

Capitolato tecnico per il servizio di gestione della server farm del gruppo Cyber Intelligence

Obiettivo del contratto	2
Descrizione server farm	2
Descrizione HW	2
Topologia di rete	3
Servizi interni	4
Descrizione servizio richiesto	5
Criteri di valutazione dell'offerta tecnica	6
Caratteristiche tecniche minime	6
Punteggi	7
Modalità di erogazione	9
Competenze minime richieste	9
Livelli di servizio	12
Termini e luogo di consegna ed installazione	13
Avvio e termine dell'esecuzione del contratto	13
Penalità	13
Oneri ed obblighi dell'Aggiudicatario	14
Proprietà Intellettuale e diritti di privativa	14
Divieto di cessione del contratto	15
Verifica di Conformità della fornitura	15
Fatturazione e condizioni di pagamento	15
Tracciabilità dei Flussi finanziari	16
Risoluzione e Recesso	16

Obiettivo del contratto

L'obiettivo del contratto è quello di effettuare la gestione della server farm a supporto delle attività del gruppo di ricerca Cyber Intelligence dell'IIT. L'attività prevede la fornitura del servizio di gestione sistemistica ed applicativa della server farm, dalla scelta dell'HW all'installazione/configurazione ed integrazione nell'infrastruttura virtualizzata, alla gestione sistemistica ed applicativa, al troubleshooting HW/SW, al monitoraggio, al ripristino dai disservizi, all'evoluzione della farm e dei servizi, alla gestione della sicurezza informatica e degli accessi, alla implementazione di misure nell'ambito della Privacy, alla definizione di policy e procedure interne.

Descrizione server farm

La server farm comprende 7 server fisici alloggiati nei rack del datacenter IIT e virtualizzati principalmente con tecnologia vmware; ospitano circa 110 macchine virtuali, per la maggior parte linux Ubuntu, ma ve ne sono anche CentOS, Fedora, bsd e windows; la farm è articolata su più reti interne (fisiche e virtuali) il cui traffico è mediato da vps che agiscono come firewall/transparent firewall e reverse proxy; i servizi interni comprendono nfs (freenas), dns (bind), gestione centralizzata utenze (freeipa), monitoraggio (nagios), backup (ghettoVCB), svn, git e server openvpn; la farm eroga servizi ai ricercatori sia di tipo tradizionale (es. vm dedicate, web server, db sql) che BigData (es. elasticserch/kibana, spark/hadoop) ed in generale supporta la sperimentazione ed adozione di strumenti innovativi.

Descrizione HW

La farm si articola su 7 server fisici, le cui caratteristiche sono descritte di seguito:

server	Model	core	ram	storage	ssd
wafivm5	Dell R415	12	128GB	2TB	-
wafivm6	Dell R430	16	192GB	4TB	1TB
wafivm7	Fujitsu RX2530M2	24	256GB	6TB	1TB
wafivm8	Dell R430	20	256GB	8TB	-
wafivm9	Dell R430	20	256GB	8TB	512GB
freenas3	HP DL380 G5	4	24GB	32TB	-
freenas5	Supermicro	8	8GB	20TB	-

E' inoltre presente uno switch netgear XS716E collegato in trunk con i server.

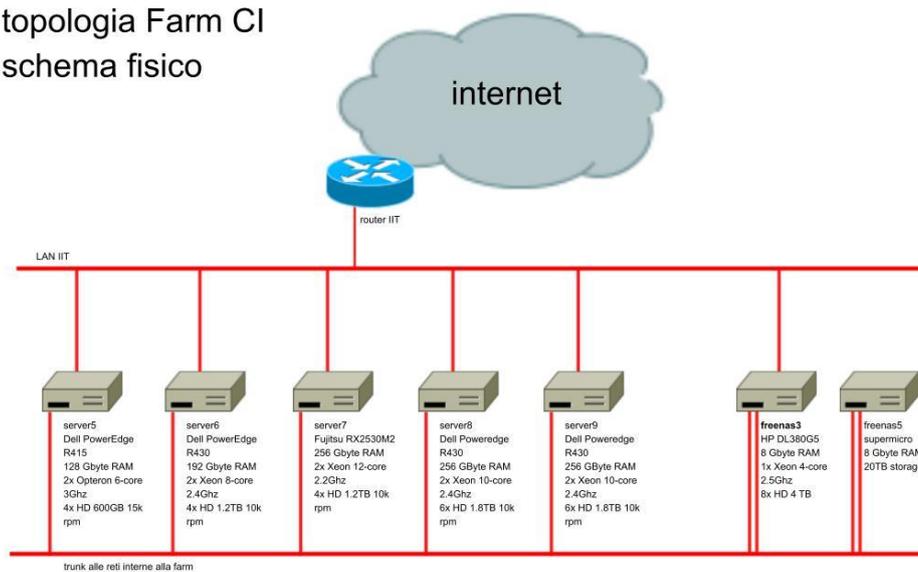
Sui server sono installate le seguenti versioni di OS:

server	Versione OS
wafivm5	Esxi 5.5
wafivm6	Esxi 6.0
wafivm7	Esxi 6.0
wafivm8	Esxi 6.0
wafivm9	Esxi 6.5
freenas3	freenas 9
freenas5	freenas 9

Topologia di rete

Lo schema fisico della rete della farm è riportato di seguito:

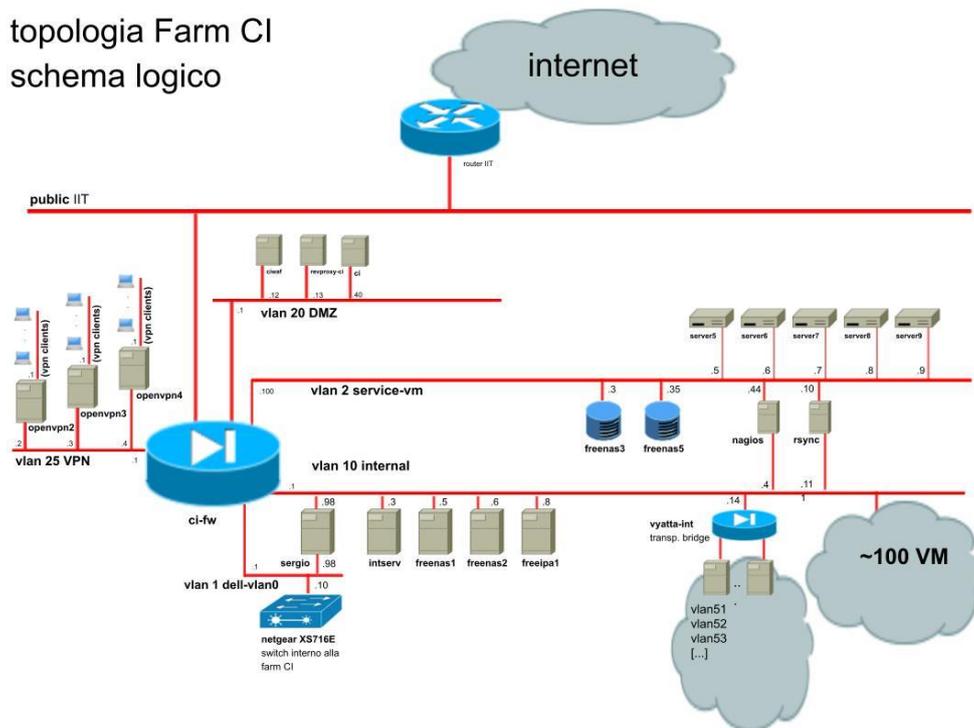
topologia Farm CI
schema fisico



Ciascuno dei server vmware ha una interfaccia fisica attestata su rete pubblica (su switch gestiti da terzi) ed una o due interfacce fisiche collegate in trunk allo switch interno della farm.

Sui server vmware è configurata una topologia di rete logica basata su numerose vlan configurate in modo opportuno anche sullo switch interno, in modo da ottenere lo schema logico di rete descritto di seguito:

topologia Farm CI schema logico



La comunicazione fra le vlan è mediata da istanze di VM vyatta.

Servizi interni

Di seguito sono descritti i principali servizi interni alla farm:

servizio	descrizione
Sso	gestione utenze personali basata su freeipa 4, per accessi ssh, vpn e web
Dns	dns interno basato su bind 9
Vpn	accessi vpn con permessi differenziati, basati su openvpn 2
Ssh	accessi ssh tramite bastion host in dmz
Git	servizio git interni, basato su gitlab ce 11
Nfs	servizio interno nfs ridondato su due vps con freenas 8
Backup	backup delle vm effettuato da esxi su nfs, basato su ghettovcb 2017 e su sistema custom di rotazione dei backups
monitoring	monitoring di oltre 400 servizi interni distribuiti su oltre 100 vm, basato su nagios 3
Firewall	la comunicazione fra vlan è mediata da più istanze di firewall/transparent firewall, basate su vyatta 6 con configurazione da linea di comando
Waf	web application firewall implementato tramite reverse proxy e basato su apache2 e modproxy/modsecurity
siti web	l'infrastruttura ospita decine di siti web accessibili anche da internet e gestiti anche tramite virtual hosting su varie vm

db sql	l'infrastruttura ospita numerose istanza di db sql, principalmente mysql/mariadb in varie versioni
Elastic	l'infrastruttura ospita numerose istanze di elasticsearch/kibana, principalmente versione 7

La farm si articola su oltre 100 macchine virtuali, principalmente linux, che supportano le attività di ricerca del gruppo CyberIntelligence.

Descrizione servizio richiesto

Il servizio richiesto punta a supportare efficacemente il gruppo di ricerca nelle attività quotidiane, sfruttando al meglio le risorse HW/SW della server farm e limitando al minimo gli investimenti necessari per la sua evoluzione e mantenimento, come di seguito descritto:

1. attività legate all'HW:
 - a. supporto alla definizione caratteristiche HW da acquistare (server, network e componenti) per il mantenimento e l'evoluzione della farm; installazione, collaudo, prima configurazione del nuovo HW on-site e successiva integrazione nella farm virtualizzata
 - b. supporto on-site per gestione problematiche legate all'HW
 - c. eventuale spostamento di apparati, minimizzando i disservizi ed adeguando le configurazioni
2. attività gestionali:
 - a. gestione sistemistica dei server fisici, virtualizzati principalmente in tecnologia vmware
 - b. gestione del networking sia HW che virtualizzato
 - c. gestione applicativa dell'infrastruttura della farm, che include: dns interno, gestione centralizzata utenze, monitoraggio, backup, storage con livelli di ridondanza differenziati, provisioning di nuove macchine virtuali su misura per le varie esigenze
 - d. gestione delle utenze sistemistiche ed applicative, con profilazione adeguata ai differenti ruoli
 - e. gestione sistemistica degli oltre 100 VPS, principalmente Ubuntu, orientata a massimizzare l'uptime e le prestazioni dei servizi critici per la ricerca, nonché la salvaguardia dei relativi dati, sfruttando al meglio le risorse HW/SW disponibili
 - f. capacity management/planning delle risorse di calcolo e di storage dei servizi della farm
 - g. aggiornamento delle componenti SW obsolete ed applicazione delle patch, in accordo con le esigenze del gruppo; in particolare questa attività richiederà uno sforzo rilevante per essere condotta aggiornando i servizi obsoleti e migrandoli su vps con versioni più recenti di linux, minimizzando l'impatto sulle attività di ricerca
 - h. supporto al troubleshooting applicativo sulle tecnologie innovative testate o utilizzate dai ricercatori
 - i. gestione di tutti gli aspetti di sicurezza informatica: configurazione di opportune politiche di protezione sui FW/WAF e sui sistemi (da concordare con il cliente), rilevazione ed approfondimento di anomalie, gestione di eventuali incidenti; l'attività include l'effettuazione di periodiche analisi di sicurezza dei servizi esposti dalla farm
 - j. produzione e mantenimento di documentazione aggiornata relativa alla farm (es. topologia di rete, indirizzamento, descrizione generale e dei principali compiti di amministrazione, produzione di documentazione ad hoc a supporto dell'uso di specifici servizi)

3. attività progettuali:
 - a. progettazione della evoluzione HW e SW della farm
 - b. analisi dell'impatto dei requisiti di sicurezza informatica e della normativa Privacy; studio di soluzioni sia tecniche che procedurali in grado di permetterne l'adozione minimizzando i rischi e l'impatto sulla produttività dei ricercatori
 - c. consulenza tecnica orientata a supportare nuove attività progettuali basate sulla farm

4. supporto alla gestione dei dati dei progetti di ricerca, che può prevedere a titolo esemplificativo e non esaustivo le seguenti attività:
 - a. la definizione congiunta iniziale della infrastruttura che può essere allocata (in base alle risorse disponibili), e la valutazione degli aspetti di sicurezza informatica e privacy
 - b. la creazione di varie vm e la definizione del relativo monitoring e backup
 - c. l'installazione del SW necessario, preferibilmente utilizzando container docker
 - d. l'integrazione dei servizi che vengono resi disponibili ai ricercatori, che tipicamente sono di tipo innovativo ed orientati ai Big Data quindi in generale sono poco maturi e costituiscono spesso oggetto di nuova sperimentazione
 - e. la creazione di opportune utenze personali per l'accesso alla farm e l'accesso ai servizi per il personale necessario
 - f. il supporto ai ricercatori per eventuale troubleshooting o tuning prestazionale, anche scalando le risorse messe a disposizione
 - g. il mantenimento dei servizi, rilevando eventuali problemi ed intervenendo per risolverli
 - h. a termine progetto il ridimensionamento delle risorse allocate e l'archiviazione dei dati di interesse, nonché la disattivazione delle utenze personali non più necessarie

Criteria di valutazione dell'offerta tecnica

L'offerta tecnica presentata dovrà comprendere la descrizione:

- delle competenze ed organizzazione del team proposto
- delle modalità di presa in carico
- delle modalità di gestione del servizio
- del piano di miglioramento proposto per l'infrastruttura

L'offerta dovrà includere adeguata descrizione dell'esperienza maturata dal soggetto proponente e degli skill del team proposto per la gestione del servizio, che dovranno soddisfare i requisiti minimi di competenza previsti all'interno della sezione "Competenze minime richieste".

Caratteristiche tecniche minime

Si evidenziano le caratteristiche tecniche minime obbligatorie che devono essere trattate, a pena di esclusione, nella stesura della relazione tecnica:

#	Macro requisito	#	Dettaglio
RM1	qualità dei servizi professionali	RM1.1	esperienza di almeno 3 anni nella scelta, installazione e manutenzione di apparati HW in ambito datacenter
		RM1.2	esperienza di almeno 3 anni nella progettazione di architetture ICT complesse, integrazione di sistemi e documentazione
		RM1.3	esperienza di almeno 2 anni nello sviluppo di codice in ambito di supporto alle Operations ICT
		RM1.4	esperienza di almeno 3 anni nella gestione sistemistica ed applicativa in ambito datacenter
		RM1.5	esperienza di almeno 3 anni nella gestione di progetti in ambito ICT
		RM1.6	esperienza di almeno 3 anni nella gestione di ambienti virtualizzati in tecnologia vmware
		RM1.7	esperienza di almeno 2 anni nella integrazione e gestione di ambienti in tecnologia Docker
		RM1.8	esperienza di almeno 2 anni nella gestione di tecnologie BigData ed in particolare di elasticsearch
RM2	sicurezza informatica e privacy	RM2.1	esperienza di almeno 3 anni nella gestione della sicurezza informatica in ambito datacenter
		RM2.2	esperienza di almeno 3 anni nella definizione ed implementazione di misure tecniche e procedurali per il rispetto della normativa Privacy
RM3	esperienza in ambito ricerca ICT	RM3.1	esperienza di almeno 3 anni nella gestione di datacenter a supporto di attività di ricerca ICT
RM4	Competenze tecniche del team di lavoro	RM4.1	Vedi il paragrafo “Competenze minime richieste dei componenti del team di lavoro” all’interno dei Livelli di servizio

Punteggi

Il punteggio dell’offerta tecnica è attribuito sulla base dei criteri di valutazione elencati nella sottostante tabella con la relativa ripartizione dei punteggi, sino ad un massimo di 80 punti di cui sino a 50 tabellari e sino a 30 discrezionali.

Nella colonna punti D vengono indicati i “Punteggi discrezionali”, vale a dire i punteggi il cui coefficiente è attribuito in ragione dell’esercizio della discrezionalità spettante alla Commissione giudicatrice. Nella colonna punti T vengono indicati i “Punteggi tabellari”, vale a dire i punteggi i cui coefficienti fissi e

predefiniti che saranno attribuiti o non attribuiti in ragione dell'offerta o mancata offerta di quanto specificamente richiesto.

#	Criteri di valutazione	Punti MAX	#	sub criteri di valutazione	Punti T	Punti D
C1	qualità dei servizi professionali	20	C1.1a	esperienza di 4 anni nella gestione sistemistica ed applicativa in ambito datacenter	2	0
			C1.1.b	esperienza di 5 anni nella gestione sistemistica ed applicativa in ambito datacenter	5	0
			C1.1.c	esperienza di 6 o più anni nella gestione sistemistica ed applicativa in ambito datacenter	10	0
			C1.2a	esperienza di 4 anni nella gestione di ambienti virtualizzati	1	0
			C1.2b	esperienza di 5 anni nella gestione di ambienti virtualizzati	2	0
			C1.2c	esperienza di 6 o più anni nella gestione di ambienti virtualizzati	10	0
C2	sicurezza informatica e privacy	15	C2.1	possesso della certificazione CISSP in corso di validità	10	0
			C2.2a	esperienza di 2 anni in attività progettuali riservate con LEA (Law Enforcement Agencies) o DIS	2	0
			C2.2b	esperienza di 4 anni in attività progettuali riservate con LEA (Law Enforcement Agencies) o DIS	5	0
C3	esperienza in ambito ricerca ICT	10	C3.1a	esperienza di 4 anni nella gestione di datacenter a supporto di attività di ricerca ICT	2	0
			C3.1b	esperienza di 5 anni nella gestione di datacenter a supporto di attività di ricerca ICT	5	0
			C3.1c	esperienza di 6 o più anni nella gestione di datacenter a supporto di attività di ricerca ICT	10	0
C4	Qualità e composizione team	15	C4.1	Competenze ed esperienza complessive del team proposto	0	5
			C4.2	organizzazione del team per la fornitura del servizio. Sarà ritenuto elemento preferenziale la messa a disposizione di un solo referente	0	10

				che abbia competenze sufficienti per garantire il servizio		
C5	qualità della proposta progettuale	15	C5.1	efficacia del piano di rapida presa in carico della gestione della farm	0	10
			C5.2	qualità del piano di miglioramento	0	5

Modalità di erogazione

Il servizio di gestione e supporto si intende erogato di norma da remoto via internet, tranne nelle occasioni in cui sia necessario o preferibile intervenire on-site, per attività di manutenzione programmate o per il ripristino da disservizi; anche le interazioni quotidiane con il gruppo di ricerca si intendono effettuate di norma da remoto, sfruttando strumenti di collaborazione e di teamworking online adottati dal gruppo, in particolare la chat di gruppo che dovrà essere seguita con continuità, costituendo la forma principale di interazione e di richiesta di collaborazione per tutte le attività; per le emergenze dovrà comunque essere indicato anche un numero di telefono mobile presso il quale il gestore sia di norma reperibile.

Gli strumenti di produttività individuale usati dal gestore non saranno forniti dall'IIT, e non saranno riconosciuti costi aggiuntivi per eventuali interventi in sede. Il gestore del servizio avrà facoltà di proporre l'acquisto di componenti HW/SW utili a migliorare l'infrastruttura e avrà facoltà di installare eventuali propri componenti (es. dispositivi di accesso remoto) a supporto della gestione, concordandone i dettagli con il responsabile del gruppo di ricerca.

Competenze minime richieste

Il Gruppo di Lavoro (GdL) dovrà comprendere persone che siano in grado di svolgere le attività previste nel presente capitolato e nell'offerta dell'aggiudicatario con la massima professionalità.

Il GdL dovrà essere composto almeno dalle seguenti professionalità con i seguenti livelli minimi di competenze di base:

- Il Gruppo di Lavoro (GdL) dovrà essere composto da persone dotate delle competenze individuate nel proseguo del paragrafo;
- I componenti del GdL potranno far parte dell'organico aziendale oppure essere collaboratori incaricati all'uopo, nei tempi e nei modi ritenuti opportuni dall'Aggiudicatario. In nessun caso potranno formarsi e derivare a carico del CNR oneri aggiuntivi di qualsiasi natura come conseguenza di azioni intraprese dall'Aggiudicatario per la realizzazione del servizio, ivi comprese le eventuali azioni per la formazione dei rapporti di collaborazione professionale con i componenti del gruppo di lavoro; la presentazione dei curricula dei componenti del GDL è obbligatoria e dovrà essere fornita prima della stipula del contratto.
- Prima della stipula del contratto l'operatore economico deve indicare il/i professionista/i che designati allo svolgimento dell'attività e dovranno fornire i loro CV e tutta la documentazione comprovante il possesso dei requisiti dichiarati. La struttura appaltante si riserva di visionare e appurare le competenze dichiarate anche attraverso colloquio diretto con i designati.
- Il gruppo di lavoro presentato in sede di offerta tecnica non potrà essere modificato nei suoi componenti durante la fase di esecuzione del contratto senza la previa approvazione della stazione appaltante;

- I nuovi componenti che sostituiscono dovranno, in ogni caso, possedere requisiti o esperienza professionale equivalenti o superiori a quelli delle persone sostituite, da comprovare mediante l'esibizione di curricula adeguati;
- Il gruppo di lavoro dovrà essere composto da max. 3 professionisti. Sarà attribuito un punteggio preferenziale (come descritto all'interno della griglia dei criteri di valutazione al punto C4.2) agli operatori economici che offriranno il servizio attraverso la messa a disposizione di un unico professionista in maniera continuativa per tutta la durata di copertura del servizio, il quale avrà le competenze necessarie a garantire l'effettuazione dell'intero servizio a regola d'arte; si ritiene infatti, che tale fattispecie garantisca una maggiore efficacia e continuità nel tempo del servizio offerto. Il professionista unico individuato per l'espletamento dell'intero servizio dovrà possedere le skills minime individuate per ciascuno dei tre profili di seguito descritti.

Segue la composizione del gruppo di lavoro, con le relative skills minime richieste per ciascun profilo:

- Un responsabile di progetto, con i requisiti riportati in tabella:

Responsabile di progetto	
Titolo di Studio	Laurea in Ingegneria Informatica o Informatica o Scienze dell'Informazione
Esperienze Lavorative	<ul style="list-style-type: none"> • Almeno 3 di provata esperienza lavorativa nella conduzione di progetti complessi in ambito ICT • Almeno 5 anni di provata esperienza nella gestione di Operations ICT
Conoscenze	<ul style="list-style-type: none"> • Conoscenze ed uso di tecniche e prodotti SW per project management • Redazione di specifiche di progetto, stima di risorse e tempistiche • Analisi e progettazione, testing e documentazione di sistemi informativi

- Un amministratore di sistema senior, con i requisiti riportati in tabella:

Responsabile tecnico	
Titolo di Studio	Laurea in Ingegneria Informatica o Informatica o Scienze dell'Informazione
Esperienze Lavorative	<ul style="list-style-type: none"> • Minimo 10 anni di esperienza nelle ICT Operations in ambito datacenter • Minimo 5 anni di esperienza nella realizzazione di sistemi informativi • Analisi, progettazione ed integrazione di sistemi informativi • Partecipazione a gruppi di lavoro nell'ambito di progetti internazionali • Redazione di specifiche di progetto • Installazione e configurazione di macchine virtuali linux in datacenter virtualizzati con tecnologia vmware • Progettazione e gestione di architetture di rete fisiche e virtualizzate • Installazione e configurazione di middleware • Integrazione di prodotti e/o componenti • Redazione documentazione di progetto a supporto delle Operations • Esperienza ed attitudine al troubleshooting ed al problem solving • Autonomia nell'individuare, pianificare e progettare adeguamenti tecnologici infrastrutturali • partecipazione alla definizione delle misure di sicurezza e successiva implementazione in ambito datacenter

Conoscenze	<ul style="list-style-type: none"> • installazione, configurazione ed amministrazione di HW (server ed apparati di rete) in ambito datacenter • amministrazione ambienti virtualizzati in tecnologia vmware • amministrazione sistemi linux (principalmente ubuntu) • amministrazione apparati di rete • amministrazione firewall/transparent firewall vyatta • amministrazione web application firewall basati su apache2/nginx • amministrazione database sql • amministrazione ambienti e middleware BigData, in particolare elasticsearch/kibana • amministrazione dns (bind) • amministrazione sistemi di SSO (freeipa) • amministrazione sistemi di monitoring (nagios) • amministrazione server vpn (openvpn) • amministrazione sistemi di backup vmware (ghettoVcb) • amministrazione di sistemi di revisione del codice (svn/git) • sviluppo script di shell (bash) • integrazione sistemi • troubleshooting sia a livello di sistema (strace) che di rete (tcpdump/wireshark) • amministrazione ambienti a microservizi (swarm docker) • lingua inglese (efficacia nella interazione verbale in conference call e nella redazione di documentazione tecnica)
-------------------	---

- Un esperto in sicurezza informatica con conoscenza delle problematiche relative alla normativa Privacy, con i requisiti riportati in tabella:

Esperto in sicurezza informatica	
Titolo di Studio	Laurea in Ingegneria Informatica o Informatica o Scienze dell'Informazione
Esperienze Lavorative	<ul style="list-style-type: none"> • Almeno 5 anni di esperienza lavorativa nel settore della sicurezza informatica in ambito datacenter • analisi dei rischi legati alla sicurezza informatica e stesura di proposte per la loro mitigazione • supporto alle operations ICT su aspetti di sicurezza in ambito datacenter • gestione di incidenti ICT • analisi delle problematiche legate al rispetto della normativa Privacy e individuazione di soluzioni per garantirne il rispetto contenendo i costi ed l'impatto sulla produttività • almeno 2 anni di esperienza nel supporto a progetti di ricerca ICT, anche in ambito internazionale

Conoscenze	<p>e' gradita la certificazione CISSP in corso di validita' o conoscenze equivalenti sui seguenti ambiti, declinate nell'ambito di Operations e progetti ICT:</p> <ul style="list-style-type: none">• Security and Risk Management• Asset Security• Security Architecture and Engineering• Communications and Network Security• Identity and Access Management• Security Assessment and Testing• Security Operations• Software Development Security
-------------------	--

Per tutto il personale che costituisce il Gdl dovranno essere forniti i curricula che attestano il possesso dei requisiti precedentemente specificati.

Livelli di servizio

La proposta di progetto deve necessariamente includere la copertura dei livelli di servizio descritti di seguito, sia relativamente agli interventi in orario lavorativo che in orario non lavorativo.

Interventi in orario lavorativo

Per gli interventi dichiarati come **urgenti** da parte del cliente si applicano i livelli di servizio descritti di seguito, calcolati all'interno dell'orario lavorativo standard (dal lunedì al venerdì, dalle ore 9 alle ore 18, esclusi i giorni festivi):

1. intervento da remoto entro 30 minuti dalla chiamata almeno nell'80% delle occasioni, calcolato su almeno 5 interventi consecutivi nell'arco della durata contrattuale; si intendono calcolabili per questo fine al massimo 10 richieste di questo tipo nell'arco di 30gg solari
2. intervento on-site entro 2 ore dalla chiamata almeno nell'80% delle occasioni, calcolato su almeno 5 interventi consecutivi nell'arco della durata contrattuale; si intendono calcolabili per questo fine al massimo 4 interventi on-site classificati come urgenti nell'arco di 30gg solari

Interventi al di fuori dell'orario lavorativo

Per gli interventi classificati come urgenti da parte del cliente si applicano i livelli di servizio descritti di seguito, calcolati al di fuori dell'orario lavorativo standard:

1. intervento da remoto entro 4 ore dalla chiamata almeno nell'80% delle occasioni, calcolato su almeno 5 interventi consecutivi nell'arco della durata contrattuale; si intendono calcolabili per questo fine al massimo 2 richieste di questo tipo nell'arco di 30gg solari
2. intervento on-site entro 12 ore dalla chiamata almeno nell'80% delle occasioni, calcolato su almeno 5 interventi consecutivi nell'arco della durata contrattuale; si intendono calcolabili per questo fine al massimo 2 interventi on-site classificati come urgenti nell'arco di 30gg solari

Esclusioni

Sono escluse dal calcolo le tempistiche di intervento:

- a. non rispettate per cause di forza maggiore
- b. indotte da malfunzionamenti ripetuti per mitigare i quali il cliente non abbia adottato le raccomandazioni indicate dal gestore (es. mancanza di ricambi o sovraccarico dei sistemi)

- c. relative a periodi limitati (al massimo per il 10% delle giornate di supporto previste contrattualmente) e concordati in anticipo, per i quali il gestore potrà richiedere la sospensione del calcolo dei livelli di servizio

Termini e luogo di consegna ed installazione

I termini di consegna dei servizi, sono da intendersi in giorni naturali e consecutivi decorrenti dal giorno successivo alla sottoscrizione del contratto.

La consegna e l'installazione dei beni e servizi della fornitura dovrà essere effettuata presso l'indirizzo indicato in tabella, in accordo con il Direttore esecutivo del Contratto:

# Prodotto	Luogo di consegna e installazione
	Istituto di Informatica e Telematica del Cnr di Pisa, via G. Moruzzi 1, 56124 Pisa

Avvio e termine dell'esecuzione del contratto

Il Direttore dell'esecuzione del contratto (DEC), sulla base delle disposizioni del Responsabile Unico del Procedimento (RUP), dopo che il contratto è divenuto efficace, dà avvio all'esecuzione della prestazione, fornendo all'Aggiudicatario tutte le istruzioni e direttive necessarie e redigendo, laddove sia indispensabile in relazione alla natura e al luogo di esecuzione delle prestazioni, apposito verbale come meglio disciplinato all'Art. 19 del DM n° 49 del 7 marzo 2018 del Ministero delle Infrastrutture e dei Trasporti. In tutti i casi in cui ricorrano circostanze speciali che impediscano in via temporanea l'esecuzione dell'appalto si applicano le disposizioni di cui all'Art. 107 del D. Lgs. 50/2016 e s.m.i. e all'Art. 23 del già citato DM. L'Aggiudicatario è tenuto a comunicare alla Stazione Appaltante l'intervenuta ultimazione delle prestazioni contrattuali. Il DEC, entro 5 giorni da tale comunicazione, effettua, in contraddittorio con l'Aggiudicatario medesimo, i necessari accertamenti e trasmette al RUP, entro i successivi 5 giorni, il certificato di ultimazione della prestazione, che ne rilascerà copia conforme all'Aggiudicatario.

Penalità

Per ogni giorno solare di ritardo nell'esecuzione della fornitura oggetto del presente contratto si applicherà una penale pari all'0,6‰ (0,6 per mille) dell'importo contrattuale, al netto dell'IVA.

Nel caso in cui la prima verifica di conformità della fornitura abbia esito sfavorevole non si applicano le penali; qualora tuttavia l'Aggiudicatario non renda nuovamente la fornitura disponibile per la verifica di conformità entro i 30 giorni solari successivi al primo esito sfavorevole, ovvero la verifica di conformità risulti nuovamente negativa, si applicherà la penale sopra richiamata per ogni giorno solare di ritardo.

Nell'ipotesi in cui l'importo delle penali applicabili superi l'importo pari al 20% (venti per cento) dell'importo contrattuale, al netto dell'IVA, l'Ente risolverà il contratto in danno all'Aggiudicatario, salvo il diritto al risarcimento dell'eventuale danno patito.

Gli inadempimenti contrattuali che daranno luogo all'applicazione di penali di cui ai precedenti periodi verranno contestati all'Aggiudicatario per iscritto.

L'Aggiudicatario dovrà comunicare in ogni caso le proprie deduzioni nel termine massimo di 5 (cinque) giorni lavorativi dalla stessa contestazione. Qualora dette deduzioni non siano accoglibili a giudizio della Stazione

Appaltante ovvero non vi sia stata risposta o la stessa non sia giunta nel termine indicato, si applicheranno le penali sopra indicate.

Le penali verranno regolate dalla Stazione Appaltante, o sui corrispettivi dovuti all'Aggiudicatario

Oneri ed obblighi dell'Aggiudicatario

L'aggiudicatario si impegna ad eseguire le prestazioni oggetto del presente contratto, senza alcun onere aggiuntivo, salvaguardando le esigenze della Stazione Appaltante e di terzi autorizzati, senza recare intralci, disturbi o interruzioni all'attività lavorativa in atto.

Rinuncia a qualsiasi pretesa o richiesta di compenso nel caso in cui lo svolgimento delle prestazioni contrattuali dovesse essere ostacolato o reso più oneroso dalle attività svolte dalla Stazione Appaltante e/o da terzi.

E' direttamente responsabile dell'inosservanza delle clausole contrattuali anche se questa dovesse derivare dall'attività del personale dipendente di altre imprese a diverso titolo coinvolto.

Deve avvalersi di personale qualificato in regola con gli obblighi previsti dai contratti collettivi di lavoro e da tutte le normative vigenti, in particolare in materia previdenziale, fiscale, di igiene ed in materia di sicurezza sul lavoro.

Risponderà direttamente dei danni alle persone, alle cose comunque provocati nell'esecuzione dell'appalto che possano derivare da fatto proprio, dal personale o da chiunque chiamato a collaborare. La Stazione Appaltante è esonerata da ogni responsabilità per danni, infortuni o altro dovesse accadere al personale di cui si avvarrà l'Aggiudicatario nell'esecuzione del contratto.

Si fa carico, intendendosi remunerati con il corrispettivo contrattuale, di tutti gli oneri ed i rischi relativi alle attività ed agli adempimenti occorrenti all'integrale espletamento dell'oggetto contrattuale, ivi compresi, a mero titolo esemplificativo e non esaustivo, gli oneri relativi ad eventuali spese di viaggio e di missione per il personale addetto alla esecuzione della prestazione, nonché i connessi oneri assicurativi.

Inoltre l'aggiudicatario si obbliga a quanto segue:

- Ad eseguire le prestazioni oggetto del presente contratto a perfetta regola d'arte e nel rispetto di tutte le norme e le prescrizioni tecniche e di sicurezza in vigore e di quelle che dovessero essere emanate nel corso del presente contratto, nonché secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel presente contratto e nei suoi allegati;
- Per consentire il corretto svolgimento del progetto entro i termini indicati nel presente capitolato, tutte le persone coinvolte nello svolgimento delle attività dovranno, quindi, operare in stretto coordinamento con lo staff preposto dalla Stazione Appaltante.
- Per tutta la durata delle attività saranno necessari aggiornamenti sul progresso delle attività mediante riunioni da remoto o in presenza tra il personale dell'azienda assegnataria e quello di progetto.
Indicazione dei soggetti coinvolti

Proprietà Intellettuale e diritti di privativa

Il CNR acquista la proprietà piena ed esclusiva di tutto il materiale sviluppato per l'esecuzione del servizio, della proprietà intellettuale del software prodotto ad hoc con la sola eccezione dei diritti morali ove applicabili. Sono fatti salvi in ogni caso i diritti connessi al software open source e alle licenze di software utilizzati per la realizzazione dei prodotti o servizi.

Il CNR non assumerà alcuna responsabilità nel caso in cui l'Aggiudicatario fornisca soluzioni tecniche, estetiche o funzionali ed in genere opere dell'ingegno, simboli, segni distintivi o trovati, di cui altri detengano la privativa. L'Aggiudicatario assumerà l'obbligo di tenere indenne la Stazione appaltante da tutte le rivendicazioni, le responsabilità, perdite e danni pretesi da chiunque, nonché da tutti i costi, le spese o responsabilità ad essi relativi a seguito di qualsiasi rivendicazione di violazione dei diritti d'autore o di qualsiasi marchio italiano o straniero, derivante o che si pretendesse derivare dalla prestazione.

Ciascuna parte si obbliga a dare immediato avviso all'altra di qualsiasi azione di rivendicazione o altri atti o fatti di terzi di cui al precedente comma, della quale sia venuta a conoscenza.

Divieto di cessione del contratto

E' vietata la cessione del contratto ai sensi dell'art. 105, comma 1 del D. Lgs. 50/2016 e s.m.i.

Per quanto riguarda le modificazioni soggettive che comportino cessioni di azienda e atti di trasformazione, fusione e scissione relative all'Aggiudicatario, si applicano le disposizioni di cui all'art. 106 del D. Lgs. 50/2016 e s.m.i.

L'Aggiudicatario è tenuto a comunicare tempestivamente alla Stazione Appaltante ogni modificazione intervenuta negli assetti proprietari e nella struttura organizzativa.

Verifica di Conformità della fornitura

La fornitura sarà soggetta a verifica di conformità per certificare che l'oggetto del contratto in termini di prestazioni, obiettivi e caratteristiche tecniche, economiche e qualitative sia stato realizzato ed eseguito nel rispetto delle previsioni contrattuali e delle pattuizioni concordate in sede di aggiudicazione, ai sensi dell'art. 102 del D. Lgs. 50/2016 e s.m.i..

Le attività di verifica saranno effettuate entro 30 (trenta) giorni solari dalla data di consegna della fornitura.

Fatturazione e condizioni di pagamento

La fatturazione avverrà come di seguito indicato:

- 30% dell'importo contrattuale a titolo di anticipo. L'erogazione dell'anticipazione, consentita anche nel caso di consegna in via d'urgenza, ai sensi dell'articolo 32, comma 8, del presente codice, è subordinata alla costituzione di garanzia fidejussoria bancaria o assicurativa di importo pari all'anticipazione maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma della prestazione. Il pagamento dell'anticipo avverrà entro 15 giorni dal ricevimento della garanzia suindicata;
- 40% dell'importo contrattuale al termine dei primi sei mesi di attività e pagamento entro 30 giorni dal positivo esito della verifica di conformità.
- 40% dell'importo contrattuale al termine dell'attività e pagamento entro 30 giorni dal positivo esito della verifica di conformità.

Il pagamento verrà effettuato entro 30 giorni dall'attestazione di regolare esecuzione da parte del Responsabile del Servizio. La fatturazione avverrà successivamente alla consegna totale dell'ordine.

La fattura dovrà essere emessa in forma elettronica ai sensi e per gli effetti del Decreto del Ministero dell'Economia e delle Finanze N. 55 del 3 aprile 2013, inviando il documento elettronico al Sistema di Interscambio che si occuperà di recapitare il documento ricevuto all'Ente destinatario, identificata dal seguente Codice Univoco Ufficio – CUU “LVHDFJ”. Le fatture sono soggette a “Split Payment”. La fattura, intestata all'Ente, dovrà contenere, pena il rifiuto della stessa:

- La partita IVA dell'Ente: 02118311006;
- Il riferimento al contratto (n° di protocollo e data);
- CIG **8858269AD2**
- Il CUU (Codice Univoco Ufficio);;

- L'importo imponibile;
- L'IVA;
- Il totale della fattura;
- L'oggetto del contratto;
- Il codice IBAN del conto corrente dedicato di cui alla Legge 136/2010.

Ai fini del pagamento del corrispettivo l'Ente procederà ad acquisire il documento unico di regolarità contributiva (D.U.R.C.), attestante la regolarità in ordine al versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti. L'Ente, in ottemperanza alle disposizioni previste dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973, con le modalità di cui al Decreto del Ministero dell'Economia e delle Finanze del 18 gennaio 2008 n. 40, parzialmente modificati dalla Legge 205/2017, per ogni pagamento di importo superiore ad euro 5.000,00 procederà a verificare se il beneficiario è inadempiente all'obbligo di versamento derivante dalla notifica di una o più cartelle di pagamento per un ammontare complessivo pari almeno a tale importo. Nel caso in cui la società Equitalia S.p.A. comunichi che risulta un inadempimento a carico del beneficiario l'Ente applicherà quanto disposto dall'art. 3 del decreto di attuazione di cui sopra. L'Operatore economico, sotto la propria esclusiva responsabilità, renderà tempestivamente note all'Ente le variazioni che si verificassero circa le modalità di accredito di cui sopra. In difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, l'Operatore economico non potrà sollevare eccezioni in ordine ad eventuale ritardo del pagamento, né in ordine a pagamento già effettuato. In sede di liquidazione delle fatture potranno essere recuperate le spese per l'applicazione di eventuali penali, di cui all'articolo 16 del presente contratto, l'Ente potrà sospendere, ferma restando l'applicazione delle eventuali penali, i pagamenti all'Operatore economico cui sono state contestate inadempienze nell'esecuzione della fornitura, fino al completo adempimento degli obblighi contrattuali (art. 1460 C.C.). Tale sospensione potrà verificarsi anche qualora insorgano contestazioni di natura amministrativa.

Tracciabilità dei Flussi finanziari

L'Aggiudicatario assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della legge 13 agosto 2010 n. 136 e successive modificazioni ed integrazioni.

Il mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti di incasso o pagamento idonei a consentire la piena tracciabilità delle operazioni costituisce causa di risoluzione del contratto ai sensi dell'art. 3, comma 9-bis, della legge 13 agosto 2010 n.136.

L'Aggiudicatario si impegna a dare immediata comunicazione alla Stazione Appaltante e alla prefettura-ufficio territoriale del Governo della provincia di Roma della notizia dell'inadempimento della propria controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.

Risoluzione e Recesso

Ai sensi e per gli effetti dell'art. 108 del d.lgs. 50/2016, la stazione appaltante, fatto salvo quanto previsto ai commi 1, 2 e 4, dell'articolo 107 del d.lgs. 50/2016, può risolvere il contratto durante il periodo di sua efficacia, se una o più delle seguenti condizioni sono soddisfatte:

- a) l'aggiudicatario si è trovato, al momento dell'aggiudicazione dell'appalto in una delle situazioni di cui all'articolo 80, comma 1, per quanto riguarda i settori ordinari ovvero di cui all'articolo 170, comma 3, per quanto riguarda le concessioni e avrebbe dovuto pertanto essere escluso dalla procedura di appalto o di aggiudicazione della concessione, ovvero ancora per quanto riguarda i settori speciali avrebbe dovuto essere escluso a norma dell'articolo 136, comma 1, secondo e terzo periodo;

- b) l'appalto non avrebbe dovuto essere aggiudicato in considerazione di una grave violazione degli obblighi derivanti dai trattati, come riconosciuto dalla Corte di giustizia dell'Unione europea in un procedimento ai sensi dell'articolo 258 TFUE, o di una sentenza passata in giudicato per violazione del presente codice.
- c) rifiuto ingiustificato per almeno 3 (tre) volte anche non consecutive, delle richieste della Stazione Appaltante; si evidenzia che, a titolo esemplificativo, può ritenersi "giustificato" quel rifiuto derivante da obiettive e ragionevoli difficoltà tecniche nell'eseguire la prestazione richiesta.

In caso di risoluzione del contratto sarà facoltà del CNR di procedere allo scorrimento automatico della graduatoria approvata con determinazione di aggiudicazione definitiva, oppure di indire una nuova procedura di gara.

Ai sensi dell'articolo 1455 Codice Civile, il CNR si riserva la facoltà di risolvere unilateralmente il presente contratto nei seguenti casi di gravi inadempimenti:

- a) per sopravvenuti motivi di pubblico interesse;
- b) in caso di frode, di grave negligenza, di contravvenzione nell'esecuzione degli obblighi e condizioni contrattuali;
- c) in caso di cessione dell'attività, oppure nel caso di concordato preventivo, di fallimento, di stato di moratoria e di conseguenti atti di sequestro o di pignoramento a carico dell'Aggiudicatario;
- d) per violazione degli obblighi di riservatezza;
- e) nel caso in cui la prestazione non sia stata eseguita nei termini prescritti, ovvero in caso di esito negativo dei controlli delle verifiche in corso di esecuzione, dai quali emerga un grave e reiterato inadempimento;
- f) qualora la Società perda i requisiti di carattere generale richiesti per l'affidamento del servizio previsti dall'articolo 80 del D. Lgs. n. 50 del 2016;
- g) per mancata osservanza delle disposizioni di cui alla Legge 13/08/2010, n. 136.

Ove il CNR ravvisi la sussistenza di una delle cause sopra descritte, provvederà a contestarle per iscritto all'impresa, tramite PEC fissando un termine non inferiore a 10 (dieci) giorni per le eventuali controdeduzioni. Decorso tale termine l'Amministrazione adotterà le determinazioni ritenute più opportune, dandone notizia motivata alla Società. La risoluzione del contratto viene disposta con atto del Direttore della Stazione Appaltante.

Con la risoluzione del contratto sorge il diritto della Stazione appaltante di affidare a terzi la fornitura o la parte rimanente di questa, in danno della Società inadempiente. Allo stesso, pertanto, saranno addebitate le spese sostenute in più dal CNR rispetto a quelle previste dal contratto risolto. La risoluzione del contratto non esime la Società dalla responsabilità civile e penale in cui la stessa può incorrere per i fatti che hanno motivato la risoluzione.