ALLEGATO 3 – CAPITOLATO TECNICO DI APPALTO SPECIFICO

AFFIDAMENTO DELLA FORNITURA SISTEMA DI GESTIONE DEGLI ACCESSI PRIVILEGIATI DEGLI AMMINISTRATORI DI SISTEMA – PAM PER UNIVERSITA' DEGLI STUDI DELL'INSUBRIA E CORRELATI SERVIZI DI MANUTENZIONE PER LA DURATA DI 24 MESI, MEDIANTE APPALTO SPECIFICO NELL'AMBITO DELL'ACCORDO QUADRO STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI
ID 2174 – Lotto Unico

INDICE

1. APPALTO SPECIFICO "AFFIDAMENTO DELLA FORNITURA SISTEMA DI GESTIONE DEGLI ACCESSI PRIVILEGIATI DEGLI AMMINOSTRATORI DI SISTEMA – PAM PER UNIVERSITA' DEGLI STUDI DELL'INSUBRIA E CORRELATI SERVIZI DI MANUTENZIONE PER LA DURATA DI 24 MESI"

Il presente Appalto Specifico rientra nell'ambito dell'Accordo Quadro stipulato da Consip per la *fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni*

Per tutto quanto non espressamente indicato nel Capitolato Tecnico di Appalto Specifico, dovrà farsi riferimento alle previsioni del Capitolato Tecnico di Accordo Quadro (Generale e Speciale) per le parti di pertinenza, che devono intendersi quindi obbligatorie e vincolanti.

In particolare i requisiti minimi del presente documento sono aggiuntivi ai requisiti minimi espressi in Accordo Quadro così come l'offerta migliorativa di Appalto Specifico deve essere aggiuntiva dell'offerta migliorativa di Accordo Quadro.

2. DEFINIZIONI

Nel corpo del presente Capitolato Tecnico, con il termine:

- **AQ** si intende l'Accordo Quadro stipulato da Consip;
- **AS** si intende il presente Appalto Specifico;
- **Amministrazione/Amministrazione Contraente**, si intende nel complesso le strutture organizzative facenti capo a Università degli Studi dell'Insubria
- **Punto Ordinante o, brevemente, PO** l'Amministrazione richiedente l'AS sul sistema di E-Procurement di Consip;
- **CTAQ** si intende il Capitolato Tecnico Speciale dell'Accordo Quadro;
- **OEAQ** si intende l'offerta economica vincolante del Fornitore Aggiudicatario per l'AQ;
- **OTAQ** si intende l'offerta tecnica vincolante del Fornitore Aggiudicatario per l'AQ;
- **OTAS** si intende l'offerta tecnica vincolante del Fornitore aggiudicatario dell'AS, che integra e migliora l'OTAQ;
- **CTGAQ** si intende il Capitolato Tecnico Generale dell'Accordo Quadro
- **CdO** si intende il Capitolato d'oneri dell'Accordo Quadro
- **Concorrente** o **Offerente**: il RTI che partecipa alla presente gara;
- **Contratto Esecutivo**: il contratto stipulato dall'Amministrazione con il Fornitore, che si perfeziona dopo l'aggiudicazione dell'Appalto Specifico;

- **CV:** centri di valutazione del Ministero dell'interno e del Ministero della difesa;
- **CVCN:** Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia per la cybersicurezza nazionale;
- **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;
- **Meta-prodotto**: rappresenta l'offerta di riferimento per ogni prodotto richiesto in prima fase. Ogni meta-prodotto è caratterizzato dalla sua descrizione funzionale, da requisiti minimi, dai requisiti migliorativi offerti in prima fase e da un prezzo di riferimento che non potrà essere superato in AS, **ma non da una specifica tecnologia** (marca, modello, release firmware/software);
- **Prodotto**: rappresenta uno specifico prodotto (marca, modello, release firmware/software) offerto in seconda fase come istanza del meta-prodotto offerto in prima fase. Lo specifico prodotto offerto avrà quindi descrizione funzionale, requisiti minimi, requisiti migliorativi del corrispondente meta-prodotto offerto in prima fase ed eventuali ulteriori requisiti migliorativi offerti in base alle richieste dell'Amministrazione Contraente. Il prezzo del prodotto non potrà superare quello del corrispondente meta-prodotto a meno di quanto espressamente previsto nel Capitolato d'Oneri;
- **Portale della fornitura**: il Portale implementato dal Fornitore aggiudicatario secondo le specifiche tecniche descritte nel Capitolato Tecnico parte Generale al paragrafo 4.1
- **Servizi Base**: i servizi, a condizioni non tutte definite, che possono essere richiesti dalle Amministrazioni a completamento della fornitura richiesta in AS, ad eccezione dei servizi inclusi nella fornitura che dovranno essere obbligatoriamente erogati;
- **Servizi Aggiuntivi**: i servizi, a condizioni da definire da parte delle Amministrazioni, che possono essere richiesti a completamento della fornitura prevista in AS. L'Amministrazione potrà valorizzare i servizi accessori secondo le regole riportate nel Capitolato d'Oneri;
- **Sistema telematico (o semplicemente "Sistema")**: indica la piattaforma telematica attraverso cui saranno gestiti gli Appalti Specifici;
- **Responsabile dell'Amministrazione:** la persona indicata dall'Amministrazione nel contratto esecutivo e individuata come interlocutore tecnico con il Fornitore per tutte le attività contrattuali.
- **Responsabile del Fornitore:** la persona indicata dal Fornitore, nell'ambito di ciascun contratto esecutivo, come referente operativo per le attività di fornitura ed erogazione dei relativi servizi connessi, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.2 del Capitolato Tecnico Generale di AQ;
- **RUAC:** responsabile unico delle attività contrattuali, cioè il referente del Fornitore nei confronti di Consip S.p.A. per tutte le attività di gestione relative all'AQ, dotato di appositi poteri di firma tali da impegnare in maniera esecutiva il Fornitore nei confronti delle Amministrazioni, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.1 del Capitolato Tecnico Generale di AQ;
- **Vendor/produttore**: si intende il produttore dello specifico prodotto.
- **RDA**: Rete Dati di Università degli Studi dell'Insubria
- **ASI**: Area Sistemi Informativi di Università degli Studi dell'Insubria

- **PAM**: sistema di gestione Accessi Privilegiati Amministratori di Sistema

3. CONTESTO DELL'APPALTO SPECIFICO ED ELEMENTI TRASVERSALI AI VARI SERVIZI

L'adozione massiva delle tecnologie dell'informazione a supporto dei processi necessari allo svolgimento dei compiti istituzionali dell'Ateneo, nonché il ruolo centrale svolto dagli strumenti ICT a supporto della Ricerca Accademica, ha portato nel tempo l'Ateneo a utilizzare largamente infrastrutture e sistemi informatici e di telecomunicazioni.
Gli *asset* ICT costituiscono un fattore strategico che richiede necessariamente specifici investimenti e adeguamenti infrastrutturali al fine di implementare strumenti e politiche di sicurezza allo stato dell'arte. L'Agenzia per l'Italia Digitale (AgID) ha sollecitato tutte le Pubbliche Amministrazioni a elevare i propri standard di sicurezza con la Circolare 18 aprile 2017, n. 2 e pubblicata in G.U.R.I il 5 maggio 2015, n. 103 in cui ha emanato le *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni.*
Nelle misure di sicurezza richieste (ABSC), un'intera sezione riguarda la corretta gestione degli accessi ai sistemi ICT con privilegi di amministrazione, al ciclo di vita degli account privilegiati, alla robustezza delle credenziali usate, all'esclusivo utilizzo di protocolli sicuri e al monitoraggio di eventuali eventi anomali nell'utilizzo degli accessi stessi.
L'Ateneo adotta soluzioni architetturali IT basate su modelli di *cloud ibrido*, con la coesistenza di installazioni su piattaforme di *cloud* privato, principalmente in modalità IaaS, affiancate da infrastrutture IT presenti presso le proprie sedi e quindi connesse alla rete locale. L'ecosistema dei sistemi ICT dell'Ateneo è molto variegato, sia dal punto di vista tecnologico sia dal punto di vista dell'impiego degli stessi. Tipicamente tutti i sistemi ICT prevedono la presenza di credenziali di accesso con privilegi di amministratore, necessarie per la loro conduzione tecnica, con modalità di accesso eterogenee e con gradi di sicurezza non omogenei.
Gli obiettivi di sicurezza ICT che si vogliono perseguire sono l'utilizzo esclusivo di protocolli sicuri per accesso remoto con finalità di amministrazione, il consolidamento delle *policy* di sicurezza (protocolli utilizzati, complessità delle *password*, etc.), la limitazione della superfice d'attacco esposta verso Internet (*gateway* sicuri), consolidamento del ciclo vita degli account con privilegi di amministrazione sia del personale interno sia dei fornitori ICT esterni.

Il presente appalto specifico è finalizzato alla fornitura di una infrastruttura per la gestione degli accessi con credenziali di amministratore di sistema per l'Area Sistemi Informativi (ASI) di Università degli Studi dell'Insubria.
L'adozione di una piattaforma PAM è finalizzata a perseguire i seguenti obiettivi:

- implementare le funzionalità richieste dalle ABSC 5 delle *Misure minime di sicurezza ICT* per le pubbliche amministrazioni emanate da AgID;
- implementare un unico punto di ingresso per gli accessi con credenziali di amministrazione di sistemi, applicazioni e apparati ICT, consolidando su un unico gateway il canale di accesso, evitando così una pluralità di abilitazioni attraverso i firewall di frontiera con pluralità di protocolli (SSH, RDP, etc.), pluralità di *target* (server, bastion host, apparati di rete, *appliance*, etc.) acceduti da una molteplicità di indirizzi IP esterni (fornitori, operatori remoti, etc.) ed interni (personale dell'Ateneo);

- garantire la confidenzialità delle sessioni remote (tramite cifratura sicura del canale di comunicazione) senza l'utilizzo di accessi *Virtual Private Network* (VPN) al fine di evitare la frammentazione e duplicazione del processo di gestione del ciclo di vita degli account di accesso amministrativo;
- disaccoppiare i client *desktop* usati dagli amministratori dai sistemi amministrati, evitando che postazioni di lavoro compromesse possano veicolare *malware* verso i sistemi IT core;
- consolidare in un unico punto il controllo del ciclo di vita delle credenziali amministrative, con account personali dei singoli operatori, evitando l'utilizzo di account condivisi ed utenze standard quali *administrator, root, manager*, etc.;
- consolidare in un unico punto la raccolta dei log degli accessi amministrativi richiesti dalle direttive del Garante della Privacy, con possibilità di audit delle sessioni in ottica di *accountability* richieste dal Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
- minimizzare i punti di accesso con privilegi di amministrazione esposti sulla frontiera della Rete Dati dell'Ateneo;
- automatizzare il cambio *password* degli account con privilegi di amministrazione, evitando dispendiose procedure manuali e adottando politiche uniformi e facilmente verificabili per i vari *host* in base a gruppi omogenei di criticità;
- consentire le attività amministrazione dei sistemi IT adottando esclusivamente protocolli sicuri per le sessioni remote di amministrazione;
- implementare flussi di autorizzazione per l'accesso a target critici e contenenti dati particolarmente sensibili;
- conservare le credenziali di amministrazione dei sistemi IT in modalità sicura e confidenziale;
- implementare funzionalità di *strong authentication* per l'accesso a target critici e contenenti dati particolarmente sensibili.

Con riferimento alle *Misure minime di sicurezza ICT* per le pubbliche amministrazioni emanate da AgID, si richiamano di seguito, le misure pertinenti:

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE				
ABSC_ID			Livello	Descrizione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
				Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.

5	6	1	A	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.

5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

La fornitura del sistema PAM oggetto dell'appalto specifico andrà a sostituire un pre-esistente sistema già in uso all'Area Sistemi Informativi ed implementato con una soluzione realizzata con prodotti Cyber Arc, divenuto nel tempo obsoleto ed inglobando alcuni componenti software per le quali non è più disponibile il supporto del Vendor.
L'infrastruttura verrà utilizzata dai tecnici con incarico di amministratore di sistema ed appartenenti al personale afferente all'Area Sistemi Informativi, nonché da tecnici qualificati di società esterne a cui l'area Sistemi Informativi ha appaltato la gestione e/o la conduzione operativa di alcuni servizi o infrastrutture, pertanto verrà anche richiesta l'erogazione dei necessari moduli formativi finalizzati a rendere autonomo il personale del committente nella operatività ordinaria della soluzione PAM fornita.
L'oggetto della fornitura di cui al presente appalto specifico ricomprende anche tutti i servizi di manutenzione per la durata di 24 mesi sui beni forniti.
L'oggetto della fornitura di cui al presente appalto specifico ricomprende anche tutti i servizi di istallazione configurazione dei beni forniti nonché la migrazione delle configurazioni dal pre-esistente sistema Cyber Arc a quello di nuova fornitura quale essa sia la tecnologia selezionata dal fornitore.
Da ultimo, l'appalto specifico prevederà anche la fornitura di un monte giornate di supporto professionale, per un numero massimo e non garantito, finalizzato ad erogare supporto tecnico specialistico a richiesta sulla soluzione PAM oggetto della fornitura, al fine di supportare l'Ente nella risoluzione di eventuali problematiche complesse o nell'evoluzione delle configurazioni del prodotto fornito.

4. CONTESTO ORGANIZZATIVO, TECNOLOGICO E NORMATIVO

4.1 Contesto organizzativo

Università degli Studi dell'Insubria è una università pubblica fondata il 14 luglio 1998, persegue come gli altri Atenei italiani i propri compiti istituzioni negli ambiti Formazione, Ricerca e Terza Missione.
Università degli Studi dell'Insubria appartiene alla categoria delle Pubbliche Amministrazioni Locali (PAL).

L'Ateneo è stato istituito con due poli paritetici nelle città di Como e di Varese, inoltre ha una terza sede a Busto Arsizio (VA). 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.

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

- Amministrazione Centrale (AC) e relative Aree Dirigenziali:

  - Area Sistemi Informativi (ASI)
  - Area Infrastrutture ed Approvvigionamenti (AIA)
  - Area Didattica e Ricerca (ADR)
  - Area Risorse Umane e Finanziarie (ARUF)
  - Area Servizi Bibliotecari e Documentali (ASBD)
  - Area Affari Generali ed Istituzionali
- Dipartimento di Medicina e Chirurgia (DMC);
- Dipartimento di Medicina ed Innovazione Tecnologica (DMIT)
- 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).

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
- 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
- Gestione postazioni di lavoro per il personale amministrativo dell'Amministrazione Centrale, per i laboratori informatizzati per la didattica e per le postazioni informatiche delle aule didattiche.

Il presente Appalto Specifico ha come struttura referente l'Area Sistemi Informativi - ASI.

4.2 Contesto tecnologico

Il contesto tecnologico di competenza dell'Area Sistemi Informativi può essere schematizzato nei seguenti macro ambiti:

- Datacenter e servizi in cloud
- Infrastrutture e Servizi Networking, Network Security e Network Management
- Servizi Telefonici
- Gestione Identità Digitali e Sistemi di autenticazione
- Sistemi Informativi
- Servizi a supporto della Comunicazione Avanzata e Digital Learning
- Gestione EndPoint ed Assistenza Tecnica

4.2.1 Data Center e Servizi in Cloud

A seguito di una progressiva politica di migrazioni a soluzioni cloud based, la maggior parte dei sistemi server gestiti dall'Area Sistemi Informativi 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.

4.2.1.1 Data Center "Colonia"

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

Un HPE Proliant DL 650 Gen10 NVMe: un nodo fisico, sedici dischi e quattro interfacce di rete esterne attivate che ospita una 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
-

Un Dispositivo NAS con funzione di repository locale delle copie di backup dei dati e delle macchine virtuali.

Due Appliance per i servizi di supporto alla Rete Dati:
- 1 Controller wifi Huawei
- 1 appliance Infoblox dotata del sistema di Network Automation Infoblox NetMRI

4.2.1.2 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 che ospita una 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

Un Dispositivo NAS con funzione di repository locale delle copie di backup dei dati e delle macchine virtuali.

Una Appliance per i servizi di supporto alla Rete Dati: Controller wifi Huawei

Appliance per i servizi di comunicazione H.323:
- Polycom DMA: Gatekeeper H.323
- Polycom Access Director
- Polycom Resource Manager:
- Polycom Media Suite Gold
- Polycom RMX virtuale
- Polycom Media Suite Gold Backup

4.2.1.3 Cloud "Azure" Microsoft – infrastruttura IaaS

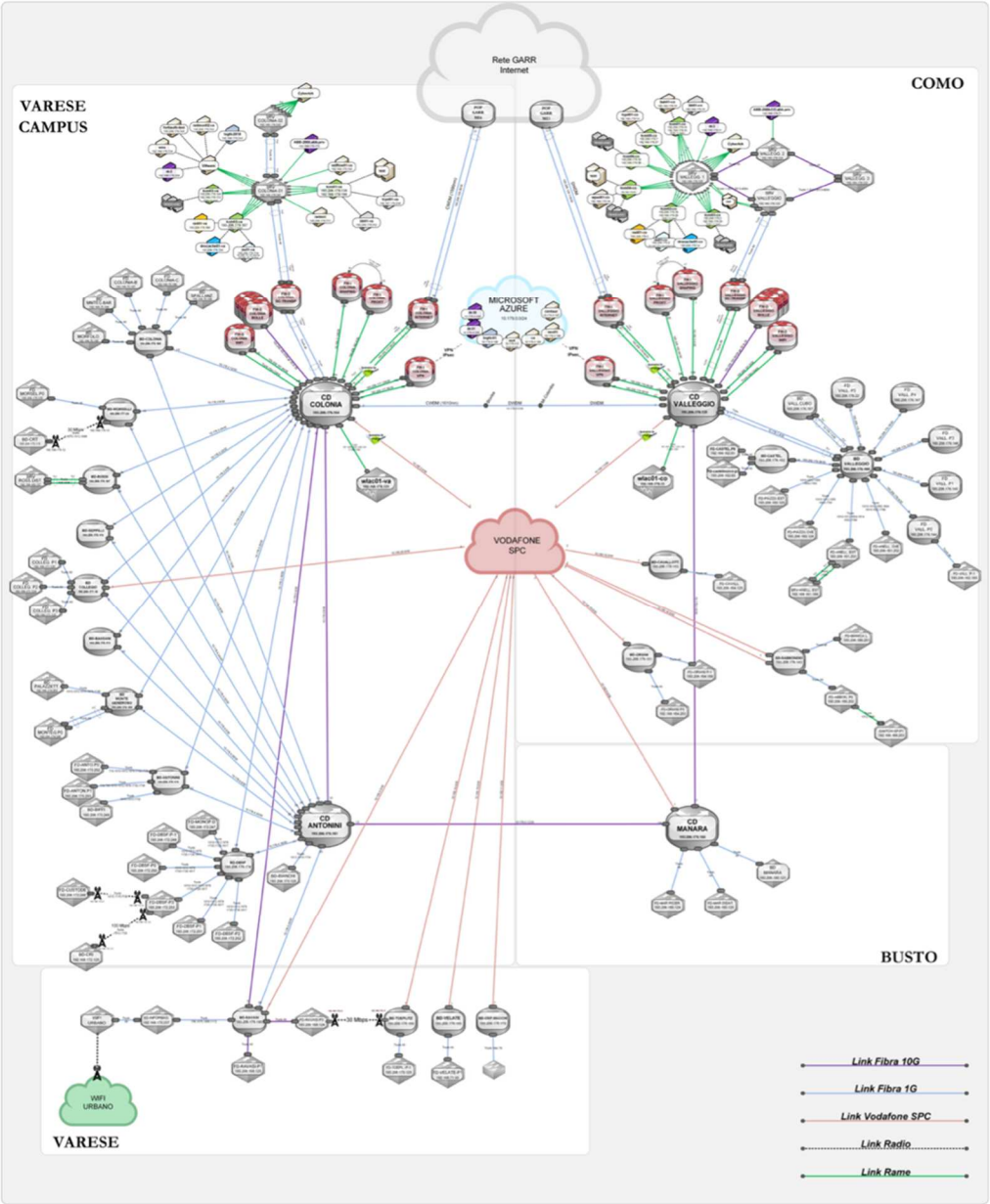
L'Ateneo adotta per le proprie infrastrutture una architettura di tipo Hybrid Cloud, dove convivono infrastrutture on-premises ed infrastruttura on-cloud.

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

- Linux Debian
- Microsoft Windows Server 2019

4.2.2 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 e Dipartimenti. 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'interconnessone 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').

4.2.2.1 Rete Dati di Ateneo - Connettività

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 Montegenerso 71 (Colonia) ed il secondario dalla sede di Como via Valleggio 11 (Valleggio); attualmente l'Ateneo è connesso alla rete GARR-T con due collegamenti una capacità di banda pari ciascuno a 2 Gbps,.
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).
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).

4.2.2.2 Rete Dati di Ateneo – 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, (forniti in modalità as a service all'interno del *Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni*) e collocati rispettivamente uno nel data center di Varese Colonia ed il secondo in quello di Como Valleggio.

Firewall Interni: presso i data center di Varese Colonia ed di Como Valleggio sono presenti complessivamente 2 firewall Fortigate di Fortinet (forniti in modalità as a service all'interno del *Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni*) 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. I client, segregati attraverso la rete overlay Ipsec, accedono alla navigazione Internet attraverso un web proxy per l'accesso sicuro a Internet (fornito in modalità as a service all'interno del *Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni*).
Web Application Firewall: i portali web ospitati nel cloud privato Microsoft Azure, sono protetti tramite il servizio Web Application Firewall – WAF reso disponibile da Azure, i portali Web ospitati all'interno della Rete dati di Ateneo, sono protetti tramite Web Application Firewall di Fortinet (fornito in modalità as a service all'interno del *Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni*)
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 Spamhaus; tutti gli host interni alla rete utilizzano come resolver DNS due server gestiti dall'Area Sistemi Informativi con blocco della risoluzione delle URL dannose.

4.2.2.3 Rete Dati di Ateneo – accesso 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 Entreprise 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.

4.2.2.4 Rete Dati di Ateneo – Connettività verso Private 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.

4.2.3 Il 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 11 Centrali Telefoniche Alcatel OmiPCX. 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 istallazioni singole di centrali telefoniche Alcatel OmniPCX presenti nelle sedi:

- Varese via Ravasi 2
- Varese via Medaglie D'Oro 35 (Collegio City)
- 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)

4.2.4 Sistemi Informativi Gestionali

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.
A completamento della soluzione integrata del consorzio CINECA sono in uso una serie di applicativi "satellite" che coprono aree funzionali più verticali e specifiche.
Al momento, tutti gli applicativi a supporto della attività gestionali non realizzati all'interno dell'Ateneo sono acquisiti in modalità *as a service.*

4.2.5 Sistemi di Comunicazione Avanzata e Collaboration

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).

4.2.5.1 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

4.2.5.1 Servizi multimediali asincroni H.323 e Azure Media Service

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.
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 e caricati in cloud.

4.2.6 Servizi di supporto alla Cyber Security

La modalità di approccio ai servizi Cyber Security dell'Ateneo è fortemente correlata con il modello organizzativo dell'Ateneo che prevede una forte autonomia dei singoli dipartimenti per tutto ciò che attiene gli ambiti di ricerca, questo si declina poi con l'autonomia dei singoli dipartimenti anche in ambito informatico.
Conseguentemente, l'Area Sistemi Informativi cura a livello centrale la sicurezza per:

- la Rete Dati di Ateneo intesa come infrastruttura centralizzata di trasmissione dati
- servizi DNS autoritativi dominio uninsubria.it ed uninsubria.eu, resolver DNS per i client della Rete Dati di Ateneo
- accesso remoto in modalità VPN client to site e site tu site
- le identità digitali di Ateneo ed i sistemi deputati alla loro gestione (Microsoft Active Directory e Microsoft Azure Active Directory)

- infrastrutture server on-prem e cloud gestiti dall'Area Sistemi Informativi
- Data Base gestiti dall'Area Sistemi Informativi
- Web application gestite dall'Area Sistemi Informativi
- End point gestiti dall'Area Sistemi Informativi (Desktop, Notebook, Tablet, Smartphone)
- Sistemi di multimediali e di videoconferenza gestiti dall'Area Sistemi Informativi

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 – protezione perimetrale:
Per la protezione perimetrale della Rete Dati di Ateneo sono previsti appositi next generation firewall con funzionalità Statefull firewall L7, IPS; URL Filtering, Application Control, Traffic Shaping. Il perimetro è costituto dai due accessi alla rete Internet, gli accessi tramite reti wifi e gli accessi in modalità VPN

Sicurezza logica – segregazione interna:
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

- Rete overlay VPN Ipsec per le postazioni degli operatori dell'Assistenza tecnica IT
- Reti overlay VPN Ipsec per le postazioni dipartimentali (7 dipartimenti)

La Rete dati di Ateneo prevede firewall perimetrali 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.
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.

Sicurezza delle reti wifi
La rete di accesso wifi è tipicamente utilizzata in modalità BYOD, per questo motivo 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 Controll 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
- Partecipanti ad Eventi 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 ed Eventi: 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.

Sicurezza dei resolver DNS (DNS Firewall)
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.

Sicurezza degli accessi degli Amministratori di sistema dell'Area Sistemi Informativi
L'accesso remoto agli apparati della Rete Dati, server ed appliance, non è consentito con connessioni dirette dall'esterno, ma avviene 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.

Sicurezza delle identità digitali di Ateneo
L'accesso dell'Ateneo avviene tramite autenticazione con le credenziali associate alle Identità digitali di Ateneo, inoltre per tutte le applicazioni ed i servizi compatibili anche tramite credenziali SPID e CIE.
Le identità digitali di Ateneo sono gestite tramite back-end Microsoft Active Directory sincronizzato anche con l'ambiente cloud Microsoft Azure Active Directory. L'Ateneo adotta misure di sicurezza protezione delle credenziali digitali di Ateneo, quali criteri di complessità delle password, cambio obbligatorio della password ogni 90gg, protezione da attacchi brute force, accesso da reti esterne con autenticazione a due fattori per i servizi e le applicazioni compatibili, servizi cloud di monitoraggio degli accessi ed identificazione eventi di sicurezza, correlazione degli eventi tramite SIEM Microsoft Sentinel.

Sicurezza dei Server
I server gestiti dall'Area, ove compatibili, sono integrati nella piattaforma Microsoft Defender for Cloud, al fine di monitorarne la postura di sicurezza e raccogliere gli eventi di sicurezza tramite Microsoft Log Analitics e poi vengono processati e gestiti dal servizio SIEM Microsoft Sentinel.
Tutti gli apparati della Rete Dati ed i server dell'Area Sistemi Informativi, sono inoltre 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.
Per gli ambienti data center on-prem sono previsti next generation firewall dedicati, mentre per i server ospitati in ambiente IaaS Microsoft Azure, si utilizzano i servizi messi a disposizione dalla piattaforma (NSG, Azure Firewall, Azure Web Application Firewall).

Sicurezza degli EndPoint
La sicurezza degli end point gestiti dall'Area Sistemi Informativi (desktop, notebook, tablet e smartphone) viene gestita attraverso i servizi cloud di Microsoft Azure: Intune e Defender for EndPoint. Il servizio Defender for End Point è integrato con il servizio SIEM Microsoft Sentinel per la correlazione ed identificazione degli eventi di sicurezza.

4.3 Contesto Normativo

L'intervento oggetto del presente Appalto Specifico riguarda esclusivamente servizi interni alla propria Amministrazione, conseguentemente è al Piano triennale in accordo al paragrafo 2.3 del CTGAQ come *Obiettivo 1° livello 'Servizi' – Servizi Interni alla propria PA*.

L'Amministrazione, attraverso i beni e servizi acquisiti nel presente Appalto specifico, concorre inoltre a perseguire gli obiettivi definiti nel Capitolo 6 – *Sicurezza Informatica* del Piano Triennale per l'Informatica della PA 2022-2024, in modo sinergico e complementare ai servizi di cyber Security acquisti tramite apposito Contratto Esecutivo stipulato in adesione "Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni - ID Sigef 2296".

Indicatori di Digitalizzazione - Indicatore Generale:

L'intervento oggetto del presente Appalto specifico, comporterà una riduzione di costi per Amministrazione rispetto a quanto sostenuto in precedenza attraverso l'acquisizione in autonomia della piattaforma PAM Cyber Arc, si adotterà quindi l'indicatore generale di tipo quantitativo *"Riduzione % della spersa per l'erogazione del servizio"*.

Indicatori di Digitalizzazione - Indicatore Specifico:

In particolare, il presente Appalto Specifico, interviene sui livelli di adozione delle ABSC 5 delle *Misure minime di sicurezza ICT* per le pubbliche amministrazioni emanate da AgID, conseguentemente in accordo alle modalità definite nel paragrafo 1.4.2.1 del CTGAQ, l'indicatore specifico di digitalizzazione adottato sarà il livello di implementazione delle ABSC 5 secondo lo schema:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Richiesta di Offerta dell'AS
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		

Regole di campionamento	Nessuna
Formula	$Ip = (N_1 – N_0)/N_T$
Regole di arrotondamento	Nessuna
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*
Applicazione	Amministrazione Contraente

L'Appalto specifico in oggetto non afferisce agli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 o dal PNC.

L'Appalto specifico in oggetto non include prodotti e servizi tra quelli indicati nell'elenco dei prodotti, sistemi e servizi da sottoporre al Technology screening dal DPCM 15 giugno 2021 pubblicato il 19 agosto 2021.

Per l'Appalto specifico in oggetto non è stata effettuata la comunicazione di affidamento al CVCN o CV di cui all'art. 3 del DPR n. 54/2021.

5. OGGETTO, DURATA DELL'APPALTO SPECIFICO E LUOGO DI ESECUZIONE

5.1 Oggetto della fornitura

Il presente AS ha ad oggetto i seguenti prodotti/servizi:

Prodotti: Privileged Access Management (PAM)

- Funzionalità Migliorative:
  - ID 7.2 Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto
  - ID 7.4 Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata
  - ID 7.9 Possibilità di effettuare un'analisi di dettaglio delle minacce informatiche per identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità:
- Requisiti Migliorativi:
  - AS.7.4 Supporto di dispositivi di rete e di dispositivi e sistemi di sicurezza specifici richiesti dall'Amministrazione
  - AS.7.6 Integrazione con una specifica soluzione di MFA richiesta dall'Amministrazione

Servizi base connessi alla fornitura:

- installazione e configurazione (inclusi nella fornitura)
- formazione e affiancamento
- manutenzione profilo LP (comprensiva di help desk)
- Contact Center (incluso nella fornitura)
- supporto specialistico

Si rimanda al paragrafo "Descrizione della fornitura" per le caratteristiche specifiche dei prodotti e servizi richiesti.

5.2 Durata del contratto

La durata del contratto è pari a **24 mesi** a decorrere dalla verifica di conformità con esito positivo.

5.3 Luogo di esecuzione ed orario di erogazione dei servizi

La fornitura della soluzione PAM oggetto dell'appalto specifico, prevedrà l'istallazione dei prodotti presso il Data Center di via Monte generoso 71 Varese, nel caso di soluzione basata su prodotti Hardware, mentre se la soluzione adotta componenti Software da istallarsi in ambient virtuale, sarà possibile implementarli o nell'ambiente di virtualizzazione Microsoft Hyper-V dell'Ateneo ospitato presso il presso il Data Center di via Monte generoso 71 Varese o in alternativa nell'ambiente private cloud Microsoft Azure del Tenant di Università degli Studi dell'Insubria.
Le attività di configurazione della soluzione PAM fornita dovranno essere effettuate on-site presso la sede di Varese dell'Area Sistemi Informativi in via Ravasi 2.
I servizi di manutenzione potranno essere erogati da remoto, oppure on-site presso il sito di istallazione della soluzione PAM, quando questo lo richieda.
Il servizio erogato tramite i moduli di formazione per l'utilizzo della soluzione PAM fornita, potrà essere erogato da remoto, purché in modalità didattica sincrona ed interattiva con i discenti.
I servizi di supporto specialistico potranno essere erogati da remoto con profilo 'LP' come previsto nel CTAQ e nell'OTAQ.

6. DESCRIZIONE DELLA FORNITURA

6.1 Garanzia

Per la garanzia dei prodotti, il Fornitore faccia riferimento al par. 2.1.10 del CTAQ.

6.2 Prodotti -PAM

Con riferimento ai meta prodotti offerti in prima fase di aggiudicazione dell'Accordo Quadro, il presente Appalto Specifico ha per oggetto la fornitura di una infrastruttura PAM di cui al Paragrafo 2.18 del CTAQ.
La soluzione PAM richiesta nel presente Appalto Specifico, come specificato nella Richiesta d'Offerta, deve gestire sino a **50 utenti** del servizio (account nominativi), conseguentemente rientra nella tipologia **PAM_2 (Fascia 2)** offerta in prima fase e prevista al Paragrafo 2.18 del CTAQ.
Al fine di identificare il prodotto più idoneo per il presente appalto specifico, la soluzione proposta potrà essere realizzata tramite prodotti Hardware da istallare presso l'Ateneo, oppure componenti esclusivamente Software da istallarsi in ambiente virtuale; questi ultimi sarà possibile implementarli o nell'ambiente di virtualizzazione Microsoft Hyper-V dell'Ateneo o in alternativa nell'ambiente private cloud Microsoft Azure del Tenant di Università degli Studi dell'Insubria.
La soluzione PAM richiesta ha lo scopo di andare a sostituire l'attuale soluzione PAM in uso presso l'Amministrazione basata sulla piattaforma Cyber Arc.
La soluzione attualmente in uso è impiegata quasi esclusivamente per accedere a target standard (network device in modalità SSH, server Linux in modalità SSH, server Windows in modalità RDP).
L'attuale soluzione è costituita da una architettura di macchine ospitate presso l'Amministrazione ed in grado di erogare tutti i servizi correlati e necessari (autenticazione, gestione ciclo di vita account, cambio password/ reset password, autenticazione MFA, logging delle sessioni, storage) in modo autoconsistente senza dipendenze da altre infrastrutture o servizi dell'amministrazione.

Al fine di identificare il prodotto più adatto, fra quelli selezionati come idonei al meta-prodotto previsto in Accordo Quadro, si precisano i seguenti requisiti funzionali di base richiesti:

- La nuova soluzione proposta dovrà egualmente garantire l'autoconsistenza ed erogare tutti i servizi e funzionalità richieste nel presente appalto specifico senza la necessità di utilizzare altri servizi dell'Amministrazione.
- La nuova soluzione verrà utilizzata per accedere alla stessa tipologia di host attualmente gestititi tramite il PAM Cyber Arc, quindi con l'utilizzo di modalità SSH (network device Cisco e server Linux Debian) e modalità RDP (server Windows).
- La soluzione proposta, nel caso preveda di essere istallata in un ambiente di virtualizzazione dell'Amministrazione, dovrà necessariamente essere compatibile con i due ambienti in uso:
    - Microsoft Huper-V, nel caso di istallazione preso i locali dell'Amministrazione
    - IaaS Microsoft Azure, nel caso di istallazione in ambiente cloud

- se la soluzione prevede l'utilizzo di virtual machine e/o virtual appliance ospitate su infrastrutture dell'Ateneo, per limiti di disponibilità delle stesse per l'ambiente on-prem e contenimento dei costi per la soluzione cloud, queste non dovranno essere complessivamente superiori a 3 macchine/appliance virtuali

- La soluzione proposta dovrà essere dimensionata in modo opportuno (in termini di numero di nodi ed architettura) al fine di supportare adeguatamente il carico di lavoro stimato:
  - Numero di target gestiti 300
  - Numero di utenti singoli gestiti: 50
  - Tasso di contemporaneità utenti: 20%
  - Numero massimo di sessioni contemporanee (RDP+SSH): 50
- La soluzione proposta dovrà consentire l'accesso remoto sicuro tramite un portale web Https integrato, garantendo il disaccoppiamento fra il client remoto dell'operatore e l'asset a cui sta facendo accesso come amministratore.
- La soluzione proposta dovrà consentire l'accesso remoto sicuro attraverso un portale web HTTPS senza l'utilizzo di accessi tramite VPN.
- La soluzione proposta dovrà consentire di gestire di gestire i permessi in modo granulare in base a gruppi di appartenenza per utenti ed asset, garantendo almeno le seguenti abilitazioni base:
  - Gruppo di utenti amministratori della piattaforma PAM;
  - Gruppo di utenti abilitati esclusivamente alla creazione di account sulla piattaforma PAM;
  - Gruppo di utenti abilitati esclusivamente alle funzionalità di auditing;
  - Gruppo di utenti abilitati all'inserimento, modifica ed eliminazione di asset da un gruppo di risorse asset;
  - Gruppo di utenti abilitati all'accesso a risorse di un gruppo asset con possibilità di ceckout delle password;
  - Gruppo di utenti abilitati all'accesso a risorse di un gruppo asset senza possibilità di ceckout delle password;

ogni singolo utente potrà appartenere ad uno o più gruppi di abilitazione.

La soluzione proposta in ogni caso dovrà garantire tutte le funzionalità base e le funzionalità migliorative previste in sede di aggiudicazione dell'Appalto Quadro e descritte nel Paragrafo 2.18 del CTAQ.

6.2.1 PAM- Funzionalità Migliorative di AQ

Al fine di identificare il prodotto più adatto fra quelli selezionati come idonei al meta-prodotto previsto in Accordo Quadro, relativamente alle Funzionalità Migliorative offerte in sede Accordo Quadro con riferimento al Paragrafo 2.18 del CTAQ, nel presente Appalto Specifico si richiedono:

ID 7.2 *Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto*: la soluzione di Privileged Account Management dovrà gestire localmente in modo autoconsistente gli account dei fruitori del servizio PAM, sia ossia appartenenti allo staff dell'Ateneo piuttosto che fornitori o consulenti esterni; la gestione degli account dovrà avvenire senza necessità di utilizzare i sistemi di autenticazione già in uso in Ateneo, al fine di realizzare un completo disaccoppiamento delle credenziali di accesso come amministratori di sistema delle credenziali utilizzate per la fruizione dei servizi correnti di produttività. La soluzione di Privileged Account Management dovrà prevedere la possibilità di gestire localmente in modo autoconsistente gli account dei fruitori dei servizi; la soluzione dovrà consentire la gestione dell'intero ciclo di vita degli account degli utenti del servizio PAM, con la definizione delle politiche di complessità e scadenza delle password utilizzate e il blocco dell'account automatico a fronte di tentativi di accesso non autorizzato, nonché rendere disponibili le funzionalità standard legate alle gestione delle credenziali di un account (regole di complessità della password, scadenza della password, cambio password e reset password in modalità self service, obbligo di cambio password al primo accesso per i nuovi account). La soluzione dovrà consentire di definire gruppi di utenti a cui assegnare privilegi differenziati, sia in termini di privilegi di accesso accordati verso i target gestiti sia in termini di target visibili e accedibili.

ID 7.4 *Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata:* Gli utenti devo poter accedere ai vari target gestiti senza venire a conoscenza della password di amministrazione degli stessi; qualora il sistema consenta di fare il ceckout della password di un determinato dispositivo gestito, nel momento in cui viene visualizzata deve essere configurata la possibilità che il sistema PAM cambi la password sul sistema target al termine della sessione in modo da impedirne il ri-utilizzo.

ID 7.9 *Possibilità di effettuare un'analisi di dettaglio delle minacce informatiche per identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità*: il sistema dovrà inviare avvisi di sicurezza via mail a fronte di eventi critici in termini di sicurezza, quali ad esempio: ripetuti blocchi di un account utilizzatore per inserimento di una password errata, acceso in consultazione di password di amministrazione di target gestiti (check out), accesso a target gestiti fuori dalle fasce ordinarie di operatività degli amministratori IT, accesso alla piattaforma da IP remoti appartenenti ad aree geografiche diverse da quelle abitualmente frequentate dagli amministratori IT, etc. La soluzione proposta dovrà rendere disponibili funzionalità di analisi comportamentale degli accessi atte ad identificare e segnalare accessi anomali in base ad algoritmi per attribuzione di un indice di rischio.

6.2.2 PAM- Requisiti Migliorativi di AS

Fermo restando la necessità di supportare tutte le funzionalità minime e migliorative previste in prima fase dal Paragrafo 2.18 del CTAQ, nel presente appalto specifico (seconda fase) si richiedono i seguenti requisiti migliorativi descritti nel presente paragrafo, selezionate fra quelli previsti dal CTAQ. I seguenti requisiti migliorativi, riportati anche nella richiesta d'Offerta, saranno oggetto di valutazione di AS:

AS.7.4 Supporto di dispositivi di rete e di dispositivi e sistemi di sicurezza specifici richiesti dall'Amministrazione.
Sarà valutata la capacità di supportare l'accesso con protocollo SSH verso gli apparati di networking di Cisco System (attualmente gli apparati che costituiscono l'infrastruttura di trasmissione dati dell'Ateneo sono del brand Cisco System)

AS.7.6 Integrazione con una specifica soluzione di MFA richiesta dall'Amministrazione.

Fermo restando il rispetto di quanto richiesto al par. 6.2.1 per la funzionalità aggiuntiva ID 7.2, (accesso alla piattaforma PAM con credenziali locali memorizzate esclusamene all'interno della piattaforma stessa) l'accesso alla piattaforma PAM fornita deve avvenire esclusivamente tramite con processo di autenticazione sicura a più fattori (MFA), per tutti i 50 utenti singoli previsti nel dimensionamento di licenza della soluzione PAM.

La funzionalità MFA per l'accesso al PAM dovrà essere implementata per tutti gli utenti (50) gestiti localmente (local user) sul PAM e deve essere disponibile per tutto il periodo di validità del contratto.

L'Amministrazione sta implementando una propria soluzione di MFA realizzata con la soluzione tecnologica composta dal sistema Fortinet Forti Authenticator abbinato all'MFA Fortinet Forti Token Mobile. Si richiede che la soluzione PAM proposta consenta di effettuare l'accesso MFA integrandosi con l'architettura Fortinet Forti Authenticator - Forti Token Mobile, la soluzione PAM dovrà quindi consentire di interfacciare le utenze configurate localmente al PAM (riferimento par. 6.2.1), con il server Fortinet Forti Authenticator ospitato all'interno della Rete dati dell'Ateneo (ad esempio esponendole tramite protocollo LDAPs). Nel caso in cui il fornitore renda disponibile il Requisito Migliorativo di Appalto Specifico AS.7.6, le attività necessarie per l'integrazione sono da intendersi ricomprese nella fornitura.

In alternativa la soluzione PAM proposta può rendere disponibile una propria soluzione integrata di autenticazione MFA, in cui il secondo fattore è gestito tramite una sua APP mobile dedicata disponibile sia per Androind che per Aplle IOS, oppure con invio di codice OTP via mail o SMS, purché tali funzionalità siano ricomprese nell'architettura PAM proposta, senza la necessità per l'Amministrazione di mettere a disposizione ulteriori servizi o componenti (eventuali virtual machine e/o virtual appliance da istallare su infrastruttura dell'Amministrazione, rientreranno nel conteggio complessivo di VM ammesse di cui all'art.6.2, fermo restando quindi il limite complessivo massimo di 3 Virtual Machine/ Virtual Appliance), senza richiedere l'utilizzo di credenziali gestite dai servizi di directory dell'Amministrazione e senza ulteriori oneri economici a carico dell'Amministrazione per tutto il periodo di validità del contratto.

Nel caso in cui il fornitore renda disponibile il Requisito Migliorativo di Appalto Specifico AS.7.6, eventuali licenze aggiuntive richieste per implementare la funzionalità MFA, sia nel caso di integrazione con la soluzione MFA dell'Amministrazione, sia nel caso di soluzione MFA incorporata nella fornitura PAM proposta, dovranno essere ricomprese nella fornitura per il presente appalto specifico.

6.3 Servizi

Con riferimento al Paragrafo 2.2 del CTAQ, sono richiesti:

6.3.1 Servizi Base obbligatori

6.3.1.1 Servizi di istallazione e configurazione

Istallazione

E' richiesta l'istallazione delle soluzione PAM di cui al Paragrafo 6.2 – Prodotti, comprensiva di tutti gli accessori eventualmente necessari per renderla completamente funzionante.

L'istallazione dovrà avvenire presso il Data Center di via Montegeneroso 71 Varese, nel caso di soluzione basata su prodotti Hardware, mentre se la soluzione offerta adotta componenti Software da istallarsi in ambient virtuale, sarà possibile implementarli o nell'ambiente di virtualizzazione Microsoft Hyper-V dell'Ateneo ospitato presso il presso il Data Center di via Montegeneroso 71 Varese o in alternativa nell'ambiente private cloud Microsoft Azure del Tenant di Università degli Studi dell'Insubria; in ogni caso ciò non dovrà comportare ulteriori costi aggiuntivi a carico dell'Amministrazione per acquisire componenti o servizi non ricompresi nel presente appalto ma che si rendano necessari per la messa in funzione e l'operatività della soluzione proposta.

Configurazione
La nuova soluzione PAM fornita, andrà a sostituire un precedente ambiente PAM di Cyber Arc in uso presso l'Amministrazione; conseguentemente, le attività di configurazione dovranno prevedere anche l'analisi delle impostazioni/policy/configurazioni in precedenza previste e la loro migrazione, con le specificità dovute alla nuova tecnologia acquistata, sul nuovo prodotto.

In particolare:
- nell'attività di configurazione dovranno essere agganciati alla nuova soluzione PAM tutti i target (Server, appliance, apparati di rete, applicazioni) precedentemente gestiti tramite Cyber Arc e compatibili con la nuova soluzione PAM fornita (250 sistemi target attualmente gestiti);
- nell'attività di configurazione dovranno essere creati tutti i profili utente precedentemente presenti in CyberArc ed abbinati i relativi profili di abilitazione (target accessibili e privilegi abbinati), gli utenti attualmente configurati sono complessivamente 35, ed i gruppi di utenti sono 30.

Attualmente i target gestiti in CyberArc sono raggruppati in gruppi omogenei, anche gli utenti sono organizzati in gruppi, e per ogni gruppo di utenti sono abbinati i permessi sui gruppi di target:

Relazione gruppi utente vs abilitazioni:

Ruolo	Descrizione	Nuovo Nome Gruppo Active Directory

Amministratore Safe	- Creazione/modifica/cancellazione users/groups - Assegna permessi utenze/groups sulle safe	S_DIG-Admins
Manager Safe	- Aggiunge/modifica/cancella accounts dei sistemi target su safe - Accede ad i sistemi target - Visualizza password dei sistemi target	S_DIG-SafeManagers-Rete
		S_DIG-SafeManagers-Accessi
		S_DIG-SafeManagers-Data-Center
		S_DIG-SafeManagers-DBA
		S_DIG-SafeManagers-Fonia
Auditors	- Visione logs/registrazioni video accessi sui sistemi target - Creazione reports attività	S_DIG-Auditors
Users	- Accede ad i sistemi target - Non visualizza la password dei sistemi target	S_DIG-Users-Rete
		S_DIG-Users-Accessi
		S_DIG-Users-Data-Center
		S_DIG-Users-DBA
		S_DIG-Users-Fonia
External	- Accede ad i sistemi target - Non visualizza la password dei sistemi target	S_DIG-External-Safe-TLC-servizi
		S_DIG-External-Safe-TLC-monitor
		S_DIG-External-Safe-TLC-sicurezza
		S_DIG-External-Safe-TLC-RDA-wifi
		S_DIG-External-Safe-TLC-RDA-network
		S_DIG-External-Safe-TLC-fonia
		S_DIG-External-Safe-server-on-prem
		S_DIG-External-Safe-server-cloud
		S_DIG-External-Safe-VMWare
		S_DIG-External-Safe-accessi

		S_DIG-External-Safe-DBA
Amministratore Safe	- Creazione/modifica/cancellazione users/groups - Assegna permessi utenze/groups sulle safe	S_FOF-Admins
Manager Safe	- Aggiunge/modifica/cancella accounts dei sistemi target su safe - Accede ad i sistemi target - Visualizza password dei sistemi target	S_FOF-safeManagers-Videconferenza
		S_FOF-SafeManagers-Aule
Auditors	- Visione logs/registrazioni video accessi sui sistemi target - Creazione reports attività	S_FOF-Auditors
Users	- Accede ad i sistemi target - Non visualizza la password dei sistemi target	S_FOF-Users-Videoconferenza
		S_FOF-Users-Aule
External	- Accede ad i sistemi target - Non visualizza la password dei sistemi target	S_FOF-External-Safe-Videoconferenza
		S_FOF-External-Safe-Aule

Relazione gruppo utenti vs risorse target:

Nomi Safe (gruppo target)	Safe-S_DIG-network-servizi	Safe-S_DIG-network-monitor	Safe-S_DIG-network-sicurezza	Safe-S_DIG-network-wifi	Safe-S_DIG-network-apparati	Safe-S_DIG-fonia	Safe-S_DIG-ctrl-accessi	Safe-S_DIG-server-on-prem	Safe-S_DIG-server-cloud	Safe-S_DIG-VMWare	Safe-S_DIG-DBA
Gruppo Utenti											
S_DIG-Admins	x	x	x	x	x	x	x	x	x	x	x
S_DIG-SafeManagers-Rete	x	x	x	x	x						
S_DIG-SafeManagers-Accessi							x				
S_DIG-SafeManagers-Fonia						x					
S_DIG-SafeManagers-Data-Center								x	x	x	
S_DIG-SafeManagers-DBA											x
S_DIG-Auditors	x	x	x	x	x	x	x	x	x	x	x
S_DIG-Users-Rete	x	x	x	x	x						
S_DIG-Users-Accessi							x				
S_DIG-Users-Fonia						x					
S_DIG--Users-Data-Center								x	x	x	
S_DIG-Users-DBA											x
S_DIG-external-Safe-TLC-servizi	x										
S_DIG-external-Safe-TLC-monitor		x									
S_DIG-external-Safe-TLC-sicurezza			x								
S_DIG-external-Safe-TLC-RDA-wifi				x							

S_DIG-external-Safe-TLC-RDA-network					x						
S_DIG-external-Safe-TLC-fonia						x					
S_DIG-external-Safe-accessi							x				
S_DIG-External-Safe-server-on-prem								x			
S_DIG-External-Safe-server-cloud									x		
S_DIG-External-Safe-VMWare										x	
S_DIG-exsternal-Safe-DBA											x

Nomi Safe (gruppi di target)	Safe-S_FOF-videoconferenza	Safe-S_FOF-aule
Gruppo Utenti		
S_FOF-Admins	x	x
S_FOF-SafeManagers-Videoconferenza	x	
S_FOF-SafeManagers-Aule		x
S_FOF-Auditors	x	x
S_FOF-Users-Videoconferenza	x	
S_FOF-Users-Aule		x
S_FOF-external-Safe-Videoconferenza	x	
S_FOF-external-Safe-Aule		x

Il fornitore dovrà provvedere a personalizzare il servizio di istallazione e configurazione dettagliando:

- definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio per consentire la migrazione delle configurazioni del sistema pre-esistente verso quello di nuova fornitura;
- competenze ed esperienze specifiche sulla soluzione PAM offerta da parte del personale addetto al servizio di installazione e configurazione.

6.3.1.2 Contact Center

E' richiesta la messa a disposizione del servizio Contact Server previsto senza costi aggiuntivi dai servizi di base dell'Accordo Quadro e come descritto nel paragrafo 2.2.1.6 del CTAQ e dovrà possedere competenze ed esperienze specifiche relativamente alla soluzione PAM oggetto dell'Appalto Specifico.

6.3.2 Servizi Base Opzionali

6.3.2.1 Servizio di formazione ed affiancamento

La fornitura dovrà essere corredata dal servizio di formazione ed affiancamento volto a fornite piena padronanza operativa ai tecnici IT dell'amministrazione sulla soluzione PAM fornita.
In particolare la formazione dovrà essere finalizzata a:

- conoscenza della soluzione PAM fornita in termini di caratteristiche, configurazione e funzionalità;
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti PAM installate in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate fra la soluzione PAM e prodotti già presenti presso l'Amministrazione e le relative finalità;
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

L'attività formative verranno erogate tramite **due moduli**, ciascuno di 16 ore distribuite in due giornate di 8 ore, per un complessivo di 32 ore in 4 giorni di formazione così ripartire:

- 8 ore di formazione per conoscenza della soluzione PAM fornita in termini di caratteristiche, configurazione e funzionalità e per descrivere le eventuali attività di integrazione effettuate fra la soluzione PAM e prodotti già presenti presso l'Amministrazione e le relative finalità
- 24 ore di formazione per mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti PAM installate in maniera autonoma ed ottimale e per realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

I moduli formativi dovranno essere erogati in modalità sincrona, eventualmente da remoto; l'attività formativa dovrà essere erogata entro 60 giorni dalla messa in esercizio della soluzione PAM oggetto dell'Appalto specifico.

A moduli formativi parteciperanno un massimo di 10 discenti, con profilo tecnico selezionati fra il personale afferente all'Area Sistemi Informativi che già attualmente utilizzano la soluzione PAM in uso presso l'Amministrazione.

Sarà a carico dell'Aggiudicatario la predisposizione di una scheda di valutazione che rispecchi gli argomenti riportati nel programma del corso di addestramento specifico e preveda una valutazione del trattamento degli stessi da parte del personale dell'Amministrazione Contraente partecipante al corso con tre livelli di gradimento, di cui uno insufficiente. Al termine di ciascuna sessione l'Amministrazione Contraente valuterà le schede compilate dai partecipanti e, in caso di una valutazione negativa di una percentuale dei partecipanti superiore al **50%**, dovrà essere ripetuta la sessione per gli argomenti che hanno avuto gradimento negativo.

6.3.2.2 Servizi di manutenzione

E' richiesta l'erogazione del servizio di manutenzione di tipologia **Low Profile (Business Day),** a cui sono associati i relativi SLA di cui al par. 4.1.4 del CTAQ, relativamente ai prodotti PAM previsti al Paragrafo 6.2.

La durata dei sevizi di manutenzione dovrà essere di **24 mesi** a decorrere dalla verifica di conformità con esito positivo

Personalizzazioni del Servizio di manutenzione:

- sarà possibile concordare con l'Amministrazione la possibilità di predisporre un accesso remoto a supporto delle attività di manutenzione del fornitore
- processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio: le richieste di interventi di manutenzione verranno sottomesse al Fornitore esclusivamente dal personale tecnico del Committente appartenente all'Area Sistemi Informativi, a tal fine durante la fase di avvio dei servizi l'Amministrazione provvederà a comunicare l'elenco dei nominativi autorizzati ed i relativi recapiti
- competenze ed esperienze specifiche del personale addetto al servizio di manutenzione: il personale adibito ai servizi di manutenzione dovrà possedere competenze specifiche sulla soluzione PAM offerta.

Le seguenti caratteristiche migliorative saranno oggetto di valutazione delle singole offerte di appalto specifico:

- *ID Caratteristica AS.9.1:* Certificazioni di tipo technical sulla tecnologia PAM proposta in seconda fase.

6.3.2.3 Supporto Specialistico

Le attività di supporto specialistico richiesto, sono relative alla soluzione PAM oggetto dell'appalto e conseguentemente richiedono che il personale adibito al servizio possieda specifiche competente tecniche sul prodotto PAM fornito.
Il servizio verrà richiesto in modalità 'a chiamata' per il periodo di 24 mesi della durata dei servizi di manutenzione del presente appalto specifico, previa apposita 'Richiesta di attivazione del servizio di supporto specialistico' da parte dell'Amministrazione.
A titolo esemplificativo, ma non esaustivo, durante i 24 mesi di durata dei servizi di manutenzione, l'Amministrazione potrà richiedere al supporto specialistico interventi da remoto finalizzati a:

- ulteriori attività di configurazione post configurazione iniziale, volte creare nuovi gruppi di risorse gestite e/o nuovi gruppi di utenti e configurazione delle relative policy (rif. lettera (c) Par. 2.2.1.4 CTAQ)
- modifica policy per gruppi di risorse o gruppi di utenti (rif. lettera (b) Par. 2.2.1.4 CTAQ)
- aggiornamenti del software della soluzione PAM non ricompresi nei servizi di manutenzione (rif. lettera (c) Par. 2.2.1.4 CTAQ)
- configurazione e/o modifica di configurazioni o funzionalità della piattaforma PAM (rif. lettera (b) Par. 2.2.1.4 CTAQ)
- ulteriori integrazioni della piattaforma PAM con i sistemi IT dell'Amministrazione (rif. lettera (a) Par. 2.2.1.4 CTAQ)

La fascia oraria di erogazione del servizio è quella Standard: 8 ore lavorative complessive nella fascia oraria feriale Lun-Sab 8.00-20.00.

Per quanto sopra viene stimato il seguente fabbisogno massino e non garantito di giornate di supporto specialistico e relative Figure Professionali (come descritte nel Par. 2.2.1.4 del CTAQ) per l'intera vigenza dell'appalto specifico (24 mesi):

- Security Principal – orario standard: **30 giornate** complessive da fruirsi nel 24 mesi del contratto

Le seguenti caratteristiche migliorative saranno oggetto di valutazione delle singole offerte di appalto specifico:

- *ID Caratteristica AS.10.1 - Security Principal:* Certificazioni Certificazioni di tipo technical sulla tecnologia PAM proposta in seconda fase.

7. Livelli di servizio e Penali

Trovano applicazione i livelli di servizio previsti all'articolo 4 del CTAQ, non sono previsti ulteriori livelli di servizio e penali; per le Penali si rimanda all'articolo 5 del CTAQ.

8. Piano Operativo dell'AS

Il Fornitore dovrà presentare entro 15 giorni lavorativi dalla data di stipula del Contratto e pena l'applicazione delle penali di cui al CTAQ, un "*Piano Operativo*" che riporti almeno i contenuti di cui al par. 3.2.1 del CTAQ.