



**UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA**

Servizi System Management per
Università degli Studi dell'Insubria, per il
periodo dal 1° luglio 2022 al 30 giugno
2026, con opzione di rinnovo per
ulteriori due anni. CIG 9034264E7C –
Capitolato Speciale d'Appalto

CAPITOLATO SPECIALE D'APPALTO - CSA

**PROCEDURA APERTA PER L'AFFIDAMENTO DEI SERVIZI DI SYSTEM
MANAGEMENT PER L'UNIVERSITÀ DEGLI STUDI DELL'INSUBRIA PER IL PERIODO
1° LUGLIO 2022 – 30 GIUGNO 2026 CON OPZIONE DI RINNOVO PER ULTERIORI DUE
ANNI.**

CIG 9034264E7C



SOMMARIO

I - DISPOSIZIONI GENERALI E DEFINIZIONI	6
I.1. Definizioni.....	6
I.2. Disposizioni generali.....	8
II - DISPOSIZIONI GIURIDICO AMMINISTRATIVE	10
II.1. Oggetto dell'Appalto.....	10
II.2. Documenti del contratto	12
II.3. Durata, opzioni e importo del contratto	12
II.3.1. Opzione di rinnovo.....	14
II.3.2. Proroga tecnica	14
II.3.3. Estensione del quinto	14
II.3.4. Revisione dei prezzi	15
II.3.5. Valore complessivo stimato dell'appalto.....	15
II.4. Fatturazione e pagamenti	16
II.5. Penali	17
II.6. Forza maggiore	18
II.7. Personale addetto.....	18
II.7.1. Clausola sociale.....	19
II.7.2. Clausola di gradimento del personale.....	20
II.8. Sicurezza	20
II.9. Subappalto	21
II.10. Divieto di cessione del contratto.....	21
II.11. Risoluzione del contratto.....	21
II.12. Recesso.....	22
II.13. Fallimento dell'OEA.....	22
II.14. Obblighi a carico dell'OEA.....	23
II.15. Responsabilità e coperture assicurative	23
II.16. Garanzie definitive	24
II.17. Tutela della privacy e trattamento dei dati.....	25



II.18. Controversie e foro competente	27
II.19. Oneri e spese contrattuali.....	28
III - GOVERNO DELLA FORNITURA	29
III.1. Condizioni minime di esecuzione delle Prestazioni.....	29
III.2. Pianificazione.....	29
III.3. Fase di Avvio del contratto	29
III.4. Conduzione del contratto	30
III.5. Fase di Conclusione del Contratto	31
III.6. Modifiche delle Prestazioni e variazioni	31
III.7. Assicurazione Qualità.....	32
III.7.1. Indicatori Servizi in ambito ICT.....	32
III.8. Esecuzione e valutazione delle Prestazioni	32
III.9. Uso delle macchine, attrezzature, materiali di consumo, locali, energia, linee telefoniche e di trasmissione dati.....	33
III.10. Strumenti Informatici messi a disposizione dall'Università a supporto dell'erogazione dei servizi 33	
IV - CONTESTO ORGANIZZATIVO DEL COMMITTENTE.....	40
V - CONTESTO TECNOLOGICO DEL COMMITTENTE.....	43
V.1. Data Center e servizi in cloud.....	43
V.1.1. Data Center “Colonia”	43
V.1.2. Data Center “Valleggio”	44
V.1.3. Cloud “Azure” Microsoft.....	45
V.2. Infrastrutture e servizi di Networking, Network Security e Network Management.....	47
V.2.1. La Rete Dati di Ateneo	47
V.2.2. Rete Dati di Ateneo – servizi di connettività wired.....	53
V.2.3. Rete Dati di Ateneo – servizi di connettività wireless.....	59
V.2.4. Rete Dati di Ateneo – servizi di network security	62
V.2.5. Rete Dati di Ateneo – servizi di accesso da remoto/VPN	63
V.2.6. Rete Dati di Ateneo – servizi di connettività cloud.....	63
V.2.7. Rete Dati di Ateneo – Servizi back end Network Authentication.....	63
V.2.8. Rete Dati di Ateneo – Servizi di network core, DNS, DHCP, NTP.....	64



V.3. Sistema Telefonico di Ateneo	64
V.4. Servizi Sistemi Informativi	66
V.5. Infrastrutture e servizi Data Base	67
V.5.1. DBMS ORACLE	67
V.5.2. DBMS Microsoft SQL Server	67
V.6. Servizi a supporto della Comunicazione Avanzata.....	68
V.6.1. Servizi multimediali sincroni basati su H.323.....	68
V.6.2. Servizi multimediali asincroni o live non interattivi basati su H.323 e Azure Media Services.....	68
V.6.3. Servizi collaborativi e multimediali sincroni e asincroni basati su MS Teams e Stream	69
V.7. Servizi di supporto EndPoint ed Helpdesk	69
V.7.1. Helpdesk	69
V.7.2. Laboratori informatizzati ed Endpoint	70
VI - SERVIZI OBBLIGATORI DELLA FORNITURA	73
VI.1.1. Servizio Supporto specialistico Sistemista Senior della Rete Dati di Ateneo - SSRD	73
VI.1.2. Servizio Supporto Specialistico Specialista – Cyber Security – SSCS.....	75
VI.1.3. Servizio Supporto Specialistico Specialista Business Analyst -SSBA	76
VI.1.4. Servizio Supporto Specialistico Sistemista Specialista – Data Center on prem e cloud – SSDC	78
VI.1.5. Servizio Supporto Specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – SSVCDL.....	79
VI.1.6. Servizio Supporto Specialistico Sistemista – Laboratori informatici ed Endpoint- SSEP....	82
VI.1.7. Servizio Conduzione Operativa da remoto per Istanze DBMS – CODB	85
VII - SERVIZI OPZIONALI DELLA FORNITURA.....	90
VII.1. Opzione 1 - Servizio Supporto specialistico Sistemista Senior della Rete Dati di Ateneo – estensione ambienti Linux.....	90
VII.2. Opzione 2 - Servizio Supporto specialistico Sistemista Senior Rete Dati di Ateneo – copertura estesa da remoto.....	91
VII.3. Opzione 3 - Servizio Supporto specialistico Specialista Data Center on prem e cloud – formazione specialistica.....	91
VII.4. Opzione 4 - Servizio Supporto specialistico Specialista Cyber Security – Servizi PEN Test e Vulnerability Assesment.....	92



VII.5. Opzione 5 - Servizio Supporto specialistico Specialista Cyber Security – Servizio supporto on-demand on-site per incidenti informatici.....	93
VII.6. Opzione 6 - Servizio Supporto specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – supporto on demand da remoto eventi fuori orario.....	93
VII.7. Opzione 7 - Servizio Supporto specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – Servizio continuativo feriale.....	94
VII.8. Opzione 8 - Servizio Supporto specialistico Sistemista – Laboratori Informatici ed End Point – Servizio continuativo feriale.....	94
VII.9. Opzione 9 - Servizio Conduzione Operativa da remoto istanze DBMS – security assesment..	95
VII.10. Opzione 10 – Dotazione telefoni mobili aziendali per tutto il personale dell'OEA adibito ai servizi di supporto specialistico.....	95
VIII - INDICATORI DI QUALITA' DELLA FORNITURA.....	96
VIII.1. Indicatori di Qualità Generali.....	97
VIII.1.1. Personale della fornitura inadeguato – IQ01.....	97
VIII.1.2. Turn over del personale – IQ02.....	98
VIII.1.3. Inadeguatezza del personale proposto – IQ03.....	99
VIII.1.4. Inserimento/sostituzione del personale – IQ04.....	100
VIII.1.5. Attivazione degli Interventi – IQ05.....	101
VIII.1.6. Rilievi sulla Fornitura – IQ06.....	102
VIII.2. Indicatori di Qualità Operativi.....	103
VIII.2.1. Tempestività di risoluzione degli Incident – IQ07.....	103
VIII.2.2. Tempestività di esecuzione dei change standard/predefiniti – IQ08.....	106
VIII.2.3. Tempestività di esecuzione dei change non standard – IQ09.....	109
IX - DESCRIZIONE DEI PROFILI PROFESSIONALI.....	111
IX.1.1. Profilo professionale Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo.....	112
IX.1.2. Profilo professionale Specialista – Cyber Security.....	115
IX.1.3. Profilo professionale – Specialista Business Analyst.....	119
IX.1.4. Profilo professionale Specialista per il contesto Data center on prem e cloud.....	121
IX.1.5. Profilo professionale Sistemista Sistemi di Videoconferenza e Digital Learning.....	124
IX.1.6. Profilo professionale Sistemista laboratori informatici e gestione Endpoint.....	125
Sistemista laboratori informatici e gestione Endpoint.....	125



I - DISPOSIZIONI GENERALI E DEFINIZIONI

I.1. Definizioni

Si riportano di seguito le definizioni dei termini e l'estensione degli acronimi impiegati nei Documenti di Gara.

Nell'ambito del presente capitolato speciale e in tutti gli atti di gara si intende per:

“Appalto”: Contratto con il quale una parte assume, con organizzazione dei mezzi necessari e con gestione a proprio rischio, il compimento di un'opera o di un servizio verso un corrispettivo in danaro (art. 1655 C.C.);

“Apparato passivo”: qualsiasi oggetto che per espletare la sua funzione, dopo la fase di configurazione non necessita di alcuna forma di energia, non abbia componenti in movimento.

“Apparato attivo”: qualsiasi oggetto che non ricade nella definizione di apparato passivo.

“C.C.”: Codice Civile;

“Codice dei Contratti”: il D.Lgs. 50/2016;

“Contratto”: ai sensi dell'Art. 1321 C.C., il contratto è l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale;

“Controllore”: Il Titolare: è una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che, da solo o congiuntamente con altri, determina le finalità e i mezzi di trattamento dei dati personali;

“CSA”: Capitolato speciale d'Appalto e s.m.i.

“Custodia”: attività di controllo di un bene finalizzata a prevenire sia alterazioni naturali della cosa, sia danneggiamenti o sottrazione da parte di terzi, sia ancora violazioni dello stato giuridico del bene secondo le disposizioni del Codice Civile;

“CWDM”: “Coarse Wavelength Division Multiplexing”, tecnologia di trasporto di lunghezze ottiche multiple tramite moltiplicazione di lunghezza d'onda, sulla medesima fibra ottica.

“DWDM”: “Dense Wavelength Division Multiplexing”, tecnologia di trasporto di lunghezze ottiche multiple tramite moltiplicazione di lunghezza dense, sulla medesima fibra ottica.

“DNS”: servizio di risoluzione diretta ed inversa dei nomi a dominio.

“DHCP”: servizio di assegnazione dinamica degli indirizzi IP agli host.

“DBMS”: Sistema di gestione di basi di dati

“DURC”: documento di regolarità contributiva.

“Fibra ottiche spenta”: connessione fisica in fibra ottica in cui sono stati predisposti i cavi e i necessari componenti passivi ma non le apparecchiature di trasmissione che li dovrebbero utilizzare per trasmettere il segnale ottico



“IDS”: Intrusion Detection System, sistema di sicurezza di rete volto ad identificare potenziali minacce di intrusione

“IP”: indirizzo IP, etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete

“IaaS”: Infrastructure as a service, soluzione di cloud computing in cui un vendor fornisce agli utenti l'accesso alle risorse di calcolo

“Legge/i”: tutte le leggi, regolamenti, disposizioni, circolari, norme tecniche, usi e consuetudini, vigenti con particolare riferimento a quelle in materia di lavori pubblici, forniture e servizi pubblici, progettazione, costruzione, strutture, impianti, sicurezza ambiente, igiene, tutela della privacy, tutela ai lavoratori, applicabili al Contratto di Appalto;

“NAT”: network address translation

“NTP”: Network Time Protocol, protocollo per sincronizzare gli orologi dei computer all'interno di una rete a commutazione

“OEA”: operatore economico aggiudicatario dell'appalto di che trattasi;

“PaaS”: Platform as a service, consiste nel servizio di messa a disposizione di piattaforme di elaborazione (Computing platform)

“Prestazioni”: tutti i servizi oggetto di Appalto;

“Processore”: il Responsabile Esterno del Trattamento: E' una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che elabora dati personali per conto del controllore;

“Radius”: servizio di autenticazione

“Referenti di servizio”: Responsabili dell'Università, collaborano con il DEC, hanno il compito di verificare la corretta esecuzione del contratto;

“Referente dell'OEA”: soggetto designato a rappresentare l'OEA per tutte le esigenze connesse con l'esecuzione del presente appalto;

“Università”: Università degli Studi dell'Insubria, ovvero Amministrazione appaltante;

“SPC”: Sistema Pubblico di Connettività

“SSID”: chiave alfanumerica di 32 caratteri che identifica in modo univoco una rete LAN wireless

“SaaS”: Software as a service, modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera (direttamente o tramite terze parti) e gestisce un'applicazione web che mette a disposizione dei propri clienti via Internet

“Tratta in fibra ottica”: connessione tra due sedi realizzata totalmente in fibra ottica spenta, attestata alle estremità su casseti ottici e composta di una coppia di fibre che seguono lo stesso percorso fisico.



“**UTM**”: sistema di sicurezza di rete che integra le funzionalità di Firewall, URL filtering, IPS, VPN gateway, etc

“**URL**”: Uniform Resource Locator, sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer

“**VPN**”: Virtual Private Network, sistema di estensione della rete locale attraverso sistemi di tunneling cifrato.

“**VLAN**”: Virtual Local Area Network, insieme di tecnologie che permettono di segmentare il dominio di broadcast che si crea in una rete locale

I.2. Disposizioni generali

Il presente CSA regola il rapporto tra l'Università, e l'OEA.

La sottoscrizione del Contratto equivale a dichiarazione di perfetta conoscenza, piena e incondizionata accettazione, integrale ed assoluta applicazione, da parte dell'OEA:

- del livello prestazionale richiesto con il presente CSA;
- di tutte le Leggi;
- del contesto tecnologico all'interno del quale debbono essere eseguite le prestazioni oggetto del contratto, nonché dei rispettivi e relativi vincoli e sottoservizi presenti;
- della necessità che le Prestazioni, dovranno essere eseguite durante il normale svolgimento delle attività istituzionali didattiche e di ricerca dell'Università, che proseguiranno senza interruzione alcuna;
- della consistenza delle Prestazioni ricomprese nel Contratto;
- di aver attentamente vagliate tutte le circostanze generali e particolari, di tempo e di luogo, nonché di tutte le altre circostanze generali e particolari che possono influire sulla determinazione dei prezzi e delle condizioni contrattuali e sulla esecuzione delle prestazioni.

La sottoscrizione del Contratto equivale altresì a dichiarazione di perfetta conoscenza e piena e incondizionata accettazione di tutti i documenti di gara, nessuno escluso, ai fini della esecuzione/prestazione “a perfetta Regola dell'Arte” delle Prestazioni.

Le disposizioni e prescrizioni e gli ordini impartiti dall'Università, dovranno essere eseguiti dall'OEA con la massima cura e prontezza, nel rispetto delle Leggi. L'OEA, non potrà mai rifiutarsi di dare immediata esecuzione alle disposizioni e prescrizioni dell'Università, sotto pena della esecuzione di ufficio, con addebito della maggior spesa che l'Università avesse a sostenere rispetto alle condizioni del Contratto e con le penalità previste dal presente CSA.

Fatto salvo per l'OEA, il diritto di avanzare per iscritto le osservazioni che ritenesse opportune in merito alle disposizioni/ordini impartiti.

L'Università declina ogni responsabilità per sottrazioni o danni che possano essere apportati da terzi ai materiali e ai beni di proprietà dell'OEA.



Deve essere garantita la qualità delle Prestazioni nei singoli processi di lavorazione, relativamente a ciascuna delle attività costituenti la gestione dei servizi, nel rispetto dei tempi, delle procedure gestionali richieste e/o proposte, delle garanzie igienico-sanitarie di sicurezza, prevenzione e protezione, nonché della continuità del servizio.

Spetta all'OEA la direzione e l'organizzazione gestionale delle Prestazioni per l'intero periodo contrattuale, in modo da non dare adito alla benché minima lamentela da parte della Università e degli utenti.

Tutte le Prestazioni oggetto del presente CSA devono essere espletate dall'OEA a proprio rischio e con propria autonoma organizzazione, secondo quanto definito dal presente Capitolato e in attuazione delle soluzioni migliorative proposte dall'OEA in sede di offerta, nel caso in cui queste siano state accolte dalla Università.

Le Prestazioni devono essere svolte in coordinamento e nel rispetto delle attività della Università, garantendo un alto grado di flessibilità a fronte di una Prestazione che deve mirare, per quanto possibile, ad una elevata qualità dei servizi richiesti.

L'OEA nell'esercizio della propria attività non dovrà arrecare alcun pregiudizio alle opere ed ai diritti ed ai Beni dell'Università ed al corretto svolgimento delle rispettive attività didattiche, di ricerca e amministrative.

L'Università, intende avvalersi della capacità organizzativa e gestionale dell'OEA, lasciando alla sua esperienza e professionalità il compito di utilizzare la tecnica più idonea.

All'OEA è quindi consentita la possibilità di effettuare le Prestazioni nel modo più opportuno per darle perfettamente compiute nei termini contrattuali, fatti salvi i criteri, i termini, i livelli e qualità prestazionali minimali, nonché la durata richiamati nei successivi articoli del Capitolato Speciale.

L'OEA, pertanto, assume anche l'impegno di assistere attivamente l'Università per consentire a quest'ultima di raggiungere l'obiettivo dell'ottimale gestione delle Prestazioni, mettendo a disposizione la propria professionalità ed operando in modo da assicurare il crescente miglioramento dell'organizzazione e dell'erogazione delle Prestazioni, privilegiando altresì la prevenzione dei danni e la programmazione degli interventi.



II - DISPOSIZIONI GIURIDICO AMMINISTRATIVE

II.1. Oggetto dell'Appalto

Il presente appalto ha per oggetto l'affidamento in un unico lotto dei Servizi di System Management in ambiente Information Technology - IT, suddivisi fra Servizi di Supporto Specialistico IT da esercitarsi presso i Luoghi dell'Università (CPV 72220000-3 Servizi di consulenza in sistemi informatici ed assistenza tecnica) e servizi di Conduzione Operativa IT (CPV 72510000-3 Servizi di gestione connessi all'informatica) da esercitarsi da remoto.

Le Prestazioni sono descritte nel prospetto che segue e più analiticamente dettagliate nel prosieguo del presente CSA, unitamente a tutta la documentazione di gara, che ne costituisce parte integrante.

Per l'effettuazione delle Prestazioni, oggetto del presente Appalto, è stimato il seguente fabbisogno massimo e non garantito, per il periodo presunto dal 1° luglio 2022 al 30 giugno 2026:

		Anno 2022 (6 mesi)	Anno 2023	Anno 2024	Anno 2025	Anno 2026 (6 mesi)	TOTALE
Servizio	Unità di Misura						
Supporto Specialistico - Sistemista Senior Rete Dati di Ateneo	Giorni/Uomo	220	440	440	440	220	1760
Supporto Specialistico - Specialista Cyber Security	Giorni/Uomo	110	220	220	220	110	880
Supporto Specialistico - Specialista Business Analyst	Giorni/Uomo	220	440	440	440	220	1760
Supporto Specialistico - Specialista Data Center	Giorni/Uomo	10	20	20	20	10	80
Supporto Specialistico - Sistemista Videoconferenza e Digital Learning	Giorni/Uomo	110	220	220	220	110	880
Supporto Specialistico - Sistemista Laboratori informatici e gestione End Point	Giorni/Uomo	110	220	220	220	110	880



Conduzione Operativa da remoto DBMS	Numero DBMS/mese	12	24	24	24	12	96
--	------------------	----	----	----	----	----	-----------

per il periodo dell'Opzione di Rinnovo di cui al successivo Articolo II.3.1:

Servizio	Unità di Misura	Rinnovo ulteriori 2 Anni			TOTALE rinnovo
		Anno 2026 (6 mesi)	Anno 2027	Anno 2028 (6 mesi)	
Supporto Specialistico - Sistemista Senior Rete Dati di Ateneo	Giorni/Uomo	220	440	220	880
Supporto Specialistico - Specialista Cyber Security	Giorni/Uomo	110	220	110	440
Supporto Specialistico - Specialista Business Analyst	Giorni/Uomo	220	440	220	880
Supporto Specialistico - Specialista Data Center	Giorni/Uomo	10	20	10	40
Supporto Specialistico - Sistemista Videoconferenza e Digital Learning	Giorni/Uomo	110	220	110	440
Supporto Specialistico - Sistemista Laboratori informatici e gestione End Point	Giorni/Uomo	110	220	110	440
Conduzione Operativa da remoto DBMS	Numero DBMS/mese	12	24	12	48



e per l'eventuale Opzione di Proroga di cui all'Articolo II.3.2:

Servizio	Unità di Misura	Opzione Proroga (Anno 2028 – 6 mesi)
Supporto Specialistico - Sistemista Senior Rete Dati di Ateneo	Giorni/Uomo	220
Supporto Specialistico - Specialista Cyber Security	Giorni/Uomo	110
Supporto Specialistico - Specialista Business Analyst	Giorni/Uomo	220
Supporto Specialistico - Specialista Data Center	Giorni/Uomo	10
Supporto Specialistico - Sistemista Videoconferenza e Digital Learning	Giorni/Uomo	110
Supporto Specialistico - Sistemista Laboratori informatici e gestione End Point	Giorni/Uomo	110
Conduzione Operativa da remoto DBMS	Numero DBMS/mese	12

II.2. Documenti del contratto

Formano parte integrante del contratto d'appalto ancorché non materialmente allegati allo stesso:

- il presente CSA;
- l'offerta tecnica ed economica;

Per quanto non espressamente previsto dal presente CSA si rinvia al D. Lgs. 50/2016 e s.m.i. "Codice dei Contratti".

II.3. Durata, opzioni e importo del contratto

Il Contratto oggetto della presente procedura avrà la durata massima di quattro anni (48 mesi). Indicativamente il periodo presunto è dal 1° luglio 2022 e fino al 30 giugno 2026.



L'importo complessivo presunto dell'appalto posto a base di gara per il periodo di quattro anni è pari a € 1.873.715,20 oltre IVA (22% ove dovuta), e non sono presenti oneri per la sicurezza non soggetti a ribasso.

n.	Descrizione servizi	CPV	P (<i>principale</i>) S (<i>secondaria</i>)	Importo (4 anni)
1	Servizi di supporto specialistico	72220000-3	P	1.720.115,20 €
2	Servizi di conduzione operativa	72510000-3	S	153.600,00 €
B) Oneri per la sicurezza da interferenze non soggetti a ribasso				0,00 €
Importo totale a base d'Asta				1.873.715,20 €

L'importo a base d'Asta è calcolato in base alle quantità dei singoli servizi indicate nell'Articoli I.1 ed applicando i seguenti costi unitari a base d'Asta:

Servizio	Unità di Misura	Importo Unitario a base d'Asta
Supporto Specialistico - Sistemista Senior Rete Dati di Ateneo	Giorno/Uomo	281,04 €
Supporto Specialistico - Specialista Cyber Security	Giorno/Uomo	287,28 €
Supporto Specialistico - Specialista Business Analyst	Giorno/Uomo	287,28 €
Supporto Specialistico - Specialista Data Center	Giorno/Uomo	287,28 €
Supporto Specialistico - Sistemista Videoconferenza e Digital Learning	Giorno/Uomo	252,32 €
Supporto Specialistico - Sistemista Laboratori informatici e gestione End Point	Giorno/Uomo	252,32 €



Servizio	Unità di Misura	Importo Unitario a base d'Asta
Conduzione Operativa da remoto DBMS	DBMS/mese	1.600,00 €

L'importo contrattuale, corrispondente all'importo delle Prestazioni, è quello risultante dall'offerta presentata dall'OEA in sede di gara, aumentato dell'importo relativo agli oneri per la sicurezza.

L'importo complessivo offerto dall'OEA in sede di gara ha valore ai soli fini dell'assegnazione del punteggio relativo all'“Offerta Economica” e, pur essendo parametrato sulle giornate/ numero DBMS stimate di appalto, sarà corrisposto sulla base delle giornate effettivamente prestate e ai DBMS effettivamente gestiti.

L'importo contrattuale si intende comprensivo di tutte le prestazioni, spese accessorie, oneri, indennità, assicurazioni di ogni specie, manodopera, mezzi d'opera, trasporto, e quanto occorre per offrire il servizio compiuto a perfetta regola d'arte, secondo le disposizioni del presente CSA.

L'appalto non comporta rischi interferenziali ai sensi dell'articolo 26, comma 5, del D. Lgs. 81/2008 e s.m.i; conseguentemente sono valutati pari a zero gli oneri di sicurezza dovuti a rischi da interferenza.

È ammesso l'avvio dell'esecuzione del contratto in via d'urgenza come previsto dell'art 32 D. Lgs.50/2016, ai sensi dell'art 8 comma 1 lett. a) della legge 120/2020.

II.3.1. Opzione di rinnovo

Al termine del quarto anno, la Stazione Appaltante si riserva la facoltà di esercitare l'opzione di rinnovo ex art. 35, comma 4 del D. Lgs. 50/2016 e s.m.i. per ulteriori due anni alle medesime condizioni contrattuali.

Qualora l'Università voglia avvalersi dell'opzione di cui sopra è tenuta a darne comunicazione per iscritto all'Affidatario, almeno sei mesi prima della scadenza del contratto, mediante PEC o mediante altra forma idonea a garantire data certa.

II.3.2. Proroga tecnica

L'Università, alla scadenza del contratto, si riserva la facoltà di disporre la proroga agli stessi prezzi o condizioni più favorevoli per l'Università, per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione di un nuovo contraente, secondo le modalità di cui all'art. 106, comma 11 del D. Lgs. 50/2016 e s.m.i. In tale caso verrà data comunicazione per iscritto all'OEA prima della scadenza naturale del contratto, mediante PEC o mediante altra forma idonea a garantire data certa.

II.3.3. Estensione del quinto

In corso di esecuzione del Contratto l'Università potrà richiedere, in relazione a sopravvenute necessità, l'incremento o la diminuzione di ogni singolo servizio in cui sono articolate le Prestazioni oggetto d'Appalto nel limite del 20% di quanto già affidato, agli stessi patti, prezzi e condizioni senza eccezioni. L'importo in aggiunta o in diminuzione, a seguito di variazione del Contratto, verrà determinato moltiplicando il prezzo unitario, offerto dall'OEA in sede di gara, per le quantità oggetto di variazione. Le modifiche sopraggiunte nonché il relativo importo in aggiunta/diminuzione saranno comunicate per iscritto dall'Università all'OEA, il quale dovrà sottoscrivere per accettazione il documento che, una volta firmato, formerà parte integrante e sostanziale del Contratto.



II.3.4. Revisione dei prezzi

L'importo resterà fisso e invariabile per i primi quattro anni di esecuzione contrattuale. Nel caso di esercizio dell'opzione di rinnovo per i successivi due anni, è ammessa la clausola di revisione dei prezzi ai sensi dell'art. 106 comma 1 lett. a), pertanto, si procederà alla revisione su richiesta dell'OEA sulla base delle variazioni degli indici ISTAT dei prezzi al consumo per le famiglie di operai e impiegati (Italia - Indice generale). La variazione sarà determinata prendendo come riferimento l'ultimo indice disponibile alla data di ricezione della richiesta di revisione e l'indice del mese dell'anno di effettivo inizio delle prestazioni contrattuali (o dell'eventuale ultima revisione applicata).

Il nuovo prezzo così determinato sarà applicato alle prestazioni svolte successivamente all'accoglimento della revisione, non sono ammesse revisioni con effetto retroattivo.

II.3.5. Valore complessivo stimato dell'appalto

La base d'asta è stata stimata in complessivi € 1.873.715,20 oltre IVA (22% ove dovuta), per le prestazioni per la durata di 4 anni, ed € 0,00 per oneri per la sicurezza derivanti da interferenze non soggetti a ribasso di cui all'art. 26, comma 3 del D. Lgs. 81/2008.

Ai sensi dell'art. 35, comma 4 del D.Lgs. 50/2016 il valore stimato dell'appalto, comprensivo delle opzioni¹ di rinnovo e proroga tecnica, è pari ad € 3.044.787,20 oltre IVA 22%, come da prospetto sotto riportato:

Base Asta	Importi
Importo per l'esecuzione del servizio (appalto 4 anni)	1.873.715,20 €
Oneri per la sicurezza (appalto 4 anni)	- €
Base Asta servizio appalto 4 anni (IVA esclusa)	1.873.715,20 €
Opzioni	
Importo esecuzione dei servizi Opzione rinnovo 2 anni	936.857,60 €
Oneri per la sicurezza periodo di rinnovo	- €
Importo Totale Opzione di Rinnovo (IVA esclusa)	936.857,60 €
Proroga	
Importo per esecuzione dei servizi Opzione Proroga 6 mesi	234.214,40 €
Oneri per la sicurezza periodo di proroga	- €
Importo totale opzione proroga (IVA esclusa)	234.214,40 €
Valore complessivo dell'Appalto (oltre IVA 22%)	3.044.787,20 €

¹ Il quinto d'obbligo non assume rilevanza ai fini della determinazione del valore dell'appalto in oggetto in quanto rientra tra le modifiche contrattuali oggetto di variante (TAR Milano 10/2/2020, n. 284 e Parere MIT 18/22/2019).



II.4. Fatturazione e pagamenti

La fatturazione avrà cadenza mensile posticipata, calcolata sulla base dei servizi effettivamente erogati. Nelle fatture dovrà essere indicato l'importo complessivo derivante dalla somma degli importi di ciascuno dei seguenti servizi così determinati:

Servizio	Elemento misurato	Modalità di definizione dell'importo
Supporto Specialistico - Sistemista Senior Rete Dati di Ateneo	Giorni/Uomo	Costo giornata offerto dall'OEA (come indicato in offerta economica) moltiplicato per l'effettivo numero di giornate prestate nel corso del mese fatturato.
Supporto Specialistico - Specialista Cyber Security	Giorni/Uomo	
Supporto Specialistico - Specialista Business Analyst	Giorni/Uomo	
Supporto Specialistico - Specialista Data Center	Giorni/Uomo	
Supporto Specialistico - Sistemista Videoconferenza e Digital Learning	Giorni/Uomo	
Supporto Specialistico - Sistemista Laboratori informatici e gestione End Point	Giorni/Uomo	
Conduzione Operativa da remoto DBMS	DBMS/mese	Costo mensile di gestione di un DBMS (come indicato in offerta economica) moltiplicato per l'effettivo numero di DBMS gestiti nel corso del mese fatturato.

Dagli importi comunque dovuti, saranno detratte tutte le somme dovute all'OEA per penalità, multe o ripristini di danni arrecati e precedentemente notificati.

La liquidazione del corrispettivo sarà effettuata, salvi gli eventuali atti di autotutela dell'Università, entro 30 giorni dalla ricezione della fattura, previa verifica di avvenuta regolare esecuzione delle prestazioni da parte del DEC e previa verifica di regolarità contributiva mediante acquisizione da parte dell'Università del DURC in corso di validità, ai sensi di quanto previsto dal D.M. 24 ottobre 2007.

L'Università accetta esclusivamente fatture trasmesse in forma elettronica secondo il formato di cui all'allegato A "Formato della fattura elettronica" del D. M. 3 aprile 2013, n. 55.

Le fatture dovranno essere intestate esclusivamente all'Amministrazione Contraente "Università degli Studi dell'Insubria – Area Sistemi Informativi – ASI", dovranno fare riferimento al Codice unico ufficio 1000AR così come censito su www.indicepa.it

Le fatture elettroniche dovranno riportare obbligatoriamente il codice identificativo di gara CIG 9034264E7C, nonché gli eventuali ulteriori dati richiesti dall'Università finalizzati ad agevolare le operazioni di contabilizzazione e pagamento delle fatture nei tempi concordati.

Ai sensi del DM del 23 gennaio 2015 attuativo delle disposizioni in materia di scissione dei pagamenti "Split payment" previste dall'art. 1, comma 629, lettera b) della Legge 190/2014 (Legge di stabilità 2015), l'IVA dovuta sarà trattenuta e versata direttamente dall'Università all'Amministrazione finanziaria. Non saranno pertanto accettate fatture sprovviste della dicitura "Scissione dei pagamenti".



L'OEA assumerà tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della L. 136/2010 e s.m.i. L'OEA sarà tenuto a pagare i propri dipendenti, consulenti, fornitori di beni e servizi rientranti tra le spese generali, nonché gli acquisti di immobilizzazioni tecniche, tramite conto corrente dedicato, indicando il codice CIG della procedura aggiudicata.

Gli estremi del predetto conto corrente dovranno essere comunicati all'Università prima della stipula del Contratto.

L'OEA si impegna, altresì, a comunicare all'Università ogni variazione relativa alle notizie ogniqualvolta si verificano degli eventi modificativi relativi a quanto sopra riportato.

Ai sensi dell'art. 3, comma 8, della L. 136/2010 e s.m.i. l'OEA che ha notizia dell'inadempimento della controparte (subappaltatore/subcontraente) agli obblighi della tracciabilità ne dà immediata comunicazione all'Università ed alla Prefettura - Ufficio Territoriale del Governo della Provincia di Varese.

Ai sensi dell'art. 3, comma 9, della L. 136/2010 e s.m.i. il Contratto di subappalto e i subcontratti stipulati con imprese a qualsiasi titolo interessate alle Prestazioni dovranno riportare, a pena di nullità assoluta, apposita clausola con la quale il contraente e i sub contraenti attestino di ben conoscere ed assumere gli obblighi di tracciabilità finanziaria di cui alla L. 136/2010 e s.m.i.

Ai sensi dell'art. 3, comma 9-bis) della Legge n. 136/2010 e s.m.i. il Contratto sarà risolto di diritto qualora le transazioni, inerenti e derivanti dal Contratto stesso, siano eseguite senza avvalersi dello strumento del bonifico bancario o postale o di altri strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni.

La liquidazione dei corrispettivi avverrà esclusivamente nei confronti dell'OEA salvo il caso in cui ricorrano le condizioni di cui all'art. 105, comma 13, del D. Lgs. 50/2016 e s.m.i.

II.5. Penali

In caso di inadempimento contrattuale, ivi compresi il ritardo nell'esecuzione delle Prestazioni e la difformità delle Prestazioni rispetto alle caratteristiche previste dal CSA, l'Università sarà legittimata ad applicare, a proprio insindacabile giudizio le seguenti penali per ogni inadempimento che comporti un superamento dei singoli valori soglia fissati dai rispettivi indicatori di qualità così come descritto nell'articolo. III.7 e definiti nella Sezione VIII.

Indicatore	Unità misura	Soglia	Inadempienza	Periodo di osservazione	Unità penale	Moltiplicatore penale
IQ01 - Personale della fornitura inadeguato	Risorse inadeguate	1	Non conformità	Trimestre	1% dell'importo annuo contrattuale	Per ogni ulteriore unità di personale non idonea
IQ02 - Turn over del personale	Risorse sostituite	1	Non conformità	Trimestre	0,5% dell'importo annuo contrattuale	Per ogni ulteriore unità di personale sostituita dal fornitore
IQ03 - Inadeguatezza del personale proposto	Curriculum Vitae/attestazioni/diplomi	2	Non conformità	Trimestre	0,3% dell'importo annuo contrattuale	Per ogni ulteriore CV/attestazione/diploma non conforme



IQ04 - Inserimento/sostituzione del personale	Giorno lavorativo	0	Ritardo	Trimestre	0,5 ‰ dell'importo annuo contrattuale	Per ogni giorno lavorativo di ritardo
IQ05 - Attivazione degli interventi	Giorno lavorativo	2	Ritardo	Trimestre	0,3‰ dell'importo annuo contrattuale	Per ogni giorno lavorativo di ritardo
IQ06 – Rilievi sulla Fornitura	Rilievo	3	Non conformità	Trimestre	1‰ dell'importo annuo contrattuale	Per ogni rilievo ulteriore
IQ07 - Tempestività risoluzione degli Incident	Minuti	95%	Non conformità	Mese	0,5‰ dell'importo annuo contrattuale	Per ogni punto percentuale eccedente il valore soglia
IQ08 - Tempestività di esecuzione dei change standard/predefiniti	Percentuale	95%	Non conformità	Mese	0,5‰ dell'importo annuo contrattuale	Per ogni punto percentuale eccedente il valore soglia
IQ09 - Tempestività di esecuzione dei change non standard	Percentuale	95%	Non conformità	Mese	0,5‰ dell'importo annuo contrattuale	Per ogni punto percentuale eccedente il valore soglia

Per l'applicazione delle penali suddette, si procederà, innanzitutto, alla contestazione all'OEA del relativo inadempimento contrattuale da parte del RUP, rivolgendosi alla sede legale o al domicilio eletto dall'OEA. Entro il limite di cinque giorni successivi alla data di detta comunicazione, l'OEA potrà presentare all'Università eventuali osservazioni; decorso il suddetto termine l'Università, nel caso non abbia ricevuto alcuna giustificazione oppure anche nel caso le avesse ricevute e non le ritenesse fondate procederà discrezionalmente all'applicazione delle penali e, in ogni caso, all'adozione di ogni determinazione ritenuta opportuna.

Le penali si applicano mediante ritenuta sul primo pagamento utile al verificarsi della contestazione. Tutte le penali si intendono salvo il maggior danno.

II.6. Forza maggiore

Nel caso di sospensione delle Prestazioni, determinata da causa di forza maggiore, in nessun modo imputabile a responsabilità, diretta o indiretta, dell'OEA, qualora detta sospensione sia comunicata e giustificata tempestivamente per iscritto all'Università, dando prova dell'impossibilità dell'esecuzione delle Prestazioni, non si procederà all'applicazione di penali in capo all'OEA.

In ogni caso l'Università non sarà tenuta a pagare quanto corrisponde al valore della mancata Prestazione.

II.7. Personale addetto

Ogni attività relativa alle Prestazioni oggetto di Contratto deve essere svolta da personale professionalmente



adeguato e qualificato ad operare nel rispetto delle specifiche norme di legge e con mezzi, attrezzature e materiali adeguati e conformi alla Legge.

L'OEA deve osservare le norme derivanti dall'applicazione del Contratto Collettivo Nazionale di Lavoro, nonché dalle vigenti normative in tema di prevenzione degli infortuni sul lavoro, di igiene del lavoro, di assicurazione contro gli infortuni sul lavoro e altre malattie professionali e ogni altra disposizione in vigore o che potrà intervenire in corso di esercizio per la tutela dei lavoratori.

L'OEA si impegna, nei confronti della totalità del personale posto alle sue dipendenze ed impiegato nell'esecuzione delle Prestazioni, oggetto del presente Appalto, a rispettare le disposizioni in tema di condizioni di lavoro. In particolare, nell'organizzazione del servizio l'OEA dovrà garantire il rispetto delle disposizioni di cui al D.lgs. 66/03 "Attuazione delle direttive 93/104/CE e 2000/34/CE concernenti taluni aspetti dell'organizzazione dell'orario di lavoro".

L'OEA si obbliga ad applicare nei confronti dei lavoratori di cui sopra condizioni retributive non inferiori a quelle risultanti dal CCNL di settore in vigore alla data di pubblicazione del bando di gara, così come determinato dal Ministero del Lavoro e delle Politiche sociali. Nel corso dell'esecuzione del contratto l'OEA è tenuto all'adeguamento delle condizioni retributive in base alle nuove determinazioni relative al costo del lavoro del Ministero del Lavoro e delle Politiche sociali.

L'Università è esplicitamente sollevata da ogni obbligo e/o responsabilità nei confronti di tutto il personale adibito dall'OEA all'esecuzione delle attività relative al funzionamento del servizio affidato in gestione.

Tutti i lavoratori suddetti devono essere assicurati presso l'INAIL contro gli infortuni sul lavoro e presso l'INPS per quanto riguarda le malattie e le assicurazioni sociali. L'OEA, entro 15 giorni n.s.c. dall'avvio del servizio e ogni qual volta dovesse provvedere alla sostituzione di personale addetto alle Prestazioni, dovrà aggiornare nei tempi previsti dalla normativa in vigore, la documentazione relativa alle rispettive posizioni.

Tale documento dovrà essere aggiornato e trasmesso per ogni cessazione o nuova assunzione, contestualmente alla presa di servizio.

L'Affidatario dovrà trasmettere all'Università degli Studi dell'Insubria l'elenco nominativo del personale impiegato. Tale documento dovrà essere aggiornato e trasmesso per ogni cessazione o nuova assunzione, contestualmente alla presa di servizio.

La sorveglianza sanitaria di tutto il personale impiegato è a carico dell'OEA.

In caso di inottemperanza agli obblighi sopra precisati, accertata dall'Università o a essa segnalata dall'Ispettorato del Lavoro, l'Università medesima potrà procedere alla risoluzione del Contratto.

Qualora venissero riscontrate o venissero denunciate, da parte dell'Ispettorato del Lavoro, violazioni alle disposizioni sopra elencate, l'Università si riserva il diritto insindacabile di sospendere l'emissione dei mandati di pagamento sino a quando l'Ispettorato del Lavoro non abbia accertato che ai lavoratori sia stato corrisposto il dovuto ovvero che la vertenza sia stata risolta.

II.7.1. Clausola sociale

L'OEA si obbliga ad attuare, nei confronti dei lavoratori dipendenti occupati nelle Prestazioni oggetto dell'Appalto - ovvero dei prestatori ad essi equiparati e, se cooperative, nei rapporti con i soci - condizioni normative e retributive non inferiori a quelle risultanti dalle norme di settore, dai contratti collettivi e dagli accordi integrativi territoriali di categoria, applicabili alla data dell'offerta, alla categoria e nella località in cui si svolgono i servizi, nonché le condizioni risultanti da successive modifiche e integrazioni delle stesse norme, contratti e accordi. Tali obblighi vincolano l'OEA anche nel caso che non sia aderente alle



associazioni stipulanti o receda da esse e indipendentemente dalla struttura e dimensione dell'Appaltatore stesso e da ogni altra qualificazione giuridica, economica o sindacale. L'OEA si obbliga, altresì, a continuare ad applicare dette condizioni normative e retributive anche dopo la loro scadenza e fino alla stipulazione del contratto successivo.

Il CCNL applicato e il livello di trattamento economico del personale dovranno essere coerenti con l'oggetto dell'Appalto. L'Università si riserva la facoltà di eseguire verifiche sulla regolarità dei rapporti di lavoro, anche agli effetti contributivi e assicurativi. L'OEA si impegna a esibire la documentazione contabile e amministrativa necessaria per l'esecuzione dei controlli.

Al fine di promuovere la stabilità occupazionale, nel rispetto dei principi dell'Unione Europea, ferma restando la dovuta armonizzazione con la propria organizzazione aziendale, compatibilmente con le prestazioni richieste dal presente CSA e secondo la propria autonomia organizzativa, l'OEA s'impegna ad assorbire prioritariamente nel proprio organico il personale già operante alle dipendenze dell'OEA uscente, come previsto dall'articolo 50 del D. Lgs 50/2016 e s.m.i., garantendo l'applicazione dei CCNL di settore, di cui all'art. 51 del d.lgs. 15 giugno 2015, n. 81.

A tal fine, è riportato nel progetto l'elenco del personale attualmente impiegato, con indicazione di: CCNL di inquadramento, qualifica, livello di anzianità e monte ore.

Il CCNL di inquadramento del personale oggetto della presente clausola sociale, applicabile in ragione della sua pertinenza rispetto all'oggetto prevalente dell'affidamento, è il Contratto per le lavoratrici e i lavoratori delle cooperative del settore socio-sanitario-assistenziale-educativo che prevede la clausola sociale (art. 37). È fatta salva l'applicazione ove più favorevole, dell'eventuale clausola sociale prevista dal Contratto collettivo nazionale prescelto dall'OEA.

L'OEA allega alla documentazione amministrativa un progetto di assorbimento atto ad illustrare le concrete modalità di applicazione della presente clausola sociale con particolare riguardo al numero dei lavoratori che beneficeranno della stessa e alla relativa proposta contrattuale di inquadramento e trattamento economico. La mancata presentazione del progetto equivale alla mancata accettazione della presente clausola sociale e costituisce motivo di esclusione dalla gara, previo esperimento del soccorso istruttorio.

II.7.2. Clausola di gradimento del personale

L'OEA deve impegnarsi a mantenere il turnover di tutti gli addetti nei limiti più bassi possibili.

In ogni caso l'Università si riserva di chiedere a suo insindacabile giudizio all'OEA la sostituzione (con altre figure professionali equivalenti) delle singole risorse messe a disposizione qualora le stesse non siano giudicate idonee allo svolgimento del servizio richiesto. Tale comunicazione sarà inviata con un preavviso di 15 giorni lavorativi; dopo tale termine, qualora non si sia provveduto alla sostituzione, si procederà ad applicare le corrispondenti penali.

II.8. Sicurezza

L'OEA è tenuto al rispetto del D.Lgs. 81/08 in materia di tutela della salute e della sicurezza nei luoghi di lavoro e, dove necessario, dovrà intervenire con personale appositamente formato in materia.

Si precisa che, con riferimento alle disposizioni contenute nella L. 123/2007 (secondo quanto previsto dalla determinazione dell'Autorità per la Vigilanza sui contratti pubblici di lavori, servizi e forniture 5 marzo 2008, n. 3), non sussistono rischi da interferenze che richiedono misure preventive e protettive supplementari rispetto a quelle misure di sicurezza, a carico dell'OEA, connesse ai rischi derivanti dalle proprie attività.



Non sono stati identificati rischi di sicurezza da interferenze. Nella base d'asta **non sono computati oneri per la sicurezza** derivanti da rischi specifici da interferenze.

Ai sensi dell'art. 26, comma 1, lettera b), del D. Lgs. 81/2008, l'Università degli Studi dell'Insubria fornisce le informazioni sui rischi esistenti negli ambienti in cui l'Affidatario è destinato ad operare e sulle misure di prevenzione e di emergenza adottate in relazione all'attività dell'Ateneo, nel Regolamento per la predisposizione del DUVRI disponibile sul sito internet dell'Ateneo all'indirizzo <https://www.uninsubria.it/statuto-e-regolamenti> sezione "Regolamenti in tema di Lavori Servizi e Forniture".

II.9. Subappalto

È ammesso il subappalto purché espressamente autorizzato dall'Università, ai sensi dell'art. 105, comma 4, del d.lgs. 50/2016 e s.m.i.

A pena di nullità non può essere affidata a terzi l'integrale esecuzione delle prestazioni oggetto del contratto di appalto, nonché la prevalente esecuzione delle lavorazioni relative al complesso dei contratti ad alta intensità di manodopera, come previsto dal comma 1 dell'art 105 del D. Lgs. 50/2016 e s.m.i.

Il concorrente che intenda chiedere il subappalto deve indicare nell'offerta quali prestazioni intende concedere in subappalto.

L'OEA provvede a sostituire i subappaltatori relativamente ai quali apposita verifica abbia dimostrato l'esistenza di motivi di esclusione di cui all'art. 80 del D. Lgs. 50/2016 e s.m.i., ai sensi dell'art. 105, comma 12, del D. Lgs. 50/2016 e s.m.i.

Il contraente principale e il subappaltatore sono responsabili in solido nei confronti della stazione appaltante in relazione alle prestazioni oggetto del contratto di subappalto. L'aggiudicatario è responsabile in solido con il subappaltatore in relazione agli obblighi retributivi e contributivi, ai sensi dell'art. 29 D.Lgs. 10 settembre 2003, n. 276. Nelle ipotesi di cui al comma 13 lettere a) e c) dell'art 105 del Codice l'appaltatore è liberato dalla responsabilità solidale di cui al primo periodo.

Il subappalto non autorizzato comporta le sanzioni penali ed amministrative previste per legge.

Per quanto riguarda il pagamento dei subappaltatori si rinvia a quanto previsto dall'art. 105, comma 13 del d.lgs. 50/2016 e s.m.i.

II.10. Divieto di cessione del contratto

È vietata la cessione del Contratto, in tutto o in parte a pena di nullità, ai sensi dell'art. 105, comma 1, del D. Lgs. 50/2016 e s.m.i.

In caso di inadempimento da parte dell'OEA degli obblighi di cui sopra, l'Università, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolto il Contratto.

II.11. Risoluzione del contratto

L'Università si riserva di risolvere il Contratto in tutti i casi in cui sia rilevata una situazione di grave inadempimento, l'Università invierà all'OEA, a mezzo PEC, diffida ad adempiere o a presentare le proprie controdeduzioni al RUP entro il termine di quindici giorni dalla ricezione.

Se l'OEA non provvederà all'adempimento nel termine predetto ovvero il RUP valuti negativamente le controdeduzioni, l'Università procederà alla risoluzione di diritto del Contratto, ai sensi dell'art. 1454 c.c.,



fatta salva l'azione per il risarcimento del maggior danno subito compresa la maggior spesa sostenuta per affidare ad altra impresa il Contratto ed ogni altra azione che l'Università ritenesse opportuno intraprendere a tutela dei propri interessi.

L'Università, in particolare, ha il diritto di risolvere il Contratto ex art. 1456 c.c., mediante semplice PEC, senza bisogno di messa in mora o di intervento dell'Autorità Giudiziaria, nei seguenti casi:

- mancato rispetto dei termini previsti dall'art.1 comma 1 L.120/2020 per cause imputabili all'OEA (tardivo avvio dell'esecuzione del contratto);
- emanazione di un provvedimento definitivo che dispone l'applicazione di una o più misure di prevenzione di cui all'art. 6 del D. Lgs 159/2011;
- sentenza di condanna passata in giudicato per frodi nei riguardi dell'Università, di subappaltatori, di fornitori, di lavoratori o di altri soggetti comunque interessati al Contratto;
- violazione delle previsioni contrattuali in materia di subappalto;
- violazione degli obblighi attinenti alla sicurezza sul lavoro;
- servizio eseguito con personale non regolarmente assunto o contrattualizzato;
- situazione di fallimento, concordato preventivo (salvo il caso di cui all'art. 186 – bis del R.D. 67/42) e liquidazione coatta amministrativa dell'OEA o nei cui riguardi sia in corso un procedimento per la dichiarazione di una di tali situazioni;
- frode nell'esecuzione delle Prestazioni;
- manifesta incapacità nell'esecuzione delle prestazioni oggetto dell'appalto;
- mancato utilizzo da parte dell'OEA del conto corrente indicato nello specifico articolo per i movimenti finanziari relativi al presente contratto, secondo quanto disposto dall'art. 3, comma 9-bis, della legge n. 136/2010;
- applicazione di penali per un importo pari o superiore al 10% dell'importo di aggiudicazione
- necessità di ricorrere, per più di quattro volte, all'istituto del c.d. "intervento sostitutivo" previsto dalla normativa vigente.

II.12. Recesso

L'Università potrà recedere in qualunque momento dal Contratto, anche se è stata iniziata l'esecuzione delle Prestazioni, tenendo indenne l'OEA delle spese sostenute, delle Prestazioni eseguite, oltre al decimo dell'importo delle Prestazioni non eseguite, ai sensi dell'art. 109 del D. Lgs 50/2016 e s.m.i. e dell'art. 1671 c.c.

Si precisa inoltre che, in base al comma 13 dell'articolo 1 del D.L. 95/2012, come convertito in Legge n. 135/12, l'Università ha diritto di recedere in qualsiasi tempo dal Contratto, previa formale comunicazione all'OEA con preavviso non inferiore a quindici giorni e previo pagamento delle Prestazioni già eseguite, oltre al decimo delle prestazioni non ancora eseguite, nel caso in cui, tenuto conto anche dell'importo dovuto per le Prestazioni non ancora eseguite, i parametri delle convenzioni stipulate da Consip S.p.A. ai sensi dell'articolo 26, comma 1, della legge 23 dicembre 1999, n. 488, successivamente alla stipula del presente Contratto, siano migliorativi e l'OEA non acconsenta ad una modifica delle condizioni economiche tale da rispettare il limite di cui all'articolo 26, comma 3 della legge 23 dicembre 1999, n. 488.

II.13. Fallimento dell'OEA



In caso di fallimento dell'OEA l'Università si avvale, senza pregiudizio per ogni altro diritto e azione a tutela dei propri interessi, della procedura prevista dall'art. 110 del D. Lgs. 50/2016 e s.m.i.

II.14. Obblighi a carico dell'OEA

L'OEA deve:

- assumere su di sé ogni e qualsiasi responsabilità, sia in sede civile che penale, per danni che dovessero derivare per qualsiasi motivo, a persone e/cose derivanti dalle prestazioni inerenti al Contratto, tenendo sollevata l'Università da ogni conseguenza diretta o indiretta;
- rispettare l'obbligo per il personale addetto ai servizi di indossare, oltre a idonei abiti da lavoro e dotazioni DPI nel rispetto delle normative vigenti in materia di sicurezza di cui al D. Lgs. n. 81/2008 e s.m.i., anche la tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione dell'OEA;
- far osservare in modo scrupoloso al personale addetto alle Prestazioni cui gli stessi sono assegnati il rispetto delle modalità di svolgimento dei servizi di cui alla II parte del presente CSA;
- informare gli operatori addetti circa i doveri di riservatezza nell'espletamento delle Prestazioni;
- assicurare che nell'espletamento delle Prestazioni gli operatori addetti si astengano dal prendere visione delle pratiche d'ufficio, documenti, corrispondenza, nonché di qualsiasi altra informazione e/o dato personale soggetto a tutela, ai sensi del Regolamento UE 2016/679 per i quali non siano stati formalmente autorizzati;
- ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di contratti di lavoro ed eventuali contratti integrativi, ivi compresi quelli in tema di igiene e sicurezza sui luoghi di lavoro, tutela dei lavoratori, nonché previdenza, assistenza e disciplina infortunistica, assumendo a proprio carico tutti i relativi oneri;
- allontanare dal servizio, su richiesta motivata dell'Università, i propri dipendenti o soci che abbiano tenuto un comportamento non consono, o che non siano ritenuti idonei a svolgere le mansioni assegnate;
- applicare la normativa in materia di tutela della salute e della sicurezza nei luoghi di lavoro di cui al D. Lgs. 81/2008 e preventivamente formare il proprio personale anche in materia di primo soccorso aziendale e di lotta antincendio, anche secondo le direttive impartite dall'Università.

L'inosservanza degli obblighi previsti dal presente articolo è causa di risoluzione del contratto a insindacabile giudizio dell'Università e fa sorgere il diritto per l'Università al risarcimento di ogni conseguente maggiore danno ovvero di risoluzione contrattuale qualora si riscontri il grave inadempimento.

II.15. Responsabilità e coperture assicurative

L'OEA dichiara e garantisce che è in grado di fornire le Prestazioni servizi oggetto di Appalto e che gli stessi saranno effettuati a Regola d'Arte, conformemente a tutte le Leggi ed i regolamenti applicabili al momento in cui verranno resi.

L'Università non potrà in alcun modo essere considerata depositaria delle attrezzature e dei materiali in genere, di proprietà dell'OEA che si trovino nei locali dell'Università, per cui solo all'OEA spetterà la loro custodia e conservazione, restando così l'Università sollevata da ogni responsabilità per furti, danneggiamenti, incendi o altre cause.



L'OEA userà la massima diligenza nella realizzazione delle Prestazioni, in considerazione dell'importanza che questo riveste per l'Università. Nell'effettuazione delle Prestazioni, l'OEA dovrà ritenersi direttamente ed esclusivamente responsabile di ogni danno arrecato dal proprio personale, ai beni mobili ed immobili di proprietà dell'Università o comunque da quest'ultimo detenuti o posseduti a diverso titolo.

L'OEA dovrà altresì ritenersi direttamente ed esclusivamente responsabile di ogni danno arrecato dal proprio personale a persone presenti, a vario titolo (corpo docente, personale amministrativo, studenti, ospiti, ecc.), negli ambienti dell'Università.

L'OEA è obbligato a costituire per l'intera durata dell'Appalto e consegnare all'Università, almeno dieci giorni prima della stipula del Contratto o prima dell'inizio delle Prestazioni in caso d'urgenza, una polizza di assicurazione di Responsabilità Civile Terzi (R.C.T.) e responsabilità civile verso prestatori di lavoro (R.C.O.) a copertura di danni eventualmente arrecati a persone e cose tanto dell'Università che di terzi, nell'esecuzione delle prestazioni di cui al presente CSA, anche in caso di intervento di eventuali subappaltatori.

I massimali di garanzia per l'assicurazione R.C.T./R.C.O. non dovranno essere inferiori all'importo di € 500.000,00 per sinistro e per persona. In tale polizza l'Università dovrà risultare espressamente inclusa nel novero dei terzi.

In mancanza di tale polizza non si procederà alla stipula del Contratto, e ciò comporterà la decadenza dall'aggiudicazione; in tal caso l'Università si riserva la facoltà di procedere allo scorrimento della graduatoria. La copertura assicurativa decorre dalla data di inizio delle Prestazioni e cessa alla data di emissione del certificato di verifica di conformità ai sensi dell'art 102 codice contratti. L'omesso o il ritardato pagamento delle somme dovute a titolo di premio o di commissione da parte dell'OEA non comporta l'inefficacia della garanzia nei confronti dell'Università.

Qualora l'OEA sia un Raggruppamento Temporaneo d'Imprese, giusto il regime della responsabilità disciplinato dall'art. 103, comma 10, del D. Lgs. 50/2016 e s.m.i., le stesse garanzie assicurative prestate dalla mandataria capogruppo coprono senza alcuna riserva anche i danni causati dalle imprese mandanti.

II.16. Garanzie definitive

Prima della stipula del Contratto l'OEA dovrà prestare una cauzione definitiva a garanzia dell'adempimento di tutte le obbligazioni del contratto e del risarcimento di danni derivati dall'inadempimento delle obbligazioni stesse, fatto salvo il ricorso ad ogni altra azione nel caso in cui la cauzione risultasse insufficiente.

La cauzione definitiva è stabilita in ragione del 10% (dieci per cento) dell'importo di aggiudicazione del servizio per l'intera durata del contratto; in caso di aggiudicazione con ribasso superiore al 10% l'importo della cauzione sarà aumentato secondo quanto previsto dall'art. 103 del D. Lgs. 50/2016 e s.m.i.

Ai sensi del medesimo art. 103, comma 1, alla garanzia definitiva si applicano le riduzioni previste dall'art. 93, comma 7, del D. Lgs. 50/2016 e s.m.i. per la garanzia provvisoria.

Qualora nel corso dell'esecuzione del Contratto, per qualsiasi motivo, si verificassero variazioni significative dell'ammontare netto dello stesso, la cauzione dovrà essere conseguentemente integrata ovvero ridotta su richiesta della parte interessata.

La cauzione definitiva dovrà essere prestata mediante fideiussione bancaria o mediante polizza assicurativa, secondo le modalità previste dall'art. 103 del D. Lgs. 50/2016 e s.m.i.

La garanzia decorrerà dalla data di inizio servizio e dovrà avere termine alla data di fine Prestazioni.

Lo svincolo della cauzione verrà disposto dall'Università dopo la completa estinzione di tutti i rapporti



contrattuali e comunque non prima dell'emissione del certificato di regolare esecuzione del servizio.
La mancata costituzione della garanzia definitiva determina la decadenza dell'affidamento, ai sensi dell'art. 103, comma 3, del D. Lgs. 50/2016 e s.m.i.

II.17. Tutela della privacy e trattamento dei dati

L'OEA ha l'obbligo di trattare i dati personali di cui verrà a conoscenza nell'esecuzione del Contratto in qualità di "responsabile", e ai sensi del D. Lgs. 196/2003 assicurando il rispetto di tutte le prescrizioni di legge e con gli obblighi civili e penali conseguenti.

L'OEA sarà nominato "Responsabile esterno del trattamento dei dati" e i singoli operatori impiegati nell'espletamento del servizio presso le sedi dell'Università saranno nominati "autorizzati al trattamento" ai sensi dell'art. 29 del Regolamento (UE) 2016/679 successivamente alla stipula del contratto.

L'Università tratta i dati ad essa forniti esclusivamente per la gestione dell'Appalto e per la sua esecuzione, per l'adempimento degli obblighi legali ad esso connessi, nonché per fini di studio, statistici e gestionali.

a) Oggetto trattamento dei dati

Lo scopo del presente articolo è definire le condizioni alle quali l'OEA si impegna a svolgere, per conto dell'Università titolare del trattamento, le operazioni di trattamento dei dati personali definite di seguito.

Nell'ambito dei loro rapporti contrattuali, le parti si impegnano a rispettare i regolamenti in vigore applicabili al trattamento dei dati personali e, in particolare, il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 applicabile dal 25 maggio 2018 (di seguito "regolamento europeo sulla protezione dei dati") e normativa nazionale di riferimento laddove applicabile.

b) Descrizione del trattamento

L'OEA è autorizzato ad elaborare per conto dell'Università i dati personali necessari per le Prestazioni descritte nel CSA. A riguardo si precisa quanto segue:

1. Durata del trattamento: è pari alla durata del Contratto.
2. Finalità del trattamento: sono esclusivamente quelle necessarie all'espletamento delle Prestazioni descritte nel presente CSA.
3. Natura del trattamento: il trattamento dei dati personali dovrà avvenire, mediante strumenti manuali, informatici e telematici, con logiche strettamente collegate alle finalità sopra descritte e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.
4. Tipo di dati personali: sono tutti e soli i dati necessari all'esecuzione delle Prestazioni.
5. Categorie di interessati: personale tecnico-amministrativo, personale docente, collaboratori assegnisti, studenti e tutte quelle incluse nei trattamenti previsti nello specifico registro dei trattamenti dell'Università.

c) Obbligazioni dell'OEA nei confronti dell'Università

L'OEA si impegna a:

1. Elaborare i dati solo per gli scopi che sono oggetto dell'Appalto;
2. Elaborare i dati in conformità con le istruzioni documentate dell'Università come descritti nel presente CSA. Qualora l'OEA ritenesse che un'istruzione costituisca una violazione del regolamento europeo sulla protezione dei dati o di qualsiasi altra disposizione del diritto dell'Unione o della legge sulla protezione dei dati degli Stati membri, essa è tenuta ad informare immediatamente l'Università. Inoltre,



se l'OEA è tenuto a trasferire dati verso un paese terzo o verso un'organizzazione internazionale, ai sensi del diritto dell'Unione o del diritto dello Stato membro a cui è soggetto, deve informare il titolare del trattamento di questo obbligo legale prima del trattamento.

3. Garantire la riservatezza dei dati personali trattati nell'ambito del presente Contratto.
4. Assicurare che le persone autorizzate a trattare i dati personali nell'ambito del presente Contratto:
 - si impegnino a rispettare la riservatezza o ad essere soggette ad un vincolo contrattuale di riservatezza;
 - ricevere la formazione necessaria sulla protezione dei dati personali;
5. Prendere in considerazione, per quanto riguarda i propri strumenti, prodotti, applicazioni o servizi, i principi di protezione dei dati fin dall'inizio e la protezione dei dati di design e di default.

d) Diritto di informazione delle persone interessate

L'OEA, al momento della raccolta di dati personali, deve fornire alle persone interessate dalle operazioni di trattamento le informazioni relative al trattamento dei dati che esegue.

La formulazione e il formato delle informazioni devono essere concordati con il titolare del trattamento della committenza prima della raccolta dei dati.

e) Esercizio dei diritti delle persone interessate

L'OEA assiste l'Università, nella misura in cui ciò sia possibile, per l'adempimento dell'obbligo di rispondere alle richieste di esercizio dei diritti dell'interessato: diritto di accesso, rettifica, cancellazione e opposizione, diritto alla limitazione del trattamento, diritto a portabilità dei dati, diritto di non essere soggetto ad una decisione individuale automatizzata (inclusa la profilazione).

Qualora gli interessati sottopongano al responsabile richieste per l'esercizio dei loro diritti, l'OEA deve inoltrare tali richieste al Responsabile della protezione dei dati dell'Università.

f) Notifica di violazione dei dati personali

L'OEA comunica all'Università qualsiasi violazione dei dati personali entro e non oltre 8 ore dopo esserne venuto a conoscenza e a mezzo PEC. Tale notifica deve essere inviata insieme a tutta la documentazione necessaria per consentire all'Università ove necessario, di notificare tale violazione all'autorità di vigilanza competente e, in qualità di Responsabile Esterno del Trattamento è tenuto a dare pieno supporto all'Università nella gestione di eventuali violazioni di dati personali avvenute nell'ambito dei servizi previsti dal presente CSA.

g) Assistenza prestata dall'OEA all'Università per l'adempimenti dei suoi obblighi

L'OEA assiste il committente nello svolgimento delle valutazioni d'impatto sulla protezione dei dati. L'OEA assiste il committente in merito ad eventuali preventive consultazioni del Garante della Privacy.

h) Misure di sicurezza

L'OEA dovrà impegnarsi ad attuare misure minime di sicurezza con particolare riferimento alle misure tecniche e organizzative idonee per garantire un livello di sicurezza appropriato al rischio.

In particolare, dovrà essere garantita la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza di sistemi e servizi di elaborazione nonché la possibilità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo nel caso di eventi che comportino un incidente fisico o tecnico.

i) Destino dei dati

Al termine della prestazione relativa al trattamento dei dati, l'OEA si impegna in base e ad espressa



indicazione dell'Università e nel rispetto delle leggi vigenti in materia di conservazione alla distruzione dei dati personali eventualmente raccolti.

Una volta distrutti, l'OEA deve dimostrare, per iscritto, che tale distruzione è avvenuta.

j) Responsabile della protezione dei dati

Il Responsabile della protezione dei dati dell'Università, designato ai sensi dell'art. 37 del Regolamento (UE) 2016/679, è l'Avv. Stefano Ricci, e-mail: privacy@uninsubria.it.

k) Registro delle categorie di attività di trattamento

L'OEA all'atto della stipula dovrà dichiarare di conservare una registrazione scritta di tutte le categorie di attività di trattamento svolte per conto dell'Università, contenente:

- il nome e i dati di contatto del titolare del trattamento dell'OEA per conto del quale agisce il responsabile del trattamento e del responsabile della protezione dei dati dell'OEA;
- eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione di tale paese terzo o organizzazione internazionale e, nel caso di trasferimenti di cui all'articolo 49, paragrafo 1, secondo comma, del Regolamento (UE) 2016/679, la documentazione di adeguate garanzie.

Tale dichiarazione dovrà essere aggiornata in corso di vigenza contrattuale in caso di variazione.

l) Documentazione

L'OEA fornisce all'Università tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi.

m) Obblighi del controllore rispetto al processore

L'Università si impegna a:

1. fornire all'OEA i dati di cui al presente documento
2. documentare, per iscritto, tutte le istruzioni relative al trattamento dei dati da parte dell'OEA
3. assicurare, prima e durante il processo, il rispetto degli obblighi previsti dal regolamento generale sulla protezione dei dati da parte dell'OEA.
4. Supervisionare il trattamento, anche effettuando audit e ispezioni con l'OEA.

n) Adeguaenti alla normativa privacy. Obblighi

L'Università si riserva di adeguare le clausole contenute nel presente capitolato al modello di atto giuridico e/o clausole tipo predisposte dalla Commissione UE o da un'autorità di controllo per la disciplina del trattamento dei dati.

II.18. Controversie e foro competente

Qualunque contestazione dovesse eventualmente sorgere nel corso dell'esecuzione Contratto, non si ammetterà alcun diritto in capo all'OEA di sospendere unilateralmente le Prestazioni, né di procedere alla riduzione o alla modificazione del medesimo.

La definizione di tutte le controversie derivanti dall'esecuzione del Contratto è devoluta all'autorità giudiziaria competente presso il Foro di Varese ed è esclusa la competenza arbitrale. Ai sensi dell'art. 209, comma 2, del D. Lgs. 50/2016 e s.m.i. si dichiara che il contratto conseguente all'aggiudicazione definitiva non conterrà clausola



compromissoria.

L'organo che decide sulla controversia decide anche in ordine all'entità delle spese di giudizio e alla loro imputazione alle parti, in relazione agli importi accertati, al numero e alla complessità delle questioni.

II.19. Oneri e spese contrattuali

A carico dell'OEA graveranno le spese di bollo, i diritti e le spese di registrazione del contratto nonché ogni altro onere fiscale presente o futuro che per legge non sia inderogabilmente posto a carico dell'Università.



III - GOVERNO DELLA FORNITURA

III.1. Condizioni minime di esecuzione delle Prestazioni

Le indicazioni fornite nel presente CSA devono intendersi quali requisiti minimi che l'offerta dell'OEA deve soddisfare.

L'OEA è altresì obbligato ad eseguire, agli stessi termini patti e condizioni indicate nel CSA, tutte le Prestazioni aggiuntive e/o migliorative offerte in sede di gara mediante la propria proposta, senza che ciò comporti oneri ulteriori per l'Università.

Entro 10 (dieci) giorni lavorativi dalla data di stipula del Contratto, il Fornitore comunicherà all'Amministrazione i dati relativi al soggetto referente per l'esecuzione delle prestazioni contrattuali (Rappresentante del Fornitore).

Entro 10 (dieci) giorni lavorativi dalla data di stipula del Contratto, l'Amministrazione comunicherà al Fornitore i dati relativi al Direttore dell'Esecuzione.

In ogni caso, l'Amministrazione procederà alle verifiche di conformità delle prestazioni eseguite dal Fornitore al fine di accertarne la regolare esecuzione ai sensi degli artt. 312 e ss., del D.Lgs. n. 163/2006, anche facendo ricorso alla documentazione contrattuale prodotta da Fornitore o, comunque, di contenuto analogo attestante la conformità delle prestazioni eseguite alle prescrizioni contrattuali.

III.2. Pianificazione

I servizi dovranno essere erogati senza soluzione di continuità durante tutta la vigenza del contratto garantendo le quantità minime richieste nel presente capitolato, garantendo l'erogazione temporale richiesta nella Sezione VI - *Servizi Obbligatoriosi della Fornitura*.

III.3. Fase di Avvio del contratto

Durante la fase di avvio del contratto il fornitore dovrà provvedere ad:

- acquisire, anche grazie alla documentazione fornita dal committente, tutte le conoscenze necessarie a prendere in carico in modo efficace l'erogazione del presente servizio;
- apprendere le modalità di accesso agli spazi, le procedure di sicurezza e le modalità operative richieste dal committente;
- prendere visione dei luoghi e delle infrastrutture tecnologiche del committente, pertinenti all'erogazione del servizio;
- approntare tutta la strumentazione necessaria all'erogazione del servizio (postazioni di lavoro, software specifici, etc.);
- presentare all'Amministrazione i curriculum vitae delle risorse adibite ai vari servizi di supporto specialistico di cui agli Articoli VI.1.1, VI.1.2, VI.1.3, VI.1.4, VI.1.5, VI.1.6;



- comunicare i contatti di riferimento per le procedure di escalation in caso di superamento degli SLA contrattuali e più in generale di difformità rispetto agli indicatori di qualità di cui alla Sezione VIII - Indicatori di Qualità della Fornitura.

III.4. Conduzione del contratto

Tutte le attività previste dal presente contratto devono essere avviate e condotte secondo le indicazioni fornite dal Responsabile unico del procedimento e/o dal Direttore dell'esecuzione del contratto.

Queste figure sono definite e formalizzate in sede di riunione preliminare, da tenersi anteriormente alla sottoscrizione dell'accordo.

L'OEA è tenuto a garantire:

- la completa erogazione dei servizi in sistema di qualità;
- un costante flusso di informazioni riguardante l'andamento delle varie attività costituenti l'oggetto dell'appalto tramite opportuni sistemi informativi;
- il monitoraggio continuo e costante delle prestazioni rese.

A garanzia del pieno e adeguato svolgimento dei compiti assegnati, l'OEA è tenuto a garantire la disponibilità, per l'intera durata di validità contrattuale, di:

- un adeguato staff di operatori/maestranze, professionalmente qualificato;
- commisurati mezzi d'opera conformi alle Leggi e normative di sicurezza;
- documenti, procedure, buone prassi, checklist, ecc. di riferimento;
- propri referenti a coordinamento, dedicati di norma esclusivamente al DEC e reperibili 24/24h mediante numero telefonico.

Per tutti i servizi oggetto del contratto, il fornitore dovrà mettere a disposizione, senza costi aggiuntivi per l'Università, una apposita piattaforma per il governo del contratto e dei servizi, la rendicontazione e la consuntivazione degli stessi (risorse allocate e utilizzate, residui disponibili, giornate utilizzate e relativi residui, ecc.) e la verifica dell'andamento dei servizi oggetto del presente Capitolato. La piattaforma dovrà essere resa accessibile ai singoli referenti dell'Area Sistemi Informativi dell'Ateneo per ciascuno dei servizi oggetto del presente appalto oltre che al RUP e al Direttore dell'Esecuzione, al fine di garantire:

- le necessarie interazioni fra committente e fornitore per i servizi di conduzione operativa (apertura di Incidenti, richieste, ecc.)
- le verifiche del committente relative all'andamento dei servizi e la relativa reportistica, ciascuno per i propri ambiti. I referenti dovranno poter avere una visione aggiornata dell'andamento dei servizi (consumi, disponibilità, eventuali SLA, ecc.) in relazione ai termini contrattuali e rispetto ai quali verificare le fatturazioni periodiche per effettuare eventuali rilievi.

Il RUP e il Direttore dell'esecuzione del contratto devono avere visibilità completa sulla piattaforma di reportistica e SLA management.

Il sistema dovrà essere accessibile tramite una interfaccia web compatibile con i browser più diffusi (Firefox, Chrome, Safari, Opera, Edge, etc.), con sistemi operativi Windows, MacOS, IOS Linux ed Android. Il sistema dovrà essere messo a disposizione in modalità SaaS (*Software as a Service*) dal fornitore, avvalendosi



di infrastrutture e mezzi propri, oppure avvalendosi di soluzioni basate su tecnologia Cloud privato che garantiscano la segregazione e la sicurezza dei dati e dell'applicazione.

Per quanto riguarda l'OEA, il sistema dovrà essere accessibile a tutti i soggetti coinvolti nell'erogazione dei servizi del presente capitolato che l'OEA reputerà opportuno abilitare al fine di una corretta ed armonica esecuzione dei servizi.

Ogni altra modalità di comunicazione e/o di richiesta d'intervento, fatta salva la forza maggiore e i casi di emergenza, non verrà presa in considerazione e non darà diritto al pagamento delle prestazioni effettuate.

Al termine di ogni mensilità, l'OEA è tenuto a presentare il report delle attività svolte e delle giornate/uomo erogate per ogni singolo servizio oggetto dell'appalto.

In assenza del report, non si procederà alla liquidazione del corrispettivo.

L'OEA è responsabile per eventuali abusi commessi tramite le postazioni informatiche utilizzate nell'esercizio della fornitura e per eventuali attività non conformi al regolamento per l'accesso e l'utilizzo delle infrastrutture centrali di Information Technology & Communication (ITC) dell'Università (<https://www.uninsubria.it/files/regolamento-laccesso-e-lutilizzo-delle-infrastrutture-centrali-di-information-e-communication>).

Eventuali abusi sulla rete dati provenienti dai calcolatori affidati al personale dell'OEA per l'esecuzione dei servizi saranno imputati al fornitore del servizio, il quale sarà tenuto ad individuare il soggetto responsabile dell'evento.

III.5. Fase di Conclusione del Contratto

La durata della fase di chiusura è fissata in 10 giorni lavorativi a decorrere dalla data di termine del Contratto.

Durante la fase di chiusura del contratto, il fornitore dovrà provvedere a:

- redigere tutta la documentazione necessaria al passaggio di consegne verso il fornitore subentrante;
- affiancare il personale del fornitore del subentrante per un armonico e completo passaggio di consegne.

III.6. Modifiche delle Prestazioni e variazioni

L'Università si riserva il diritto di modificare, ai sensi dell'art. 106 comma 1 lett. a), senza eccezione alcuna da parte dell'OEA, l'articolazione del monte ore, oggetto di gara, riferito a ciascun servizio nel limite del 20%, fermo restando la stima presunta del monte annuo riferito alla prestazione complessivamente intesa. Sono fatti salvi eventuali accordi definiti in contraddittorio tra le parti durante la gestione dell'Appalto.

L'OEA ha l'obbligo di eseguire tutte le variazioni ritenute opportune dall'Università per garantire il corretto svolgimento delle Prestazioni, senza alcuna pretesa di indennizzo. Nessuna variazione può essere introdotta dall'OEA se non è preventivamente approvata per iscritto del DEC.

L'Università si riserva la facoltà di sospendere/estendere/modificare temporaneamente ogni singolo servizio in cui sono articolate le Prestazioni oggetto del presente Appalto, in base a proprie esigenze funzionali, quali, a titolo meramente esemplificativo, l'esecuzione di lavori di modifica o straordinaria manutenzione ai locali o agli impianti o altre motivate ragioni.

L'ammontare delle variazioni, intese come sospensioni e modifiche apportate alle Prestazioni, incluso l'inserimento di nuove strutture dell'Università, verrà retribuito sino alla concorrenza del quinto d'obbligo



sulla base del prezzo orario offerto in sede di gara, che rimarrà fisso per l'intera durata del contratto, salvo quanto previsto all'Articolo II.3.4 "Revisione dei prezzi".

III.7. Assicurazione Qualità

Di seguito, con riferimento all'Appendice 1 - Indicatori di Qualità, vengono riportati gli indicatori di qualità che verranno applicati per la misurazione di ogni singolo servizio oggetto del presente appalto; si precisa che qualora si faccia riferimento a data ed ora di apertura/chiusura di ticket per i servizi di conduzione operativa da remoto, queste sono da intendersi relative al sistema di ticketing dell'OEA.

Al fine di garantire il rispetto dei livelli di qualità richiesti, il fornitore entro la data di avvio dei servizi dovrà comunicare al committente i contatti di riferimento per le procedure di escalation in caso di superamento degli SLA contrattuali e più in generale difformità rispetto agli indicatori di qualità di cui all'Appendice 1 - Indicatori di Qualità.

Il mancato rispetto delle soglie minime per gli indicatori di qualità darà seguito all'applicazione delle penali previste dal Contratto.

III.7.1. Indicatori Servizi in ambito ICT

La qualità del servizio verrà valutata tramite i seguenti indicatori della Sezione VIII - Indicatori di Qualità della Fornitura, ed in particolare:

Per i servizi di Supporto Specialistico si applicano i seguenti Indicatori di Qualità:

- IQ01 - Personale della fornitura inadeguato
- IQ02 - Turn over del personale
- IQ03 - Inadeguatezza del personale proposto
- IQ04 - Inserimento/sostituzione del personale
- IQ05 - Attivazione degli interventi
- IQ06 – Rilievi sulla fornitura

Per i servizi di Conduzione Operativa da Remoto si applicano i seguenti indicatori di Qualità:

- IQ107 - Tempestività di risoluzione degli incident
- IQ08 - Tempestività di esecuzione dei change standard/predefiniti
- IQ09 - Tempestività di esecuzione dei change non standard

III.8. Esecuzione e valutazione delle Prestazioni

L'OEA dovrà svolgere le Prestazioni di cui al presente CSA con organizzazione dei mezzi necessari e gestione a proprio rischio ai sensi dell'art. 1655 c.c. L'OEA, nell'ambito della propria autonoma organizzazione, eserciterà il potere direttivo, disciplinare, di formazione e di istruzione professionale nei



confronti dei propri dipendenti e controllerà le modalità di svolgimento delle singole prestazioni.

L'OEA deve rispettare i seguenti principi generali:

- a) puntuale conoscenza da parte degli addetti dei Regolamenti di competenza, delle attività loro richieste e dell'organizzazione dell'Università in generale;
- b) massima cortesia e disponibilità nei confronti degli utenti all'atto dell'erogazione delle Prestazioni.

Per quanto riguarda la valutazione delle prestazioni, il DEC controllerà tempi e modalità di esecuzione, anche tramite propri delegati, che provvederanno a rilasciare mensilmente un'attestazione di regolare svolgimento delle Prestazioni, necessaria per la liquidazione delle fatture.

III.9. Uso delle macchine, attrezzature, materiali di consumo, locali, energia, linee telefoniche e di trasmissione dati

L'OEA, per lo svolgimento delle Prestazioni di cui al presente Appalto, dovrà dotare il proprio personale di tutte le attrezzature, materiali di consumo necessari per lo svolgimento delle attività richieste, salvo nel caso in cui sia previsto l'utilizzo della dotazione tecnologica dell'Università.

In particolare, il personale dell'OEA è tenuto, nel caso di utilizzo della dotazione tecnologica dell'Università, a:

- mantenere in stato ottimale di funzionamento e di ordine gli spazi, le macchine e le attrezzature affidategli per l'espletamento delle Prestazioni;
- utilizzare i locali, le macchine, le attrezzature, i materiali di consumo, l'energia elettrica, le linee telefoniche e di trasmissione dati esclusivamente per le attività oggetto del presente contratto e secondo le modalità concordate con i Referenti di ciascun servizio;

In ogni caso il personale dell'OEA è tenuto a:

- non abbandonare materiali personali nei locali di svolgimento delle Prestazioni.

III.10. Strumenti Informatici messi a disposizione dall'Università a supporto dell'erogazione dei servizi

L'Area Sistemi Informativi – ASI, previa nomina del personale del Fornitore quale incaricato ai sensi del GDPR, abiliterà ogni singolo operatore tecnico dell'affidatario che ne abbia necessità in base alla tipologia di servizi a cui e per cui è incaricato con un profilo idoneo ad accedere ai dati pertinenti alle attività affidate. Gli operatori dell'OEA avranno a disposizione diversi strumenti fra i quali si citano i principali:

- Webapp SIC on Line
- Sistema di Ticketing
- Microsoft Intune
- TeamViewer
- Sistemi di monitoraggio Nagios e Cacti
- Infoblox NetMRI



WebApp SIC on Line

La webapp 'Sic On-Line' (SOL) è un sistema custom pensato per la gestione del cablaggio strutturato per rete dati e fonia (attivazione, disattivazione e trasloco utenze di rete o telefoniche), gestione del ciclo vita degli account per staff ed ospiti, gestione degli accessi a caselle di posta in delega).

Sistema di Ticketing

L'Area Sistemi Informativi – ASI, mette a disposizione un sistema di ticketing che permette agli utenti dei vari servizi (personale tecnico amministrativo e docente dell'Ateneo) di sottoporre, attraverso diversi canali, le richieste di assistenza o di intervento a fronte di incidenti. Ad ogni singola richiesta viene attribuito un identificativo (ticket) che permette una tracciatura del workflow di lavorazione della richiesta comprensiva di indicazioni precise sui tempi e gli addetti alla lavorazione.

Il sistema è accessibile tramite una interfaccia web compatibile con i browser più diffusi browser (FireFox, Chrome, Safari, Opera, Edge, etc.), con sistemi operativi Windows, MacOS, IOS Linux ed Android.

Caratteristiche dei Ticket:

Comunemente ad ogni *attività* viene assegnata una struttura dati contenenti informazioni necessarie ad identificarla in maniera univoca nel tempo e gestirne lo stato di lavorazione. Questa struttura dati viene denominata generalmente “ticket”.

I ticket sono organizzati in tassonomie multilivello per definire contesto e tipologia di issue (Anomalia/Incidente, Richiesta); ad ogni ticket sono assegnate queste caratteristiche:

- Un oggetto sintetico
- Una descrizione analitica
- Una priorità/urgenza
- Una indicazione della gravità della issue
- Un identificativo univoco (assegnato dal sistema)
- Uno stato (assegnato dal sistema)
- Data di apertura (assegnato dal sistema)

Il sistema consente che ogni ticket collegato ad una issue possa essere nel tempo, a parte la fase iniziale di screening, assegnato chiaramente ad una persona/attore che si occupa di far avanzare lo stato di lavorazione del problema (magari riassegnandolo ad altro operatore).

I Ticket sono suddivisi in 2 macrocategorie:

- *richieste*: ossia tutte le istanze degli utenti volte a richiedere l'erogazione di un servizio (es. installazione di un software, trasloco di una postazione, configurazione di una periferica, etc.);
- *segnalazione/incidente*: ove è possibile sottoporre una problematica, con associato un indicatore di gravità (es: problema bloccante, problema non bloccante, anomalia, richiesta di servizi); è possibile,



ad opera del personale tecnico di back office, modificare la categoria e la gravità indicata dall'utente in sede di apertura del ticket.

Interfaccia utente finale – Front End:

Il sistema di ticketing è fornito di interfaccia web per l'attivazione dei ticket e verifica dello loro ciclo di vita da parte dell'utente finale. Questa interfaccia verrà indicata come "front-end".

L'accesso al sistema di ticketing avviene esclusivamente previa autenticazione con credenziali personali degli utenti.

Interfaccia Operatori e Supervisor – Back End:

Il sistema di ticketing è dotato di una sezione dedicata alla gestione ed agli operatori che si occupano della assegnazione e gestione dei vari ticket, questa sezione sarà denominata comunemente Back End; questa interfaccia permette di assegnare ticket, gestirne i workflow, definire service level agreement collegabili ad allarmi e procedure di escalation, definire ruoli, gruppi, diritti e attori e configurare i parametri globali del sistema.

L'accesso alla sezione di back-end avviene esclusivamente previa autenticazione con credenziali personali degli operatori.

Microsoft Intune

L'Ateneo ha adottato dispone il sistema centralizzato di gestione device e di gestione applicazioni Microsoft² Intune

Microsoft Intune è un servizio basato su tecnologia cloud Azure di Microsoft per la gestione di dispositivi mobili (MDM, Mobile Device Management) e per la gestione di applicazioni mobili (MAM, Mobile Application Management). Attraverso Intune è possibile gestire centralmente i dispositivi di proprietà dell'Ateneo, inclusi telefoni cellulari, tablet e calcolatori. È anche possibile configurare criteri specifici per la gestione centralizza delle applicazioni (es. aggiornamento, installazione ecc.)

Con Intune, è possibile:

- Impostare le regole e configurare le impostazioni nei dispositivi di proprietà dell'organizzazione per accedere ai dati e alle reti.
- Distribuire e autenticare le applicazioni nei dispositivi, in locale e nei dispositivi mobili.
- Proteggere le informazioni di Ateneo controllando il modo in cui gli utenti accedono alle informazioni e le condividono.
- Assicurarsi che i dispositivi e le applicazioni siano conformi ai requisiti di sicurezza e sempre aggiornati

I device attualmente gestiti con il sistema Intune sono:

² <https://docs.microsoft.com/it-it/mem/intune/fundamentals/what-is-intune>



- Calcolatori dei laboratori didattici (uso pubblico - studenti)
- Calcolatori d'aula dedicati alla didattica in aula (uso pubblico – docenti)
- Surface Hub 2S per didattica ibrida

Nel corso del 2022, saranno progressivamente registrati in Intune i seguenti device:

- Calcolatori ad uso esclusivo del personale dell'Amministrazione Centrale
- Calcolatori ad uso esclusivo del personale Tecnico ed Amministrativo dei dipartimenti

Microsoft Teams per gruppi di coordinamento e risorse condivise

L'Area Sistemi Informativi ha realizzato un articolato gruppo di supporto attraverso lo strumento "Microsoft Teams". Questo strumento, privato e ad accesso controllato, rappresenta lo strumento di scambio e sviluppo collaborativo di progetti, modalità operative e documentazione dei servizi erogati dall'Area, nonché lo strumento di gestione della knowledge base.

Attualmente è organizzato con un solo canale pubblico e numerosi canali privati a cui sono ammessi singoli account di personale strutturato o collaboratori in base alle specifiche attività. A titolo puramente esemplificativo si presenta la struttura dei canali aggiornata a luglio 2021; ogni canale contiene normalmente un canale di comunicazione asincrona (post) e sincrona (videoconferenza teams), file, wiki e altri strumenti come liste e database di supporto. La documentazione è organizzata con lo strumento wiki nei singoli canali privati ma con unico indice generale nel canale pubblico.

Nome canale	ambito	Servizio/prodotto	Descrizione
S-FOF		S-FOF	udc
UDIG		UDIG	Canale privato ufficio Digital Learning e Multimedialità
S-DIG		S-DIG	Canale Privato del Servizio Infrastrutture Digitali
UDC		UDC	Canale privato dell'Ufficio Data Center
UNF		UNF	Canale Privato dell'Ufficio Networking e Fonia
S-FOF Presidii dipartimentali		S-FOF	Canale Privato per Presidii dipartimentali
UDC	Identità digitali di Ateneo	Specifiche tecniche	Specifiche tecniche delle identità digitali di Ateneo
UDC	Identità digitali di Ateneo	Procedure	Procedure per la gestione del ciclo di vita delle identità digitali di Ateneo e dei servizi associati
UDC	Servizi di datacenter	Backup e Restore	Servizio per il salvataggio e il ripristino dei dati e delle macchine virtuali
UDC	Posta elettronica	Posta elettronica	Servizio di posta elettronica e liste di distribuzione
UDC	Servizi di datacenter	Advanced Threat Protection	Servizio di protezione avanzata per le applicazioni della piattaforma Microsoft Office 365
UDC	Servizi di datacenter	Conditional Access	Servizio di accesso con doppio fattore di autenticazione
UDC	Servizi di datacenter	File Server	Servizio centralizzato per la gestione storage personale e per gruppi di lavoro
UDC	Servizi di datacenter	Print Server	Servizio centralizzato per la gestione delle code di stampa
UDC	Servizi di datacenter	Macchine virtuali	Servizio centralizzato per la gestione del ciclo di vita delle macchine virtuali



Nome canale	ambito	Servizio/prodotto	Descrizione
UDC	Servizi di datacenter	Analisi dei log	Servizio di interrogazione e analisi dei log di sistema delle macchine fisiche e virtuali gestite dall'Ufficio Data Center
S-FOF	Applicazioni web verticali	Sistema ID	
S-FOF	Applicazioni web verticali	Sistema SOL	Web App verticale per richiedere collegamento pc, caselle con delega, telefoni
S-FOF	Applicazioni web verticali	Sistema SOLG	
S-FOF	Applicazioni web verticali	Sistema GPS	Web App verticale per presenza in sede Covid personale con ID di Ateneo
S-FOF	Applicazioni web verticali	Sistema PAGOPA spontaneo	
S-FOF	Applicazioni web verticali	Sistema Gestione Eventi Web (GEW) 1.0	
S-FOF	Applicazioni web verticali	Sistema Gestione Eventi Web (GEW) 3.0	
UDIG	E-learning	Piattaforma di E-learning didattica	Supporto all'attività didattica d'Ateneo - Spazi di lavoro (condivisione-collaborazione) per il PTA
UDIG	E-learning	Piattaforma di E-learning Esami	Supporto all'attività didattica d'Ateneo
UDIG	E-learning	Connettore CIELO	Gestisce le iscrizioni automatiche di docenti e studenti agli insegnamenti della piattaforma di E-learning
UDIG	Videocomunicazione	Videoconferenza H.323	
UDIG	Videocomunicazione	Videregistrazione H.323 (insubREC)	
UDIG	Videocomunicazione	Supporto Teams	
UDIG	Videocomunicazione	Dirette ed eventi	
UDIG	Videocomunicazione	Riprese video e postproduzione	
UDIG	Videocomunicazione	Infrastruttura videoconf	Gestione sistemistica Hypervisor, appliance virtuali ecc
UDIG	Videocomunicazione	Stream	
UDIG	Videocomunicazione	Sistema custom con criptazione	
UDIG	Videocomunicazione	Gestione Liberatorie	
S-FOF	Sistemi di collaborazione	Sistemi di collaborazione (one drive) ecc.	
S-FOF	Assistenza Primo Livello	Assistenza AC	
S-FOF	Assistenza Primo Livello	Assistenza utenza Dipartimento	
S-FOF	Assistenza Primo Livello	Assistenza didattica in aula	
S-FOF	Assistenza Primo Livello	Informazioni generali	
S-FOF	Gestione Endpoint	Richiesta fornitura calcolatore	
S-FOF	Gestione Endpoint	Problematica/aggiornamento HW	
S-FOF	Gestione Endpoint	Problematica/aggiornamento SW	
S-FOF	Gestione Endpoint	Attività di backoffice	
S-FOF	Sistemi di comunicazione	Communication Builder	Strumento per comunicazioni di massa e per openday
S-FOF	Sistemi di comunicazione	Sistema editoriale Portale IT	fare unica voce per le diverse istanze?
S-FOF	Sistemi di comunicazione	Sistema editoriale Portale EN	
S-FOF	Sistemi di comunicazione	Sistema editoriale Intranet	
S-FOF	Sistemi di comunicazione	Sistema editoriale Home Page Personali	
S-FOF	Sistemi di comunicazione	Portali di Ateneo	
UNF	Networking	Rete Dati di Ateneo (wired) - accesso client	



Nome canale	ambito	Servizio/prodotto	Descrizione
UNF	Networking	Rete Dati di Ateneo (wired) - accesso server	
UNF	Networking	Rete Dati di Ateneo (wired) - accesso IoT	
UNF	UninsubriaWireless	Rete WiFi di Ateneo (uninsubriawireless)	
UNF	Networking	Accesso remoto VPN - accesso client	
UNF	Networking	Registrazione nomi a dominio (DNS) - server	
UNF	Networking	Rilascio certificati SSL - server	
UNF	Networking	Rilascio certificati SSL - client vpn docenti	
UNF	Networking	Monitoring via Rete (Nagios, Cacti)	
UNF	Telefonia Fissa	Sistema Telefonico di Ateneo	
UNF	Telefonia Mobile	Telefonia Mobile di Ateneo (personale)	
UNF	Telefonia Mobile	Telefonia Mobile per DAD (studenti)	
S-DIG	Controllo accessi di Ateneo	Sistema Controllo accessi di Ateneo - registrazione badge	
USIG	Servizi per gli studenti	Mobilità internazionale	
USIG	Servizi per gli studenti	Student Booking	
USIG	Servizi per gli studenti	Diritto allo studio	
USIG	Servizi per gli studenti	Scuole specializzazione Qualità - libretto	
USIG	Servizi per gli studenti	gestione Tesi dottorati di ricerca	
USIG	Servizi per gli studenti	Gestione utenze accesso ai servizi applicativi	
USIG	Servizi Gestionali	Tracciati per CSA	
USIG	Servizi Gestionali	Facility Management	
USIG	Servizi Gestionali	PICA	
USIG	Servizi Gestionali	U-GOV didattica	
USIG	Servizi Gestionali	Rilevazione Presenze	
USIG	Servizi Gestionali	ESSE3	
USIG	Servizi Gestionali	UP	
USIG	Servizi per gli studenti	App Uninsubria	App ufficiale di Ateneo

TeamViewer

L'Area Sistemi Informativi -ASI dispone di una soluzione software per l'accesso in modalità remota alle postazioni di lavoro per erogare il servizio di assistenza tecnica-office automation e il supporto applicativo agli utenti. Questa soluzione è necessaria per ottenere da un lato tempestività di intervento in caso di malfunzionamento e dall'altro realizzare economie di scala significative nella sua erogazione, riducendo sia i tempi di intervento che gli spostamenti fisici del personale addetto al servizio che anziché doversi recare presso l'edificio in cui è collocata la postazione di lavoro per cui è stata richiesta l'assistenza possono intervenire in tempo reale dalla sede in cui presso cui è collocato il servizio. La soluzione adottata da ASI è Teamviewer Corporate, con 6 canali simultanei; è in fase di attivazione l'integrazione di Teamviewer con la soluzione Intune di Ateneo.



Nagios e Cacti

L'Area Sistemi Informativi – ASI ha in uso una serie di strumenti open source per il monitoraggio degli asset IT:

- Nagios - monitoraggio ed allarmistica su disponibilità apparati e servizi
- Cacti - raccolta storica dati di traffico, latenza, carico, temperatura, etc.

Al personale del Fornitore, ove necessario, verrà dato accesso alle interfacce utente dei servizi di cui sopra e potranno essere configurati alert automatizzati via email.

In aggiunta, il Fornitore, qualora lo ritenga necessario, potrà interfacciare i propri sistemi di monitoraggio con le piattaforme in uso presso l'Ateneo, al fine di raccogliere i dati necessari per i servizi di conduzione operativa oggetto del contratto. Tale attività non dovrà comportare oneri aggiuntivi per l'Ateneo.

Network Automation con Infoblox NetMRI

Area Sistemi Informativi – ASI ha in uso il sistema Infoblox NetMRI con funzionalità di network automation & control, in particolare, il sistema consente l'inventario dei device di rete, il monitoraggio dello stato di occupazione delle porte utente della rete di accesso, la raccolta del trap di eventi di sicurezza degli apparati, il salvataggio e la storicizzazione delle configurazioni di tutti gli apparati della Rete dati di Ateneo.



IV - CONTESTO ORGANIZZATIVO DEL COMMITTENTE

L'Università degli Studi dell'Insubria è caratterizzata da un modello organizzativo a rete, distribuito tra i siti di Como, Varese e Busto Arsizio. Le attività, amministrative, didattiche e di ricerca, si svolgono quindi nelle diverse sedi presenti in ciascun sito.

Le sedi di Varese si trovano in:

- Via Ravasi 2: edificio 'Ravasi'
- Viale O. Rossi 9: edifici 'Rossi', 'Bianchi', 'Antonini', 'Morselli', 'Biffi', 'CRT', 'Seppilli'
- Via Montegeneroso 71: edifici 'Montegeneroso', 'Colonia', 'Spallanzani', 'Bar Ristoro', 'Morfologia' e 'Spallanzani'
- Via Dunant 3: edificio 'DBSF'
- Via Dunant 5: edificio 'Bassani'
- Via Dunant 7: edificio 'Collegio Cattaneo'
- Via GB Vico 46: edificio 'Villa Toeplitz'

Nella sede di Varese, gli edifici presenti in Viale Ottorino Rossi, Via Dunant e via Montegeneroso, costituiscono il 'Campus Bizzozero'.

Le sedi di Como si trovano in:

- Via Valleggio 9: edificio 'Cubo Chimici'
- Via Valleggio 11: edifici 'Torre Valleggio', 'Anello Valleggio' e 'Piazza Valleggio'
- Via Castelnuovo: edificio 'Castelnuovo'
- Via Bossi 5: edificio 'Oriani'
- Via S. Abbondio: edifici 'Chiostrò S. Abbondio' e 'Manica Lunga'
- Piazza S. Teresa: edificio 'Collegio S. Teresa'

Nella sede di Como, gli edifici presenti in via Valleggio e via Castelnuovo, costituiscono il 'Campus Valleggio'.

Le sedi di Busto Arsizio si trovano in:

- Via Alberto da Giussano 9: edificio 'Molini Marzoli (Tecno City)';
- Via Manara: edificio 'Villa Manara'.



L'organizzazione dell'Ateneo è articolata in unità organizzative aventi diversi gradi di autonomia tecnica e organizzativa rispetto alla gestione dei servizi informatici. Le principali strutture sono:

- Amministrazione Centrale (AC);
- Dipartimento di Medicina e Chirurgia (DMC);
- Dipartimento di Scienze Umane e dell'innovazione per il territorio (DiSUIT);
- Dipartimento di Scienza e Alta Tecnologia (DISAT);
- Dipartimento di Scienze Teoriche e Applicate (DISTA);
- Dipartimento di Biotecnologie e Scienze della Vita (DBSV);
- Dipartimento di Economia (DIECO);
- Dipartimento di Diritto Economia e Culture (DIDEC);
- Scuola di Medicina (SMED),
- Centri Speciali

L'Area Sistemi Informativi - ASI gestisce, progetta ed eroga servizi informatici, di telecomunicazioni e di comunicazione per le strutture ed il personale dell'Ateneo.

L'Area Sistemi Informativi - ASI si occupa a livello centrale dei seguenti servizi per tutto l'Ateneo:

- Servizi di rete trasmissione dati
- Servizi telefonici
- Servizi di posta elettronica e collaboration (Microsoft 365)
- Servizi di autenticazione centrali
- Sistemi di videoconferenza e streaming
- Portali web istituzionali
- Portale e-learning
- Sistemi informativi per la gestione della didattica e della carriera studenti
- Sistemi informativi per la gestione del personale
- Sistemi informativi per la gestione economico patrimoniale
- Sistemi informativi di supporto alla ricerca
- Sistemi informativi per la gestione documentale



- Sistemi di business intelligence e di Pianificazione e Controllo
- Postazioni di lavoro per il personale amministrativo, per i laboratori informatizzati per la didattica e postazioni informatiche delle aule didattiche
- Strumenti di Office Automation per le postazioni del personale amministrativo e per i laboratori informatici
- Software didattici con licenza campus

L'Area Sistemi Informativi - ASI si occupa a livello centrale dei seguenti servizi esclusivamente per l'Amministrazione Centrale:

- File server
- Print server
- Gestione degli EndPoint (desktop, notebook, ecc.)

Il presente appalto specifico ha per oggetto servizi informatici che hanno come struttura referente l'Area Sistemi Informativi - ASI.



V - CONTESTO TECNOLOGICO DEL COMMITTENTE

Le sedi dell'Università ospitano i nodi della rete dati ed in alcune di esse sono collocati i DataCenter su cui insistono le infrastrutture di elaborazione e i sistemi di controllo e gestione dei servizi telematici di Ateneo.

Di seguito sono descritti i contesti tecnologici specifici per l'erogazione dei servizi oggetto dell'Appalto Specifico per Università degli Studi dell'Insubria.

Il contesto tecnologico può essere schematizzato nei seguenti macro ambiti:

- Datacenter e servizi in cloud
- Infrastrutture e servizi Networking, network Security e network management
- Sistemi Informativi
- Infrastrutture e servizi Data Base
- Servizi a supporto della Comunicazione Avanzata
- Servizi di Gestione EndPoint ed Assistenza Tecnica

V.1. Data Center e servizi in cloud

A seguito di una parziale esternalizzazione dei servizi di datacenter, alcuni server sono stati virtualizzati e trasferiti presso i datacenter europei di Microsoft e sono gestiti mediante la soluzione Microsoft Azure, conseguentemente l'Ateneo adotta una architettura di Cloud Ibrido.

Il servizio di posta elettronica dell'Ateneo è basato su Microsoft 365/Exchange Online e gli account di accesso al servizio sono sincronizzati fra Azure Active Directory e la directory centralizzata di Ateneo basata su Microsoft Active Directory Domain Services.

V.1.1. Data Center “Colonia”

Presso la sede “Colonia”, in Varese via Montegeneroso 71, risiede un datacenter che ospita le seguenti apparecchiature:

- HPE Proliant DL 650 Gen10 NVMe: un nodo fisico, sedici dischi e quattro interfacce di rete esterne attivate. Il server è utilizzato come illustrato di seguito:
 - o piattaforma di virtualizzazione basata su Microsoft Hyper-V 2019 per la gestione di circa 15 macchine virtuali su cui girano i seguenti:
 - sistemi operativi:
 - Linux Debian
 - Microsoft Windows Server 2019
 - applicativi e servizi:



- Microsoft Active Directory Domain Services
 - Microsoft DNS
 - Microsoft IIS + PHP
 - Microsoft File Server
 - Microsoft Print Management
 - Oracle Database 12c Standard Edition
 - Apache + PHP
 - ISC Bind - Servizi DNS
 - ISC DCCP - Servizi assegnazione dinamica indirizzi IP
 - Servizi Network Time Server (NTP)
 - FreeRadius - Servizi autenticazione di Rete
 - Nagios
 - Cacti
 - NFSen
 - RSSylog
 - Nessus
- Dispositivo NAS QNAP TS-453U-RP con circa 10TB di spazio disco con funzione di repository locale delle copie di backup dei dati e delle macchine virtuali.
- 2 Appliance per i servizi di supporto alla Rete Dati:
- 1 Controller wifi Huawei 6605-26-PWR
 - 1 appliance Infoblox 1400 dotata del sistema di Network Automation Infoblox NetMRI

V.1.2. Data Center “Valleggio”

Presso la sede “Valleggio”, in Como via Valleggio 11, risiede un datacenter che ospita le seguenti apparecchiature:

- HPE Proliant DL 650 Gen10 NVMe: un nodo fisico, sedici dischi e quattro interfacce di rete esterne attivate. Il server è utilizzato come illustrato di seguito:
 - piattaforma di virtualizzazione basata su Microsoft Hyper-V 2019 per la gestione di circa 20 macchine virtuali su cui girano i seguenti:
 - sistemi operativi:
 - Linux Debian
 - Microsoft Windows Server 2019
 - Appliance virtuali linux-based custom
 - applicativi e servizi:
 - Microsoft Active Directory Domain Services



- Microsoft DNS
 - ISC Bind - Servizi DNS
 - ISC DCCP - Servizi assegnazione dinamica indirizzi IP
 - Servizi Network Time Server (NTP)
 - FreeRadius - Servizi autenticazione di Rete
 - RSSylog
- Appliance per i servizi di supporto alla Rete Dati:
 - 1 Controller wifi Huawei AC6605-26-PWR
 - Appliance per i servizi di comunicazione H.323
 - FreeNas: espone share SMB\CIFS per uso da parte di utenti e NFS per uso da parte del registratore multimediale che memorizza i filmati registrati direttamente sulla share nfs.
 - Polycom DMA: Gatekeeper H.323, riceve le registrazioni di tutti i terminali di videoconferenza.
 - Polycom Access Director: Server per il collegamento di utenti esterni alla rete di Ateneo al sistema di videoconferenze
 - Polycom Resource Manager: Sistema di gestione degli accessi. Consente l'integrazione tra dma, access director e l'accesso da parte di utenti esterni utilizzando il software di videoconferenza Polycom Real Presence. Gestisce inoltre le licenze di tipo standard e di tipo Clariti.
 - Polycom Media Suite Gold: Registratore multimediale, con una versione del software aggiornata. Usa una singola rete ed esporta automaticamente i filmati su una share nfs impostata sul server freenas.
 - Polycom RMX virtuale: Unità multipunto virtuale per collegamenti in videoconferenza fino a 13 punti HD.
 - Polycom Media Suite Gold Backup: Registratore multimediale, con una versione del software aggiornata. Usa una singola rete ed esporta automaticamente i filmati su una share nfs impostata sul server freenas.

V.1.3. Cloud “Azure” Microsoft

L'Ateneo adotta per le proprie infrastrutture una architettura di tipo Hybrid Cloud, dove convivono infrastrutture on-premises ed infrastruttura on-cloud.

L'Ateneo ha in produzione presso i data-center Microsoft 15 server virtuali su cui girano i seguenti:

- Sistemi operativi:
 - Linux Debian
 - Microsoft Windows Server 2019
- Applicativi e servizi:
 - Microsoft Active Directory Domain Services
 - Microsoft DNS
 - Microsoft ADFS 2019
 - Microsoft SQL Server ver. 14.0.2037.2



**UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA**

Servizi System Management per
Università degli Studi dell'Insubria, per il
periodo dal 1° luglio 2022 al 30 giugno
2026, con opzione di rinnovo per
ulteriori due anni. CIG 9034264E7C –
Capitolato Speciale d'Appalto

- Microsoft Azure Active Directory Connect, per la sincronizzazione degli account di accesso della directory locale con la piattaforma Microsoft 365
- Microsoft IIS 7 .net framework 4.x
- ISC Bind (servizi DNS)



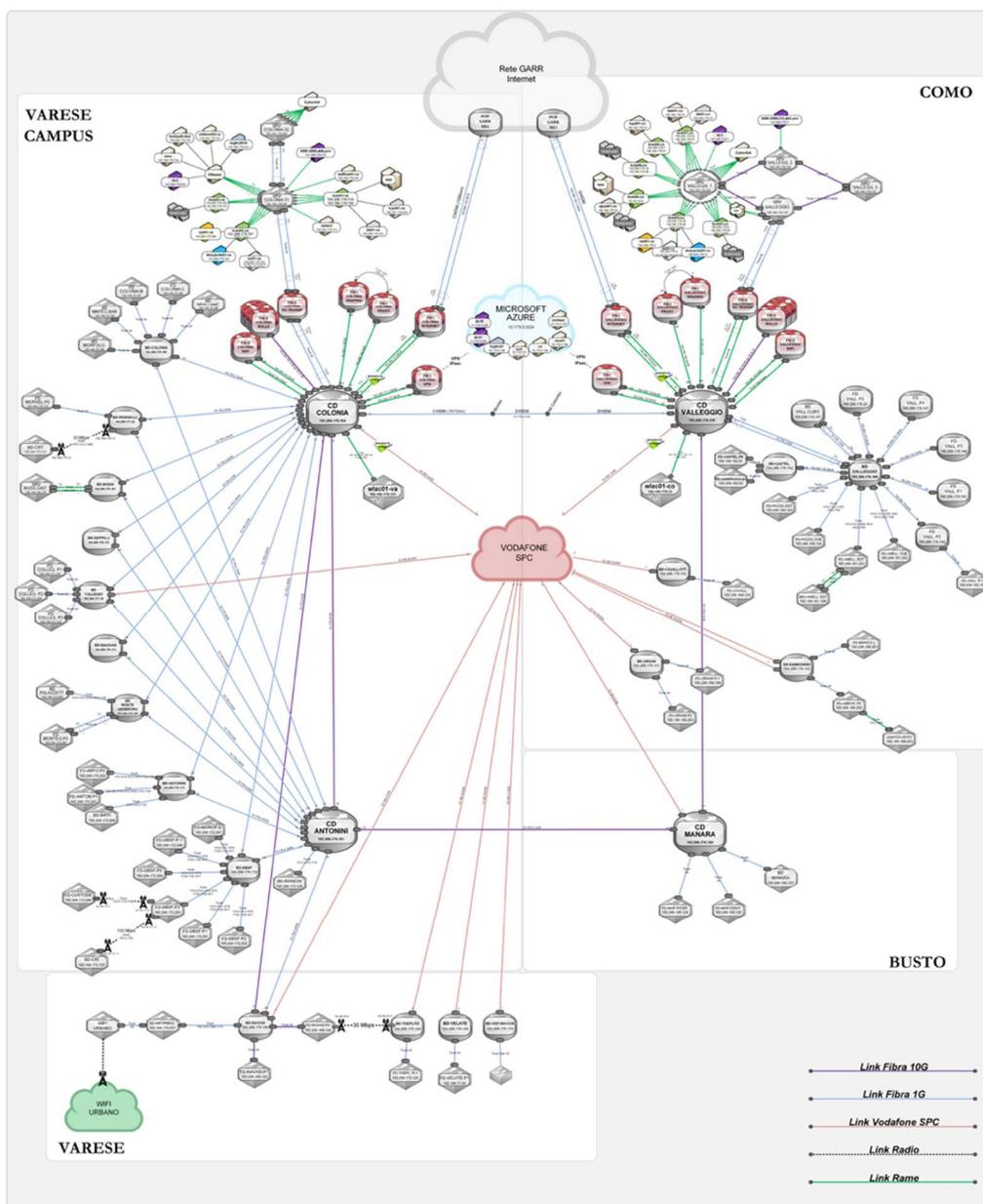
V.2. Infrastrutture e servizi di Networking, Network Security e Network Management

Questo macro ambito racchiude tutti i servizi che afferiscono strettamente alla rete dati dell'Ateneo, contemplando servizi connettività wired e wireless, i servizi core network (DNS, DHCP, Radius) ed i servizi di sicurezza di rete (firewall, IDS, UTM, gateway VPN). Di seguito vengono descritte le infrastrutture e le tecnologie specifiche di questi ambiti.

V.2.1. La Rete Dati di Ateneo

La Rete Dati di Ateneo costituisce una infrastruttura di trasmissione dati con la finalità di interconnettere dispositivi di rete all'interno dell'Ateneo e fornire a questi ultimi accessibilità alla Rete Internet. La Rete Dati di Ateneo eroga servizi di connettività alle varie strutture dell'Ateneo: Amministrazione Centrale, Dipartimenti Scuola di Medicina. Gli utilizzatori della Rete dati di Ateneo, le modalità di accesso e le regole di funzionamento sono definiti all'interno del *Regolamento per l'accesso e l'utilizzo delle infrastrutture centrali di Information e Communication Technology (ICT)* dell'Ateneo (<https://www.uninsubria.it/statuto-e-regolamenti>). L'infrastruttura di rete wired utilizza apparati di accesso allo stato dell'arte, dotati di porte Ethernet che integrano la funzionalità Power Over Ethernet per la tele alimentazione degli host che implementano tale funzionalità (Access Point, Telefoni VoIP, lettori di badge, etc.).

Graficamente, la topologia della Rete Dati di Ateneo e dei servizi di infrastruttura IT ad essa connessi, può essere così esemplificata:



Architettura Rete Dati di Ateneo

In termini architetturali, sulla rete si possono distinguere vari livelli:

Border Router e Campus Distributor

L'implementazione sul campo vede la coesistenza delle funzioni di Border Router e di Campus Distributor nei nodi di Varese 'Colonia' e Como 'Valleggio', i nodi invece di Varese 'Antonini' e Busto Arsizio svolgono solamente il ruolo di Campus Distributor. I Border Router utilizzano BGP per il routing esterno, le rotte



sono poi redistribuite in OSPF internamente (default route); le funzionalità di Campus Distributor sono implementate con routing OSPF. L'interconnessione fra i Campus distributor è realizzata in fibra ottica con backup su rete SPC Vodafone.

Building Distributor e Floor Distributor

I vari siti vedono come nodo principale il Building Distributor, l'algoritmo di routing è OSPF, l'interconnessione con i Campus Distributor è realizzata o con link in fibra ottica di proprietà o con ponti radio WiMax, ove non presenti queste tecnologie, tramite trasposto intranet sulla Rete SPC Vodafone.

Apparati di Accesso

Gli apparati di accesso implementano esclusivamente funzionalità layer 2, con segmentazione della rete tramite VLAN. L'interconnessione verso i building/floor distributor è realizzata con collegamenti in fibra ottica.

Appartiene allo strato di accesso anche l'infrastruttura WiFi, sul campo sono collocati Think AP che effettuano tunneling del traffico sino al proprio Controller WiFi Centralizzato; sono presenti 2 Controller Centralizzati (1 a Como 'Valleggio' e 1 a Varese 'Colonia').

Resilienza della Rete Dati di Ateneo

L'Architettura della Rete Dati di Ateneo è pensata in ottica di resilienza: ove possibile e significativo, i collegamenti sono realizzati in ridondanza in modo che il fault di un singolo link non pregiudichi il funzionamento dei servizi, ad esempio:

- l'accesso alla rete Internet è realizzato con 2 link di capacità equivalente, rispettivamente attestati a Varese e Como;
- l'interconnessione dei nodi geografici (backbone) è realizzata con topologia ad anello in fibra ottica (Como-Varese-Busto A. -Como) a cui si affiancano per ulteriore protezione, accessi di backup su infrastruttura Intranet SPC
- la connessione dei vari siti ai nodi di backbone è realizzata con collegamenti in fibra ottica; nel campus di Bizzozero sono disponibili 2 nodi di backbone e i principali siti sono dotati di attestazione su entrambi i nodi di Campus (bi attestazione)
- ove non presente infrastruttura in fibra ottica di proprietà o a noleggio, la connettività viene realizzata acquisendo accessi SPC Intranet, in alcuni casi l'accesso Intranet SPC svolge funzione di back up rispetto ad un link principale realizzato con tecnologia WiMax
- i servizi core network (DNS, DHCP, RADIUS), sono realizzati in modo duplicato nei siti di Varese e di Como, in modo tale che la non disponibilità di un sito non pregiudichi il funzionamento della rete
- tutte le alimentazioni elettriche degli armadi contenenti apparecchiature di rete sono protette dalla mancanza di energia da appositi sistemi UPS; inoltre, uno dei due nodi core (quello sito a Varese in via



Montegeneroso 71) dispone anche di un gruppo elettrogeno per sopperire ad eventuali interruzioni prolungate.

Sicurezza logica e fisica della Rete Dati di Ateneo

Sicurezza fisica:

Tutti gli armadi di rete ospitanti apparecchiature di rete sono dotati di serratura e, nella maggior parte dei casi, sono ospitati all'interno di locali tecnici chiusi a chiave.

L'accesso ai nodi Core di Como via Valleggio 11 e Varese via Montegeneroso 71 è ulteriormente protetto da sistema di controllo degli accessi (apertura delle porte tramite appositi badge) e sistema antintrusione con combinatore telefonico collegato alla società di vigilanza.

Ove necessario, i locali tecnici ospitanti gli apparati di trasmissione dati, sono dotati di sistemi di condizionamento per evitare il surriscaldamento delle apparecchiature.

Sicurezza logica:

La Rete Dati di Ateneo è pensata principalmente per offrire un servizio di connettività alle varie strutture dell'Ateneo che poi, a loro volta, adottano misure di sicurezza logica per proteggere i loro client ed i loro server. Ove l'accesso di rete non sia riconducibile ad una struttura definita o ad un utente identificato, le prese di rete sono configurate per offrire un set di servizi limitato (solo navigazione web) e previa autenticazione sul proxy di navigazione web.

Sono implementate reti dedicate e segregate per particolari tipologie di host:

- Centrali Telefoniche e telefoni VoIP (Sistema Telefonico di Ateneo)
- Centraline e sistemi di controllo impianti
- Access point wifi (Uninsubria Wireless)
- Laboratori informatici
- Postazioni informatiche nelle aule didattiche
- Postazioni consultazione bibliografica nelle biblioteche
- Stampanti
- Apparati Scientifici
- Apparati di videosorveglianza
- Apparati di Videoconferenza
- Rete overlay VPN IPsec per le postazioni di lavoro dell'Amministrazione Centrale (AC)
- Rete overlay VPN IPsec per le postazioni degli amministratori IT



- Reti overlay VPN Isec per le postazioni dipartimentali (7 dipartimenti)

La Rete dati di Ateneo dispone di firewall perimetrale con funzionalità Intrusion Prevention, URL filtering ed Application Control che implementano le regole di filtraggio generali e comuni a tutta la rete di Ateneo in conformità alle policy generali.

Come ulteriore strumento di protezione generale, la risoluzione dei nomi DNS da parte degli Host connessi alla rete avviene esclusivamente attraverso i resolver DNS centrali, i quali implementano anche la funzione DNS Firewall per impedire la risoluzione di nomi corrispondenti ad host ritenuti potenzialmente pericolosi in base a liste aggiornate quotidianamente da SpamHause.

La rete di accesso wifi è tipicamente utilizzata in modalità BYOD, per questo motivi tutti gli access point sono configurati in modalità tunnel mode verso i controller centrali; il traffico, prima di essere immesso nella Rete dati di Ateneo, viene analizzato tramite firewall con funzionalità Intrusion Prevention, URL filtering, Application Control e rate limiting. I controller wifi implementano la funzionalità isolation fra i client wifi in modo da inibire il traffico diretto da client a client obbligando tutti i flussi a transitare attraverso il firewall. I client wifi sono ulteriormente raggruppati in classi di utenza omogenea:

- Personale (docente e tecnico-amministrativo)
- Studenti regolarmente iscritti all'ateneo
- Personale e studenti degli enti aderenti alla federazione internazionale Eduroam (<http://www.eduroam.org/>)
- Ospiti dell'Ateneo registrati a cura del personale dell'Ateneo

L'accesso alle reti wifi avviene previa autenticazione, utilizzando come back end dei server radius, la cui autenticità è attestata tramite opportuni certificati digitali rilasciati da una Certification Authority pubblica, in base alle categorie di appartenenza:

- Personale dell'Ateneo: tutto il personale docente e tecnico-amministrativo in possesso di una identità digitale di Ateneo è abilitato ad usufruire del servizio.
- Studenti attivi: tutti gli studenti con carriera attiva, in possesso di una identità digitale di Ateneo, potranno accedere alla rete wireless.
- Ospiti: l'accesso è consentito previa registrazione sul portale Web Servizi on Line effettuata da personale strutturato dell'Ateneo. Le credenziali per accedere alla rete sono inoltrate all'indirizzo email dell'ospite indicata in sede di registrazione.
- Personale e studenti di organizzazioni aderenti ad Eduroam: l'accesso avviene con le credenziali rilasciate dalla propria organizzazione di appartenenza.

Al fine di garantire la segregazione e compartimentazione sulla Rete Dati di Ateneo, l'accesso dei client afferenti all'Amministrazione Centrale e quelli degli amministratori IT è gestito tramite una infrastruttura logica overlay VPN IPSEC, la quale ha lo scopo di mantenerli isolati ed invisibili dal resto della rete e di veicolare il traffico in uscita ed ingresso dalla rete esclusivamente tramite firewall con policy dedicate. La



navigazione web di tali client avviene esclusivamente tramite apposito security gateway che implementa policy di sicurezza sulla navigazione.

È messa a disposizione delle varie strutture dell'Ateneo (dipartimenti e scuola di Medicina), la possibilità di isolare i client per la gestione amministrativa all'interno di bolle sicure dedicate, realizzate con reti overlay IPsec -VPN.

L'accesso da remoto alla Rete dati di Ateneo è consentito solo ad una popolazione ristretta di utenti specificatamente abilitati, tramite utilizzo di accesso sicuro VPN previa autenticazione con l'account istituzionale e solo con client autorizzati.

Tutti gli apparati della Rete Dati ed i server eroganti i servizi Network Core, sono costantemente scansionati con cadenza settimanale con il vulnerability scanner Nessus, i relativi report vengono verificati e, ove possibile, attuate misure correttive per la risoluzione delle vulnerabilità riscontrate.

Il firmware degli apparati della Rete Dati viene costantemente aggiornato qualora fossero note delle vulnerabilità o problemi di sicurezza nelle versioni in uso.

I server eroganti i servizi Network core sono configurati per installare in modo automatico gli aggiornamenti di sicurezza relativi al sistema operativo ed ai servizi installati.

L'accesso remoto agli apparati della Rete Dati è protetto da password, esclusivamente con protocolli sicuri (SSH ed HTTPS) ed esclusivamente attraverso il gateway di accesso sicuro per gli amministratori di sistema (CyberArc) che svolge anche funzione di raccolta dei log degli Amministratori di Sistema e piattaforma di auditing. Eccezionalmente, in caso di non disponibilità della piattaforma CyberArc, l'accesso è possibile anche in modalità diretta dai client 'fidati', ossia i client appartenenti alla bolla overlay IPsec dei tecnici IT.

Le password di accesso agli apparati della Rete Dati di Ateneo ed ai server che erogano i servizi network core, rispettano criteri di complessità e sono soggette a policy di rotazioni a scadenze definite tramite la gestione centralizzata ed automatizzata resa possibile dall'infrastruttura di accesso remoto sicuro CyberArc.

Gestione della Rete Dati di Ateneo

La gestione della Rete Dati di Ateneo è effettuata esclusivamente con l'utilizzo di personale specializzato a cui è stato conferito apposito incarico di Amministratore di Sistema e di "autorizzato al trattamento" dei dati.

Come detto in precedenza, l'accesso ai vari apparati e server da parte degli Amministratori di Sistema avviene tramite l'infrastruttura CyberArc, la quale si occupa di gestire in modo centralizzato le policy di complessità e rotazione delle password nonché del log di auditing delle attività degli amministratori di sistema. La stessa piattaforma è utilizzata anche per fornire accesso ai tecnici delle società di manutenzione incaricate, fornendo così accesso circoscritto alle sole risorse pertinenti e senza che terzi vengano a conoscenza delle reali credenziali con permessi di amministrazione sui device.

Monitoraggio Centralizzato

I server per il monitoraggio centralizzato e la raccolta dati sono:



- netmon.uninsubria.it (Varese) Server Linux Debian con web server Apache, su cui sono installati i seguenti servizi:
 - Nagios - monitoraggio ed allarmistica su disponibilità apparati e servizi
 - Cacti - raccolta storica dati di traffico, latenza, carico, temperatura, etc. per i vari device della Rete Dati
- netflow01-va.uninsubria.it (Varese) Server Linux Debian con web server Apache, su cui è installato il servizio Nfsen - raccolta flussi di comunicazione netflow
- logtlc.uninsubria.it (Varese) Server Linux Debian, su cui è installato il servizio rsyslog di raccolta syslog provenienti da apparati di rete e server

I syslog raccolti centralmente ed i log generati dai singoli server sono memorizzati localmente con una retention di 1 mese ai soli scopi di troubleshooting, mentre i log conservati per eventuali istanze dell'autorità giudiziaria vengono inviati alla piattaforma Microsoft Log Analytics tramite appositi agent installati sui server; la conservazione dei log su Azure ha una retention di 12 mesi.

I log raccolti dagli apparati firewall (Fortigate) sono raccolti dal sistema centralizzato Forti Analyzer.

I sistemi Nagios e Cacti integrano meccanismi di verifica della disponibilità dei servizi e di carico delle linee e delle risorse hw, di valori ambientali dei siti ospitanti le infrastrutture, ed inviano e-mail automatiche di alert a fronte di host o servizi non disponibili o di superamento di soglie di attenzione.

Network Automation

Sempre al livello centrale è in uso il sistema Infoblox NetMRI con funzionalità di network automation & control, in particolare, il sistema consente l'inventario dei device di rete, il monitoraggio dello stato di occupazione delle porte utente della rete di accesso, la raccolta del trap di eventi di sicurezza degli apparati, il salvataggio e la storicizzazione delle configurazioni di tutti gli apparati della Rete dati di Ateneo.

V.2.2. Rete Dati di Ateneo – servizi di connettività wired

La Rete Dati di Ateneo costituisce l'infrastruttura di trasmissione dati dell'Ateneo. L'infrastruttura è incentrata su una infrastruttura RAN (Regional Area Network) realizzata con collegamenti in fibra ottica dedicata.

L'interconnessione a Internet avviene tramite la Rete nazionale dell'Università e della Ricerca gestita dal Consortium GARR (www.garr.it), tramite 2 collegamenti dedicati, il principale nella sede di Varese via Montegenero 71 (Colonia) ed il secondario dalla sede di Como via Valleggio 11 (Valleggio); attualmente l'Ateneo è connesso alla rete GARR-X con due collegamenti una capacità di banda pari ciascuno a 2 Gbps, in fase di upgrade a due collegamenti ciascuno con capacità 10 Gbps sulla nuova rete GARR-T.

La maggior parte delle sedi dell'Ateneo (collocate nelle città di Como, Varese e Busto Arsizio) sono interconnesse fra loro tramite infrastrutture di trasmissione dati gestite direttamente dall'Ateneo (collegamenti in fibra ottica). Sono presenti anche 4 ponti radio con tecnologia WiMax/AirMax, per collegare i siti di:

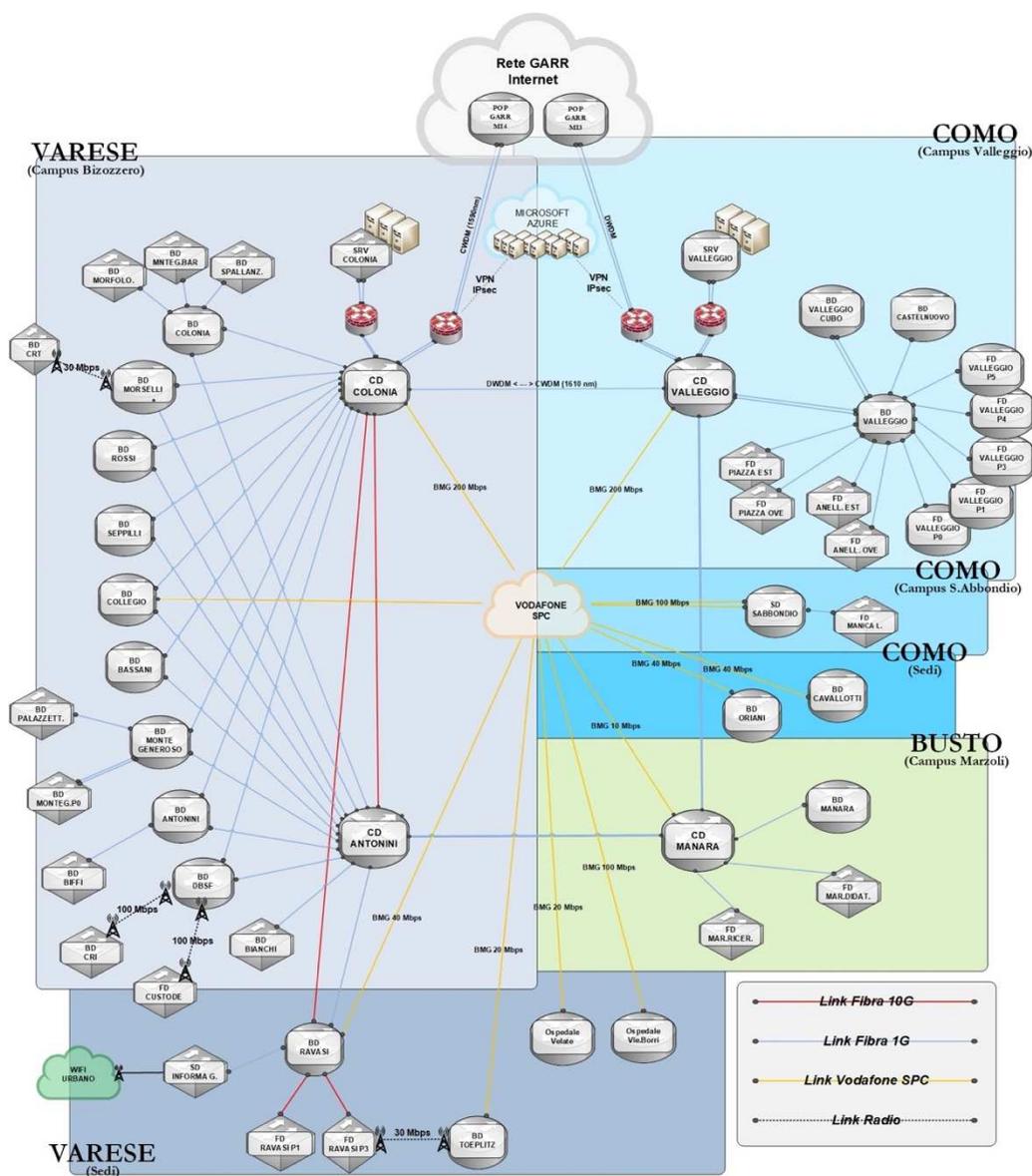
- Villa Toeplitz dalla sede 'Ravasi' a Varese (WiMax)



- Padiglione CRT dalla sede 'Antonini' a Varese (WiMax)
- Sede CRI da Sede DBSF (AirMax)
- Palazzina Custode DBSF dalla sede DBSF (AirMax)

Alle infrastrutture dell'Ateneo si affiancano i servizi di trasmissione dati tramite Intranet del Servizio Pubblico di Connettività (SPC), per collegare le sedi non raggiunte da infrastrutture dell'Ateneo (stub) e per implementare servizi di connettività di backup (bi-attestate).

Schematicamente, la macrostruttura della Rete di Ateneo può essere così rappresentata:





Rete Dati di Ateneo – infrastrutture fisiche passive

Le infrastrutture fisiche passive, la loro realizzazione, gestione e manutenzione, non sono oggetto dei servizi del presente appalto specifico; vengono di seguito descritte esclusivamente per offrire un quadro informativo completo all'impresa offerente.

Tutti gli edifici dell'Ateneo sono dotati di impianti di cablaggio strutturato a standard ISO/IEC 11801 UTP cat.5e e cat.6 per realizzare le infrastrutture di accesso attestata in appositi armadi rack. L'interconnessione dei vari armadi rack, ove possibile, è realizzata tramite cavi in fibra ottica monomodale (9/125 um) o multimodale (50/125 um).

I singoli punti di concentrazione delle infrastrutture fisiche della Rete dati di Ateneo, sono organizzati gerarchicamente in Campus Distributor, Building Distributor e Floor Distributor.

- *Floor Distributor*: contiene le attestazioni del cablaggio strutturato di piano e dei cavi in fibra ottica e rame che lo collegano al Building Distributor; contiene altresì gli apparati di trasmissione dati di piano.
- *Building Distributor*: contiene le attestazioni del cablaggio strutturato del piano o dell'edificio in cui si trova, le attestazioni dei cavi in fibra ottica che collegano i floor distributor se presenti, i cavi in fibra ottica e rame che lo collegano al Campus Distributor se presente; contiene altresì gli apparati di trasmissione dati, la centrale telefonica se presente e gli apparati attivi e passivi dei Carrier (Telecom Italia, Fast Web, Vodafone, etc) se presenti.
- *Campus Distributor*: contiene le attestazioni del cablaggio strutturato del piano o dell'edificio in cui si trova, le attestazioni dei cavi in fibra ottica che collegano i floor distributor se presenti, le attestazioni dei cavi in rame e fibra ottica che lo collegano ai Building Distributor del Campus, i cavi in fibra ottica per i collegamenti geografici; contiene altresì gli apparati di trasmissione dati, la centrale telefonica se presente e gli apparati attivi e passivi dei Carrier (Telecom Italia, Fast Web, Vodafone, etc.) se presenti.

Rete Dati di Ateneo – infrastrutture fisiche attive

La messa in servizio, configurazione e gestione degli apparati attivi di trasmissione dati (switch e router) è oggetto dei servizi richiesti nel presente appalto specifico; il personale del fornitore affiancherà il personale tecnico dell'Ateneo nelle attività di messa in esercizio, configurazione e gestione degli apparati switch e router afferenti alla rete dell'Ateneo.

Gli apparati di trasmissione dati afferenti alla Rete Dati di Ateneo sono organizzati a livello gerarchico.

Apparti di Accesso: la rete di accesso è realizzata tramite apparati switch di tipo stand alone, stackable e chassis a seconda dei casi; attualmente gli apparati in uso appartengono alle seguenti famiglie di prodotti:

- Switch Cisco Catalyst 3650
- Switch Cisco Catalyst 2960
- Switch Cisco Catalyst 1000

Gli apparati di accesso, per alcune network specifiche, implementano configurazioni per l'autenticazione IEEE 802.1x basata su back end Radius.



Nel corso di validità dell'appalto, l'Ateneo potrebbe acquisire apparati di Vendor e tipologie differenti rispetto a quelle sopra elencate, anche in base alla tipologia di prodotti messe a disposizione nelle specifiche Convenzioni Consip.

Apparati di Core di Edificio: gli apparati di core di edificio, oltre ad implementare le funzionalità layer 2 (Ethernet), implementano anche funzioni layer 3 e 4 (Routing OSPF ed Access list); attualmente gli apparati in uso a livello di core di edificio appartengono alle seguenti famiglie:

- Switch router Cisco Catalyst 3600x e 3650

Apparati di Core di Campus: gli apparati di core di campus implementano funzioni layer 3 e 4 (Routing OSPF, iBGP ed Access list); attualmente gli apparati in uso a livello di core di edificio appartengono alle seguenti famiglie:

- Switch router Cisco Catalyst 3850
- Switch router Cisco Nexus serie 7000

Apparati Border Router: le interfaccie fra la rete dell'Ateneo e la rete Internet (attraverso la rete del Consortium GARR) implementano funzioni layer 3 e 4 (Routing OSPF, eBGP ed Access list); attualmente gli apparati in uso a livello di core di edificio appartengono alle seguenti famiglie:

- Switch router Cisco Nexus serie 7000

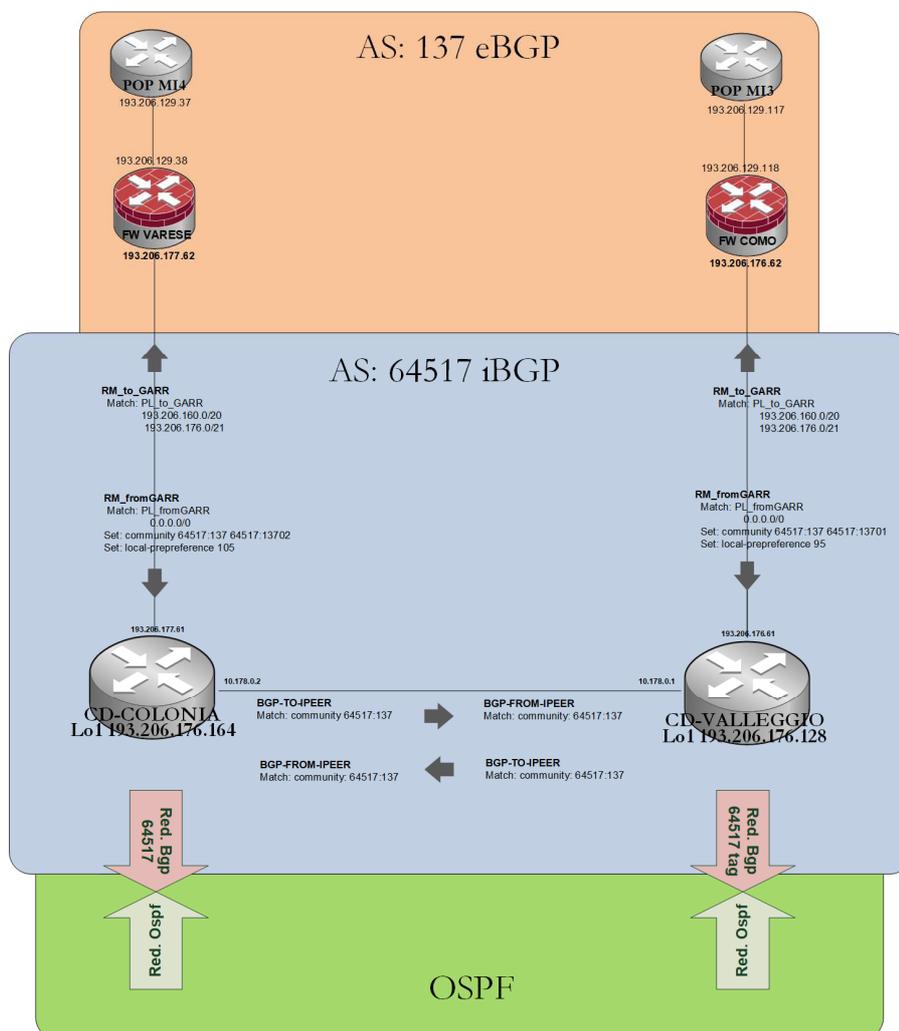
Rete Dati di Ateneo – architettura logica ed indirizzamento IP

Nel sito di Varese vi sono 2 nodi dell'anello geografico di backbone in fibra ottica: nella sede 'Colonia' (sita in via Montegeneroso 71 in Varese) e nella sede 'Antonini' (sita in Viale O. Rossi 9 in Varese). Presso la sede 'Colonia' è presente il datacenter di cui all'Articolo V.1.1 che, fra gli altri, ospita anche gli apparati che erogano i servizi di network (DNS, DHCP, PROXY, RADIUS). La sede 'Colonia' costituisce il centro stella del campus di 'Bizzozero' da cui si diramano sia i collegamenti in fibra ottica verso i vari edifici del campus stesso, sia l'accesso principale ad Internet attraverso la rete del Consortium GARR; la sede 'Antonini' svolge il ruolo di centro stella di back up del Campus di Bizzozero.

Presso la sede di Como 'Valleggio' sono presenti sia la sala server che ospita gli apparati che erogano i servizi di network (DNS, DHCP, PROXY, RADIUS) descritta all'Articolo V.1.2, sia l'accesso secondario ad Internet attraverso la rete del Consortium GARR.

Sulla rete dell'Ateneo è utilizzato il protocollo BGP esclusivamente verso l'esterno, ossia verso la rete del Consortium GARR, è stato configurato un AS privato e sono in essere peering con il Consortium GARR nei punti di raccolta del traffico di Valleggio e Colonia.

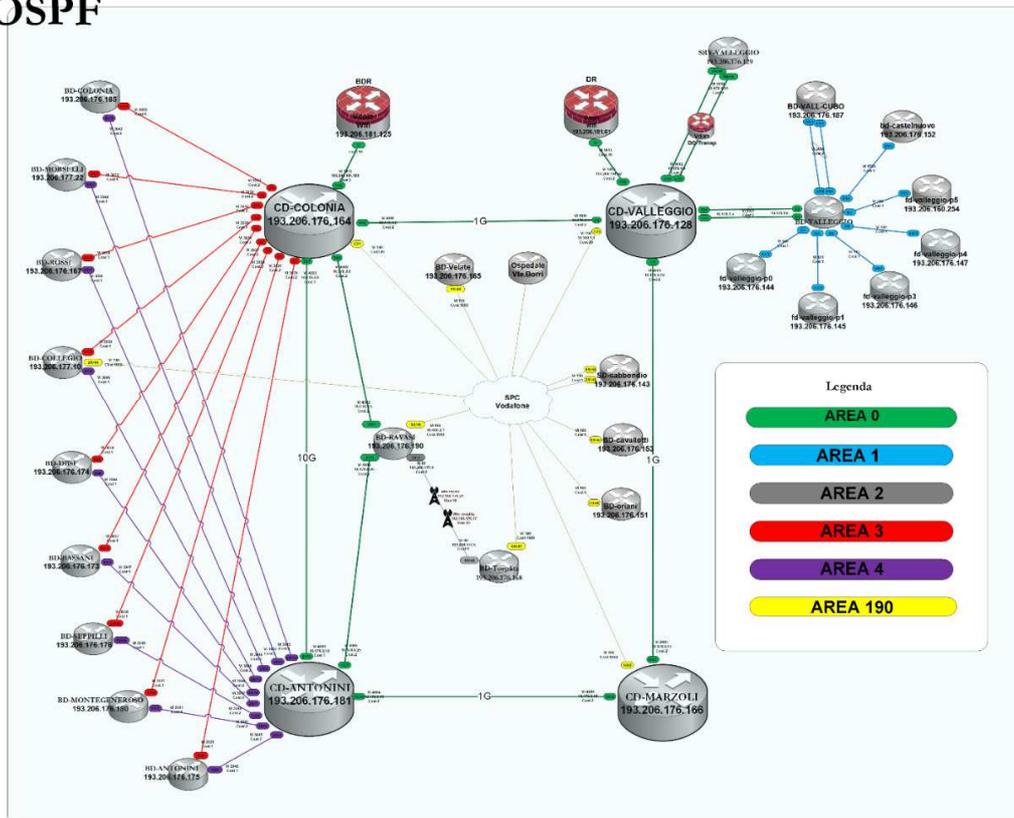
Inoltre, è attivo iBGP fra i nodi di backbone di Colonia e Valleggio.



Il protocollo di routing interno è invece OSPF, sono configurate 6 aree, rispettivamente:

- Area 0: nodi di backbone e nodi building distributor connessi attraverso intranet SPC
- Area 1: nodi building e floor distributor afferenti al campus distributor 'Valleggio'
- Area 2: nodi building e floor distributor afferenti al campus distributor 'Ravasi'
- Area 3: nodi building e floor distributor afferenti al campus distributor 'Colonia'
- Area 4: nodi building e floor distributor afferenti al campus distributor 'Antonini'
- Area 190: routing verso CPE SPC (Vodafone)

OSPF



Il trasporto interno sulla Rete dell'Ateneo è basato su instradamento dinamico dei pacchetti con il protocollo OSPF. Le politiche di gestione del traffico sono prevalentemente di tipo best effort, ad eccezione dei flussi VoIP e di Videoconferenza su IP, per le quali si applicano politiche di QoS sui link trasmissivi più congestionati.

L'indirizzamento è esclusivamente IPv4, sono in uso 20 Classi C oltre a reti con indirizzamento privato conforme alle RFC.

Le reti ad indirizzamento privato sono usate prevalentemente per:

- Laboratori informatici
- Reti wifi
- Stampanti
- Telefoni VoIP
- Apparati IoT
- Server che non espongono servizi all'esterno

L'allocazione di indirizzi privati è univoca su tutta la rete e tali network sono ruotate internamente.



Le reti ad indirizzamento pubblico sono principalmente usate per:

- Apparati server
- Postazioni di lavoro personali

La distribuzione degli indirizzi IP appartenenti alle classi di indirizzi di cui sopra avviene dinamicamente tramite due server DHCP ospitati rispettivamente il primo nel data center della sede 'Valleggio' a Como e il secondo nel data center della sede 'Colonia' a Varese, configurati in modalità fail over.

I server DHCP rilasciano indirizzi IP, sulle reti wired, esclusivamente a host 'noti', registrati nel sistema di provisioning interno delle utenze (SIC On Line: <http://w3.ateneo.uninsubria.it/sol>)

Gli indirizzi IP statici sono configurati esclusivamente su macchine di classe server. L'assegnazione di indirizzi statici per altre tipologie di host è gestita mediante i server DHCP con apposite reservation.

La maggior parte delle sedi dell'Ateneo (collocate nelle città di Como, Varese e Busto Arsizio) sono interconnesse fra loro tramite infrastrutture di trasmissione dati gestite direttamente dall'Ateneo (collegamenti in fibra ottica e link wireless WiMax); alle infrastrutture dell'Ateneo si affiancano i servizi di trasmissione dati tramite Intranet del Servizio Pubblico di Connettività (SPC), per collegare le sedi non raggiunte da infrastrutture dell'Ateneo (stub) e per implementare servizi di connettività di backup (bi-attestate).

Per le sedi non raggiunte dal backbone geografico o dai collegamenti di campus, l'interconnessione alla Rete di Ateneo è tramite link Intranet su rete SPC. L'architettura è trasparente per la rete dell'Ateneo in quanto incapsula e trasporta il routing OSPF interno dell'Ateneo; l'infrastruttura SPC svolge anche il ruolo di backup ai collegamenti principali in fibra ottica. I siti di Valleggio e Colonia sono i punti di raccolta del traffico dei siti raggiunti dalla 'intranet' SPC.

L'infrastruttura SPC è utilizzata in modalità INTRANET come servizi di connettività esclusiva nelle sedi STUB e come connettività di backup alternativa alle connessioni rea-lizzate con infrastrutture dell'Ateneo in tutte le altre sedi.

Conseguentemente, le sedi servite da rete SPC possono essere classificate in 3 categorie:

- Sedi CORE
- Sedi BI-ATTESTATE
- Sedi STUB

L'accesso della Rete di Insubria con il General Internet è realizzato esclusivamente tramite la rete GARR. Attualmente, l'accesso GARR è realizzato con tecnologia CWDM presso la sede di Varese via Montegenerso 71 (Colonia) con attestazione sul POP di Milano Bovisa (sito in via Lambruschini 4a in Milano) presso il Politecnico di Milano e ridondato presso la sede di via Valleggio con attestazione sul POP di Milano Colombo (presso la sede sono ospitati anche gli apparati DWDM di GARR).

V.2.3. Rete Dati di Ateneo – servizi di connettività wireless



Presso la totalità degli edifici dell'Università è presente una copertura totale o parziale con servizio di accesso wifi alla rete dati di Ateneo. La popolazione di utenti del servizio è raggruppata nelle seguenti categorie:

- Personale (docente e tecnico-amministrativo)
- Studenti con carriera attiva
- Personale e studenti degli enti aderenti alla federazione internazionale Eduroam (<http://www.eduroam.org/>)
- Ospiti dell'Ateneo registrati a cura del personale dell'Ateneo

L'accesso alle reti wifi avviene previa autenticazione. Il rilascio delle credenziali è differenziato in base alle categorie di appartenenza:

- Personale dell'Ateneo: tutto il personale docente e tecnico-amministrativo in possesso delle credenziali del dominio Ateneo è abilitato ad usufruire del servizio; per costoro, le credenziali usate per accedere alla posta elettronica sono valide anche per l'accesso alla rete wireless.
- Studenti attivi: tutti gli studenti con carriera attiva, possono accedere alla rete wireless utilizzando le stesse credenziali di accesso impiegate per accedere ai servizi web di Segreteria Studenti.
- Ospiti: l'accesso è consentito previa registrazione sul portale Web Servizi on Line effettuata da personale strutturato dell'Ateneo. Le credenziali per accedere alla rete sono inoltrate all'indirizzo e-mail dell'ospite indicata in sede di registrazione.
- Personale e studenti di organizzazioni aderenti ad Eduroam: l'accesso avviene con le credenziali rilasciate dalla propria organizzazione di appartenenza.

I servizi disponibili tramite rete wifi, sono differenziati in funzione dell'utenza:

- Personale dell'Ateneo: viene offerta una gamma di servizi analoga a quella disponibile attraverso la rete cablata.
- Studenti: i servizi disponibili sono HTTP, HTTPS, POP3S, IMAPS, SMTP START-TLS ed SSH
- Ospiti: i servizi disponibili sono HTTP, HTTPS ed SSH
- Personale e studenti di organizzazioni aderenti ad Eduroam: i servizi erogati sono quelli definiti dal regolamento della federazione Eduroam: IPsec VPN; OpenVPN; IPv6 Tunnel; IPsec NAT-Traversal; Cisco IPsec VPN; PPTP VPN; SSH; http; HTTPS; IMAP4; IMAPS; IMAP3; POP3; POP3S; (S)FTP passivo; SMTPS; SMTP via STARTTLS; RDP.

Interfacciamento fisico delle infrastrutture wifi

L'architettura wifi dell'Ateneo è basata su una tecnologia Light Weight AP ad incapsulamento CAPWAP con la soluzione WiFi di Huawei, dove ogni singola antenna instaura un tunnel verso il suo controller di riferimento entro cui veicola il traffico raccolto dagli SSID configurati su di essa.

I controller centralizzati sono 2, collocati uno a Varese ed uno a Como (Huawei AC 6605-26-PWR).

Gli Access Point in uso sono complessivamente 350 (di cui 35 outdoor) delle tipologie Huawei AP8150DN, AP6150DN e AP5130DN.



Le configurazioni sono distribuite ai singoli AP dai controller centralizzati, i singoli AP sanno quali controller contattare tramite apposita opzione del DHCP o tramite risoluzione DNS (Opzione Vendor Class (DHCP) e WLAN-SWITCH (DNS)).

Centralmente si gestiscono i canali usati dagli AP, la potenza del segnale, gli SSID e le politiche di autenticazione.

L'infrastruttura è organizzata in modo tale che ogni AP abbia 2 controller di riferimento (uno a Varese e l'altro a Como o viceversa) in modo tale che in caso di non disponibilità di un controller, l'AP si associa all'altro.

Il traffico raccolto dai singoli AP viene trasportato in un tunnel sino al controller di riferimento, dopo di che uscirà in chiaro sulla rete diretto verso i gateway che sono costituiti da firewall Fortinet Fortigate; dopo l'applicazione delle policy previste, il traffico viene veicolato sulla Rete Dati di Ateneo.

Implementazioni SSID sul wifi

Come detto in precedenza, gli accessi sono differenziati per tipologia di utenza; per questo motivo sono stati usati SSID distinti:

- Personale dell'Ateneo: SSID 'insubria-ateneo-full' -> accesso modalità WPA2 Enterprise autenticazione EAP-PEAP MSChapV2
- Studenti: SSID 'insubria-campus-studenti' -> accesso modalità WPA2 Enterprise autenticazione EAP-PEAP MSChapV2
- Ospiti: SSID 'insubria-ospiti' -> accesso modalità WPA-personal ed autenticazione con captive portal
- Personale e studenti di organizzazioni aderenti ad Eduroam: SSID 'eduroam' -> accesso modalità WPA2 Enterprise autenticazione EAP-PEAP MSChapV2.

Ciascun SSID è associato ad una distinta network, e quindi una VLAN distinta.

L'assegnazione degli indirizzi IP è effettuata dai server DHCP dell'Università., Sugli apparati di accesso sono configurati gli helper address con i 2 indirizzi i IP dei server DHCP dell'Ateneo (in failover tra di loro).

Il traffico degli host wifi che stanno su reti con indirizzamento privato, viene poi trattato con NAT dai firewall Fortigate su pool di indirizzi su cui viene nattato il traffico.

L'applicazione delle policy a livello network e a livello applicativo è gestita dall'Università, per questo il Gateway delle network sopra citate sarà costituito dai firewall dedicati ai servizi wifi, i quali applicheranno le policy sui servizi abilitati, l'URL filtering ed il traffic shaping, oltre a nattare i flussi in uscita su un pool di indirizzi IP pubblici.

Servizi di autenticazione per l'accesso alle reti wifi

L'accesso alle reti wifi avviene previa autenticazione. Il protocollo di autenticazione utilizzato è radius, così riassumibile:

- Servizio radius per autenticazione Ospiti dell'Ateneo, utilizzato per accesso al wifi con captive portal,



è erogato direttamente dai server Linux con demone FreeRadius, si appoggiano sul DBMS Sql;

- Servizio radius EAP per autenticazione personale e studenti dell'Ateneo, utilizzato per accesso alla rete wifi, le sessioni EAP sono terminate dai demoni FreeRadius su Linux, che a loro volta interrogano i server Active Directory dell'Ateneo con protocollo LDAPS;
- Servizio radius proxy per IdP Eduroam, il demone FreeRadius proxa le richieste di autenticazione ricevute dal radius server di GARR, girandole al server radius interno di pertinenza a seconda del realm di appartenenza (studenti o personale);
- Servizio radius proxy per Service Provider Eduroam, inoltre le richieste di autenticazione della rete Eduroam verso il radius proxy di GARR.

V.2.4. Rete Dati di Ateneo – servizi di network security

Firewall Esterni: sulla frontiera fra la Rete di Ateneo e la rete Internet (collegamento verso la rete GARR) sono attivi 2 dispositivi UTM con funzionalità di firewall, application control, URL filtering ed IPS, attualmente forniti in modalità as a service all'interno dell'Accordo Quadro SPC Cloud Lotto 2, e collocati rispettivamente uno nel data center di Varese Colonia ed il secondo in quello di Como Valleggio.

I Firewall Esterni sono realizzati 2 con apparati Fortigate di Fortinet, implementano le policy di sicurezza (statefull firewall, application control, URL filtering ed IPS, traffic shaping) da e verso il Generali Internet, implementano le funzionalità di NAT, il secure web gateway per la navigazione Internet, ed il gateway VPN SSL.

Firewall Interni: presso i data center di Varese Colonia ed di Como Valleggio sono presenti complessivamente 2 firewall Fortigate di Fortinet che implementano le policy di sicurezza (statefull firewall ed IPS) per reti di data center, le policy di sicurezza (statefull firewall ed IPS) per le reti di accesso wifi (BYOD), i gateway di accesso VPN IPsec per le reti overlay cifrate per la segregazione dei client 'sensibili' dal resto della rete accademica focalizzata su esigenze di didattica e ricerca.

Sistema di raccolta log: i Firewall Fortigate sono interfacciati con il sistema di raccolta log FortiAnalyzer di Fortinet con lo scopo di raccogliere e analizzare centralmente i log prodotti dai sistemi Fortinet, ulteriore copia dei log viene inviata sul cloud Microsoft per la conservazione ai fini giudiziari.

Sistema di gestione dei client VPN: i client dotati di accesso VPN hanno a bordo il software specifico FortiClient di Fortinet, la gestione centralizzata delle configurazioni e delle abilitazioni dei client viene effettuata tramite il software Forticlient Enterprise Management Server– EMS di Fortinet.

Sistema DNS Firewall: al fine di inibire la risoluzione di URL dannose (siti compromessi, BOT Net, etc.) è in uso la specifica funzionalità DNS Firewall di BIND alimentata con i feed rilasciati da SpamHause.

Sistema di Vulnerability Scan: al fine di identificare eventuali vulnerabilità presenti sui sistemi 'sensibili' collegati alla Rete Dati di Ateneo, con cadenza settimanale vengono effettuate scansioni di vulnerabilità con l'utilizzo del software specifico Nessus di Tenable.



V.2.5. Rete Dati di Ateneo – servizi di accesso da remoto/VPN

Accesso VPN SSL Client to Site: il servizio SSL VPN client to site, permette la connessione da remoto principalmente degli host di docenti e ricercatori, l'accesso da remoto avviene tramite tunnel cifrato SSL, con accesso con autenticazione utente basato su credenziali del dominio di autenticazione di Ateneo e contestuale autenticazione utente tramite verifica del certificato X.509 caricato negli host. Il gateway VPN SSL è attestato sui firewall di frontiera.

Accesso VPN IPsec Client to Site: il servizio VPN IPsec client to site, permette la connessione da remoto principalmente degli host del personale di staff, l'accesso da remoto avviene tramite tunnel cifrato IPsec, con accesso con autenticazione utente basato su credenziali del dominio di autenticazione di Ateneo e l'abilitazione del client avviene attraverso la piattaforma centralizzata Forticlient Enterprise Management Server– EMS di Fortinet. Il gateway VPN IPsec è attestato sui firewall interni.

Accesso VPN IpSec Site to Site è invece utilizzato per estendere la intranet verso l'ambiente Cloud Microsoft Azure che ospita parte dei servizi informatici di Ateneo in modalità IaaS.

Entrambe le soluzioni, VPS SSL client to site e VPN IpSec site to site, sono implementate in modalità ridondata per il failover fra Varese e Como. I gateway VPN Ipsec site-to-site sono attestati sui firewall di frontiera.

V.2.6. Rete Dati di Ateneo – servizi di connettività cloud

L'Ateneo adotta per le proprie infrastrutture una architettura di tipo Hybrid Cloud, dove convivono infrastrutture on-premises ed infrastruttura on-cloud.

La Rete Dati di Ateneo si estende logicamente nell'infrastruttura IaaS private cloud Microsoft Azure grazie ad un collegamento dedicato VPN site-to-site.

L'infrastruttura IaaS è attestata su apposite VNET accessibili dalla Rete Dati di Ateneo attraverso il tunnel VPN, mentre la visibilità dal General Internet avviene direttamente dai data center Microsoft su indirizzamento pubblico assegnato da Microsoft.

I servizi di connettività cloud si occupano di gestire la raggiungibilità dell'infrastruttura IaaS dalla Rete Dati di Ateneo, le regole di routing e la segregazione delle Vlan.

Sono inoltre gestite le policy di sicurezza a livello network, quali i Network security group, i network firewall e gli application firewall.

V.2.7. Rete Dati di Ateneo – Servizi back end Network Authentication

I servizi back end di Network Authentication non sono oggetto dei servizi obbligatori della fornitura, il supporto specialistico per questi sistemi è parte dei servizi migliorativi che l'OEA può prevedere nella formulazione della propria offerta tecnica.



Il servizio di autenticazione di rete per l'accesso alla rete wifi, prese di rete ad accesso 'pubblico' e le postazioni dei laboratori informatici, è implementato tramite back end Radius. Il servizio di autenticazione Radius è realizzato utilizzando il pacchetto open source Free Radius installato in ambiente Linux Debian.

In termini architetturali, il servizio è implementato in modalità ridondata tramite 2 server rispettivamente collocati a Varese e Como.

La tipologia di utenze è raggruppabile in tre insiemi omogenei: personale, studenti ed ospiti. Il back end di autenticazione per personale e studenti è costituito da server Microsoft Active Directory interrogati con protocollo LDAPS, il back end per gli ospiti è un Data Base Microsoft SQL Server.

I due server Free Radius di Varese e Como, oltre a ospitare le istanze del demone Radius per l'autenticazione di personale, ospiti e studenti, gestiscono (sempre in logica duplicata fra Varese e Como) le istanze per l'Identity Provider e il Service provider dei servizi di autenticazione federati Eduroam per l'accesso alla rete wifi di Ateneo (www.eduroam.org).

V.2.8. Rete Dati di Ateneo – Servizi di network core, DNS, DHCP, NTP

I servizi di network core, DNS, DHCP, NTP non sono oggetto dei servizi obbligatori della fornitura, il supporto specialistico per questi sistemi è parte dei servizi migliorativi che l'OEAE può prevedere nella formulazione della propria offerta tecnica.

La Rete Dati dell'Ateneo utilizza l'assegnazione dinamica degli indirizzi IP. Il servizio è implementato attraverso 2 server DHCP (collocati rispettivamente a Varese con una macchina virtuale e a Como su una macchina fisica) in modalità 'pool fail over'; la piattaforma software utilizzata è ISC DHCP il cui demone è installato su sistema operativo Linux Debian.

I servizi di risoluzione dei nomi a dominio (DNS) sono suddivisi in 2 ambiti distinti: il DNS autoritativo per i domini uninsubria.it e uninsubria.eu e il servizio di resolver DNS per gli Host della rete di Ateneo. Il servizio DNS autoritativo è realizzato con il pacchetto software ISC Bind in ambiente Linux Debian, i server in esercizio sono 3, uno a Varese, uno a Como ed uno su private Cloud Microsoft Azure. Il servizio DNS resolver (o DNS cache) per gli host della rete di Ateneo, è implementato tramite 2 server, uno a Varese ed uno a Como; oltre alla funzionalità DNS Cache, è implementata anche la funzionalità di sicurezza 'DNS Firewall' per la protezione verso URL contenenti minacce per la sicurezza informatica. I DNS Cache si occupano anche di filtrare le URL dei siti per il gioco d'azzardo illegale, come disposto da AAMS (<http://www.servizi.garr.it/garr-nic/filtri-aams>).

Ulteriore servizio di core, è il servizio NTP, anch'esso erogato in modalità ridondata da due server Linux collocati rispettivamente a Varese e Como.

V.3. Sistema Telefonico di Ateneo

Il Sistema Telefonico dell'Ateneo è costituito dall'insieme dell'infrastruttura composta dalle centrali telefoniche, apparecchi telefonici ed interfacce verso gli operatori telefonici pubblici (rete PSTN).



Le centrali telefoniche che costituiscono il Sistema Telefonico dell'Ateneo non sono parte dei servizi richiesti nell'appalto oggetto del presente capitolato. Vengono però brevemente descritte in quanto i servizi telefonici sono erogati in modalità VoIP, per cui, la comunicazione fra le singole centrali e da e per i singoli derivati telefonici avviene esclusivamente con protocolli IP. Sia le centrali telefoniche che i telefoni sono, a tutti gli effetti, utilizzatori della Rete Dati di Ateneo descritta nell'articolo precedente.

Centrali Telefoniche

Il network del Sistema Telefonico di Ateneo è composto da 10 Centrali Telefoniche Alcatel OmiPC. I terminali utente sono principalmente di tipo VoIP, con un piccolo numero di utenze FAX direttamente attestate sulle centrali telefoniche.

Anche l'architettura delle centrali telefoniche è configurata con criteri di resilienza: il nodo master è ospitato presso la sede di Como via Valleggio 11 e realizzato con un cluster costituito da 2 centrali Alcatel OmniPCX. In caso di fault del sito master, subentrano i siti locali di backup costituiti da installazioni singole di centrali telefoniche Alcatel OmniPCX presenti nelle sedi:

- Varese via Ravasi 2
- Varese viale O.Rossi 9 (pad. Antonini)
- Varese via Dunat 3
- Varese via Dunant 7 (Collegio Cattaneo)
- Varese via Montegeneroso 71
- Varese via Vico 34 (Villa Toeplitz)
- Como via Bossi 5 (Oriani)
- Como via Teodolinda (S.Abbondio)
- Busto A. via Manara 14 (Villa Manara)

Terminali Telefonici:

I terminali telefoni utente sono di varie tipologie:

- Telefoni VoIP top: telefoni Alcatel-Lucent 8078s Premium DeskPhone
- Telefoni VoIP intermedi: telefoni Alcatel-Lucent 8008G Deskphone
- Telefoni VoIP standard: telefoni Alcatel-Lucent 8001 Deskphone
- Telefoni VoIP per sala riunioni: Alcatel-Lucent OmniTouch 4135 IP Conference Phone
- SoftPhone: Softphone con software Counterpath Bria 5
- Adattatori ATA per terminali analogici BCA e FAX: Audiocodes MP-202

Piattaforma di gestione centralizzata dell'infrastruttura Alcatel:



L'infrastruttura del Sistema Telefonico di Ateneo è monitorata e gestita centralmente attraverso il software proprietario Alcatel OmniVista.

V.4. Servizi Sistemi Informativi

L'Università dispone di un Sistema Informativo, che nella configurazione corrente è costituito da una serie di applicativi gestionali che coprono le esigenze di gestione amministrativa e contabile, di gestione del personale e degli studenti e relativi servizi, di programmazione, organizzazione, ed erogazione della didattica, di gestione dei progetti di ricerca, di gestione e conservazione documentale, di analisi dei dati e di pianificazione e controllo.

La parte principale dei sistemi applicativi è acquisita dal Consorzio Universitario CINECA, cui l'Ateneo aderisce. La suite di applicativi del Consorzio è strutturata in macroaree funzionali:

- Portali e comunicazione
- Didattica e Studenti
- Digital Education
- Ricerca
- Pianificazione e Controllo e supporto alle decisioni
- Finanza e Contabilità
- Risorse Umane
- Gestione Documentale e Dematerializzazione

ciascuna delle quali comprende una serie di moduli applicativi “verticali” che coprono specifiche funzioni o processi dell'amministrazione e di gestione universitaria relativi all'ambito funzionale.

I moduli applicativi del consorzio CINECA sono acquisiti in modalità Software as a Service e sono installati presso l'infrastruttura presente nel data center del consorzio CINECA. Non è perciò onere dell'Ateneo provvedere alla conduzione sistemistica e operativa degli stessi, ma è tuttavia necessaria una continua attività di accompagnamento nell'uso degli applicativi nei confronti dell'utenza, sia come gestione di malfunzionamenti, sia come supporto all'uso degli stessi nel rispetto dei vincoli funzionali e organizzativi definiti, sia come supporto all'introduzione e/o all'attivazione di nuove funzionalità eventualmente rese disponibili ex novo o ancora da avviare; L'adozione di nuovi moduli applicativi o l'implementazione di nuove funzionalità comporta inoltre una importante attività di gestione e un importante coinvolgimento e partecipazione ai progetti di avvio.

A completamento della soluzione integrata del consorzio CINECA sono in uso una serie di applicativi “satellite” che coprono aree funzionali più verticali e specifiche. Ne sono un esempio (non esaustivo) le applicazioni di Rilevazione delle presenze del personale tecnico amministrativo, della gestione del diritto allo studio, della gestione della sorveglianza sanitaria e formazione per area medica, i servizi di partner tecnologico per l'interfacciamento con la piattaforma Siope+ e funzionalità o applicazioni realizzate ad hoc dal personale dell'Ateneo per specifiche esigenze.

Al momento, tutti gli applicativi a supporto della attività gestionali non realizzati all'interno dell'Ateneo sono acquisiti in modalità *as a service*.



Nel corso della validità del contratto l'Ateneo potrà provvedere all'espletamento di procedure per l'affidamento di servizi applicativi in aggiunta e/o in sostituzione di quelli attualmente in uso a supporto delle attività gestionali di Ateneo.

V.5. Infrastrutture e servizi Data Base

L'architettura dei sistemi DB in uso presso l'Ateneo è composta da diverse tecnologie: un sistema DBMS ORACLE, un sistema DBMS Microsoft SQL.

V.5.1. DBMS ORACLE

Il DBMS ORACLE presente presso il data center dell'Ateneo in Varese è costituito da un server virtuale a singolo nodo.

Il DBMS è utilizzato principalmente per la predisposizione di viste di dati/tabelle presenti sul DBMS della suite applicativa utilizzata dall'Ateneo e presente presso il data center del fornitore.

Il DB è composto da un'istanza di produzione avente una decina di schemi (alcuni dei quali in fase di dismissione) e relative utenze, e una di test che è sostanzialmente la replica dell'istanza di produzione, alla quale è aggiunto uno schema contenente la copia dei dati di un applicativo dismesso, ma mantenuti in linea per eventuali consultazioni e verifiche sui dati.

Il server *host* è un server virtualizzato sull'infrastruttura tecnologica Microsoft Hyper-V, come descritto nell'Articolo V.1.1

V.5.2. DBMS Microsoft SQL Server

Il DBMS Microsoft SQL Server è costituito da un server virtuale in esecuzione in soluzione IAAS presso la piattaforma di virtualizzazione Microsoft Azure.

Il sistema è attualmente alla versione 14 (Sql Server 2017) ed è in esecuzione su un sistema operativo Windows Server 2016 Datacenter.

Il database è utilizzato come back-end per applicazioni verticali web e consta di circa una dozzina di database specializzati di entità da piccole a medie e di complessità nella maggior parte dei casi ridotta. Il database utilizza l'autenticazione integrata Active Directory di Ateneo per l'accesso personalizzato degli utenti agli oggetti db. Si utilizzano trigger per marciare temporalmente le tuple e sempre con trigger vengono collezionati altri metadati relativi alle operazioni svolte dagli utenti. I database contengono generalmente dati personali ma non contengono dati sensibili o giudiziari. Sono state attivate politiche di auditing strutturate. Il sistema utilizza Sql SSSDB (Sql Integration Services) per allineamento e comunicazione con database e fonti dati esterne (Oracle, e sistemi terzi Cineca, AD etc).

Un monitoraggio dello stato del server ed alcune funzionalità di analisi e impostazione di regole di networking etc. sono disponibili attraverso l'interfaccia web Portal Azure. Sempre attraverso la stessa interfaccia è possibile interrogare, utilizzando le funzionalità fornite dallo strumento Log Analytics, i dati di



accesso, quantità di banda e analisi degli eventi di sistema che vengono collezionati dallo strumento, partendo da origini differenti (Log IIS, Event Log Windows etc).

V.6. Servizi a supporto della Comunicazione Avanzata

Questo macro ambito racchiude la gestione delle infrastrutture e i servizi di supporto alla Comunicazione Avanzata di carattere sincrono e asincrono di tipo multimediale e ipertestuale. In particolare, nei seguenti articoli saranno descritti i servizi multimediali sincroni interattivi (videoconferenza h.323 e teams), i servizi per applicazioni multimediali asincrone o non interattive (stream, streaming vod e live) e i servizi per lo sviluppo e la pubblicazione di web applications verticali.

V.6.1. Servizi multimediali sincroni basati su H.323

L'Ateneo dispone di una completa infrastruttura di videoconferenza on premises che supporta il protocollo H.323 composta da apparati centralizzati i quali svolgono diverse funzioni quali la gestione delle chiamate (gatekeeper) o che offrono la possibilità di operare chiamate multipunto (mcu), registrare chiamate (video recorder), di interfacciarsi con sistemi di videoconferenza software anche da reti esterne all'Ateneo ecc.

Le varie componenti operano in una sottorete privata ruotata all'interno dell'Ateneo e configurata per poter dialogare solo con sottoreti dedicate ai terminali di videoconferenza hardware dislocati nelle aule per lezioni o nelle sale riunioni (circa una quarantina di terminali hardware relativamente omogenei). Tramite un apposito sistema firewall ottimizzato per applicazioni multimediali, viene gestita l'interoperabilità verso le reti esterne.

Le componenti infrastrutturali sono in esecuzione sotto forma di appliance e server virtuali nel data center di Como

V.6.2. Servizi multimediali asincroni o live non interattivi basati su H.323 e Azure Media Services

Il sistema di videoconferenza di Ateneo integra una funzione di registrazione delle chiamate H.323. Tale funzione permette di salvare in formato nativo o transcodificato le chiamate di videoconferenza per poi renderle fruibili in asincrono con tecnologia streaming e/o progressive download. Questo servizio viene usato in particolare per lezioni accademiche, seminari ma anche eventi particolari come interventi chirurgici o riprese in esterna (non utilizzando in questo caso i sistemi di registrazione H.323).

Il sistema di registrazione centralizzato permette di creare delle cosiddette "code" che attraverso varie fasi di transcodifica, etichettatura e spostamento in particolare cartelle permettono di rendere fruibili al pubblico le registrazioni delle videoconferenze organizzate per ambiti di interesse (normalmente un singolo insegnamento accademico di videoconferenza registrato). I flussi H.323 catturati nativamente vengono convertiti in filmati ad alta definizione con formato wmv e h.264 e messi a disposizione attraverso Azure Media Services in cloud. I filmati catturati dal registratore digitale H.323 vengono salvati con una cache locale (attualmente basata su freenas) e caricati in cloud.



V.6.3. Servizi collaborativi e multimediali sincroni e asincroni basati su MS Teams e Stream

Il sistema di comunicazione sincrono e asincrono durante la pandemia Covid-19 è stata arricchita di strumenti di web-conferenze e *collaboration* della suite Microsoft 365. In particolare, Teams e Stream sono stati diffusamente utilizzati per meeting organizzativi e la didattica a distanza. Per valorizzare gli investimenti operati negli anni nell'infrastruttura e terminali di videoconferenza basati su standard internazionali (h.323 o sip) si è provveduto ad acquisire un gateway cloud che permette ai terminali h.323 di interoperare con Teams permettendo di trarre vantaggio da entrambe le tecnologie.

V.7. Servizi di supporto EndPoint ed Helpdesk

V.7.1. Helpdesk

Attualmente è attivo un servizio di help desk centralizzato e appaltato a fornitore esterno. Esso è attualmente focalizzato sulla gestione delle problematiche di carattere informatico dell'Amministrazione Centrale e sulla gestione dei calcolatori delle strutture centrali con esclusione dei dipartimenti.

A fronte di recenti cambiamenti negli assetti organizzativi, il servizio di HelpDesk assumerà il ruolo di punto di contatto unico, in quanto l'Area Sistemi Informativi (ASI) ha introdotto un coordinamento con i tecnici informatici dipartimentali, con i quali vengono condivisi obiettivi, strategie e tecnologia.

Tipo di helpdesk

L'help desk è di tipo multicanale, e-mail, numero telefonico unico con gruppo di risposta multipla, portale semplificato³ per la sottomissione delle issue e un sistema di ticketing.

I canali di ingaggio sono quindi molteplici e, anche se si è cercato nel corso degli anni di indirizzare l'utenza all'uso del sistema "semplificato" di creazione ticket come canale privilegiato, le e-mail, i contatti diretti e soprattutto il telefono rappresentano i canali ancora più utilizzati. Attualmente i contatti telefonici e via mail non vengono sistematicamente tradotti in ticket.

Attualmente il sistema "semplificato" di creazione ticket rappresenta uno strato dedicato esclusivamente alla raccolta delle issue e non alla comunicazione dello stato di lavorazione nel tempo.

Attualmente l'organizzazione è su singolo livello e basata essenzialmente su una pertinenza di tipo territoriale (gli operatori di una sede servono i clienti locali); sono in uso di tecnologie di intervento remoto.

Le eventuali escalation vengono operate normalmente verso specialisti di tecnologia interni (strutturati e non) o verso fornitori esterni (Cineca soprattutto, Microsoft e fornitori hardware); in questi casi non vi è alcuna integrazione tra il sistema di ticketing interno e quello dei fornitori.

Nell'attuale organizzazione l'help desk di primo livello non risponde trasversalmente per tutti i servizi erogati dall'Area Sistemi Informativi ma quasi esclusivamente per quelli relativi alle problematiche dell'Amministrazione Centrale; l'assistenza per i sistemi informativi di supporto alla didattica (lezioni) e alla collaborazione, ad esempio, vengono svolti da personale dedicato (con presidio nelle principali sedi

³ <https://ati.uninsubria.it/richiedi-assistenza>



didattiche quali i padiglioni Montegeneroso e Morselli in Varese e Valleggio e S. Abbondio in Como); è in corso però un processo di revisione organizzativa volta a rendere il servizio di Help Desk in primo punto di contatto ed assistenza tecnica per tutti i servizi informatici erogati dall'Area Sistemi Informativi – ASI.

V.7.2. Laboratori informatizzati ed Endpoint

Gestione ciclo di vita degli endpoint

Di seguito dettaglio su numerosità, tipologia e distribuzione geografica dei dispositivi gestiti dall'attuale servizio di help desk e del servizio di supporto per aule dotate di videoconferenza.

Tipologia e numerosità calcolatori portatili e fissi per amministrazione centrale e relativa distribuzione geografica:

SEDE	n
BUSTO	20
PC fisso	20
Desktop small form factor	20
COMO	127
PC fisso	112
Desktop small form factor	112
PC portatile	15
Portatile Alta Mobilità	5
Portatile Altissima Mobilità	1
Portatile Bassa Mobilità	8
Portatile Ibrido	1
VARESE	337
PC fisso	274
Desktop small form factor	274
PC portatile	63
Portatile Alta Mobilità	26
Portatile Alte prestazioni grafiche	2
Portatile Altissima Mobilità	21
Portatile Bassa Mobilità	14
A magazzino o in mobilità	218
PC fisso	82



Desktop small form factor	82
PC portatile	136
Portatile Alta Mobilità	5
Portatile Alte prestazioni grafiche	14
Portatile Altissima Mobilità	11
Portatile Bassa Mobilità	106
Totale complessivo	702

Numerosità calcolatori fissi laboratori informatizzati e linguistici e relativa distribuzione geografica:

Città	Sede	Campus	n. PC
Varese	Monte Generoso	Bizzozero	161
Varese	Pad. Morselli	Bizzozero	36
Varese	Pad. Seppilli	Bizzozero	12
Busto Arsizio	Molini Marzoli	-	20
Como	V. Cavallotti	-	14
Como	S. Abbondio	S. Abbondio/umanistico	32
Como	Valleggio	Valleggio/scientifico	38

Numerosità calcolatori e apparecchiature per didattica ibrida in aula didattica e relativa distribuzione geografica:

Città	Sede	Campus	n. PC
Varese	Monte Generoso	Bizzozero	12
Varese	Pad. Morselli	Bizzozero	19
Varese	Pad. Antonini	Bizzozero	8
Varese	Pad. Seppilli	Bizzozero	5
Varese	Pad. Bassani	Bizzozero	1
Varese	Dunant	Bizzozero	1
Varese	Collegio Cattaneo	Bizzozero	1
Varese	Ravasi	Rettorato	1
Busto Arsizio	Molini Marzoli	-	8
Como	V. Cavallotti	-	9
Como	Castelnuovo	Valleggio/scientifico	5
Como	S. Abbondio	S. Abbondio/umanistico	9
Como	Valleggio	Valleggio/scientifico	7

Oltre a questi calcolatori sono presenti 35 Surface Hub 2S4 50" così distribuiti:

Città	Sede	Campus	n. Surface
Varese	Monte Generoso	Bizzozero	6
Varese	Pad. Morselli	Bizzozero	3

4 Surface Hub 2S: Lavagna interattiva per le aziende – Microsoft Surface per le aziende



Città	Sede	Campus	n. Surface
Varese	Pad. Antonini	Bizzozero	3
Varese	Pad. Seppilli	Bizzozero	2
Varese	Centro Genomica	Bizzozero	2
Varese	Ravasi	Rettorato	3
Busto Arsizio	Molini Marzoli	-	2
Busto Arsizio	Villa Manara	-	1
Como	S. Abbondio	S. Abbondio/umanistico	3
Como	Valleggio	Valleggio/scientifico	10

La dotazione informatica delle aule è completata da numerose telecamere ad alta definizione usb Poly Studio (42), tavolette grafiche Wacom Cintiq 16" (20) collegate ai calcolatori d'aula e 36 terminali di videoconferenza H.323 (standard e alta definizione) distribuiti come segue:

Terminale h.323	36
Terminale hd	31
Como	15
Via Castelnuovo	2
Via s. Abbondio, 12	3
Via Valleggio, 11	10
Varese	16
Amministrazione centrale, via ravasi 2,	3
Collegio cattaneo, via Dunant 7,	1
Pad. Dista-dbsv, via dunant 3,	1
Polo didattico pad. Morselli, via Ottorino rossi 9,	5
Polo didattico via monte generoso 71,	6
Terminale sd	5
Busto Arsizio (VA)	1
Polo didattico Molini Marzoli, via A. da Giussano 12	1
Como	2
Via Cavallotti	1
Via Valleggio, 11	1
Varese	2
Polo didattico pad.morselli, via Ottorino rossi 9,	2
Totale complessivo	36



VI - SERVIZI OBBLIGATORI DELLA FORNITURA

La fornitura ha per oggetto la fornitura di servizi di System Management ICT. Il complesso dei servizi richiesti prevede l'interazione con il personale strutturato dell'Area Sistemi Informativi, con precisi ambiti e referenti.

Negli articoli seguenti verranno descritti i livelli minimi di fornitura che i servizi dell'OEA dovranno garantire all'Università (servizi obbligatori) sia i servizi opzionali che l'OEA potrà discrezionalmente offrire in sede di formulazione della propria offerta tecnica senza oneri aggiuntivi per l'Università e che saranno oggetto di apposita attribuzione del punteggio tecnico in sede di valutazione delle offerte.

VI.1.1. Servizio Supporto specialistico Sistemista Senior della Rete Dati di Ateneo - SSRD

Per tutta la durata dell'appalto specifico, dovrà essere garantita la presenza continuativa di due unità di personale, una presso la sede di Varese via Ravasi 2, ed una presso la sede di Como via Valleggio 11, per 220 giornate annue ciascuna, pari a quanto indicato nella SEZIONE II – DISPOSIZIONI GIURIDICO AMMINISTRATIVE, da erogarsi nei giorni lavorativi dal lunedì al venerdì, esclusi i giorni festivi e di chiusura degli uffici amministrativi dell'Università, per 8 ore giornaliere nella fascia oraria dalle 8:00 alle 18:00 con relativa pausa per il pranzo di durata minima 30 minuti da svolgersi nella fascia oraria dalle 12:00 alle 14:00.

Ferma restando l'erogazione di complessive 220 giornate annue per ciascuna delle due unità di personale adibite al *Supporto Specialistico Sistemista Senior della Rete Dati di Ateneo - SSRD*, le eventuali assenze dovranno garantire la presenza on site di almeno una unità di personale in tutti i giorni lavorativi con esclusione dei giorni di chiusura dell'Ateneo.

Il servizio consiste nella messa a disposizione presso le sedi del Committente di unità di personale in grado di operare con efficacia nel contesto tecnologico descritto negli Articoli V.2.1, V.2.2, V.2.3, V.2.4, V.2.5 e V.2.6 e con competenze conformi all'Articolo IX 1.1 *Profilo Professionale Sistemista Senior della Rete dati di Ateneo*. Se necessario a garantire il buon funzionamento e lo sviluppo delle infrastrutture della Rete Dati di Ateneo, il personale di presidio dovrà intervenire anche presso gli altri stabili dell'Ateneo collocati nelle altre sedi di Varese, Como e Busto Arsizio, come elencate alla Sezione IV – CONTESTO ORGANIZZATIVO DEL COMMITTENTE.

Si fornisce un esempio indicativo e non necessariamente esaustivo delle attività routinarie richieste per il servizio:

- monitoraggio del regolare funzionamento degli apparati della Rete Dati di Ateneo wired e wireless e dei servizi da essi erogati, anche con l'ausilio dei sistemi di monitoraggio in uso (si veda l'Articolo V.2), esecuzione delle necessarie attività reattive e proattive per ripristinare e garantire il regolare funzionamento;
- installazione e configurazione di nuovi apparati wired di ateneo (switch e router);
- installazione e configurazione dei controller e degli access point della rete wifi di Ateneo;



- gestione degli apparati di trasmissione dati della rete wired di Ateneo (apparati di accesso, apparati core di edificio, apparati core di Campus, apparati border router);
- gestione dei controller e degli access point della rete wifi di Ateneo;
- ripristino a fronte di malfunzionamenti degli apparati di trasmissione dati della rete wired di Ateneo (apparati di accesso, apparati core di edificio, apparati core di Campus, apparati border router), eventualmente con apparati sostitutivi messi a disposizione dall'Ateneo;
- ripristino a fronte di malfunzionamenti dei controller e degli access point della rete wifi di Ateneo, eventualmente con apparati sostitutivi messi a disposizione dall'Ateneo;
- aggiornamenti di sicurezza delle configurazioni e dei firmware degli apparati di rete wired e wireless della Rete Dati di Ateneo;
- gestione di eventuali incidenti di sicurezza che interessino la rete wired e wireless della Rete Dati di Ateneo;
- regolare verifica ed analisi dei log generati dagli apparati della rete wired e wireless della Rete Dati di Ateneo ed interventi proattivi per la risoluzione di malfunzionamenti o problematiche di sicurezza;
- verifica degli adeguati livelli di performance della Rete Dati di Ateneo;
- sviluppo e progettazione delle evoluzioni della Rete Dati di Ateneo wired e wireless;
- gestione delle configurazioni e delle policy di sicurezza dei servizi di networking su private cloud Microsoft Azure (VNet, Network Security Group, Firewall, etc.);
- gestione delle configurazioni e delle policy di sicurezza sui firewall di frontiera ed interni della Rete Dati di Ateneo;
- gestione delle configurazioni e delle policy di sicurezza dei gateway VPN (ssl client to site, Ipv4 client to site ed Ipv6 site to site);
- regolare verifica ed analisi dei log generati dagli apparati firewall UTM della Rete Dati di Ateneo ed interventi proattivi per la risoluzione di malfunzionamenti o problematiche di sicurezza;
- attivazione di tutti gli accorgimenti applicabili per ridurre al minimo il rischio di attacchi informatici o *data breach*;
- altre attività che si rendano necessarie per affrontare l'evoluzione tecnologica e normativa;
- interazione con i fornitori di servizi per la Rete Dati di Ateneo (servizi connettività, servizi di manutenzione e hardware replacement per gli apparati attivi, servizi network security, etc.);
- interazione e collaborazione con i tecnici dell'Area Sistemi Informativi – ASI, in particolare con il personale addetto alla gestione dei servizi data center e con quello addetto ai servizi network e fonia.

Il personale del fornitore che affiancherà e supporterà il personale tecnico del committente nella gestione, conduzione e manutenzione dei servizi e delle infrastrutture che costituiscono la Rete Dati di Ateneo; ove necessario si interfacerà con i referenti di altre strutture e/o con i fornitori esterni per quanto necessario alle attività di cui sopra.

Le unità di personale messe a disposizione dovranno altresì contribuire alla realizzazione e all'aggiornamento della documentazione tecnica dei servizi e delle infrastrutture afferenti alla Rete dati di Ateneo.

Il personale adibito al servizio dovrà



- monitorare il regolare funzionamento dell'infrastruttura della Rete Dati di Ateneo e dei servizi da essa erogata con l'ausilio dei servizi di monitoraggio messi a disposizione dal committente (Nagios e Cacti). A fronte di problematiche di disponibilità dei servizi o relative a non adeguati livelli di performance, il personale adibito al servizio dovrà intraprendere le azioni reattive e correttive attuabili, registrando le azioni attraverso il sistema di gestione ticket dell'Area Sistemi Informativi - ASI e provvedendo all'escalation verso il referente del servizio nel caso in cui non sia possibile procedere in autonomia alla risoluzione dell'incident.
- monitorare la sicurezza dell'infrastruttura della Rete Dati di Ateneo e dei servizi erogati, verificando ed analizzando con cadenza quotidiana i log raccolti dagli apparati e sistemi che costituiscono la Rete Dati dell'Ateneo e i relativi servizi di network security, provvedendo ad attuare le contromisure reattive e proattive necessarie a garantire la sicurezza dell'infrastruttura e dei servizi, registrando le azioni attraverso il sistema di gestione ticket dell'Area Sistemi Informativi - ASI e provvedendo all'escalation verso il referente del servizio nel caso in cui non sia possibile procedere in autonomia alla risoluzione dell'incident.

Le attività svolte per l'evoluzione e sviluppo della Rete Dati Ateneo, dovranno essere tracciate attraverso il sistema di ticketing messo a disposizione dall'Ateneo, usando le apposite attività di gestione change.

Il Referente del Servizio Supporto Specialistico Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo è il capo ufficio Networking e Fonia dell'Area Sistemi Informativi – ASI.

VI.1.2. Servizio Supporto Specialistico Specialista – Cyber Security – SSCS

Gli aspetti di Cyber Security impattano trasversalmente su tutti i contesti tecnologici ed organizzativi descritti nella SEZIONE V – CONTESTO TECNOLOGICO DEL COMMITTENTE. Le professionalità e le competenze del personale adibito all'erogazione del Servizio Supporto Specialistico Specialista-Cyber Security devono quindi essere in grado di padroneggiare tutti gli ambiti.

Si vuole altresì evidenziare i seguenti contesti specifici per i quali è richiesta una peculiare padronanza negli ambiti tecnologici:

- Rete Dati di Ateneo – network security;
- Rete Dati di Ateneo – accesso remoto VPN;
- Sistemi di gestione delle identità digitali – sicurezza delle identità;
- Architetture di cloud ibrido - cloud Security & Compliance;
- Applicazioni cloud - e-mail security, anti-Phishing, Advanced Threat Protection, Data Loss Prevention, etc.
- End Point Security;
- Raccolta ed analisi dei log.

Parallelamente, si richiedono competenze specifiche in ambito di gestione dei processi ed organizzazione in ambito IT security ed IT service management.



Il personale adibito all'erogazione del servizio dovrà supportare il personale del committente nella gestione di eventuali incidenti informatici o data breach.

Il personale adibito all'erogazione del servizio dovrà altresì contribuire alla realizzazione e all'aggiornamento della documentazione tecnica dei servizi e delle infrastrutture di Sicurezza Informatica.

Il profilo professionale delle unità di personale adibite al Servizio Supporto Specialistico Specialista– Cyber Security - SSCS dovrà essere conforme al profilo descritto nell'Articolo IX.1.2 *Profilo Professionale Specialista – Cyber Security*.

Per tutta la durata dell'appalto specifico, dovrà essere garantita la presenza continuativa di una unità di personale presso la sede di Varese via Ravasi 2 per 220 giornate annue, pari a quanto indicato nella SEZIONE II – DISPOSIZIONI GIURIDICO AMMINISTRATIVE, da erogarsi nei giorni lavorativi dal lunedì al venerdì, esclusi i giorni festivi e di chiusura degli uffici amministrativi dell'Università, 8 ore giornaliere nella fascia oraria dalle 8:00 alle 18:00 con relativa pausa per il pranzo di durata minima 30 minuti da svolgersi nella fascia oraria dalle 12:00 alle 14:00.

Il referente del servizio Supporto Specialistico Specialista – Cyber Security - SSCS è il dirigente dell'Area Sistemi Informativi – ASI.

VI.1.3. Servizio Supporto Specialistico Business Analyst -SSBA

Il Servizio Supporto Specialistico Business Analyst – SSBA agisce nel contesto tecnologico descritto all'Articolo V.4.

Questa figura professionale si occupa di analizzare, raccogliere e formalizzare i requisiti espressi dai responsabili di processo e dagli utenti dei sistemi informativi di Ateneo e di predisporre tutta la documentazione necessaria a identificare una tipologia adeguata di soluzioni.

Partecipa alla valutazione degli impatti, dei benefici e dei rischi connessi all'introduzione di soluzioni applicative e/o di nuove funzionalità, analizzando i processi e approfondendo il contesto di utilizzo.

Partecipa alle attività di analisi dei requisiti e del contesto relative allo sviluppo di nuove soluzioni, quando queste siano sviluppate all'interno dell'area ASI e interagisce con l'utenza direttamente coinvolta dall'operazione per gli approfondimenti eventualmente necessari, la messa a punto dei requisiti, la verifica della rispondenza della soluzione alle aspettative.

Contribuisce alla redazione di documenti di analisi e report che permettano di valutare la fattibilità tecnica ed economica delle soluzioni di business e di processo individuate e alla valutazione dell'impatto sui processi che esse comportano.

Contribuisce alla predisposizione e alla gestione dei piani di progetto, all'analisi su costi, benefici e rischi, tenendo conto dei requisiti di funzionalità a fronte di vincoli di tempo, costi e qualità.

Fornisce supporto e contribuisce alle attività di predisposizione di capitolati tecnici e funzionali per l'acquisizione di servizi applicativi e fornisce supporto al coordinamento dei progetti di adozione delle



soluzioni applicative effettuando analisi di processo e funzionale, supportando gli utenti nella transizione, interagendo con i fornitori dei servizi, gestendo le problematiche legate all'introduzione di un nuovo ambito funzionale e le eventuali criticità correlate con la migrazione dei dati.

Opera in sinergia e in collaborazione con altri Referenti applicativi dell'Area Sistemi Informativi -ASI per analizzare requisiti operativi e problematiche funzionali che possano avere un impatto su aree funzionali e applicative più estese.

Prende in carico, gestisce e, ove possibile, risolve direttamente le richieste e le segnalazioni degli utenti che riguardano i vari moduli applicativi in uso del sistema informativo dell'Ateneo, anche eseguendo operazioni sui moduli applicativi.

Si interfaccia, quando necessario, con i referenti di altre strutture, con i referenti interni e/o direttamente con i fornitori degli applicativi verificando l'intero ciclo di vita dalla segnalazione e/o della richiesta fino alla sua completa chiusura.

Assiste gli utenti nell'esecuzione di attività complesse e supporta gli stessi nelle interazioni con i fornitori dei servizi applicativi ove necessario. Effettua attività di valutazione delle richieste di modifica pervenute, ne valuta la fattibilità e l'impatto prima che queste possano essere formalizzate al fornitore del servizio, sulle quali successivamente effettua attività di monitoraggio e di controllo finalizzato alla verifica dei tempi di rilascio e della rispondenza ai requisiti.

Rappresenterà il terzo livello di assistenza per i servizi informativi gestionali.

Contribuisce alla realizzazione della documentazione operativa per l'utente.

Esegue attività di trasformazione di file secondo tracciati predefiniti per il caricamento massivo di dati nella procedura per la gestione dei pagamenti. Ove necessario e opportuno propone modalità di trasformazione automatica o semi-automatica basate su strumenti in uso dall'area ASI.

Effettua attività di amministrazione dei profili di accesso ai servizi applicativi, governa e tiene traccia delle abilitazioni di concerto con il referente del servizio e i referenti di dominio.

In particolare, amministra i gruppi, i profili, le autorizzazioni e i contesti per la suite applicativa U-GOV (i vari moduli in uso da parte dell'Ateneo), adeguando gli stessi a seconda delle mutate esigenze organizzative e funzionali dell'Ateneo (ad esempio dovute all'introduzione o all'attivazione di nuove funzioni o di moduli applicativi o a seguito di differenti articolazioni degli uffici o di spostamenti o variazioni delle afferenze delle persone, ecc.), per fare in modo che i profili autorizzatori corrispondano alla necessaria operatività degli utenti a seconda dei vari contesti organizzativi dell'Ateneo.

Tale figura affiancherà e supporterà il personale tecnico del committente nella gestione, conduzione e manutenzione dei sistemi informativi in uso e di prossima e futura attivazione nell'Ateneo.

Il profilo professionale delle unità di personale adibite al Servizio Supporto Specialistico Business Analyst - SSBA dovrà essere conforme profilo descritto nell'Articolo IX.1.3 *Profilo Professionale Specialista Business Analyst*.



Per tutta la durata dell'appalto specifico, dovrà essere garantita la presenza continuativa di due unità di personale presso la sede di Varese via Ravasi 2, per 220 giornate annue ciascuna, pari a quanto indicato nel SEZIONE II – DISPOSIZIONI GIURIDICO AMMINISTRATIVE, da erogarsi nei giorni lavorativi dal lunedì al venerdì, esclusi i giorni festivi e di chiusura degli uffici amministrativi dell'Università, 8 ore giornaliere nella fascia oraria dalle 8:00 alle 18:00 con relativa pausa per il pranzo di durata minima 30 minuti da svolgersi nella fascia oraria dalle 12:00 alle 14:00.

Ferma restando l'erogazione di complessive 220 giornate annue per ciascuna delle due unità di personale adibite al Supporto Specialistico Specialista Business Analyst, le eventuali assenze dovranno garantire la presenza on site di almeno una unità di personale in tutti i giorni lavorativi con esclusione dei giorni di chiusura dell'Ateneo.

Il Referente del servizio Supporto Specialistico Specialista Business Analyst – SSBA è il Capo Ufficio Sistemi Informativi Gestionali dell'Area Sistemi Informativi – ASI.

VI.1.4. Servizio Supporto Specialistico Sistemista Specialista – Data Center on prem e cloud – SSDC

Il Servizio Supporto Specialistico Specialista – Data Center on prem e cloud – SSDC agisce nel contesto tecnologico descritto all'Articolo V.1.

Tipicamente le attività richieste al personale adibito al Servizio Supporto Specialistico Specialista – Data Center on prem e cloud sono:

- Installazione e configurazione, secondo specifiche fornite dal Committente, del sistema operativo Microsoft Server e dell'ambiente di virtualizzazione Microsoft Hyper-V, anche in configurazione cluster, su nuove piattaforme hardware eventualmente acquisite.
- Creazione e configurazione, secondo specifiche fornite dal Committente, di nuove macchine virtuali nell'ambito dei sistemi di virtualizzazione operativi presso i datacenter on-prem e in cloud del Committente.
- Migrazione di sistemi e servizi a versioni più recenti del sistema operativo Microsoft Windows Server.
- Analisi e risoluzione di malfunzionamenti del sistema operativo dei server fisici e delle macchine virtuali e risoluzione dei malfunzionamenti dell'ambiente di virtualizzazione Hyper-V.
- Operazioni di ripristino da backup di macchine virtuali e dati.
- Operazioni di ripristino di server fisici per la virtualizzazione basati su Microsoft Hyper-V a seguito di guasto hardware.
- Aggiornamento dei firmware presenti nei server fisici per la virtualizzazione descritti agli Articoli V.1.1 e V.1.2.



Il profilo professionale delle unità di personale adibite al Servizio Supporto Specialistico Sistemista Senior – Data Center on prem e cloud – SSDC dovrà essere conforme profilo descritto nell'Articolo XI.1.4 *Profilo Professionale Specialista Data Center on prem e cloud*.

Per tutta la durata dell'appalto specifico, dovranno essere garantite un numero di 20 giornate complessive annue pari a quanto indicato nel SEZIONE II – DISPOSIZIONI GIURIDICO AMMINISTRATIVE, da erogarsi presso la sede di Varese via Ravasi 2 con la presenza di una unità di personale, nei giorni lavorativi dal lunedì al venerdì, 8 ore giornaliere nella fascia oraria dalle 8:00 alle 18:00 con relativa pausa per il pranzo di durata minima 30 minuti da svolgersi nella fascia oraria dalle 12:00 alle 14:00. L'erogazione delle giornate avverrà previa richiesta dell'Amministrazione con preavviso di almeno 15 giorni lavorativi. Tale richiesta indicherà la data di inizio dell'erogazione ed il numero di giornate richieste. Il monte giornate non fruito in una annualità potrà essere fruito dal committente nelle annualità successive di vigenza contrattuale.

Il Referente del servizio Supporto Specialistico Specialista – Data Center on prem e cloud – SSDC è il Capo Ufficio Data Center on prem e cloud dell'Area Sistemi Informativi – ASI.

VI.1.5. Servizio Supporto Specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – SSVCDL

L'Università degli Studi dell'Insubria è dotata di un sistema di videoconferenza composto, oltre che da numerosi terminali, anche da apparati centralizzati per le videoconferenze e lo streaming che di seguito verranno individuati come “sistemi centrali di comunicazione avanzata”, descritti all'Articolo V.6, in ambienti virtualizzati sia on premise che in cloud e la piattaforma di elearning Moodle del consorzio CINECA fruita in modalità SaaS.

Le attività richieste per questo profilo sono le seguenti:

- Gestione dell'infrastruttura relativa ai “Sistemi centrali di comunicazione avanzata” descritta nell'Articolo V.6, per garantire il massimo grado di sicurezza, disponibilità e prestazioni. A titolo esemplificativo e non esaustivo si elencano alcune operazioni comuni:
 - o Gestire le componenti infrastrutturali al servizio della videoconferenza, ovvero tutte le appliance H.323, Gatekeeper DMA, Resource manager con accesso alle Active Directory, Access Director per collegamenti esterni, multipunto virtuali e registratore multimediale. Il sistemista dovrà poter accedere alle interfacce di gestione di ogni singolo device e dovrà conoscere il funzionamento dell'architettura h.323 e l'interazione tra le componenti sopra elencate. Nel dettaglio dovrà:
 - Controllare lo stato delle appliance e il loro corretto funzionamento
 - Fornire assistenza e supporto al servizio dei sistemi avanzati di videoconferenza in caso di malfunzionamenti o segnalazioni da parte del personale addetto relative alla connettività dei terminali, su problematiche con la numerazione concordata ecc.
 - Configurare il piano di numerazione h.323, comprensivo di
 - numerazione dei nuovi terminali secondo le convenzioni stabilite;



- numerazione delle code di registrazione da indicare agli addetti in sala;
- numerazione delle stanze multipunto da usare per singoli eventi o per eventi ricorrenti;
- Controllare in tempo reale lo stato delle connessioni attive, soprattutto per eventi importanti. Consultare periodicamente le registrazioni attive controllando la presenza dell'audio e la corretta configurazione dei segnali video. Controllare a campione per le chiamate attive la presenza di problemi di rete (per esempio jitter elevati o perdite di pacchetti);
- Estrarre mensilmente le statistiche d'uso del sistema di videoconferenza secondo la procedura definita dall'Ateneo (attualmente questa procedura prevede l'estrazione manuale di un report mensile dal sistema Polycom DMA; in seguito, è necessario effettuare una normalizzazione del file per estrarre la somma totale dei minuti di chiamata mensile; infine, questo valore va inserito in un file riepilogativo utile per tenere traccia del trend di ore e per la rendicontazione dei servizi correlati);
- Gestione dal punto di vista tecnico eventi esterni. In caso l'Ateneo organizzi eventi con altri Enti o con relatori esterni, il sistemista dovrà porre in essere tutte le azioni necessarie a consentire l'interfacciamento del sistema di Ateneo con eventuali sistemi terzi. A titolo di esempio, dovrà interagire con gli organizzatori dell'evento per comprendere le esigenze e proporre la soluzione più consona, tra le seguenti opzioni:
 - Collegamento di uno o più relatori esterni mediante software di videoconferenza in gestione dell'Ateneo: in questo caso è necessario fornire istruzioni e credenziali temporanee e personali ad ogni partecipante e, una volta installato l'applicativo effettuare dei test di connettività e di misurazione della qualità del collegamento, valutando se la qualità del collegamento sia sufficiente;
 - Collegamento di uno o più relatori esterni mediante terminali esterni: in questo caso il collegamento avverrà tramite terminali hardware o software di terze parti: è quindi necessario prendere contatto con i referenti tecnici (spesso questa tipologia di collegamento richiede connessioni internazionali, quindi è necessario interagire tendenzialmente sempre in inglese) per effettuare test di connettività. Una volta effettuati i test, vista la complessità di questi scenari, è necessaria la presenza del sistemista, il giorno dell'evento, per procedere con la connessione in base agli accordi stabiliti e risolvere eventuali problematiche;
- Gestione dell'esportazione dei filmati su cloud. Tutti i filmati sorgente registrati con il registratore H.323 vengono attualmente esportati in maniera automatica sulla piattaforma Azure Media Services. In questo modo, i filmati sono protetti da backup; tali filmati però non sono direttamente fruibili in questa forma ma necessitano di essere processati secondo uno dei seguenti canali:
 - Procedura automatica caricamento filmati (per lezioni o eventi ricorrenti) - il servizio di registrazione h.323 consente di registrare un intero ciclo di lezioni di un insegnamento esportando i filmati sulla piattaforma Azure e aggiornando automaticamente la lista delle



lezioni in modo che siano fruibili da parte degli studenti. È quindi necessaria una configurazione iniziale per ogni insegnamento per definire la coda di registrazione, quindi istruire il sistema automatico per il caricamento dei filmati contrassegnati da quella numerazione; infine è necessario agire tramite una apposita web application per configurare la parte web e fornire l'accesso agli studenti.

- Procedura manuale caricamento filmati - le registrazioni di eventi non prevede un processo automatico di pubblicazione in quanto i file sorgente generati dovranno essere post prodotti ogni volta in modalità diverse. In questo caso è quindi necessario condividere i filmati (per esempio fornendo all'addetto alla post-produzione i link per il download) e, una volta terminato il lavoro di post-produzione caricare i filmati definitivi sulla piattaforma Azure e renderli fruibili per la preview e per la conseguente pubblicazione in base alle esigenze del committente dell'evento;
- Gestione nel tempo gli asset informativi (filmati, audio ecc.) memorizzati sulla piattaforma Azure Media Services: oltre alle procedure automatiche e manuali sopra descritte è possibile e a volte necessario collegarsi direttamente alla lista dei filmati pubblicati per effettuare operazioni avanzate, come il controllo degli asset presenti, stabilire le modalità di criptazione, le date di termine di pubblicazione dei filmati e di conseguenza le azioni di modifica, cancellazione o inserimento in seguito ad anomalie segnalate o riscontrate: per svolgere questa funzionalità viene fornito dall'Ateneo un software apposito.
- Gestione degli strumenti che permettono ai terminali di videoconferenza H.323 di interagire con le soluzioni Teams e, in particolare, configurare, assegnare e monitorare costantemente il corretto funzionamento dei connettori Poly Real Connect o soluzioni equivalenti.
- Supporto di terzo livello per quanto concerne l'uso base ed avanzato della soluzione Teams e degli strumenti/app collegate ad essa (onedrive, calendari wiki, ecc.): il sistemista dovrà conoscere profondamente la soluzione Teams ed aggiornarsi costantemente realizzando se necessario guide e manuali sintetici per alimentare la knowledge base interna e per gli utenti finali differenziandone contenuti e registri comunicativi in base al target (personale docente/personale tecnico amministrativo/studenti)
- Supporto di terzo livello per la piattaforma di E-learning e per la piattaforma esami di Ateneo (entrambe basata su LMS opensource Moodle) con relativi moduli di integrazione realizzati da Cineca.

Il profilo professionale delle unità di personale adibite Servizio Supporto Specialistico Sistemista – Sistemi di Videoconferenza – SSVCDL dovrà essere conforme profilo descritto nell'Articolo IX.1.5 *Profilo Professionale Sistemista Videoconferenza e Digital Learning*.

Per tutta la durata dell'appalto specifico, dovrà essere garantita la presenza continuativa di una unità di personale presso la sede di Como via Valleggio 11, per 220 giornate annue pari a quanto indicato nel SEZIONE II – DISPOSIZIONI GIURIDICO AMMINISTRATIVE, da erogarsi nei giorni lavorativi dal lunedì al venerdì, esclusi i giorni festivi e di chiusura degli uffici amministrativi dell'Università, 8 ore



giornaliere nella fascia oraria dalle 8:00 alle 18:00 con relativa pausa per il pranzo di durata minima 30 minuti da svolgersi nella fascia oraria dalle 12:00 alle 14:00.

Il referente del Servizio Supporto Specialistico Sistemista – Sistemi di Videoconferenza – SSVCDL è il Capo Ufficio Digital Learning dell'Area Sistemi Informativi – ASI.

VI.1.6. Servizio Supporto Specialistico Sistemista – Laboratori informatici ed Endpoint- SSEP

L'Ateneo mette a disposizione del proprio personale (docenti e personale tecnico amministrativo) e degli studenti immatricolati circa trecento elaboratori elettronici ad accesso condiviso con relativo corredo software. Le finalità d'uso di questi elaboratori spaziano dall'autoformazione e/o ricerche personali fino ad esigenze didattiche particolari. Generalmente, per la prima finalità ci si riferisce a “laboratori informatici”, mentre per la seconda si parla di “aule informatizzate”.

Abitualmente, quindi, nei laboratori informatizzati è permesso l'uso di software usati nei diversi ambiti di studio e di ricerca e di strumenti utili a muoversi in contesti tecnologici avanzati. L'accesso ai laboratori è generalmente libero nelle ore indicate da ciascuno spazio.

Le Aule informatizzate vengono invece utilizzate per lezioni, esami, esercitazioni, test di ingresso, concorsi interni e ministeriali che necessitano di supporto informatico e sono dotate di software specialistici installati in base alle esigenze didattiche dei corsi di studio.

Mentre i laboratori informatici sono sempre ed esclusivamente fisici, le aule informatizzate potrebbero in futuro anche essere virtualizzate.

Attualmente, l'Ateneo ha investito in strutture capaci di essere configurate a tale scopo alternativamente come laboratori o come aule informatizzate.

Il servizio di supporto specialistico si rende necessario per gestire nel tempo la continuità operativa e la sicurezza informatica dei laboratori e degli end point in generale, per rispondere all'evoluzione tecnologica e normativa e per la definizione di *best practice*, prescrizioni e standard comuni orientati alla qualità in questo ambito.

Nell'Articolo V.7.2 vengono descritte caratteristiche, numerosità e distribuzione geografica dei laboratori informatizzati e degli Endpoint a supporto della didattica e l'attività di amministrazione di pertinenza dell'Area Sistemi Informativi.

La prestazione del servizio di supporto specialistico deve essere tesa a mantenere in piena efficienza e sicurezza gli elaboratori elettronici dei laboratori e delle aule informatizzate massimizzandone al contempo la continuità operativa. Questo si esplicita nelle attività di:

- Pianificazione, su base al minimo mensile, delle attività di aggiornamento/manutenzione del sistema operativo e del software dei vari laboratori per minimizzarne l'impatto sulla operatività dei laboratori (verifica vincoli orari, lezioni, test ecc.);



- coordinamento della applicazione tempestiva, tramite distribuzione centralizzata, degli aggiornamenti dei sistemi operativi e dei software di base (in particolare antivirus, pacchetti di produttività personale ecc.);
- utilizzo di tecniche avanzate e centralizzate di gestione di un numero elevato di calcolatori;
- attivazione di tutti gli accorgimenti applicabili per ridurre al minimo il rischio di attacchi informatici o di incidenti che comportino la violazione di dati personali - *data breach* - (*hardening* sistema operativo, attivazione di *policies* centralizzate di *auto-logoff*, disabilitazione *caching password* locale, pulizia dei profili utenti al *logoff*, ecc.);
- attivazione di tutti gli accorgimenti applicabili per ridurre il consumo di energia elettrica (spegnimento monitor, spegnimenti programmati calcolatori, attivazione profili di risparmio energetico ecc.);
- monitoraggio, attraverso tecniche centralizzate ed avanzate, delle prestazioni dei calcolatori dei laboratori e delle aule informatizzate con stesura di rapporti dettagliati a supporto del miglioramento e alla soddisfazione dell'utente;
- altre attività che si rendano necessarie per affrontare l'evoluzione tecnologica e normativa non determinabili a priori ma di complessità e caratteristiche assimilabili alle precedenti.

In ottica di adeguamento tecnologico o per gestire eventuali mutazioni di contesto o di indicazioni strategiche, sarà possibile dover supportare l'Ateneo nelle fasi di progettazione, realizzazione, attivazione o radicale rivisitazione di laboratori e aule informatizzate sia in configurazione fisica che virtuale. Per questo la prestazione si potrà articolare in attività quali:

- *Capacity planning* per client e server di gestione;
- Test e validazione dei template di macchina;
- Determinazione, attraverso interazione con il corpo docente, delle specifiche dotazioni software da installare di concerto con il referente del Servizio;
- Configurazione, soprattutto in ambito virtuale, delle finestre temporali di disponibilità delle risorse computazionali, loro allocazione e de-allocazione in base alle indicazioni didattiche e ai vincoli contrattuali del gestore dell'infrastruttura di *hypervisor*;
- Determinazione, attraverso analisi di parametri di coorte, corso di studi ecc, di target ai quali associare corredi software specifici e loro installazione/somministrazione selettiva;
- Altre attività che si rendano necessarie per affrontare l'evoluzione tecnologica e normativa non determinabili a priori ma di complessità e caratteristiche assimilabili alle precedenti.

Per scopi particolari (lezioni, esami, esercitazioni, test di ingresso, concorsi interni e ministeriali) dovrà essere possibile agire sulla configurazione degli elaboratori per soddisfare esigenze particolari come, a puro titolo esemplificativo e non esaustivo:

- Attivare account personali temporanei per particolari applicazioni (es. test di ingresso, concorsi ministeriali, ecc.) dedicate a persone non dotate di una identità digitale di Ateneo;



- Bloccare la navigazione verso internet ad esclusione di un sottoinsieme determinato di url (ad esempio piattaforma di e-learning/piattaforma linguistica ecc.);
- Permettere l'esecuzione di un solo applicativo specifico (modalità chiosco singola app o similare);
- Disabilitare funzionalità degli elaboratori in contrasto con la finalità d'uso (es. Disabilitare menù di traduzione contestuale se il laboratorio viene usato per certificazioni linguistiche ecc.);
- Altre attività che si rendano necessarie per affrontare l'evoluzione tecnologica e normativa non determinabili a priori ma di complessità e caratteristiche assimilabili alle precedenti.

Il supporto specialistico “Sistemista laboratori informatici ed Endpoint” garantisce la disponibilità e l'operatività degli Endpoint in gestione all'Area Sistemi Informativi e rappresenta il punto di riferimento della gestione End Point di cui all'Articolo V.7.2.

Questo Servizio dovrà coordinarsi, per la gestione delle postazioni ad uso didattico, con il servizio di “Servizio Supporto Specialistico Sistemista – Sistemi Videoconferenza e Digital Learning” di cui all'Articolo VI.1.5

Il profilo professionale delle unità di personale adibite Servizio Supporto Specialistico Sistemista – Sistemista laboratori informatici ed Endpoint –SSEP dovrà essere conforme profilo descritto nell'Articolo IX.1.6
Profilo professionale Sistemista Laboratori informatici ed End Point

Per tutta la durata dell'appalto specifico, dovrà essere garantita la presenza continuativa di una unità di personale presso la sede di Como via Valleggio 11 per 220 giornate annue, pari a quanto indicato nel SEZIONE II – DISPOSIZIONI GIURIDICO AMMINISTRATIVE, da erogarsi nei giorni lavorativi dal lunedì al venerdì, esclusi i giorni festivi e di chiusura degli uffici amministrativi dell'Università, 8 ore giornaliere nella fascia oraria dalle 8:00 alle 18:00 con relativa pausa per il pranzo di durata minima 30 minuti da svolgersi nella fascia oraria dalle 12:00 alle 14:00.

Il Referente del Servizio Supporto Specialistico Sistemista – Sistemista laboratori informatici ed Endpoint–SSEP è il Capo Servizio Servizi Front Office e Back Office dell'Area Sistemi Informativi – ASI.



VI.1.7. Servizio Conduzione Operativa da remoto DBMS – CODB

I servizi richiesti constano delle attività di conduzione operativa da remoto per un DBMS basato su tecnologia ORACLE e per un DBMS basato su piattaforma Microsoft SQL server, descritti all'Articolo V.5. Il servizio dovrà essere erogato per tutti i giorni lavorativi dal lunedì al venerdì, e dovrà essere operativo nella fascia oraria dalle 8:00 alle 12:00 e dalle 14:00 alle 18:00.

L'assegnazione delle attività, le richieste di supporto, le richieste di change, l'apertura di incidenti, avverrà attraverso il sistema di ticketing del fornitore e che, a tal fine, dovrà essere reso accessibile al Referente del Servizio Conduzione Operativa da remoto DBMS.

Il personale adibito al servizio dovrà monitorare il regolare funzionamento dei DBMS con l'ausilio dei servizi di monitoraggio messi a disposizione dal fornitore. A fronte di problematiche di disponibilità dei servizi o relative a non adeguati livelli di performance, il personale adibito al servizio dovrà intraprendere le azioni reattive e correttive attuabili, registrando le azioni effettuate attraverso il sistema di gestione ticket messo a disposizione dal fornitore e provvedendo all'escalation verso il referente del servizio nel caso in cui non sia possibile procedere in autonomia alla risoluzione dell'incident.

Il personale adibito al servizio dovrà monitorare il regolare funzionamento dei DBMS e la sicurezza degli stessi e dei servizi erogati, verificando ed analizzando con cadenza quotidiana i log raccolti, provvedendo ad attuare le contromisure reattive e proattive necessarie a garantire la sicurezza dell'infrastruttura e dei servizi. Le attività svolte devono essere registrate attraverso il sistema di gestione ticket del fornitore (in modo che queste siano consultabili da parte del referente del servizio). Il personale addetto al servizio deve inoltre provvedere all'escalation verso il referente del servizio nel caso in cui non sia possibile procedere in autonomia alla risoluzione dell'incident o della problematica rilevata.

Il Referente del Servizio di Conduzione Operativa da remoto DBMS – CODB è il capo ufficio Data Center on prem e cloud dell'Area Sistemi Informativi – ASI.

Attività specifiche di avvio contratto per i servizi di Conduzione Operativa da remoto DBMS

Per quanto riguarda i servizi di Conduzione Operativa da remoto DBMS – CODB, la presa in carico dei servizi di conduzione operativa deve prevedere una fase di affiancamento/interazione con il precedente fornitore del servizio se il nuovo contratto verrà attivato in tempo utile per consentire il passaggio di consegne.

L'Università indicherà al Fornitore aggiudicatario un proprio referente per la fase di transizione, incaricato di svolgere funzioni di interfaccia unica tra il fornitore uscente e il fornitore aggiudicatario per le operazioni di carattere organizzativo. Lo scopo di questo supporto è garantire un avvio rapido delle operazioni e assicurare un corretto subentro del Fornitore.

Nei 10 giorni solari successivi alla stipula del contratto, il fornitore aggiudicatario dovrà:

1. comunicare i nominativi dei tecnici incaricati della conduzione operativa dei DBMS e concordare con il DEC le modalità di accesso remoto sicuro ai sistemi.



2. Il personale incaricato del servizio di conduzione operativa da remoto dovrà prendere contatti con l'attuale gestore dei DBMS del fornitore uscente, i cui riferimenti saranno forniti dall'Università al fine di definire e documentare nel dettaglio i seguenti aspetti:
- Credenziali di accesso ai DBMS
 - Modalità di accesso ai DBMS
 - Configurazione del sistema
 - Per il DBMS Oracle documentazione della configurazione delle connessioni (DBlink) con il Database remoto presso CINECA degli applicativi gestionali e modalità di verifica del corretto funzionamento
 - Utenze di sistema e relative password
 - Utenze definite sul DB e relative password
 - Istanze con relativi Schemi e utenze (con relative password)
 - Modalità di esecuzione dei backup e loro frequenza e modalità di verifica della corretta esecuzione dello stesso
 - Procedure di avvio e di spegnimento
 - Ogni altro elemento necessario per la presa in carico del sistema

Le attività di affiancamento possono essere effettuate anche in modalità remota.

Il fornitore aggiudicatario è tenuto a comunicare al referente per l'attività di transizione eventuali difficoltà nell'esecuzione delle attività di presa in carico o l'eventuale carenza di informazioni.

Durante le attività di affiancamento la responsabilità delle operazioni continuerà ad essere in capo al Fornitore uscente.

Al termine del periodo indicato o al termine delle attività di affiancamento, il fornitore aggiudicatario dovrà rilasciare un verbale di avvenuto affiancamento e che dovrà essere inviato al Direttore dell'Esecuzione, a decorrere dal quale l'onere di gestione del servizio passa al fornitore aggiudicatario.

La presa in carico definitiva della gestione deve comportare necessariamente la modifica di tutte le password di sistema (sys e system, ecc.).

La durata massima della fase di avvio dei servizi è fissata in 10 giorni lavorativi a decorrere dalla stipula del Contratto.

Attività specifiche di conclusione contratto per i servizi di Conduzione Operativa da remoto DBMS – CODB

Per quanto riguarda i servizi di Conduzione Operativa da remoto DBMS – CODB, in prossimità della conclusione del contratto, il Fornitore dovrà garantire un periodo di supporto alla transizione verso un nuovo eventuale fornitore, o alla presa in carico dei servizi da parte dell'Amministrazione. In tale periodo, il Fornitore si impegna a collaborare all'ordinata migrazione di competenze verso l'Amministrazione o ad un terzo designato dall'Amministrazione.

Dovrà esser definito un Piano di Trasferimento per attuare la migrazione del servizio di cui sopra. Il Piano di Trasferimento consisterà nella redazione di un piano di massima di tipo esecutivo, articolato in attività



con l'indicazione di scadenze di inizio e fine, di responsabilità, di contenuti e risultati tali da realizzare il "Trasferimento" e da renderne controllabile la sua effettiva attuazione.

Il piano di Trasferimento deve produrre la documentazione dettagliata e completa delle configurazioni del sistema DBMS per agevolare la presa in carico da parte del fornitore subentrante o dell'Ateneo. In particolare, la documentazione deve comprendere anche i seguenti elementi:

- Credenziali di accesso ai DBMS
- Modalità di accesso ai DBMS
- Configurazione del sistema
- Per il DBMS Oracle documentazione della configurazione delle connessioni (DBlink) con il Database remoto presso CINECA degli applicativi gestionali e modalità di verifica del corretto funzionamento
- Utenze di sistema e relative password
- Utenze definite sul DB e relative password
- Istanze con relativi Schemi e utenze (con relative password)
- Modalità di esecuzione dei backup e loro frequenza e modalità di verifica della corretta esecuzione dello stesso
- Procedure di avvio e di spegnimento
- Ogni altro elemento necessario per la presa in carico del sistema da parte del fornitore subentrante o dell'Ateneo.

DBMS ORACLE

Il servizio di conduzione operativa da remoto è finalizzato alla gestione operativa del sistema DBMS e include tutte le attività necessarie per garantire e mantenere il buono stato di funzionamento dello stesso, oltre che quelle finalizzate alla gestione di eventuali modifiche/aggiornamenti o revisioni architetturali secondo le esigenze dell'Ateneo.

Si fornisce un esempio indicativo e non necessariamente esaustivo delle attività routinarie richieste per tale servizio:

- verifica schedulata della disponibilità⁵ del data-base.
- verifica schedulata delle condizioni del database: in base ad opportuni parametri quali a titolo meramente esemplificativo ma non necessariamente esaustivo si citano ad esempio:
 - suddivisione logica degli storage di data-base (tablespaces);

⁵ si definisce disponibilità di un data-base la frazione di tempo in cui esso è operativo e in grado di rispondere alle richieste degli utenti.



- suddivisione fisica degli storage di data-base (file di dati per tablespaces);
 - storage massimo per file di data-base, con relativo confronto rispetto ad una soglia di guardia;
 - memoria RAM utilizzata dal data-base e sua suddivisione (suddivisione della global area);
 - tempi di risposta (somma del tempo di servizio e del tempo di attesa delle risorse necessarie);
 - ammontare di lavoro del data-base (throughput),
 - tempi di attesa, in particolare nel caso di contesa di risorse (oggetti del data-base, file di data-base, ecc.);
 - numero di utenti concorrenti nell'unità di tempo;
- Analisi dei malfunzionamenti rilevati sia direttamente sul DB, sia attraverso funzioni/applicazioni che utilizzano il DB e segnalati mediante i canali definiti per le segnalazioni per individuarne la causa e proporre e/o implementare soluzioni correttive. L'analisi di problematiche riscontrate su funzionalità che interagiscono con il database può richiedere approfondimenti che possono portare a dover produrre segnalazioni di anomalie su cui far intervenire i gestori delle funzioni applicative oppure nell'adeguamento della configurazione del data-base.
- Nel primo caso, l'analisi condotta deve portare alla descrizione della problematica e deve essere corredata di tutti gli elementi utili e necessari per che consentano di essere approfondita con il gestore/fornitore della funzionalità o dell'applicazione.
 - Nel secondo caso, il gestore del data-base provvede a modificarne la configurazione a fronte di conferma da parte del referente del servizio.

La diagnosi del problema potrebbe necessitare l'intervento congiunto del fornitore dell'applicazione e dell'amministratore del data-base per una diagnosi del problema e per l'identificazione di possibili correzioni all'applicazione per migliorarne le prestazioni.

- Verifica dei back-up: la politica di back-up definita si appoggia sul sistema di backup gestito dall'Area sistemi Informativi. La verifica dei backup si esplica nel verificare congiuntamente con i sistemisti dell'infrastruttura del datacenter che gli script di export abbiano correttamente esportato i dati e che questi siano stati correttamente salvati secondo le politiche definite.
- Attività di eventuale recupero e import dati secondo le necessità;
- Amministrazione di rete del database: l'amministrazione di rete implica la verifica che i singoli data-base siano raggiungibili sulla rete mantenendo le locazioni e i nomi logici rispetto alle locazioni fisiche e che gli eventuali DBlink attivi e configurati verso altri DB siano operativi ed utilizzabili.
- Rendicontazione periodica delle attività, con cadenza mensile, in un documento contenente la sintesi delle statistiche di verifica delle attività del database.



- Attività di *change standard* e *change non standard* sull'ambiente. Si fornisce un esempio indicativo e non necessariamente esaustivo di attività di *change standard* per tale servizio:
 - Richieste di gestione *password* (*reset*, cambio, ecc.) per utenze definite nel DBMS;
 - Richieste relative alla gestione delle autorizzazioni utenze: normalmente la concessione delle autorizzazioni per gli end-user è demandato a logiche applicative. In alcuni casi potrebbe essere invece necessario gestire l'eventuale autorizzazione anche di livello superiore (dbo) per utenze con gestione (definizione, abilitazione, modifica) delle utenze e dei permessi;
 - creazione e manutenzione degli schemi di data-base e degli oggetti (tabelle, indici, ecc.) e creazione delle relative utenze di accesso;
 - restore di un contenuto DB attraverso le infrastrutture di Backup Management: su richiesta o in base a verifica con esito negativo dell'attività di routine di controllo backup (incidente, malfunzionamento, ecc.) in accordo con l'Ateneo;
 - Applicazione di Patch di sicurezza. È parte integrante delle attività il patch management, secondo modalità da concordare con il responsabile del servizio, e finalizzato al mantenimento del sistema in condizioni di sicurezza. Questa attività riguarda sia il sistema Operativo, sia l'ambiente RDBMS ORACLE. Le patch rilasciate da Oracle devono essere valutate in relazione all'ambiente operativo per determinare la necessità e l'opportunità di applicazione, concordando i tempi e i fermi necessari.
 - Applicazione di Patch per esigenze applicative. È possibile che eventuali patch debbano essere applicate per esigenze applicative. In questo caso sarà l'Ateneo a proporre la valutazione e a richiederne l'applicazione (concordando modalità e tempistica).
 - Riconfigurazioni di sistema o di rete a seconda delle esigenze.
 - Creazione, eliminazione o cambiamento di database/schemi /utenze secondo le necessità dell'Ateneo.
 - Riconfigurazione del sistema in caso di necessità applicative o di nuove esigenze, anche per gli aspetti relativi alla connettività.
 - Aggiornamento del sistema a versioni *supported* del DBMS (comprensivo delle attività di analisi e pianificazione delle attività, predisposizione del nuovo ambiente e migrazione di dati dal sistema precedente) qualora, nel corso della validità del contratto la versione del DB Oracle termini il suo ciclo di supporto.
 - Migrazione del DB eventualmente necessaria verso soluzioni tecnologiche differenti (es. migrazione del DB verso soluzioni su cloud, comprensiva delle attività di analisi, pianificazione ed esecuzione operativa della migrazione o di migrazione dovuta ad aggiornamento/sostituzione dell'infrastruttura tecnologica su cui è ospitato)



È parte delle attività di gestione del DBMS supportare le attività di eliminazione di tutti gli schemi/utenze non più in uso da applicativi o funzioni così da assicurare l'ottimizzazione delle risorse ad esso dedicate.

DBMS Microsoft SQL Server

Il servizio di conduzione operativa da remoto è finalizzato alla gestione operativa del sistema DBMS e include tutte le attività necessarie per garantire e mantenere il buono stato di funzionamento dello stesso, oltre che quelle finalizzate alla gestione di eventuali modifiche/aggiornamenti o revisioni architetturali secondo le esigenze dell'Ateneo.

Il database Engine SQL server in oggetto è quasi esclusivamente utilizzato come back-end per applicazioni web verticali. Attualmente risulta integrato a livello di autenticazione con il sistema Active Directory di Ateneo. Questa autenticazione viene sfruttata da diversi database anche per operare un rafforzamento delle logiche di autorizzazione applicative (provenienti da server web IIS attraverso *trusted delegation kerberos*) prevedendo gruppi con *grant* su singoli oggetti db a granularità piuttosto fine e *triggers* di metadateazione automatica e *timestamps*. Le politiche di backup attualmente sfruttano i piani di manutenzione programmati messi a disposizione dai sistemi di gestione MS SQL con cadenza giornaliera e su file locali. La macchina che ospita l'engine è istanziata come macchina virtuale IaaS presso il cloud Azure. Il server è collegato al servizio cloud Microsoft Log Analytics, per la raccolta dei log del sistema operativo e per l'audit log dell'engine SQL.

VII - SERVIZI OPZIONALI DELLA FORNITURA

Negli Articoli seguenti verranno descritti i servizi opzionali della fornitura che l'OEA potrà discrezionalmente offrire in sede di formulazione della propria offerta tecnica, senza oneri aggiuntivi per l'Università, e che saranno oggetto di apposita attribuzione del punteggio tecnico in sede di valutazione delle offerte. I servizi opzionali sono da intendersi aggiuntivi rispetto ai servizi obbligatori descritti nella precedente Sezione VI e non sono in alcun modo ad essi sostitutivi.

L'OEA, nella formulazione della propria offerta tecnica ha facoltà di prevedere o meno la fornitura dei servizi opzionali. Qualora l'OEA preveda nella propria offerta tecnica l'erogazione di uno o più servizi opzionali fra quelli previsti nella presente Sezione VII, questi dovranno essere erogati senza costi aggiuntivi per tutta la durata del contratto, incluse le eventuali opzioni di rinnovo e di proroga tecnica.

Ulteriori servizi presenti nell'offerta tecnica dell'OEA e non previsti nel presente documento, non saranno oggetto di attribuzione di punteggio tecnico premiale in sede di valutazione delle offerte.

VII.1. Opzione 1 - Servizio Supporto specialistico Sistemista Senior della Rete Dati di Ateneo – estensione ambienti Linux



Il servizio opzionale *Supporto Specialistico Sistemista Senior della Rete Dati di Ateneo – Estensione ambienti Linux*, consiste nella presa in carico anche degli ambiti tecnologici descritti negli Articoli V.2.7 e V2.8. Questa presa in carico richiede che le competenze di almeno una delle due unità di personale adibite al servizio Supporto specialistico Sistemista Senior della Rete dati di Ateneo di cui all'Articolo VI.1.1 disponga di competenze specifiche integrative relative all'amministrazione di ambienti server Linux. In particolare, il profilo di competenza dovrà prevedere almeno le seguenti conoscenze:

Qualifica professionale	Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo – estensione ambiente Linux
Conoscenze approfondite in ambito System Administration	<ul style="list-style-type: none">– Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione del sistema operativo Linux Debian;– Amministrazione e gestione moduli applicativi DNS Bind, ISC DHCP, NTP, Squid, FreeRadius, Cacti, Nagios, Apache;– Personalizzazione di file di sistema ed hardening di sistemi Linux– Gestione delle procedure di startup e shutdown;– Attività di tuning, hardening ed ottimizzazione degli applicativi;
Conoscenze approfondite in ambito Database e prodotti middleware	<ul style="list-style-type: none">– Installazione, gestione ed amministrazione di database mysql.

VII.2. Opzione 2 - Servizio Supporto specialistico Sistemista Senior Rete Dati di Ateneo – copertura estesa da remoto

Il servizio opzionale *Supporto Specialistico Sistemista Senior della Rete Dati di Ateneo – copertura estesa da remoto*, consiste nell'erogazione da remoto dei servizi di cui all'Articolo VI.1.1 nelle giornate di sabato non festivi dalle ore 9:00 alle ore 13:00 e nei giorni non festivi di chiusura degli uffici dell'Università dalle ore 9:00 alle ore 12:00 e dalle ore 14:00 alle ore 16:00.

L'Università metterà a disposizione la piattaforma per l'accesso da remoto alla Rete Dati di Ateneo, mentre l'OEA dovrà dotare il proprio personale di tutti gli strumenti hardware e software di produttività personale necessari ivi compresa la connettività Internet remota.

L'OEA dovrà inoltre dotare il proprio personale adibito al servizio di appositi telefoni mobili di servizio i cui recapiti telefonici, dovranno essere comunicati al DEC del presente appalto nella fase di avvio del Contratto, .

VII.3. Opzione 3 - Servizio Supporto specialistico Specialista Data Center on prem e cloud – formazione specialistica



Il servizio opzionale *Supporto specialistico Specialista Data Center on prem e cloud – formazione specialistica* consiste nella messa a disposizione entro 24 mesi dall'avvio del contratto di uno o più dei seguenti corsi di formazione specialistica:

1. Windows Power Shell:
 - a. Contenuti: introduzione a Powershell, modulo Powershell ActiveDirectory;
 - b. durata; 3 giorni;
 - c. modalità di fruizione: in presenza presso le sedi dell'Università oppure on-line in modalità interattiva sincrona
 - d. materiale a corredo: slide e manualistica
 - e. numero massimo di partecipanti: 10 persone
2. Security Windows Server 2019:
 - a. Contenuti: hardening, Group Policy Objects per ambienti server, backup e restore di Active Directory;
 - b. durata; 3 giorni;
 - c. modalità di fruizione: in presenza presso le sedi dell'Università oppure on-line in modalità interattiva sincrona
 - d. materiale a corredo: slide e manualistica
 - e. numero massimo di partecipanti: 10 persone
3. Office 365 Exchange OnLine Administration:
 - a. Contenuti: gestione di Exchange Online con il modulo Powershell EXO V2;
 - b. durata: 2 giorni;
 - c. modalità di fruizione: in presenza presso le sedi dell'Università oppure on-line in modalità interattiva sincrona
 - d. materiale a corredo: slide e manualistica
 - e. numero massimo di partecipanti: 5 persone
4. Configurazione e Gestione dei Record SFP, DKIM e DMARC:
 - a. Contenuti: introduzione a SPF, DKIM e DMARC; impostare SPF, DKIM e DMARC in ambiente Exchange Online;
 - b. durata: 1 giorno;
 - c. modalità di fruizione: in presenza presso le sedi dell'Università oppure on-line in modalità interattiva sincrona
 - d. materiale a corredo: slide e manualistica
 - e. numero massimo di partecipanti: 5 persone

VII.4. Opzione 4 - Servizio Supporto specialistico Specialista Cyber Security – Servizi PEN Test e Vulnerability Assesment

Il servizio opzionale *Supporto specialistico Specialista Cyber Security – Servizi PEN Test e Vulnerability Assesment* consiste nella messa a disposizione del committente di un servizio di Penetration Test sui sistemi informatici di cui all'Articolo V.1 ed un servizio di Vulnerability Assesment sui sistemi informatici di cui agli Articoli V.1 e V.2. Le attività dovranno essere eseguite secondo gli standard di riferimento del settore (OWASP, OSSTMM o equivalenti) e con strumenti e tecniche allo stato dell'arte. Al termine delle attività dovrà essere



prodotto un apposito report analitico corredato di indicazioni relative alle attività e alle azioni rimediali suggerite per ciascuna delle quali sia inoltre data evidenza delle eventuali ricadute sui servizi e dei prerequisiti necessari per poterle attuare.

Il servizio dovrà prevedere almeno una attività di Penetration Test e una di Vulnerability Assessment per ogni annualità di validità dell'appalto, compresa l'eventuale opzione di rinnovo (con annualità si intendono moduli di 12 mesi dall'avvio dei servizi).

VII.5. Opzione 5 - Servizio Supporto specialistico Specialista Cyber Security – Servizio supporto on-demand on-site per incidenti informatici

Il servizio opzionale *Supporto specialistico Specialista Cyber Security – Servizio supporto on-demand per incidenti informatici* mette a disposizione del committente un paniere di giornate annue da fruire on-demand con preavviso di 24 ore solari, il servizio prevede la messa a disposizione on site di una unità di personale con competenze pari o superiori a quelle descritte all'Articolo IX.1.2 con la finalità di supportare l'Università nella gestione di eventuali incidenti informatici o Data Breach.

In sede di offerta, l'OEA indicherà il quantitativo massimo annuo di giornate che metterà a disposizione (con annualità si intendono moduli di 12 mesi dall'avvio dei servizi); le giornate non fruite in una annualità non potranno essere fruite nell'annualità successiva.

Le singole giornate potranno essere fruite anche in sotto unità pari a mezza giornata (ogni mezza giornata fruita conterà 0,5).

In sede di offerta l'OEA potrà indicare sino ad un massimo di 18 giornate annue.

VII.6. Opzione 6 - Servizio Supporto specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – supporto on demand da remoto eventi fuori orario

Il servizio opzionale *Supporto specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – supporto on demand da remoto eventi fuori orario* mette a disposizione del committente un paniere di giornate annue da fruire on-demand in modalità da remoto, con preavviso di due giorni lavorativi. Il servizio prevede la messa a disposizione di una unità di personale con competenze pari o superiori a quelle descritte all'Articolo IX.1.5 con la finalità di supportare i servizi di Videoconferenze, Web Meeting, Web Conference e Streaming a corredo di eventi, seminari e convegni al di fuori del normale orario di servizio, compresi eventuali giorni festivi.

In sede di offerta, l'OEA indicherà il quantitativo massimo annuo di giornate che metterà a disposizione (con annualità si intendono moduli di 12 mesi dall'avvio dei servizi); le giornate non fruite in una annualità non potranno essere fruite nell'annualità successiva.

Le singole giornate potranno essere fruite anche in sotto unità pari a mezza giornata (ogni mezza giornata fruita conterà 0,5).

In sede di offerta l'OEA potrà indicare sino ad un massimo di 18 giornate annue.



L'Università metterà a disposizione la piattaforma per l'accesso da remoto alla Rete Dati di Ateneo, mentre l'OEA dovrà dotare il proprio personale di tutti gli strumenti hardware e software di produttività personale necessari ivi compresa la connettività Internet remota.

L'OEA dovrà inoltre dotare il proprio personale adibito al servizio di appositi telefoni mobili di servizio, i cui recapiti telefonici dovranno essere comunicati al DEC del presente appalto nella fase di avvio del Contratto.

VII.7. Opzione 7 - Servizio Supporto specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – Servizio continuativo feriale

Il servizio opzionale *Supporto specialistico Sistemista – Sistemi Videoconferenza e Digital Learning – Servizio continuativo feriale* consiste nell'erogazione da remoto dei servizi di cui all'Articolo VI.1.5 nelle giornate feriali dal lunedì al venerdì non coperti dal servizio on-site dell'Articolo VI.1.5 (escluse festività e giorni di chiusura degli Uffici Amministrativi dell'Università) e nelle medesime fasce orarie del servizio on-site.

Lo scopo del servizio opzionale è garantire il servizio di supporto specialistico Sistemista Videoconferenza e Digital Learning in tutti i giorni feriali dal lunedì al venerdì (escluse festività e giorni di chiusura degli Uffici Amministrativi dell'Università).

L'Università metterà a disposizione la piattaforma per l'accesso da remoto alla Rete Dati di Ateneo, mentre l'OEA dovrà dotare il proprio personale di tutti gli strumenti hardware e software di produttività personale necessari ivi compresa la connettività Internet remota.

L'OEA dovrà inoltre dotare il proprio personale adibito al servizio di appositi telefoni mobili di servizio, i cui recapiti telefonici dovranno essere comunicati al DEC del presente appalto nella fase di avvio del Contratto.

VII.8. Opzione 8 - Servizio Supporto specialistico Sistemista – Laboratori Informatici ed End Point – Servizio continuativo feriale

Il servizio opzionale *Supporto specialistico Sistemista – Laboratori Informatici ed Endpoint – Servizio Continuativo feriale* consiste nell'erogazione da remoto dei servizi di cui all'Articolo VI.1.6 nelle giornate feriali dal lunedì al venerdì non coperti dal servizio on-site dell'Articolo VI.1.6 (escluse festività e giorni di chiusura degli Uffici Amministrativi dell'Università) e nelle medesime fasce orarie del servizio on-site.

Lo scopo del servizio opzionale è garantire il servizio di supporto specialistico Sistemista Laboratori Informatici ed End Point in tutti i giorni feriali dal lunedì al venerdì (escluse festività e giorni di chiusura degli Uffici Amministrativi dell'Università).

L'Università metterà a disposizione la piattaforma per l'accesso da remoto alla Rete Dati di Ateneo, mentre l'OEA dovrà dotare il proprio personale di tutti gli strumenti hardware e software di produttività personale necessari ivi compresa la connettività Internet remota.

L'OEA dovrà inoltre dotare il proprio personale adibito al servizio di appositi telefoni mobili di servizio, i cui recapiti telefonici dovranno essere comunicati al DEC del presente appalto nella fase di avvio del Contratto.



VII.9. Opzione 9 - Servizio Conduzione Operativa da remoto DBMS – security assesment

Il servizio opzionale *Conduzione Operativa da remoto DBMS – security assesment* consiste nella messa a disposizione del committente di un servizio di Security Assesment sui DBMS di cui all'Articolo V.5. Le attività dovranno essere eseguite secondo gli standard di riferimento del settore e con strumenti e tecniche allo stato dell'arte. Al termine delle attività dovrà essere prodotto un apposito report analitico contenente l'indicazione delle problematiche rilevate e delle azioni rimediali suggerite, per ciascuna delle quali indicare il possibile impatto sui servizi erogati attraverso il sistema DBMS e i prerequisiti per poterle attuare.

Il servizio dovrà prevedere almeno una attività di Security Assesment per ogni annualità di validità dell'appalto, compresa la eventuale opzione di rinnovo (con annualità si intendono moduli di 12 mesi dall'avvio dei servizi).

VII.10. Opzione 10 – Dotazione telefoni mobili aziendali per tutto il personale dell'OEA adibito ai servizi di supporto specialistico

Con il servizio opzionale *Dotazione telefoni mobili aziendali per tutto il personale dell'OEA adibito ai servizi di supporto specialistico* l'OEA doterà tutto il proprio personale che opera presso l'Università per l'erogazione dei servizi di supporto specialistico, di telefoni mobili aziendali al fine di migliorare l'efficacia e la tempestività delle comunicazioni. I relativi recapiti telefonici dovranno essere comunicati al DEC del presente appalto nella fase di avvio del Contratto.



VIII - INDICATORI DI QUALITÀ DELLA FORNITURA

La presente sezione riporta gli indicatori di qualità per la fornitura dei servizi di System Management. Ogni indicatore di qualità è descritto con una scheda che identifica:

- la caratteristica di qualità a cui l'indicatore fa riferimento,
- la metrica e l'unità di misura con cui effettuare le misurazioni,
- il periodo di riferimento su cui calcolare l'indicatore,
- la frequenza di esecuzione della misura dell'indicatore,
- i dati elementari da rilevare per la misura,
- le eventuali regole di campionamento,
- le formule di calcolo e gli arrotondamenti da adottare,
- gli obiettivi che l'indicatore deve soddisfare espressi tramite valori soglia,
- le azioni contrattuali conseguenti al non raggiungimento degli indicatori, in funzione della criticità della violazione nel contesto specifico,
- le possibili eccezioni da considerare nell'uso dell'indicatore (ad esempio l'indicatore potrebbe non applicarsi in fase di avviamento all'esercizio di un sistema o servizio).

Si precisa che:

- con la dizione *ore e/o giorni* si intendono le ore e/o i giorni lavorativi, in funzione dell'orario di servizio stabilito;
- con la dizione *mese e/o trimestre e/o semestre* viene indicato il mese e/o il trimestre e/o il semestre di calendario nell'ambito della durata contrattuale;
- con la dizione *periodo di riferimento* viene indicato l'arco di tempo entro il quale vengono rilevate le grandezze necessarie per la misurazione dei livelli di servizio erogati.



VIII.1. Indicatori di Qualità Generali

VIII.1.1. Personale della fornitura inadeguato – IQ01

L'indicatore di qualità riguarda tutte le risorse impiegate nell'erogazione dei servizi on-site.

Caratteristica	Efficienza	Sottocaratteristica	Utilizzazione delle Risorse
Aspetto da valutare	Numero di risorse sostituite, perché non ritenute adeguate, su richiesta dell'Amministrazione		
Unità di misura	Risorse inadeguate	Fonte dati	E-mail, lettere, verbali
Periodo di riferimento	Trimestre precedente rispetto alla data in cui si effettua la rilevazione	Frequenza di misurazione	Trimestrale
Dati da rilevare	Numero di risorse impegnate nell'erogazione dei servizi onsite di cui è richiesta la sostituzione da parte dell'Amministrazione nel periodo di riferimento (<i>Nrisorse_inadeg</i>)		
Regole di campionamento	Nessuna		
Formula	$IQ01 = Nrisorse_inadeg$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ01 = 1$		
Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5		
Eccezioni	Nessuna		



VIII.1.2. Turn over del personale – IQ02

Con questo indicatore si misurano le sostituzioni operate dal Fornitore relative alle risorse impegnate nell'erogazione dei servizi on-site nonché alle eventuali risorse aggiuntive per attività temporanee, compresi eventuali Referenti.

Caratteristica	Efficienza	Sottocaratteristica	Utilizzazione delle Risorse
Aspetto da valutare	Turn over: numero di risorse sostituite su iniziativa del Fornitore		
Unità di misura	Risorse sostituite	Fonte dati	E-mail, lettere, verbali
Periodo di riferimento	Trimestre precedente rispetto alla data in cui si effettua la rilevazione	Frequenza di misurazione	Trimestrale
Dati da rilevare	• Numero di risorse impegnate nell'erogazione dei servizi on-site sostituite su iniziativa del Fornitore nel periodo di riferimento (<i>Nrisorse_sostituite</i>)		
Regole di campionamento	Nessuna		
Formula	$IQ02 = Nrisorse_sostituite$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ02 = 1$		
Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5		
Eccezioni	<ul style="list-style-type: none">o Eventuali sostituzioni finalizzate ad un migliore funzionamento dei servizi/attività, purché preventivamente condivise e approvate dai referenti dell'Amministrazione, non contribuiscono al mancato raggiungimento del valore di soglia;o Eventuali sostituzioni operate a fronte di dimissioni/licenziamento di risorse impegnate nell'erogazione dei servizi non contribuiscono al mancato raggiungimento del valore di soglia <u>purché sia rispettata almeno una delle seguenti condizioni:</u><ul style="list-style-type: none">a) ciascuna sostituzione deve essere preventivamente condivisa e concordata con il referente dell'Amministrazione, come indicato nello schema di contratto;b) ciascuna dimissione/licenziamento sia opportunamente documentata.		



VIII.1.3. Inadeguatezza del personale proposto – IQ03

L'indicatore si applica alle risorse impegnate nelle attività on-site nonché ad eventuali risorse aggiuntive per attività temporanee.

Caratteristica	Funzionalità	Sottocaratteristica	Adeguatezza
Aspetto da valutare	Inadeguatezza dei curricula delle risorse proposte		
Unità di misura	Curriculum vitae	Fonte dati	E-mail, lettere, verbali
Periodo di riferimento	Trimestre precedente rispetto alla data in cui si effettua la rilevazione	Frequenza di misurazione	Trimestrale
Dati da rilevare	Numero totale di curriculum non accettati (Ntotale_curriculum_non accettati)		
Regole di campionamento	Nessuna		
Formula	IQ03 = Ntotale_curriculum_non accettati		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ03 = 2		
Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5		
Eccezioni	Nessuna		



VIII.1.5. Attivazione degli Interventi – IQ05

Con questo indicatore si misura la tempestività di attivazione degli interventi di supporto specialistico, a partire dalla richiesta dell'Amministrazione.

Caratteristica	Efficienza	Sottocaratteristica	Efficienza temporale
Aspetto da valutare	Il tempo di attivazione degli interventi a partire dalla richiesta dell'Amministrazione		
Unità di misura	Giorno lavorativo	Fonte dati	E-mail, Lettere, verbali
Periodo di riferimento	Trimestre precedente rispetto alla data in cui si effettua la rilevazione	Frequenza di misurazione	Trimestrale
Dati da rilevare	<ul style="list-style-type: none"> Data della richiesta di attivazione di un intervento (Data_rich_int) (1) Data di attivazione dell'intervento (Data_attiv_int) (2) 		
Regole di campionamento	Nessuna		
Formula	$IQ05 = \frac{\sum_{j=1}^{N_{\text{totale_in_terv}}} \text{ritardo_attiv}_j}{N_{\text{totale_in_terv}}}$ <p>dove:</p> $T_{\text{attiv}_j} = \text{Data_attiv_int}_j - \text{Data_rich_int}_j$ $\text{ritardo_attiv}_j = 0 \quad \text{se } T_{\text{attiv}_j} \leq 5 \text{ giorni lavorativi}$ $\text{ritardo_attiv}_j = T_{\text{attiv}_j} - 5 \text{ giorni lavorativi} \quad \text{se } T_{\text{attiv}_j} > 5 \text{ giorni lavorativi}$		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ05 = 2		
Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5		
Eccezioni	Nessuna		

- Per Data della richiesta di attivazione di un intervento si intende la data della comunicazione, da parte dell'Amministrazione, dell'intervento/attività da effettuare.
- Per Data di attivazione dell'intervento si può intendere:
 - in caso di attività da eseguire in modalità a richiesta e a tempo/spesa, la data di presentazione dei curriculum vitae proposti



- b. in caso di attività da eseguire in modalità progettuale, la data di comunicazione del nominativo o di invio del curriculum vitae del referente per il progetto.

VIII.1.6. Rilievi sulla Fornitura – IQ06

I rilievi conteggiati nella metrica sono quelli notificati al Fornitore tramite lettera/e di rilievo. Ai fini della rilevazione del presente indicatore sono conteggiati i rilievi afferenti ai servizi oggetto della fornitura nonché eventuali rilievi per inadempimenti generici o afferenti ad obblighi contrattuali non adempiuti nei tempi e nei modi stabiliti dal Capitolato Speciale d'Appalto, dal Contratto e dall'Offerta tecnica.

Caratteristica	Efficacia	Sottocaratteristica	Efficacia
Aspetto da valutare	Numero di rilievi emessi relativi ad inadempimenti della fornitura		
Unità di misura	Rilievo	Fonte dati	Lettere di rilievo
Periodo di riferimento	Trimestre precedente rispetto alla data in cui si effettua la rilevazione	Frequenza di misurazione	Trimestrale
Dati elementari da rilevare	Numero rilievi emessi nel periodo di riferimento (N_{rilievi}).		
Regole di campionamento	Si considerano tutti i rilievi inseriti nelle lettera/e di rilievo formalizzate nel periodo di riferimento		
Formula	$IQ08 = N_{\text{rilievi}}$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ08 = 3$		
Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5		
Eccezioni	Nessuna		



VIII.2. Indicatori di Qualità Operativi

VIII.2.1. Tempestività di risoluzione degli Incident – IQ07

L'Indicatore di qualità misura la tempestività nella risoluzione dei ticket di incident, compresi quelli aperti in automatico dagli Strumenti di monitoraggio e controllo.

Il tempo massimo di risoluzione è legato alla “priorità” associata all'incident ed è misurato dal momento dell'apertura di ciascun ticket fino alla sua chiusura tecnica, al netto del tempo durante il quale ciascun ticket è posto in pending.

Per la rilevazione dell'indicatore sono conteggiati i ticket chiusi nel periodo di riferimento.

Gli incident vengono classificati in base alla seguente scala, con grado di gravità decrescente:

- *Priorità 1:* Bloccante: l'Utente non è in grado di usufruire del servizio per indisponibilità dello stesso o perché le sue prestazioni risultano decisamente degradate.
- *Priorità 2:* Non bloccante critico: l'Utente è in grado di usufruire del servizio anche se le prestazioni dello stesso risultano degradate in alcune sue componenti ritenute critiche dall'Amministrazione.
- *Priorità 3:* Non bloccante non critico: l'Utente è in grado di usufruire del servizio anche se le prestazioni dello stesso risultano degradate in alcune sue componenti ritenute non critiche dall'Amministrazione.

In base alle priorità degli incident sono fissati i tempi massimi di risoluzione; di seguito è riportato un esempio:

- priorità 1 – 2 h lavorative
- priorità 2 – 4 h lavorative
- priorità 3 – 8 h lavorative

La priorità inizialmente attribuita dal Service Desk potrà essere modificata su richiesta dell'Amministrazione. A titolo esemplificativo e non esaustivo, tra gli eventi che potrebbero comportare una richiesta in tal senso si possono citare:

- la concomitanza di molteplici segnalazioni di disservizio riconducibili ad un unico servizio;



- la sussistenza di situazioni di particolare criticità per l'Amministrazione (per esempio, il manifestarsi di situazioni di emergenza operativa).

Caratteristica	Efficienza	Sottocaratteristica	Efficienza temporale
Aspetto da valutare	Percentuale di ticket di incidenti risolti entro i tempi massimi previsti, dipendenti dalla priorità attribuita ai ticket stessi		
Unità di misura	Punto percentuale	Fonte dati	Strumenti di monitoraggio e controllo
Periodo di riferimento	Mese precedente la data di rilevazione	Frequenza di misurazione	Mensile
Dati elementari da rilevare	<ul style="list-style-type: none"> • Data e Ora (hh/mm/ss) di assegnazione del ticket (Data_aper_tkt) • Data e Ora (hh/mm/ss) di risoluzione del ticket (Data_risol_tkt) • Tempo di pending complessivo (T_pending) • Numero di ticket chiusi nel periodo, tenendo conto della priorità del ticket stesso (N_tkt_priorità_x) 		
Regole di campionamento	Nessuna		
Formule	$IQ12 - 1 = \frac{N_tkt_priorità_1 (T_sol \leq 2ore)}{N_tkt_priorità_1} \times 100$ $IQ12 - 2 = \frac{N_tkt_priorità_2 (T_sol \leq 4ore)}{N_tkt_priorità_2} \times 100$ $IQ12 - 3 = \frac{N_tkt_priorità_3 (T_sol \leq 8ore)}{N_tkt_priorità_3} \times 100$ <p>dove:</p> $T_sol = Data_risol_tkt - Data_aper_tkt - T_pending$		
Regole di arrotondamento	Il risultato della misura va arrotondato al punto percentuale: - per difetto se la parte decimale è ≤ 0,5 - per eccesso se la parte decimale è > 0,5		
Valore di soglia	IQ12_x = 95%		



**UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA**

Servizi System Management per
Università degli Studi dell'Insubria, per il
periodo dal 1° luglio 2022 al 30 giugno
2026, con opzione di rinnovo per
ulteriori due anni. CIG 9034264E7C –
Capitolato Speciale d'Appalto

Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5
Eccezioni	Nessuna



VIII.2.2. Tempestività di esecuzione dei change standard/predefiniti – IQ08

L'Indicatore di qualità misura la tempestività di esecuzione dei cosiddetti “change standard/predefiniti”.

Per change standard/predefinito si intende una RFC le cui attività necessarie all'implementazione (task) sono ben note e collaudate ed il cui tempo massimo di esecuzione è definito a priori.

Il tempo massimo di esecuzione è legato alla “classe” associata al change ed è misurato dal momento dell'apertura di ciascun ticket fino alla sua chiusura tecnica, al netto del tempo durante il quale ciascun ticket è posto in pending.

Per la rilevazione dell'indicatore sono conteggiati i ticket chiusi nel periodo di riferimento.

Di seguito si riporta un esempio di definizione delle classi e dei tempi massimi previsti:

- classe 1 – tempo massimo di esecuzione 30 minuti
- classe 2 – tempo massimo di esecuzione 1 h
- classe 3 – tempo massimo di esecuzione 2 h
- classe 4 – tempo massimo di esecuzione 4 h
- classe 5 – tempo massimo di esecuzione 8 h

Di seguito è riportata una lista esemplificativa e non esaustiva delle possibili attività standardizzate e delle classi associate.

Descrizione sommaria della richiesta	Attività	Classe
Richiesta di gestione password (reset, cambio, ecc..) per utenze o Access Manager	Gestione password	Classe 1
Richieste per la gestione delle utenze (definizione, abilitazione, modifica, ecc..) definite su Dominio Microsoft o Access Manager	Gestione utenze	Classe 2
Richiesta di deploy di oggetti applicativi mediante tecniche di installazione standard	Deploy oggetti	Classe 2
Richiesta del restore di un contenuto DB attraverso le infrastrutture di Backup Management	Richiesta Restore	Classe 3
Richieste per la definizione delle regole di backup di uno specifico oggetto	Gestione Backup	Classe 4



Descrizione sommaria della richiesta	Attività	Classe
Richiesta di un backup ad hoc (non previsto dalla programmazione del backup standard) di un DB o di uno schema	Richiesta Backup	Classe 4
Configuration Mng - Aggiornamento dati relativi agli elementi di configurazione su basi dati (es. CMDB)	Configuration Management	Classe 4
Richiesta di allineamento attraverso export (totale o parziale) da uno schema di origine ad un altro di destinazione	Trasferimento tra ambienti DB	Classe 5
Richiesta di correzione dati di configurazione su CMDB	Configuration Management	Classe 5

Caratteristica	Efficienza	Sotto caratteristica	Efficienza temporale
Aspetto da valutare	Percentuale di ticket relativi a change standard/predefiniti effettuati entro i tempi massimi previsti, dipendenti dalla classe attribuita ai ticket stessi		
Unità di misura	Punto percentuale	Fonte dati	Strumenti di monitoraggio e controllo
Periodo di riferimento	Mese precedente la rilevazione	Frequenza di misurazione	Mensile
Frequenza di rendicontazione	Mensile per l'andamento del livello di servizio Trimestrale per l'applicazione delle azioni contrattuali		
Dati elementari	<ul style="list-style-type: none"> Data e Ora (hh/mm/ss) di assegnazione del ticket (Data_aper_tkt) Data e Ora (hh/mm/ss) di risoluzione del ticket (Data_risol_tkt) Tempo di pending complessivo (T_pending) Numero di ticket chiusi nel periodo, tenendo conto della classe del ticket stesso (N_tkt_classe_x) 		
Regole di campionamento	Nessuna		



<p>Formula</p>	$IQ13-1 = \frac{N_tkk_classe_1(T_sol \leq 30min)}{N_tkk_classe_1} \times 100$ $IQ13-2 = \frac{N_tkk_classe_2(T_sol \leq 1ora)}{N_tkk_classe_2} \times 100$ $IQ13-3 = \frac{N_tkk_classe_3(T_sol \leq 2ore)}{N_tkk_classe_3} \times 100$ $IQ13-4 = \frac{N_tkk_classe_4(T_sol \leq 4ore)}{N_tkk_classe_4} \times 100$ $IQ13-5 = \frac{N_tkk_classe_5(T_sol \leq 8ore)}{N_tkk_classe_5} \times 100$ <p>dove:</p> <p>T-sol = Data_risol_tkt – Data_aper_tkt – T_pending</p>
<p>Regole di arrotondamento</p>	<p>Il risultato della misura va arrotondato al punto percentuale:</p> <ul style="list-style-type: none"> - per difetto se la parte decimale è ≤ 0,5 - per eccesso se la parte decimale è > 0,5
<p>Valore di soglia</p>	<p>$IQ13_x = 95\%$</p>
<p>Azioni contrattuali</p>	<p>Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5</p>
<p>Eccezioni</p>	<p>Nessuna</p>



VIII.2.3. Tempestività di esecuzione dei change non standard – IQ09

I change non standard sono cambiamenti complessi per cui non è definito a priori l'impatto, il tempo e le modalità di esecuzione; le attività richieste sono di volta in volta oggetto di pianificazione. L'indicatore misura il rispetto di tale pianificazione.

La pianificazione è concordata in fase di costruzione e approvazione del change non standard ed è tracciata direttamente sugli Strumenti di monitoraggio e controllo. Su richiesta, il Fornitore deve produrre anche uno o più Piani di lavoro da sottoporre all'approvazione dell'Amministrazione.

Per la rilevazione dell'indicatore sono conteggiati i ticket chiusi nel periodo di riferimento.

Il rispetto della pianificazione è calcolato quale differenza tra la data di chiusura tecnica effettiva e la data di fine prevista, tenendo conto di eventuali ripianificazioni.

Caratteristica	Efficienza	Sottocaratteristica	Efficienza temporale
Aspetto da valutare	Tempestività nell'esecuzione dei change non standard rispetto ai tempi previsti		
Unità di misura	Punto percentuale	Fonte dati	Strumenti di monitoraggio e controllo
Periodo di riferimento	Trimestre precedente la rilevazione	Frequenza di misurazione	Trimestrale
Dati elementari	<ul style="list-style-type: none">• Data e ora (hh/mm/ss) prevista per risoluzione del ticket (Data_fine_prev)• Data e ora (hh/mm/ss) effettiva di risoluzione del ticket (Data_fine_eff)• Numero totale di ticket chiusi nel periodo di riferimento (N_ticket)		
Regole di campionamento	Nessuna		
Formula	$IQ14 = \frac{N_ticket(T_sol = 0)}{N_ticket} \times 100$ <p>dove: $T_sol = (Data_fine_prev) - (Data_fine_eff)$</p>		
Regole di arrotondamento	Il risultato della misura va arrotondato al punto percentuale: - per difetto se la parte decimale è $\leq 0,5$ - per eccesso se la parte decimale è $> 0,5$		
Valore di soglia	IQ14 = 95%		



**UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA**

Servizi System Management per
Università degli Studi dell'Insubria, per il
periodo dal 1° luglio 2022 al 30 giugno
2026, con opzione di rinnovo per
ulteriori due anni. CIG 9034264E7C –
Capitolato Speciale d'Appalto

Azioni contrattuali	Il superamento dei valori di soglia comporta l'applicazione di penali, come specificato nell'Articolo II.5
Eccezioni	Nessuna



IX - DESCRIZIONE DEI PROFILI PROFESSIONALI

Le figure professionali proposte per lo svolgimento dei servizi oggetto della procedura dovranno rispettare i profili di seguito descritti. Per laurea si intende la laurea triennale; qualora il soggetto abbia come titolo di studio (pertinente) una laurea magistrale, l'esperienza lavorativa richiesta può essere ridotta di due anni rispetto a quanto previsto nel relativo profilo. Si precisa che la cultura equivalente può corrispondere a 4 anni di esperienza lavorativa addizionale in ambito informatico rispetto a quanto richiesto nel profilo.

Rimane fermo l'obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del contesto tecnologico avvenute in corso d'opera, adeguando le conoscenze del personale impiegato nell'erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguati, senza alcun onere aggiuntivo per l'Amministrazione.

In ogni caso, il Fornitore si impegna ad impiegare, per l'erogazione dei servizi, risorse professionali in possesso delle certificazioni previste nel presente documento e nell'offerta tecnica se migliorativa.

I curriculum vitae del personale da impiegare nei vari servizi dovranno essere resi disponibili alla Committente secondo quanto previsto dal capitolato e dal contratto, rispettando il template riportato nel disciplinare di gara.



IX.1.1. Profilo professionale Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo

Qualifica professionale	Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 7 anni di cui almeno 4 nella funzione
Esperienze consolidate	<ul style="list-style-type: none">– Interazione e relazione con gli utenti– Interazione e relazione con il personale degli ambiti applicativi di rete e sistemistici per quanto riguarda le competenze e le responsabilità del team di assegnazione– Problem determination e problem solving– Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi– Elaborazione e redazione di specifiche di progetto e di studi di fattibilità– Tecniche di progettazione e dimensionamento di architetture hardware/software– Tecniche e strumenti di monitoraggio– Certificazione CISCO Cisco Certified Network Associate (CCNA) o equivalente



Qualifica professionale	Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo
Conoscenze approfondite in ambito networking	<ul style="list-style-type: none">- Amministrazione Sistemi operativi degli apparati di rete Cisco,- Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173)- Apparati di rete (switch, router, access point wifi, ecc.)- Tecniche di bilanciamento del traffico- Tecniche di ridondanza ed alta affidabilità- Disegno e progettazione di reti TCP/IP complesse in ambienti di campus- Implementazione di infrastrutture gestionali per reti complesse- Networking in ambiente cloud, virtual switch, virtual net, micro segmentazione- Protocolli di rete (Ethernet e Virtual LAN IEEE 802.1q)- Protocolli di routing (OSPF, iBGP, eBGP)- Protocolli e gestione della qualità del traffico (ToS e DiffSRV)- Protocolli di autenticazione di rete (IEEE 802.1x)- Protocolli di trasporto ed accesso su rete wifi (IEEE 802.11 a,b,g,n,ac etc.)- Sistemi di network management- Sicurezza delle reti- Tecniche di sniffing del traffico (TCP Dump, WireShark)
Conoscenze approfondite in ambito sicurezza	<ul style="list-style-type: none">- Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc.- Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc.- Principali vulnerabilità/tipi di attacchi di rete e dei sistemi- Tecniche di ridondanza ed alta affidabilità- Amministrazione di sistemi Next Generation Firewall Fortinet Fortigate (Firewall, Intrusion Detection/Prevention, SSL Gateways, URL Filtering, Application Controll)- Tecniche di analisi dei log- Analisi di problematiche complesse ed individuazione del componente in errore- Comprovata esperienza nella definizione e progettazione di architetture di sicurezza



Qualifica professionale	Sistemista Senior per gli apparati di rete e sicurezza della Rete Dati di Ateneo
Conoscenze approfondite in ambito Operation Management	<ul style="list-style-type: none">- Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, prodotti di analisi log;
Conoscenze approfondite in ambito Client	<ul style="list-style-type: none">- Architetture dei sistemi client Microsoft e Linux- Sistemi operativi client e dispositivi mobili (es. Windows, Apple, Android)- Principali prodotti software di informatica individuale (ad es.: suite MS Office)- Web browser (es. Internet Explorer, Firefox, Chrome, Safari)
Conoscenze Linguistiche	Lingua Italiana: fluente sia nello scritto che nell'orale Lingua Inglese: in grado di leggere, parlare e scrivere in maniera più che comprensibile



IX.1.2. Profilo professionale Specialista – Cyber Security

Qualifica professionale	Specialista - Cyber Security
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 7 anni di cui almeno 4 nella funzione
Esperienze consolidate	<ul style="list-style-type: none">- Analisi e progettazione di sistemi ed infrastrutture informatiche- Analisi e progettazione di procedure complesse- Analisi in ottica Cyber Security di ambienti ed architetture ICT complesse- Redazione di policy di sicurezza di ambienti ed architetture ICT complesse- Redazione di specifiche e documentazione di progetto- Stesura documentazione e manualistica tecnica- Stima di risorse per realizzazione di progetto- Tecniche di gestione progetti- Progettazione test integrati- Capacità di analisi e risoluzione problemi- Spiccate capacità relazionali- Interazione e relazione con il personale degli ambiti applicativi, di rete e sistemistici.
Conoscenze in ambito system architecture	<ul style="list-style-type: none">- Disegno di architetture tecnologiche complesse (multivendor);- Conoscenza delle principali tendenze evolutive delle architetture tecnologiche per sistemi enterprise;- Conoscenze approfondite e integrate degli elementi tecnologici che costituiscono un sistema complesso;



Conoscenze approfondite in ambito System Administration	Personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di Linux quali, Red Hat, Debian, ecc.) e dei sistemi operativi Microsoft Windows Server (in configurazione stand alone, member server e domain controller) anche in ambienti IaaS in Cloud;
Conoscenze approfondite in ambito Continuità Operativa	<ul style="list-style-type: none">- Disaster Recovery- Orchestrazione del backup- Data loss prevention- Data retention e deduplica- Tecniche di ridondanza ed alta affidabilità
Conoscenze approfondite in ambito networking	<ul style="list-style-type: none">- Disegno e progettazione di reti TCP/IP complesse- Sistemi di network management- Sicurezza delle reti, sistemi Firewall ed IDS
Conoscenze approfondite in ambito cloud security	<ul style="list-style-type: none">- Padronanza delle tecnologie e delle architetture public cloud, hybrid cloud e private cloud- Padronanza delle tecnologie di cloud security per servizi SaaS, IaaS e PaaS- Padronanza dell'ambiente cloud Microsoft Azure, in particolare dei moduli Microsoft: 365 Defender, Azure Security Center, Network Security Group, Azure Active Directory, Log Analytics, Sentinel



Qualifica professionale	Specialista Cyber Security
Conoscenze approfondite in ambito sicurezza	<ul style="list-style-type: none">- Configurazione di apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc.- Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc.- Definizione policy per Intrusion Detection/Prevention- Padronanza di architecture Next Generation Firewall Fortinet Fortigate (Firewall, Intrusion Detection/Prevention, SSL Gateways, URL Filtering, Application Controll)- Padronanza di architetture Web Application Firewall (WAF)- Padronanza di architetture Network Admission Controll (NAC)- Padronanza delle tecniche e delle tecnologie di sicurezza per ambienti Cloud (IaaS, SaaS e PaaS)- Padronanza delle tecnologie di cloud app security- Padronanza delle tecniche e delle tecnologie di Data Loss Prevention (DLP)- Principali vulnerabilità/tipi di attacchi di rete e dei sistemi- Padronanza dei sistemi Antimalware;- Padronanza delle tecniche di Vulnerability scan e Vulnerability Assesment- Comprovata esperienza nella definizione e progettazione di architetture di sicurezza- Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799)- Conduzione di assessment di sicurezza logica, fisica e organizzativa.
Conoscenze approfondite in ambito Operation Management	<ul style="list-style-type: none">- Padronanza dei sistemi SIEM per l'analisi e correlazione dei Log (in particolare Microsoft Azure Sentinel)
Conoscenze approfondite in ambito Service Management	<ul style="list-style-type: none">- Padronanza dei prodotti di IT Service Management- Metodologia per l'analisi, il disegno, la revisione dell'IT Service Management
Conoscenze approfondite in ambito Client	<ul style="list-style-type: none">- Architetture dei sistemi client Microsoft, Apple Mac OS e Linux- Ambienti Mobile Android ed Apple IOS

Conoscenze Linguistiche	Lingua Italiana: fluente sia nello scritto che nell'orale Lingua Inglese: in grado di leggere, parlare e scrivere in maniera più che comprensibile
----------------------------	---

IX.1.3. Profilo professionale – Specialista Business Analyst

Qualifica professionale	Specialista Business Analyst
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 9 anni di cui almeno 6 nella funzione
Esperienze e competenze consolidate	<ul style="list-style-type: none"> – Spiccate capacità relazionali e abilità di interazione e relazione con gli utenti; – Problem determination e problem solving (capacità di analisi e risoluzione problemi) – Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi; – Supporto all’elaborazione ed alla redazione di specifiche e documentazione di progetto e di studi di fattibilità; – Tecniche di gestione progetti – Metodologie di project management. – Capacità di analisi di contesto e di processo – Analisi e progettazione di sistemi informativi – Forti capacità organizzative – Conoscenza dei database relazionali e linguaggi sql e loro utilizzo per estrazione dati o reportistica – Ottima conoscenza di strumenti di Office Automation
Esperienze e competenze consolidate	<p>Consolidata esperienza nel processo di amministrazione delle utenze per l’accesso ai servizi applicativi basata su profili di accesso anche complessi;</p> <p>Capacità di analisi di richieste dell’utenza e loro trasformazione in requisiti funzionali / applicativi / di processo utilizzabili per effettuare valutazioni di impatto, valutazioni di fattibilità e definizione di progetti di implementazione.</p>
Conoscenze di contesto in ambito sistemi informativi gestionali	<p>Conoscenza approfondita – finalizzata al supporto applicativo e, ove necessario, all’esecuzione di operazioni non eseguibili dagli operatori del sistema e all’analisi di nuove richieste e/o avvio di nuove funzioni, ecc.) dei sistemi gestionali, con particolare riferimento</p> <ul style="list-style-type: none"> - ai sistemi applicativi di supporto ai processi di didattica e formazione; - ai sistemi di supporto ai processi di programmazione e pianificazione delle risorse; - ai sistemi di gestione delle risorse umane; - ai sistemi di gestione dei progetti;

	<ul style="list-style-type: none"> - all' interfacciamento dei sistemi informativi con le piattaforme SPID e PagoPA. <p>Conoscenza delle piattaforme abilitanti PagoPA e SPID e delle problematiche relative al loro utilizzo e all'integrazione nei processi applicativi gestionali.</p> <p>Capacità di interazione con l'utenza e con gli ambiti organizzativi di un Ateneo e/o con i fornitori di servizi applicativi nella gestione delle segnalazioni e delle richieste degli utenti collegate all'utilizzo dei sistemi gestionali.</p> <p>Esperienza nella trasformazione di file secondo specifici tracciati secondo le esigenze degli uffici dell'amministrazione per consentire importazioni massive di dati – mediante tracciato- nei sistemi gestionali.</p> <p>Esperienza consolidata nella gestione di progetti di adozione di sistemi applicativi (sia come nuove soluzioni, sia come sostituzione di soluzioni applicative in uso) e capacità di gestione delle problematiche legate alla transizione, all'analisi dei processi e alle criticità e attività legate alla migrazione dei dati fra sistemi applicativi</p>
<p>Conoscenze Linguistiche</p>	<p>Lingua Italiana: fluente sia nello scritto che nell'orale</p> <p>Lingua Inglese: in grado di leggere, parlare e scrivere in maniera più che comprensibile</p>

IX.1.4. Profilo professionale Specialista per il contesto Data center on prem e cloud

Qualifica professionale	Specialista Data Center
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 9 anni di cui almeno 6 nella funzione
Esperienze consolidate	<ul style="list-style-type: none"> – Interazione e relazione con gli utenti – Interazione e relazione con il personale degli ambiti applicativi, di rete e sistemistici per quanto riguarda le competenze e le responsabilità del team di assegnazione – Problem determination e problem solving – Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi – Elaborazione e redazione di specifiche di progetto e di studi di fattibilità – Tecniche di progettazione e dimensionamento di architetture hardware/software – Tecniche e strumenti di monitoraggio

Qualifica professionale	Specialista Data Center
<p>Conoscenze approfondite in ambito System Administration</p>	<ul style="list-style-type: none"> - Conoscenza approfondita (installazione, personalizzazione e gestione) della piattaforma di virtualizzazione Microsoft Hyper-V. - Conoscenza approfondita della piattaforma Microsoft Azure per la gestione di macchine virtuali, reti virtuali e connessioni VPN verso i datacenter di Ateneo. - Conoscenza approfondita (installazione, personalizzazione e gestione) Microsoft Windows Server 2019 e successivi. - Conoscenza dell'ambiente a riga di comando Microsoft PowerShell. - Conoscenza approfondita (gestione) di Microsoft Active Directory Domain Services. - Conoscenza (gestione) della soluzione per l'autenticazione federata Microsoft ADFS 2019. - Conoscenza (gestione) della soluzione Microsoft Azure Active Directory Connect per la sincronizzazione degli account della directory locale con la piattaforma Microsoft 365. - Conoscenza approfondita (gestione, personalizzazione) di Microsoft Internet Information Server. - Conoscenza approfondita (gestione, personalizzazione) di Microsoft SMTP Server. - Conoscenza (installazione) linguaggio di sviluppo Web PHP per Windows. - Conoscenza approfondita (installazione, personalizzazione e gestione) della soluzione VEEAM Backup e Replication con copia dei dati di backup su dispositivi NAS locale e replica nel cloud.
<p>Conoscenze approfondite in ambito sicurezza</p>	<ul style="list-style-type: none"> - Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. - Principali vulnerabilità/tipi di attacchi di rete e dei sistemi - Tecniche di analisi dei log (Microsoft LogAnalytics) - Analisi di problematiche complesse ed individuazione del componente in errore - Comprovata esperienza nella definizione e progettazione di architetture di sicurezza - Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799) - Conduzione di assessment di sicurezza logica, fisica e organizzativa.

Qualifica professionale	Specialista Data Center
Conoscenze approfondite in ambito Client	<ul style="list-style-type: none">– Architetture dei sistemi client Microsoft– sistemi operativi client e dispositivi mobili (es. Windows, Apple, Android)– principali prodotti software di informatica individuale (es.: suite MS Office)– web browser (es. Microsoft Edge, Microsoft Internet Explorer, Firefox, Chrome, Safari)
Conoscenze Linguistiche	Lingua Italiana: fluente sia nello scritto che nell'orale Lingua Inglese: in grado di leggere, parlare e scrivere in maniera più che comprensibile

IX.1.5. Profilo professionale Sistemista Sistemi di Videoconferenza e Digital Learning

Qualifica professionale	Sistemista Videoconferenza e Digital Learning
Titolo di studio	Laurea in discipline tecniche o diploma di perito informatico o cultura equivalente
Anzianità lavorativa	Minimo 4 anni di cui 2 anni nella funzione
Esperienze consolidate	<ul style="list-style-type: none"> - Ottima capacità di lavoro in <i>team</i> - Ottime capacità relazionali e abilità di interazione con gli utenti dei servizi informatici; - Ottime capacità di <i>Problem determination</i> e <i>problem solving</i> (analisi e risoluzione problemi) - Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi; - Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità; - Metodologie di project management e di best practices ITIL; - Ottima conoscenza degli strumenti di Office Automation
Conoscenze specifiche	<ul style="list-style-type: none"> - Padronanza dei protocolli H.323 e SIP - Conoscenza interfacce di gestione Appliance Poly/polycom - Conoscenza interfacce di gestione terminali H.323 Poly e Lifesize - Microsoft Azure Media Streaming - Microsoft Teams, Stream, Sharepoint, OneDrive e in genere le soluzioni di collaborazione soluzione M365 - Padronanza della piattaforma Moodle ed in generali dei LMS - Sistemi di authoring SCORM - Cooperazione applicativa attraverso Web Services
Conoscenze base in ambito networking	<ul style="list-style-type: none"> - Protocolli di rete (Ethernet), routing, VLAN, firewalling a bassa latenza, nat traversal
Conoscenze base nell'ambito delle tecnologie di virtualizzazione	Supporto di ambienti enterprise (HyperV) ed in particolare per attività legate alla diagnostica e all'ottimizzazione delle prestazioni e latenza delle soluzioni multimediali virtualizzate a livello di macchina e networking
Conoscenze base in ambito sicurezza	<ul style="list-style-type: none"> - Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. principali vulnerabilità/tipi di attacchi di rete e dei sistemi - Conoscenza dei principali standard di sicurezza (ITSEC, BS7799)
Conoscenze Linguistiche	<p>Lingua Italiana: fluente sia nello scritto che nell'orale</p> <p>Lingua Inglese: in grado di leggere, parlare e scrivere in maniera più che comprensibile</p>

IX.1.6. Profilo professionale Sistemista laboratori informatici e gestione Endpoint

Qualifica professionale	Sistemista laboratori informatici e gestione Endpoint
Titolo di studio	Laurea in discipline tecniche o diploma di perito informatico o cultura equivalente
Anzianità lavorativa	Minimo 4 anni nella funzione
Esperienze consolidate	<ul style="list-style-type: none"> - Ottima capacità di lavoro in <i>team</i> - Ottime capacità di coordinamento personale - Ottime capacità relazionali e abilità di interazione con gli utenti dei servizi informatici; <p>Ottime capacità di <i>Problem determination</i> e <i>problem solving</i> (analisi e risoluzione problemi)</p> <p>Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici;</p> <p>Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi;</p> <p>Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità;</p> <ul style="list-style-type: none"> - Metodologie di project management e di best practices ITIL; <p>Ottima conoscenza degli strumenti di Office Automation</p>
Conoscenze in ambito System Administration	<p>Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei sistemi operativi Client Microsoft e di tipo Open;</p> <ul style="list-style-type: none"> - Approfondita conoscenza dei sistemi MDM (Mobile device management) e MAM (Mobile Application Management) ed in particolare della soluzione Intune di Microsoft e corrispondenti MDM Apple (iOS e MacOS) e Google Android per installazione centralizzata di update e applicativi - Approfondita conoscenza in ambiti di sistemi di service desk remoto (es. teamviewer ecc.) e altre soluzioni di remotizzazione desktop (RDP, ecc.) <p>Personalizzazione sistemi endpoint (policies, accessi condizionali, definizione dei criteri di conformità, ecc.)</p> <ul style="list-style-type: none"> - Gestione delle procedure di startup e shutdown remotizzate; <p>Gestione di sistemi di automazione e controllo remoto di endpoint particolari (non solo calcolatori ma anche terminali h.323, matrici audio/video, mixer, dsp e array microfonici dante compliant, proiettori, telecamere ptz ed ndi ecc.)</p>

Qualifica professionale	Sistemista laboratori informatici e gestione Endpoint
Conoscenze base in ambito sicurezza	Amministrazione sistemi Antivirus e antimalware in configurazione centralizzata/cloud; Analisi di problematiche complesse ed individuazione del componente in errore Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799)
Conoscenze in ambito cloud	Creazione, modifica, allocazione e deallocazione macchine virtuali in ambienti cloud con particolare attenzione al controllo delle impostazioni di networking e di valutazione del capacity planning delle risorse computazionali in base al workload necessario - Collegamento a sistemi di autenticazione cloud (es. Azure Active Directory)
Conoscenze Linguistiche	Lingua Italiana: fluente sia nello scritto che nell'orale Lingua Inglese: in grado di leggere, parlare e scrivere in maniera più che comprensibile