



RETEGAS BARI

AZIENDA MUNICIPALE GAS S.P.A.

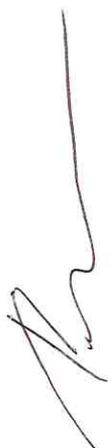
Disciplinare Tecnico d'appalto per i servizi di assistenza tecnica sistemistica sui software, sistemi operativi client e server, Switch di rete, Sicurezza, Firewall di confine, gestione dell'infrastruttura del parco hardware collegato al dominio e servizio di monitoraggio degli apparati Server

Art. 1 – Oggetto delle prestazioni richieste

L'Azienda Municipale Gas S.p.A. (di seguito – per brevità – anche ReteGas), intende affidare il servizio di gestione e assistenza della propria infrastruttura informatica con la quale gestisce il proprio patrimonio informativo.

In considerazione della necessità di garantire un elevato livello prestazionale della propria infrastruttura, orientato sia all'efficacia degli interventi sistemistici oggetto del presente disciplinare, sia all'efficienza degli stessi sia per ridurre al minimo eventuali disservizi all'infrastruttura e relativi al supporto per il personale interno dell' Azienda Municipale Gas S.p.A., nonché degli obblighi di sicurezza relativi alla protezione dei dati gestiti dall'appaltante, con particolare riguardo a quelli riferiti alle informazioni sui cittadini e comunque per garantirsi una continuità operativa, sono richieste le seguenti prestazioni:

-
1. Manutenzione ordinaria infrastruttura, consistente nella ordinaria gestione e manutenzione di tutta l'infrastruttura esistente;
 2. L'assistenza estesa anche su eventuali nuove implementazioni tecnologiche che ReteGas deciderà di aggiungere alla struttura ICT durante il periodo contrattuale, sia a livello software che hardware, oltre che di ogni altra componente infrastrutturale (switch, access point, etc.), manutenzione del parco macchine client e server con garanzia di svolgimento delle normali attività che assicurino la disponibilità della rete, di tutto il parco macchine, e del corretto funzionamento dei software e della disponibilità del collegamento internet;
 3. Assistenza in loco al personale dell'Azienda Municipale Gas S.p.A., nel caso l'attività non possa essere svolta remotamente per limiti tecnici;
 4. La riconfigurazione completa (installazione dei sistemi operativi, dei software gestionali dove presenti, del software antivirus e di altro software accessorio dove richiesto) dei personal computer client in seguito alla reinstallazione del sistema operativo (compresa la re-inclusione del personal computer all'interno del dominio Microsoft Active Directory installato sui server della società Azienda Municipale Gas S.p.A.);

- 
5. La riconfigurazione e la reinstallazione dei software di base, dei prodotti Office (Microsoft Office in caso di adeguata presenza della licenza software, o di altri prodotti office come indicato da ReteGas), dei prodotti gestionali interni (avvalendosi, quando possibile, dell'assistenza telefonica fornita dalle varie software house esterne);
 6. Attività sistemistiche di configurazione e mantenimento del dominio, delle policy di sicurezza e degli utenti concordate secondo le direttive del responsabile dell'Azienda Municipale Gas S.p.A.;
 7. Supporto progettuale ed operativo in ogni attività di ReteGas relativa a tematiche informatiche;
 8. Supporto per la creazione di VPN per utilizzo delle risorse umane di ReteGas e per le softwarehouse che gestiscono gli applicativi utilizzati dall'azienda;
 9. Supporto sistemistico delle risorse umane per l'utilizzo delle VPN in caso di necessità;
 10. Supporto e interfacciamento con i vari responsabili aziendali, analisi delle criticità del sistema e formulazione di proposte di miglioramento;
 11. Il salvataggio (ovvero con sistema di backup) dei dati presenti sui server e dei client, dei dati presenti su ogni postazione di lavoro, ed il loro eventuale trasferimento su altra in sostituzione o meno, ove ciò venga richiesto;
 12. Attività finalizzate alla sicurezza dell'infrastruttura, secondo le indicazioni del Management Aziendale;
 13. Supporto nella gestione dei Firewall Watchguard modello M400 montati in HA, secondo le esigenze aziendali;
 14. Supporto all'interrogazione dei prodotti "Quest Software" denominati Change Auditor e InTrust, nel caso in cui richiesto dalla direzione, per verificare eventuali accessi degli amministratori e utenti di dominio sui sistemi monitorati;
 15. Supporto nella gestione degli Switch di rete Cisco, Allied Telesis, HP, 3Com, Huawei;
 16. Supporto alla gestione della configurazione degli switch di rete per le VLAN esistenti e altre eventuali da generare;
 17. Supporto dello staff tecnico dell'azienda per gli aggiornamenti dei firmware, delle patch Microsoft, delle apparecchiature utilizzate dall'azienda sia server che client e degli Switch, oltre al firewall di confine, ove necessario;
 18. Supporto dello staff del centro elaborazione dati, per l'implementazione, secondo l'art. 32 GDPR, le attività di seguito descritte:
 - a. Attivare secondo una procedura e gli strumenti in dotazione all'azienda attività atte alla pseudonimizzazione e la cifratura dei dati personali, lì dove richiesto dall'Azienda, anche a livello di protocolli di comunicazione;
 - b. Attivare con gli strumenti utilizzati dall'azienda, la capacità per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - c. Attivare con gli strumenti aziendali una procedura atta al ripristino tempestivo per la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
 - d. Attivare con strumenti software e hardware una procedura (**Disaster Recovery**) per testare, almeno ogni sei mesi e comunque dietro indicazione dello staff tecnico della committente, un ripristino dei sistemi, per verificare regolarmente l'efficacia delle misure tecniche e organizzative utilizzate, atte a garantire la sicurezza dei trattamenti dell'azienda (tali attività saranno programmate in maniera tale di non causare disservizi all'operatività quotidiana);
 19. Supporto a ReteGas su:
 - a. Debug file dump a seguito di blue screen;
 - b. Troubleshooting malfunzionamenti del network.;
 - c. Troubleshooting malfunzionamenti firewall;
 - d. Troubleshooting malfunzionamenti server;

- e. Aggiornamenti Windows Server/Active Directory;
- f. Gestione controllori di dominio;
- g. Gestione policy di dominio;
- h. Design server layout;
- i. Design network layout;
- j. Troubleshooting performance network;
- k. Troubleshooting performance server;

- 20. Supporto all'analisi di incidenti di sicurezza informatica;
- 21. Supporto e censimento delle licenze utilizzate sui Server dell'Azienda generando uno scadenziario atto alla programmazione dei rinnovi licenze;
- 22. Supporto per la verifica su eventuali potenziali falle di sicurezza segnalate;
- 23. Supporto nella gestione dell'interfacciamento dei sistemi con il firewall esterno Fortinet.
- 24. Supporto amministrazione cluster VMware;
- 25. Supporto cluster Microsoft HyperV;
- 26. Supporto alla creazione e alla propagazione di VLAN sulle apparecchiature di rete, e segmentazione delle apparecchiature connesse in dominio;
- 27. Servizio di monitoraggio degli apparati Server indicati dalla committente (Circa 15 Server) relativamente ai parametri vitali di base (Disk Space, Ram, CPU), il sistema deve prevedere un invio proattivo di mail agli indirizzi di posta elettronica che verranno comunicati dalla committente, il tutto al fine di evitare blocchi dei sistemi per le cause sopra citate.

Al fine di adempiere a tutte le attività di cui al presente documento si richiede:

- **L'erogazione di interventi svolti remotamente in modalità flat senza limiti di chiamate, sino alla naturale scadenza del contratto; l'assistenza prevede la connessione diretta ai nostri sistemi; laddove ciò non sia possibile, l'affidatario dovrà intervenire in loco previo appuntamento con il responsabile. L'aggiudicatario dovrà altresì rendersi disponibile per eventuali richieste di intervento on-site per attività non gestibili remotamente.**

- **Requisiti necessari per il supporto delle attività:**

	Certificazioni Richieste
1	Possesso della certificazione CHFI o Superiore da minimo 5 anni
2	Possesso della certificazione di CompTia "Security+"
3	Possesso della qualifica Auditor /Lead Auditor ISO 27001:2013 (sistemi di gestione di sicurezza dell'informazione), rilasciato da Ente Certificatore.
4	Possesso certificazioni tecniche sui firewall WatchGuard
5	Possesso certificazione Microsoft Solution Expert: Productivity
6	Possesso certificazione Microsoft TS Windows Server Virtualization, Configuration
7	Possesso certificazione Administering Microsoft SQL Server database
8	Possesso certificazione Cisco CCNP Enterprise
9	Possesso certificazione Cisco CCNP Security
10	Possesso certificazione VMware Professional Data Center Virtualization (VCP-DCV)

-
- L'affidatario deve garantire un supporto telefonico di primo livello dal lunedì al venerdì dalle ore 9:00 – 13:00 14:00 – 17:00.
 - L'affidatario dovrà anche dietro richiesta di Rete Gas Bari, coadiuvarsi con altre aziende che gestiscono software applicativi e servizi utilizzati dall'azienda, per gestire al meglio le necessità richieste di configurazione dei server e delle apparecchiature di rete e dei firewall.
 - L'affidatario dovrà garantire la presa in carico dell'intervento entro il giorno successivo lavorativo.
 - ***Emergenze:*** *In virtù del servizio pubblico reso da ReteGas si possono presentare situazioni per cui è necessario richiedere in emergenza interventi tecnici anche nei giorni festivi e prefestivi, per un massimo 6 giornate l'anno, tali attività extra saranno fatturate oltre i canoni mensili dell'importo globale di aggiudicazione, la ditta aggiudicataria deve necessariamente avere una sede operativa entro i 50 Km dalla sede di ReteGas, oltre ad avere personale per tutta la durata contrattuale, diretto riporto dell'Affidatario e certificato per espletare i servizi richiesti nel capitolato.*
 - Una volta ultimato ogni intervento, sia in loco che in teleassistenza, l'affidatario dovrà trasmettere all'Azienda Municipale Gas S.p.A., a mezzo posta elettronica, al referente del contratto, un rapporto tecnico dettagliato connesso alla richiesta di assistenza tecnica in modo da permettere le ordinarie verifiche di corretto funzionamento degli apparati oggetto degli interventi eseguiti, atto a tracciare sia gli interventi effettuati che lo stato delle apparecchiature informatiche.
 - Mensilmente, entro i primi cinque giorni lavorativi, l'affidatario dovrà tramettere al referente del contratto, un rapporto in formato Excel con le attività anche quelle di supporto e troubleshooting eseguite, oltre a un rapporto in formato Adobe Acrobat (PDF); il documento in formato Excel deve contenere tutte le informazioni degli interventi eseguiti, numero intervento; ora di esecuzione; tempo di esecuzione; data; intervento eseguito da; test di funzionalità; ecc...

Art.2 – Durata del contratto

La durata dell'appalto è fissata in due anni, decorrenti, presumibilmente, dal 30/05/2021 E', altresì, prevista in capo a ReteGas, l'opzione di esperire procedura negoziata, ai sensi dell'art. 125 co.1 lettera f) del d.lgs. 50/2016 e s.m.i., per l'affidamento delle medesime prestazioni per ulteriori due anni.

Art. 3 – Fatturazione e pagamenti

La fatturazione del corrispettivo dovrà intervenire con cadenza mensile e dovrà essere corrispondente ad 1/24 dell'importo contrattuale.

I pagamenti avranno luogo a 30 giorni fine mese data fattura, subordinatamente agli obblighi di legge. Prima della stipula del contratto, previo accordo tra le parti, il termine di pagamento potrà essere fissato a 60 giorni fine mese data fattura. Si precisa, inoltre, che la fattura, da trasmettere in modalità elettronica (cod. SUBM70N), dovrà riportare la seguente dicitura: <<Operazione soggetta alla scissione dei pagamenti – "IVA da versare a cura del cessionario art. 17ter D.P.R. 633/72 – Split payment">>.

Art. 4 – Risoluzione Del Contratto

Nel caso si verificano una o più inadempienze agli obblighi contrattuali, contestate formalmente secondo gli artt. 1454 e 1456 del c.c., ReteGas Bari avrà facoltà di risolvere il contratto con tutte le conseguenze di legge compreso il risarcimento del danno e l'affidamento del servizio a terzi.

Art. 5 – Ricognizione infrastruttura hardware e software

Le imprese che desidereranno partecipare alla gara, dovranno obbligatoriamente, previo appuntamento con il responsabile della sezione IT, verificare e visionare l'infrastruttura informatica da assistere, (*sarà rilasciato verbale di presa visione dell'infrastruttura*). La ricognizione della infrastruttura hardware e software sarà eseguita, sempre sotto il coordinamento del responsabile della sezione IT di ReteGas, in tele assistenza tramite l'ausilio di AnyDesk.

A seguito dell'affidamento, al fine di consentire all'operatore economico affidatario, la piena ed autonoma gestione delle attività richieste dal presente documento, sia in loco che da remoto, alla presenza e sotto il coordinamento del responsabile della sezione IT, fisicamente in sede, saranno generate le chiavi d'accesso amministrative sui domain controller e gli strumenti fisici e di rete, previa consegna dei documenti inerenti gli adempimenti formali sottostanti la gestione dei dati personali.

Sezione IT e sicurezza

Il responsabile

Pirozzi Eugenio



Bari 24/02/2021



COMPETENZE

	Certificazioni Richieste
1	Possesso della certificazione CHFI o Superiore da minimo 5 anni
2	Possesso della certificazione di CompTia "Security+"
3	Possesso della qualifica Auditor /Lead Auditor ISO 27001:2013 (sistemi di gestione di sicurezza dell'informazione), rilasciato da Ente Certificatore.
4	Possesso certificazioni tecniche sui firewall WatchGuard
5	Possesso certificazione Microsoft Solution Expert: Productivity
6	Possesso certificazione Microsoft TS Windows Server Virtualization, Configuration
7	Possesso certificazione Administering Microsoft SQL Server database
8	Possesso certificazione Cisco CCNP Enterprise
9	Possesso certificazione Cisco CCNP Security
10	Possesso certificazione VMware Professional Data Center Virtualization (VCP-DCV)

La certificazione di cui al p.to 1 è richiesta per la seguente motivazione:
in caso di incidenti informatici, ReteGas deve poter richiedere supporto relativamente alle procedure da adottare per definire la catena di custodia e l'estrazione di dati per finalità di indagini forensi.

Le certificazioni di cui ai p.ti 2 e 9 sono necessarie per l'amministrazione del network e dei sistemi connessi, sulla base degli standard sulla sicurezza informatica; la certificazione di cui al p.to 2 è di tipo trasversale e garantisce la conoscenza di metodologie di sicurezza informatica applicabili su tutti i sistemi; la certificazione di cui al p.to 9 garantisce una profonda conoscenza sulle metodologie di sicurezza informatica relativamente ai dispositivi di rete.

La certificazione di cui al p.to 3 garantisce una metodologia operativa ispirata a procedure standard relativamente alla gestione dei sistemi informatici garantendo la massima tutela dell'azienda supportata in termini di processi.

La certificazione di cui al p.to 4 è richiesta in quanto il firewall di BackEnd da amministrare è di tale marchio.

La certificazione di cui al p.to 5 è richiesta in quanto la quasi totalità dei sistemi operativi dei server è Microsoft ed è richiesta profonda conoscenza degli stessi e relativa integrazione.

La certificazione di cui al p.to 6 è richiesta in quanto ReteGas utilizza Microsoft HyperV in configurazione cluster per parte dei propri sistemi server.

La certificazione di cui al p.to 7 è richiesta in quanto ReteGas utilizza Microsoft SQL in configurazioni standalone e clusterizzate per la gestione delle basi di dati aziendali.

La certificazione di cui al p.to 8 è richiesta in quanto lo strato apparati di rete di cui è provvista ReteGas rappresenta un elemento critico per la continuità operativa. Tale certificazione garantisce una profonda conoscenza degli apparati di rete e delle metodologie ottimali di configurazione ed integrazione per garantire la continuità delle operazioni.

La certificazione di cui al p.to 10 è richiesta in quanto ReteGas utilizza VMware in configurazione cluster per parte dei propri sistemi server.

Sezione IT e sicurezza

Il responsabile

Pirozzi Eugenio

