed application based) di molteplici connettività WAN;
- supporto della gestione di VPN tra i siti di ITS ed il Datacenter sia in modalità Full Mesh che Hub&Spoke con gestione di connettività multiple e di tipo diverso nelle diverse sedi ed anche in presenza di indirizzamenti IP pubblici dinamici;
- supporto del protocollo Ipv6;
- supporto delle funzionalità di routing dinamico OSPFv2 e OSPFv3 e di Policy Based Routing (PBR).

Tutti i dispositivi coinvolti nella gestione della sicurezza perimetrale, sia per il datacenter che per le sedi periferiche, dovranno essere forniti come servizio, sia per la parte hardware che per la parte software e licenze, ed esposti quindi come canone mensile.

In fase di esecuzione dovrà essere prevista una giornata del personale tecnico del fornitore in cui concordare con il personale di riferimento di ITS le politiche di sicurezza da implementare sui sistemi di difesa perimetrale. Inoltre, con cadenza almeno annuale, dovrà essere prevista un'ulteriore mezza giornata lavorativa per un'attività congiunta di revisione delle policy per verificare che queste rispondano correttamente alle esigenze del committente.

Per quanto concerne le VPN degli utenti ITS il relativo costo dovrà essere incluso nel canone mensile delle postazioni virtuali, mentre per le VPN di fornitori e utenti esterni ad ITS dovrà essere incluso nel canone di servizio base il costo di 10 VPN liberamente assegnabili da ITS ai propri fornitori o collaboratori. Il costo per ogni singola VPN aggiuntiva oltre alle 10 incluse dovrà essere esplicitato nell'offerta.

Le sedi su cui andranno installati i nuovi firewall perimetrali sono le seguenti:

- ITS: Via Peter Anich 24, 39011, Lana (BZ) – 5 utenti
- ASM Merano: Viale Europa 4, 39012, Merano (BZ) – 60 utenti
- ASM Merano: Via L.Zuegg 68c, 39012, Merano (BZ) – 5 utenti
- ASM Merano: Via Peter Anich 24, 39011, Lana (BZ) – 20 utenti
- ASM Bressanone: via Alfred Ammon 24, 39042 Bressanone (BZ) – 80 utenti

Il numero indicativo di utenti del sistema informativo per ciascuna sede è riportato in corrispondenza di ciascuna voce.

Durante il periodo di validità del contratto è prevista la revisione della connettività tra il datacenter, ITS e le sedi delle Società Socie, attualmente costituita da una rete MPLS dedicata. In tale occasione sarà valutata l'opportunità di utilizzare congiuntamente le funzionalità di SD-WAN e VPN in sostituzione della MPLS dedicata. Si richiede pertanto che le configurazioni hardware e software dei firewall già siano predisposte per questa eventuale futura necessità.
Inoltre, verosimilmente durante il primo anno di validità del contratto, diverrà operativa la nuova sede di Merano di ASM Merano e ITS; in tale occasione i sistemi installati nelle sedi di ITS (Lana) e ASM Merano Viale Europa dovranno essere spostati nella nuova sede e riconfigurati in accordo. Per tale attività il committente utilizzerà le risorse previste nel paragrafo **Errore. L'origine riferimento non è stata trovata.**.

2.13. Auditing di sicurezza dei sistemi

Al fine di garantire la sicurezza dei dati e dei sistemi di ITS, il committente eseguirà un audit periodico ed un vulnerability assessment (VA) della sicurezza dei sistemi avvalendosi di risorse proprie e/o di fornitori esterni. L'aggiudicatario si impegna a consentire le attività di auditing e di vulnerability assessment sui sistemi di ITS ed in particolare:

- possibilità di installare server virtuali nell'infrastruttura di datacenter per il monitoraggio continuo della sicurezza (tali eventuali server non saranno gestiti dall'aggiudicatario ma da ITS o altri fornitori);
- possibilità di installare agenti sui sistemi di ITS che possano colloquiare con sistemi interni ed esterni al datacenter al fine di identificare eventuali problemi di sicurezza;
- possibilità di eseguire vulnerability assessment da Internet verso gli indirizzi pubblici dedicati ai sistemi di ITS;
- possibilità di eseguire vulnerability assessment da server interni all'infrastruttura verso gli altri server virtuali o fisici dedicati ad ITS.

ITS si impegna a comunicare al fornitore la data in cui eseguirà il vulnerability assessment, ed i sistemi da cui verrà condotto, con almeno 7 giorni solari di anticipo, per consentire allo stesso di gestire in modo corretto gli attacchi virtuali condotti verso i sistemi (p.es. disabilitando le sonde IDS ed IPS per specifici IP per evitare falsi positivi). Verranno inoltre comunicati al fornitore l'inizio ed il termine del VA.
Per quanto concerne i sistemi condivisi con altri clienti, ed in particolare i server di gestione dei desktop virtuali, non saranno oggetto di vulnerability assessment da parte di ITS, ma si richiede che l'aggiudicatario esegua, con cadenza almeno semestrale, un vulnerability assessment dei sistemi che includa la verifica di tutte le vulnerabilità incluse nel database CVE (Common Vulnerability and Exposures, https://cve.org) applicabili ai sistemi ed antecedenti la data di esecuzione del VA di non più di 7 giorni.
Entro 15 giorni dall'esecuzione del Vulnerability Assessment dei sistemi condivisi dovrà essere fornito ad ITS un report sullo stato delle vulnerabilità dei sistemi e la pianificazione della risoluzione e/o mitigazione per tutte le vulnerabilità con CVSS (Common Vulnerability Scoring System) superiore a 4 (Medium, High, Critical).

Gli audit ed i vulnerability assessment eseguiti da ITS o da fornitori terzi incaricati, verranno condotti con attenzione a non compromettere i servizi erogati. Qualora in seguito e per causa dell'esecuzione dell'audit e/o del VA dovessero verificarsi disservizi nei sistemi di ITS, il fornitore sarà esonerato da qualsiasi responsabilità e gli eventuali costi per il ripristino dei servizi saranno a carico di ITS.

2.14. Gestione dei sistemi di ITS nel datacenter

Nell'elaborazione dell'offerta economica, l'azienda aggiudicataria dovrà includere nel canone del servizio tutte le attività di gestione ordinaria dei sistemi di ITS nel datacenter. In particolare, dovranno essere incluse nel canone del servizio le seguenti attività:

- monitoraggio dei sistemi per l'utilizzo delle risorse e la corretta erogazione dei servizi (monitoraggio di base di CPU, RAM, utilizzo spazio disco, servizi applicativi attivi, ecc.);
- manutenzione ordinaria dei sistemi (pulizia, riavvii periodici, ecc.);
- aggiornamento dei sistemi operativi con le ultime patch di sicurezza;
- aggiornamento degli applicativi installati sulla piattaforma di virtualizzazione delle PdL;
- controllo dei backup ed eventuali azioni correttive richieste;
- controllo dell'antivirus ed eventuali azioni correttive richieste;
- attività di gestione del database utenti Active Directory;
- definizione e manutenzione delle policy Active Directory (GPO);
- creazione di nuove macchine virtuali;
- creazione e rimozione di snapshot delle macchine virtuali per attività sui sistemi;
- monitoraggio e gestione dei certificati SSL installati sui server e notifica delle scadenze con un preavviso di almeno 15 giorni (l'eventuale acquisto, ove necessario, sarà fatto direttamente da ITS);

Per quanto riguarda le attività di creazione di nuovi server virtuali sono da includere nel canone base del servizio le attività di creazione della macchina virtuale e le eventuali configurazioni sull'infrastruttura virtuale necessarie per il suo funzionamento (p.es. definizione di nuovi Portgroup sui Virtual Switch). Sono invece escluse dal canone base del servizio le attività di installazione e prima configurazione del sistema, attività che include l'installazione del sistema operativo, l'aggiornamento con le ultime patch rilasciate dal produttore, il join al dominio Active Directory ove previsto, l'installazione del prodotto antivirus e la configurazione del backup della macchina virtuale nel sistema di backup. Per le attività di prima installazione e configurazione si richiede che in offerta venga indicata una tariffa forfettaria che dovrà rimanere invariata per l'intera durata del contratto.
Sono escluse dal canone le attività di gestione non ordinaria richieste specificamente da ITS come l'assistenza sistemistica di supporto ai fornitori degli applicativi, gestione di backup e/o restore specifici per attività sui sistemi, supporto per troubleshooting in attività di fornitori terzi, ecc. Per le attività non incluse nel canone di servizio ITS potrà, a sua discrezione, attingere alle risorse indicate nel capitolo **Errore. L'origine riferimento non è stata trovata.**.

2.15. Gestione dei dispositivi client nelle sedi ITS

L'azienda aggiudicataria dovrà includere nel canone del servizio tutte le attività di gestione ordinaria delle postazioni client fisiche di ITS. Ad oggi il numero di postazioni fisiche presenti è indicativamente di 40-45 postazioni distribuite sulle sedi di ITS e delle Società Socie.
In particolare dovranno essere incluse nel canone del servizio le seguenti attività:

- attività di gestione ordinaria dei thin client, dei desktop e dei portatili, con particolare riferimento all'aggiornamento dei sistemi e delle applicazioni di base ed alla verifica delle eventuali segnalazioni del software antivirus/antimalware;
- supporto da remoto agli utenti per problematiche di natura sistemistica di primo livello;
- definizione e manutenzione delle policy Active Directory (GPO);
- preparazione di eventuali nuove postazioni di lavoro o riassegnazione di postazioni esistenti.

Al fine di garantire una gestione ottimale del parco macchine, l'aggiudicatario dovrà dotarsi di un sistema di Management ed inventory dei dispositivi (PC, Thin Client, Portatili, dispositivi mobili, ecc.) presenti nelle varie sedi che consenta di verificare tutti i software installati con le relative versioni, lo stato di aggiornamento dei sistemi, la distribuzione di software e/o aggiornamenti sui sistemi gestiti ed il monitoraggio dei dispositivi. Lo stesso sistema potrà essere impiegato anche per l'inventory e la gestione dei sistemi nel datacenter. Dovrà essere fornito ad ITS un accesso al sistema di Management ed Inventory che le consenta di essere autonoma nella verifica dello stato dei sistemi e consenta di gestire gli aggiornamenti dei sistemi client in autonomia.
Sono escluse dal canone le attività di gestione non ordinaria richieste specificamente da ITS e le eventuali attività on-site sulle postazioni client determinate dall'impossibilità di operare remotamente. Per le attività non incluse nel canone di servizio ITS potrà, a sua discrezione, attingere alle risorse indicate nel capitolo **Errore. L'origine riferimento non è stata trovata.**.

2.16. Gestione licenze di proprietà ITS

L'azienda aggiudicataria dovrà includere nel canone del servizio tutte le attività di supporto nella gestione delle licenze di proprietà di ITS sui sistemi inclusi nel perimetro del presente capitolato, sia presso il datacenter che presso le diverse sedi. In particolare l'aggiudicatario dovrà farsi carico per conto di ITS delle seguenti attività:

- gestione dei tenant Microsoft per le licenze Office365;
- gestione delle licenze Microsoft per le postazioni di lavoro;
- gestione delle licenze degli applicativi installati sui virtual desktop;
- eventuale consulenza per la gestione delle licenze degli applicativi installati sui sistemi del datacenter;

Per gestione delle licenze si intende il supporto per la registrazione di nuove licenze, la verifica della corrispondenza tra software installati e licenze disponibili, la dismissione di licenze non più necessarie e le altre attività analoghe che dovessero rendersi necessarie durante la durata del contratto.
Le attività di consulenza potranno riguardare principalmente le strategie da attuare per determinare risparmi in ambito di licenziamento dei sistemi e degli applicativi, anche conseguenti a variazioni

strutturali o organizzative del committente. Ad oggi sono presenti due Tenant Microsoft Office365, rispettivamente di ITS e di Azienda Servizi Municipalizzati di Merano.

2.17. Gestione dei dispositivi di rete attivi nelle sedi ITS

L'azienda aggiudicataria dovrà includere nel canone del servizio tutte le attività di supporto nella gestione ordinaria dei dispositivi di rete presenti nelle sedi di ITS e non in carico al fornitore di connettività. In particolare l'aggiudicatario dovrà farsi carico per conto di ITS di tutte le attività di gestione e configurazione degli apparati presenti nelle sedi ed in particolare:

- aggiornamento dei sistemi
- salvataggio delle configurazioni
- modifiche alle configurazioni su richiesta di ITS

Sono escluse le attività di configurazione ed installazione di nuovi apparati e le attività connesse con la sostituzione di eventuali dispositivi guasti. Ad oggi rientrano nel perimetro del presente capitolato i seguenti dispositivi:

- 10 switch
- 4 router
- 20 access point

Per le attività non incluse nel canone di servizio ITS potrà, a sua discrezione, attingere alle risorse indicate nel capitolo **Errore. L'origine riferimento non è stata trovata.**.

2.18. Migrazione dei sistemi al nuovo fornitore

La migrazione dei sistemi di ITS dall'attuale gestore all'impresa aggiudicataria dovrà avvenire entro il termine di 60 giorni solari dalla data di stipula del contratto e dovrà essere portato a compimento senza comportare maggiori oneri per ITS rispetto a quelli previsti nel presente bando.
L'azienda aggiudicataria si impegnerà a produrre, entro 30 giorni dalla stipula del contratto, un progetto di migrazione in cui siano illustrati tutti i passaggi per migrare i sistemi dall'attuale datacenter al nuovo datacenter, con particolare riguardo a tutte le attività che richiedono la partecipazione di ITS, che comportino l'interruzione dei servizi di ITS o che necessitino di attività da parte dell'attuale fornitore del servizio.
In tale documento dovrà essere indicata anche la data in cui è previsto il completamento della migrazione ed un diagramma Gantt con le attività previste da ciascun attore coinvolto.
Tutte le attività che possono comportare disservizi generali per una o più sedi di ITS dovranno essere portate a compimento al di fuori dell'orario di ufficio, ovvero tutti i giorni dal lunedì al giovedì tra le ore 18:00 e le ore 07:00 del giorno successivo oppure il venerdì dalle ore 13:00 fino al lunedì alle ore 7:00. Eventuali disservizi in orario di lavoro saranno fonte di penale in ambito contrattuale. Per le attività di riconfigurazione che dovessero rendersi necessarie sui client fisici degli utenti, ove non effettuabili da remoto ed in orario non lavorativo, è accettato un disservizio massimo di 30 minuti per ciascuna postazione. Nel piano di migrazione dovranno essere indicate le attività previste e l'eventuale intervento sulle postazioni dovrà essere pianificato con ITS tenendo in considerazione le

esigenze di servizio (per esempio pianificando l'aggiornamento di postazioni omologhe per funzionalità in differenti orari o giorni).
Se ritenuto necessario o opportuno da parte dell'azienda aggiudicataria, e previa richiesta in tal senso, sarà responsabilità di ITS mettere a disposizione una copia completa degli ultimi backup dei sistemi di ITS su un supporto fornito dall'aggiudicatario (HDD o NAS) nel formato di salvataggio utilizzato dal prodotto Veeam Backup & Recovery versione 10 attualmente utilizzato. I backup saranno messi a disposizione entro 7 giorni dalla effettiva disponibilità del supporto. I costi sostenuti nei confronti dell'attuale fornitore per la suddetta attività saranno a carico di ITS.
Se ritenuto necessario o opportuno da parte dell'azienda aggiudicataria, potrà essere creata una VPN IPSec tra l'infrastruttura di Datacenter presso l'attuale fornitore e l'infrastruttura di Datacenter di destinazione. L'utilizzo della VPN non dovrà compromettere in alcun modo la fruibilità dei servizi da parte degli utenti di ITS (in particolare non dovranno essere fatti trasferimenti di dati che possano saturare la banda a disposizione di ITS per l'erogazione dei servizi). I costi di setup della VPN IPSec da parte dell'attuale fornitore del servizio saranno a carico di ITS.
Se richiesto verrà messo a disposizione un set di credenziali amministrative per tutti i sistemi di ITS che fanno parte del perimetro della gara, da utilizzare al fine della migrazione.
L'approntamento della soluzione di virtualizzazione delle postazioni di lavoro sarà a carico dell'aggiudicatario che dovrà provvedere ad installare la soluzione proposta con tutti gli applicativi indicati nell'Allegato B. Dovrà inoltre impegnarsi a fornire una postazione di lavoro di test funzionante almeno 10 giorni prima della data di termine migrazione indicata per consentire al personale di ITS di verificare il corretto funzionamento delle nuove postazioni di lavoro e correggere eventuali problemi riscontrati.
Il server fisico con Oracle di proprietà di ITS dovrà essere prelevato dall'attuale datacenter e spostato nel nuovo datacenter a cura del personale dell'azienda aggiudicataria che dovrà provvedere allo smontaggio, al trasporto, al montaggio nella nuova location ed ai test di funzionamento del server. Sarà cura di ITS garantire che il sistema sia stato spento correttamente e che esista una copia di backup dei dati al momento dello spegnimento. Eventuali problemi durante l'attività di trasloco del server (p.es. danneggiamento durante il trasporto o le attività di smontaggio/montaggio) dovranno essere risolti dall'aggiudicatario che dovrà adoperarsi per garantire la corretta erogazione dei servizi il giorno lavorativo successivo, per esempio mettendo a disposizione hardware di cortesia, senza che ciò comporti ulteriori oneri per ITS.
I server virtuali dovranno essere migrati dall'infrastruttura attuale a quella dell'azienda aggiudicataria nelle modalità definite da quest'ultima nel progetto di migrazione. La migrazione potrà essere fatta in qualunque modalità, per esempio con backup e restore, migrazione online, sincronizzazione dei sistemi via rete, installazione di nuovi server e migrazione dei dati, ecc. E' responsabilità dell'azienda aggiudicataria, in base alla modalità di migrazione scelta, accertarsi che eventuali cambiamenti nei sistemi non determinino problemi di compatibilità con i prodotti e gli applicativi installati ed utilizzati da ITS. Se richiesto e/o necessario, ITS metterà a disposizione i contatti tecnici delle aziende che distribuiscono o manutengono gli applicativi installati sui sistemi per effettuare le necesarie verifiche prima della migrazione. Eventuali disservizi causati da incompatibilità tra applicazioni e nuovi sistemi saranno fonte di penale in ambito contrattuale.

Sarà facoltà dell'impresa aggiudicataria installare sui sistemi di ITS eventuali prodotti software necessari per effettuare la migrazione, purché venga garantito che tali prodotti non interferiscano con il corretto funzionamento dei sistemi e dei software in produzione e non creino conflitti con l'infrastruttura di produzione del fornitore attuale, con particolare riguardo al backup dei dati. Se necessario per le attività di migrazione, potrà essere creato un server virtuale sull'infrastruttura attuale sulla stessa rete dei sistemi di produzione; i costi sostenuti da ITS per la creazione ed il mantenimento dell'eventuale server sull'infrastruttura attuale, comprensivi di eventuali costi di licenza, saranno rifusi dall'azienda aggiudicataria a ITS sottoforma di prestazioni professionali fino a compensazione dell'intero importo. Non sarà invece possibile per l'azienda aggiudicataria interfacciarsi direttamente con i sistemi di virtualizzazione e/o di backup dell'attuale fornitore per ovvi motivi di sicurezza.
Per quanto concerne gli indirizzamenti di rete la migrazione non dovrà comportare nessun cambiamento di indirizzamento nelle sedi di ITS che dovranno conservare il piano IP attuale. Per l'indirizzamento IP dei sistemi in Datacenter è preferibile che venga mantenuto quello attuale, ma se strettamente necessario per motivi tecnici potrà essere cambiato. In caso di cambiamento dell'indirizzamento IP dei sistemi in Datacenter sarà responsabilità dell'azienda aggiudicatrice provvedere a tutte le modifiche di configurazione dei server, degli applicativi, dei client e degli eventuali apparati di rete che si rendessero necessarie per gestire correttamente il cambio del piano di indirizzamento e ciò non potrà comportare maggiori oneri per ITS né aggravi operativi per gli utenti in fase di migrazione.
Per quanto concerne le linee di connettività attualmente presenti, l'aggiudicatario dovrà includere nel documento di progetto tutte le attività richieste agli attuali fornitori di connettività ed una pianificazione degli interventi di configurazione che dovessero rendersi necessari per portare a compimento la migrazione. I costi di riconfigurazione degli apparati esistenti saranno a carico del committente. Se si rendesse necessario approntare eventuali nuove linee presso il datacenter dell'aggiudicatario, i corrispondenti costi saranno a carico dell'impresa aggiudicataria.
In nessun caso le attività di migrazione dovranno comportare problemi per l'infrastruttura dell'attuale fornitore di servizi ed eventuali danni riportati dal fornitore attuale ed imputabili all'attività di migrazione saranno interamente a carico dell'azienda aggiudicataria.
L'azienda aggiudicataria, se ritiene che ciò possa favorire la migrazione dei sistemi, ha la facoltà di accordarsi autonomamente con l'attuale fornitore dei servizi per ottenere servizi diversi da quelli descritti nel presente capitolato (per esempio l'interfacciamento diretto con i sistemi di virtualizzazione del fornitore o l'installazione di propri dispositivi nel datacenter dell'attuale fornitore, ecc.) accollandosi i costi di tali servizi ed a condizione che tali accordi non comportino maggiori oneri per il committente.
Il completamento della migrazione verrà sancito dal collaudo dell'infrastruttura proposta, attività che verrà svolta congiuntamente dall'aggiudicatario e dal personale preposto da ITS in cui sarà verificata la piena rispondenza delle soluzioni ai requisiti del presente capitolato.

2.19. Organizzazione del servizio post migrazione

L'azienda aggiudicataria, successivamente al collaudo post-migrazione, dovrà erogare il servizio secondo quanto proposto nell'offerta tecnica ed in rispondenza di quanto richiesto nel presente

capitolato. Al fine dell'erogazione del servizio, l'azienda aggiudicataria dovrà mettere a disposizione di ITS i seguenti strumenti organizzativi:

- un sistema di Trouble Ticketing che fornisca un identificativo di riferimento univoco per ciascuna richiesta effettuata e tenga traccia di:
  - data e ora della segnalazione;
  - data e ora della presa in carico della richiesta ed identificativo del tecnico che lo gestisce;
  - data e ora di risoluzione dell'incident;
  - gestione della priorità e della severità della richiesta;
  - gestione delle eventuali escalation, sia richieste da ITS sia automatizzate in funzione del rispetto degli SLA (Service Level Agreement) come indicati nel capitolo **Errore. L'origine riferimento non è stata trovata.**;
  - descrizione delle fasi di lavorazione e soluzione per eventuali problemi o incident.

  Il sistema di Trouble Ticketing dovrà essere accessibile da parte di ITS tramite interfaccia web e dovrà essere possibile utilizzare tale interfaccia per aprire nuove richieste, verificare lo stato delle richieste in fase di lavorazione, aggiungere informazioni o requisiti a richieste esistenti, modificarne la priorità e/o farne escalation verso un livello di supporto superiore;
- un numero di telefono afferente al Service Desk del fornitore da poter contattare per problematiche di primo livello sia dai referenti del servizio di ITS che direttamente dagli utenti del servizio. A seguito di chiamata telefonica dovrà essere aperto un ticket nel sistema di Trouble Ticketing per tenere traccia delle fasi di lavorazione e l'identificativo della richiesta dovrà essere comunicato all'interlocutore;
- un indirizzo e-mail da poter contattare per aprire automaticamente una richiesta nel sistema di Trouble Ticketing e che risponda alla mail con i riferimenti dell'identificativo del ticket aperto.

Il servizio di Service Desk dovrà essere contattabile in orario lavorativo, dalle 7:30 alle 17:30 dal lunedì al venerdì, e dovrà essere erogato da personale bilingue (italiano e tedesco) rispondendo alla chiamata nella lingua scelta dal chiamante. Su richiesta del chiamante il servizio di Service Desk dovrà essere erogato anche in lingua inglese per far fronte a necessità di interloquire con eventuali fornitori terzi.

Oltre al servizio di Service Desk, l'aggiudicatario dovrà mettere a disposizione di ITS un numero di telefono di reperibilità a copertura degli orari in cui il Service Desk non è disponibile e che afferisca direttamente al supporto di secondo livello. Il numero di reperibilità sarà utilizzabile unicamente dai referenti del servizio di ITS (che saranno comunicati all'avvio del servizio) per problematiche urgenti o fuori orario lavorativo. I costi per eventuali attività fuori orario lavorativo conseguenti a chiamate verso il numero di reperibilità saranno imputati sulle risorse definite nel capitolo **Errore. L'origine riferimento non è stata trovata.**.

Si richiede inoltre che l'aggiudicatario identifichi al proprio interno un referente commerciale ed un referente tecnico da poter contattare in caso di emergenza o di necessità di escalation di eventuali segnalazioni. I contatti diretti delle figure individuate dovranno essere comunicati dall'aggiudicatario alla stipula del contratto e l'accesso a tali risorse sarà riservato esclusivamente ai referenti del servizio di ITS, a loro volta comunicati all'aggiudicatario.

3. Time & Material

Per tutte le attività non coperte dal canone del servizio, è richiesta all'azienda aggiudicataria di formulare una proposta per l'erogazione di prestazioni da utilizzare con la formula "ore a scalare" per i seguenti profili:

- sistemista junior
- sistemista senior

Viene considerato sistemista senior la figura professionale che possa vantare almeno 5 anni di esperienza sulla tecnologia interessata oppure 3 anni di esperienza ed una certificazione del vendor del prodotto (ove applicabile).
Viene considerato sistemista junior la figura professionale non in possesso delle caratteristiche del sistemista senior.
Il monte ore previsto per le due figure in maniera indistinta si prevede di 300 ore per l'intera durata del contratto. Le risorse tecniche indicate potranno essere utilizzate a discrezione di ITS per tutte le attività non coperte dal contratto di servizio e per consulenze. Le ore previste per le due figure professionali, potranno essere utilizzate a prescindere dai giorni e dagli orari in cui dovrà essere svolta l'attività richiesta ed è esclusa l'applicazione di sovrapprezzi per lavori in giornate festive, prefestive o in orario notturno. La rendicontazione del tempo lavorato dovrà essere fatta per intervalli multipli di 15 minuti arrotondati per eccesso.
Qualora le esigenze di servizio lo richiedessero sarà facoltà di ITS richiedere all'impresa aggiudicataria, nel periodo di validità del contratto, l'aggiunta di ore al pacchetto di ore lavorative disponibili, indipendentemente per uno solo o per entrambi i profili professionali sopra indicati.
Qualora al termine del contratto del servizio le ore a disposizione non fossero state interamente consumate, le stesse dovranno essere erogate su richiesta di ITS per altre attività non connesse con il servizio entro il termine di 3 anni solari dalla data di scadenza del contratto.

4. Livelli di servizio

Nella gestione del servizio, l'impresa aggiudicataria dovrà garantire l'efficiente erogazione dei servizi ed il rispetto dei livelli di servizio di seguito illustrati per i problemi di diversa severità e priorità. Per la verifica dei livelli di servizio è richiesto al fornitore la produzione di un report mensile, estratto dal sistema di Trouble Ticketing di cui al capitolo **Errore. L'origine riferimento non è stata trovata.**, che includa sinteticamente tutte le chiamate aperte da ITS e dai suoi utenti nel mese di riferimento comprensive di data e ora di apertura, di presa in carico e di chiusura di ciascuna chiamata, valori di priorità e severità assegnati, identificativo del tecnico che l'ha presa in carico e oggetto della chiamata.
Per l'assegnazione della severità dei problemi si fa riferimento alla seguente tabella:

Severità	Descrizione	Presa in carico dell'incident	Risoluzione dell'incident
Alta	problemi che causano l'interruzione nell'erogazione di un servizio che impatta su tutti gli utenti di una o più sedi di ITS o di una o più applicazioni critiche per il business.	entro 2 ore solari	entro 24 ore solari
Media	problemi che causano interruzione di servizi che impattano su un numero ridotto di utenti o che causano disservizi parziali ma non bloccanti (p.es. degrado delle performance, ripristino di un hardware ridondato, ecc.)	entro 4 ore lavorative	entro 16 ore lavorative
Bassa	problemi che non causano disservizi agli utenti del sistema informativo (p.es. warning sul software di backup, ecc.)	entro 8 ore lavorative	entro 24 ore lavorative
Nulla	richieste di informazioni o di supporto per problemi che non comportano disservizio	entro 8 ore lavorative	entro 40 ore lavorative

Per quanto riguarda la voce "Presa in carico dell'incident" si intende il tempo intercorso tra l'apertura della chiamata al Service Desk o al servizio di reperibilità e le prime azioni intraprese dal tecnico incaricato per la diagnosi e la risoluzione del problema, attività che dovrà essere comunicata via mail all'utente che ha effettuato la segnalazione con l'apertura del ticket.
Per quanto concerne la voce "Risoluzione dell'incident" si intende il tempo che intercorre tra l'apertura della chiamata al Service Desk o al servizio di reperibilità ed il momento in cui il problema segnalato viene risolto o la sua severità viene abbassata rispetto alla severità iniziale, per esempio adottando workaround che consentano di ripristinare il servizio parzialmente o implementando una soluzione temporanea da rivalutare in un secondo momento.
Il mancato rispetto degli SLA (Service Level Agreement) comporterà l'applicazione di penali come da contratto.

5. Ampliamenti

Allo stato attuale non sono previsti ampliamenti significativi del perimetro della gara durante il periodo di validità del contratto. Le uniche attività già previste e già menzionate nei capitoli precedenti sono lo spostamento dell'applicativo SAP da Bressanone al datacenter, attività che si prevede sia completata prima della stipula del contratto, e l'inizio dell'operatività della nuova sede di Via Brogliati a Merano che dovrebbe avvenire durante il primo anno di servizio. Ciò nonostante, non è escludibile che futuri sviluppi ed evoluzioni richiedano l'approntamento di nuovi server virtuali o di nuovi desktop virtuali o l'aggiunta di nuove sedi e nuovi utenti all'infrastruttura esistente. L'impresa aggiudicataria si impegna a mettere a disposizione di ITS e delle sue consociate le risorse necessarie per far fronte ad eventuali variazioni che dovessero manifestarsi durante la validità del presente contratto.
Si precisa che, in caso di incongruenze/inesattezze nel capitolato tecnico in lingua tedesca, si dovrà fare riferimento al capitolato tecnico in lingua italiana.

Sede amministrativa - Verwaltungssitz:
Via Zuegg Str. 40 I - 39012 Merano-Meran
Tel. +39 0473 498 300 - Fax +39 0473 498 303

Sede legale – Rechtssitz:
Via A.-Ammon Str. 24 I - 39042 Bressanone – Brixen
Tel. +39 0472 823 636 - Fax +39 0472 823 666
CF P.IVA St./MwSt.Nr IT / 02298140217