CAPITOLATO SPECIALE PER LA FORNITURA DI UN SISTEMA DI CONTROLLO ACCESSI PRESSO IL CAMPUS SCIENTIFICO - CIG: 7067820592

Parte Tecnica

1. Generalità e obiettivi

Scopo del documento è descrivere le specifiche tecniche del sistema di controllo accessi che l'Università Ca' Foscari Venezia intende acquisire per il Campus scientifico sito in via Torino a Mestre (Campus). Sono interessati all'intervento gli edifici Alfa, Beta, Delta, Gamma, Eta e Zeta, nei quali verranno disposti sia varchi di accesso per l'edificio che varchi delimitanti zone riservate. Inoltre, verranno dotate di serrature elettriche wireless le porte degli uffici del personale docente.

Obbiettivo dell'intervento è quello di migliorare la sicurezza complessiva degli edifici, del personale docente e tecnico amministrativo, dei ricercatori e degli studenti che lavorano e studiano nel Campus senza interferire con le esigenze di ricerca che richiedono la presenza dei ricercatori presso i laboratori anche fuori dal normale orario di lavoro.

Tutti gli edifici interessati dall'intervento sono serviti dalla rete locale dell'Ateneo. La parte server del sistema di controllo accessi sarà centralizzata nella sala server del Campus sita presso l'edificio Zeta.

Il sistema di controllo accessi dovrà essere integrato con il sistema di antifurto esistente per l'attivazione o la disattivazione degli allarmi. Inoltre, il sistema dovrà poter essere integrato con un sistema di videosorveglianza avviando la registrazione in particolari condizioni.

Il sistema di controllo accessi dovrà rispettare i requisiti descritti nella presente specifica e dovrà disporre di un'ampia modularità, flessibilità e resilienza, inoltre, dovrà essere anche in grado di recepire cambiamenti e ampliamenti dei requisiti iniziali senza perdita di prestazioni.

2. Architettura di riferimento

Il modello architetturale di riferimento per il sistema di controllo accessi sarà di tipo distribuito, basato sulla rete locale esistente ed integrato con essa. Per gli scopi del presente capitolato tecnico il modello può essere rappresentato distinguendo sei livelli, ognuno dei quali caratterizzato da specifici dispositivi e da protocolli di comunicazione tra livelli contigui.

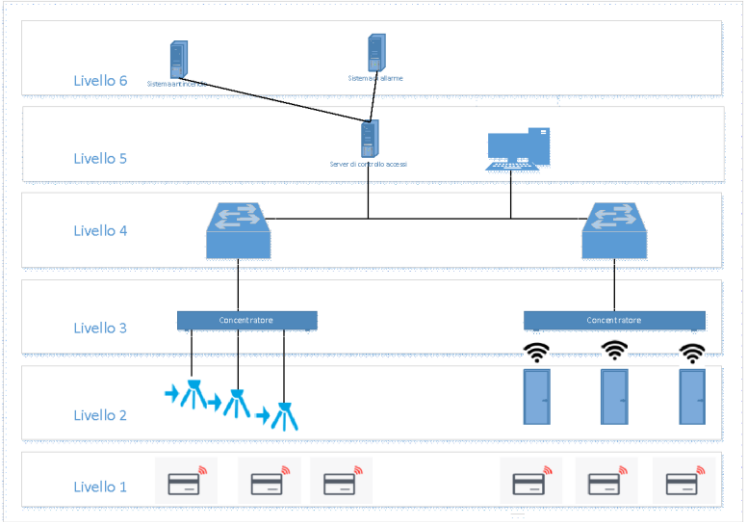

Figura 1 - Architettura del sistema di controllo accessi

Livello 1: Dispositivi personali per identificazione

I dispositivi che verranno utilizzati per l'identificazione del personale, degli studenti e dei visitatori sono badge contactless basati sull'implementazione MIFARE dello standard tecnologico ISO/IEC 14443.

Nello specifico le card MIFARE utilizzate saranno le seguenti:

- MIFARE Classic
- MIFARE Plus

Sarà cura del fornitore fare in modo che il sistema di controllo accessi ed i suoi dispositivi di lettura siano perfettamente compatibili e funzionanti con i badge in dotazione al personale e agli studenti. Inoltre, il fornitore dovrà offrire almeno 5000 badge aggiuntivi che verranno utilizzati per i visitatori. I badge aggiuntivi verranno personalizzati a cura del fornitore con il logo di Ca' Foscari, una scritta che verrà concordata con l'Ateneo, e un numero progressivo. La grafica dei badge forniti dovrà essere concordata con l'Ateneo.

Il riconoscimento dell'utente avverrà in modalità on-line tramite l'ID MIFARE del badge. Non verranno utilizzati eventuali dati memorizzati all'interno del chip.

Livello 2: Dispositivi per la lettura, varchi e serrature

I dispositivi per la lettura dei badge saranno utilizzati per l'identificazione automatica dell'utente e la conseguente apertura delle porte controllate.

I dispositivi di lettura saranno distinti per ciascuna area del controllo accessi e rispettivamente:

- porte per l'accesso degli edifici;
- porte per l'accesso a zone controllate;
- porte degli uffici.

Sono incluse nella fornitura ed a carico della Ditta fornitrice tutte le opere elettriche, di cablaggio, di fabbro e di falegnameria necessarie per l'eventuale rimozione della serratura esistente, l'installazione di una adeguata elettroserratura, l'installazione di eventuali sensori, il collegamento elettrico dell'elettroserratura all'alimentazione ed il collegamento del sistema di controllo accessi con il sistema di antifurto e il ripristino delle porte.

Ciascuna serratura dovrà essere funzionante e abilitata già al momento dell'installazione, permettendo così solo l'accesso al personale autorizzato ed evitando problemi di sicurezza.

<u>Porte di accesso degli edifici</u>

Le porte di accesso agli edifici saranno normalmente aperte durante gli orari di apertura delle portinerie. In questi orari, il sistema di controllo accessi non sarà in funzione.

Durante le ore di chiusura delle sedi, Il sistema di controllo accessi consentirà l'accesso agli edifici mediante badge ed inserimento di un PIN code personale.

La lettura del badge e la digitazione del corretto PIN code associato alla scheda permetteranno, qualora l'utente sia abilitato all'operazione, di sbloccare l'elettroserratura della porta di accesso e di disattivare l'allarme dell'edificio.

L'avvenuto sblocco dell'elettroserratura verrà indicato sulla serratura o sul tastierino numerico con una luce led verde.

Il progetto prevede che vengano installati n. 18 dispositivi di controllo accesso agli edifici ed in particolare:

- Edificio Alfa (D): n. 1 porta (accesso principale dell'edificio)
- Edificio Beta (C): n. 1 porta (accesso principale dell'edificio)
- Edificio Delta (F): n. 2 porte (accesso principale dell'edificio)
- Edificio Eta n. 2 porte (accesso principale su atrio di edificio e porta di accesso secondaria)
- Edificio Gamma (G) n. 2 porte (accesso principale dell'edificio)
- Edificio Z: n. 2 porte (accesso all'edificio presso atrio principale; uscita di sicurezza sul retro in corrispondenza alla rampa per disabili)
- Interrati (C8-C10) n. 4 porte (accesso agli edifici)
- Bunker-reagenti (c8-c10) n. 4 porta di accesso al bunker

Fermo restando il perfetto funzionamento dell'eventuale maniglione antipanico, la porta, una volta richiusa alle spalle dell'utente che ha ottenuto l'accesso, dovrà rimanere chiusa fino alla successiva riapertura tramite badge.

All'uscita dell'edificio lo stesso lettore di badge dotato di tastierino numerico consentirà all'utente l'uscita. Il sistema avviserà con un segnale luminoso ed acustico che la lettura è andata a buon fine ed attiverà l'elettroserratura, permettendo l'apertura della porta. In caso di mancata chiusura della porta dopo l'uscita dell'utente e dopo un intervallo prefissato, il sistema segnalerà la condizione anomala mediante segnale acustico. La mancata chiusura della porta verrà anche segnalata nel software di controllo attivando la procedura del caso.

Durante le ore di chiusura del campus, il sistema di controllo accessi dovrà anche essere in grado di monitorare la presenza del personale.

L'allarme di edificio verrà riattivato automaticamente all'uscita di tutte le persone che hanno avuto accesso all'edificio.

Il sistema di controllo accessi dovrà, inoltre, essere dotato di una funzione aggiuntiva di avviso, volta a prevenire condizioni anomale in relazione all'accesso o alla presenza dell'utente nell'edificio. Qualora uno degli utenti presenti nell'edificio abbia effettuato un ingresso senza che, dopo un tempo configurabile a sistema, sia stata rilevata la corrispondente uscita, l'effettiva presenza dell'utente nell'edificio andrà confermata. Il sistema invierà un SMS all'utente segnalando l'anomalia e chiedendogli di marcare tramite il badge, l'uscita, nel caso l'operazione sia stata omessa per dimenticanza. Inoltre, il sistema di controllo accessi dovrà prevedere un sistema alternativo per segnalare la dimenticanza da parte dell'utente che potrà indicare la propria presenza o segnalare l'uscita dall'edificio utilizzando apposita APP, che il fornitore dovrà offrire e mantenere per tutta la durata del contratto.

L'APP dovrà essere utilizzabile da smartphone di qualunque marca e modello con sistemi operativi Android (vers. minima 4.0.1 Ice Cream Sandwich) e IOS.

Trascorso un intervallo di tempo predeterminato dall'invio dell'SMS senza che la procedura di uscita sia stata effettuata o che sia stata eseguita alcuna segnalazione sull'APP, verranno avvisati tramite SMS alcuni numeri di emergenza.

Per quanto riguarda l'edificio Delta, una delle due porte di accesso all'edificio avrà un comportamento particolare. La porta consentirà l'accesso diretto ad un'area controllata. Di conseguenza, anche durante le ore lavorative dovrà rimanere normalmente chiusa, e poter essere aperta solo dagli utenti autorizzati ad accedere all'area.

Porte di accesso con funzionalità simili a quella che verrà installata presso l'edificio Delta saranno installate presso l'Edificio Beta, l'edificio Gamma, l'edificio Eta e l'edificio Zeta.

La porta di accesso disabili dell'edificio Zeta dovrà avere un comportamento particolare. Oltre al sistema di controllo della porta, in questo caso dovrà anche essere installato un dispositivo di apertura porta automatico che permetterà l'apertura della porta durante il normale orario di lezioni. Non appena terminato l'orario delle lezioni il sistema non permetterà l'apertura della porta senza la lettura del badge.

Per tutte le porte di edificio il sistema di controllo accessi dovrà permettere di evidenziare lo stato della porta (aperta o chiusa) e inviare allarmi in caso di manomissione della porta.

Porte per l'accesso a zone controllate

Negli edifici del campus sono state individuate 17 porte per l'accesso a zone controllate così distribuite:

- Edificio ALFA: 1 porta
- Edificio BETA: 5 porte
- Edificio GAMMA: 2 porta
- Edificio DELTA: 6 porte
- Edificio ETA: 1 porta
- Edificio ZETA: 2 porte

Per questo gruppo di porte il sistema di controllo accessi dovrà permettere di evidenziare lo stato della porta (aperta o chiusa) e inviare allarmi in caso di manomissione della porta (apertura della porta senza il passaggio di un badge autorizzato).

Le unità periferiche di controllo varchi sorveglieranno gli ingressi mediante contatti di chiusura installati sui telai della porta e sulle serrature elettriche e comanderanno l'accesso mediante l'attivazione/disattivazione delle serrature stesse.

Porte degli uffici

Per le porte degli uffici a fronte di una richiesta, la serratura cambierà di stato: se è chiusa si aprirà, se è aperta si chiuderà. Nei sei edifici dovranno essere abilitate 313 porte controllate per gli uffici dei docenti.

- Edificio ALFA: 119 porte
- Edificio BETA: 36 porte
- Edificio GAMMA: 20 porte
- Edificio DELTA: 54 porte
- Edificio ETA: 19 porte
- Edificio ZETA: 65 porte

Per minimizzare gli ingombri ed eliminare la necessità di cablaggi il dispositivo di lettura dovrà essere integrato nella serratura e dovrà essere previsto una modalità di comunicazione wireless con gli altri dispositivi che costituiscono il sistema di controllo accessi. I tempi di reazione della serratura (intervallo intercorrente tra l'atto di presentazione del badge e lo sblocco effettivo della serratura) dovranno essere inferiori a 3 secondi. La serratura dovrà funzionare con batterie standard comunemente reperibili sul mercato. La durata della batteria, in condizioni di utilizzo standard della serratura (n. medio accessi/giorno lavorativo pari a 40) dovrà non essere inferiore a 2 anni. Ciascuna serratura dovrà avere una memoria che permetta di memorizzare opportune access list, in modo che il funzionamento della serratura e l'apertura della porta non vengano inficiati dall'assenza di corrente o dalla indisponibilità della rete dati. Le access-list dovranno essere determinate sulla base dell'informazione presente nei database di Ateneo contenenti i dati di autenticazione/autorizzazione degli utenti, e di quella complementare presente nei server del sistema. L'aggiornamento delle access-list dovrà avvenire contestualmente alle variazioni operate nei suddetti database, preferibilmente in tempo reale o comunque con latenze molto ridotte (minori di 5 minuti), tali da non interferire con le esigenze operative degli utenti e con quelle della sicurezza. I protocolli di aggiornamento dovranno avere caratteristiche tali da contenere i consumi energetici della serratura e salvaguardare la durata prevista per le batterie. Sono da intendersi inclusi nella fornitura tutti i lavori necessari per l'installazione delle serrature sulle porte esistenti.

Uscite di Emergenza

Lo stato delle uscite di emergenza dovrà essere controllato dal sistema di controllo accessi permettendo di avere l'indicazione continua dello stato della porta e alla sua apertura un allarme sia locale attraverso una segnalazione acustica che riportata sul sistema di controllo accessi.

Il sistema di controllo accessi dovrà anche consentire, in caso di apertura di una porta antincendio, l'avvio di una telecamera del sistema di videosorveglianza, allo scopo di monitorare e registrare l'evento. Questa predisposizione dovrà essere posta in essere anche per tutte quelle porte di sicurezza per cui non è ancora installata una videocamera di sorveglianza

Livello 3: Dispositivi intermedi per la raccolta delle letture ed attuazione

Potranno essere previsti dei dispositivi che funzioneranno da concentratori per la raccolta delle letture sia da parte dei varchi perimetrali che dalle porte degli uffici del personale che per l'attuazione sui dispositivi di campo.

Tali dispositivi funzioneranno da gateway per i dispositivi di campo, e saranno interconnessi tra loro ed ai server di livello superiore utilizzando protocolli e tecnologia Ethernet (L2) e TCP/IP (L3) e l'infrastruttura di rete TD di Ateneo.

Il sistema non dovrà avere difficoltà a gestire un numero di porte anche doppio rispetto a quello richiesto nella fase della prima implementazione senza dovere ricorrere ad aggiornamenti tecnologici o di licenze tranne quelli legati all'installazione dei dispositivi locali sulle porte e all'aggiunta di eventuali concentratori.

I concentratori dovranno supportare il protocollo SNMP (V2c) in modo da consentirne il monitoraggio di rete da parte dei sistemi già operativi presso l'Ateneo.

Livello 4: LAN Switch di rete

L'incremento del numero di porte impegnate dagli apparati (concentratori, server etc.) potrà richiedere l'installazione di switch Ethernet layer 2 in aggiunta a quelli già presenti nella rete TD attuale.

In questo caso gli switch aggiuntivi saranno inclusi nell'offerta e dovranno essere dotati almeno di 2 porte di uplink Gigabit Ethernet, preferibilmente in grado di ospitare SFP (ottici o in rame). Tali switch dovranno integrarsi con l'architettura della rete di Ateneo già esistente, e con le caratteristiche degli apparati attivi che la compongono. In particolare, dovranno essere in grado di supportare adeguatamente la tecnologia delle VLAN (es. protocolli di spanning-tree RSTP (IEEE 802.1w) MSTP (IEEE 802.1s), trunking (IEEE802.1Q), VTP) in quanto l'attività di concentratori e server dovrà poter essere segregata in VLAN isolate e sicure. Dovranno preferibilmente poter supportare, per incrementare la sicurezza di rete, il controllo degli accessi alle porte tramite protocolli della famiglia 802.1X. Dovranno supportare, per garantire l'integrazione con i sistemi di monitoraggio attualmente attivi, i protocolli SNMP (v2c) e CDP o LLDP. Dovranno inoltre prevedere su tutte le porte lo standard di alimentazione POE (IEEE 802.3af o Extended POE).

Livello 5: Server centralizzato per il controllo accessi

Il sistema di controllo accessi verrà fornito chiavi in mano e perfettamente funzionante. La componente server deve essere installata su Virtual Machine indipendentemente dal tipo di hypervisor usato (vmware vsphere, HyperV etc).

Il software della componente server deve essere certificato almeno per Windows Server 2012 o per distribuzioni Linux recenti (Centos/RedHat 6 /7 - Ubuntu Server 16.04 LTS)

Le eventuali licenze dei database, del sistema operativo o di quant'altro necessario per il perfetto funzionamento del sistema dovranno essere intestate all'Ateneo e fornite senza alcun onere aggiuntivo.

Il server del sistema del controllo accessi avrà le seguenti macro funzioni:

- gestione della base dati del Sistema controllo accessi,
- gestione delle comunicazioni da e verso:
    - i concentratori
    - le postazioni degli operatori
- supervisione e controllo dei dispositivi di campo attraverso i concentratori,
- acquisizione e registrazione dei dati di transito sui varchi controllati,
- gestione e archiviazione degli eventi e degli allarmi di sistema,
- gestione delle anagrafiche del personale, ai fini del controllo degli accessi. Le anagrafiche devono essere sincronizzate a partire dai dati presenti nell'LDAP di Ateneo e essere mantenute allineate in tempo reale.
- gestione dei badge configurati per il controllo accessi,
- gestione delle policy per le abilitazioni di controllo accessi
- registrazione visitatori occasionali e rilascio di badge di accesso temporaneo
- produzione e gestione della reportistica,

- archiviazione e gestione dei dati storici,
- gestione della configurazione degli impianti controllo accessi,
- gestione delle procedure di back up dei dati e del sistema nel suo complesso.

Livello 6: Sistemi esistenti da integrare

I sistemi esistenti dell'infrastruttura esistente da integrare saranno:

- Sistema antincendio
- Sistema di allarme
- Sistema di videosorveglianza

Comunicazione tra livello 1 e 2

La comunicazione tra i livelli in questione sarà basata sul protocollo ISO/IEC 14443 nell' implementazione proprietaria denominata MIFARE.

Comunicazione tra livello 2 e 3

Per la comunicazione tra i livelli menzionati bisognerà distinguere tra i varchi perimetrali e delle aree controllate che potranno essere cablati e le porte degli uffici del personale dove si dovrà prevedere un collegamento wireless.

Nel primo caso si potrà utilizzare soluzioni a bus di campo basate su collegamenti seriali, con protocolli di comunicazione preferibilmente standard e non proprietari, come ad esempio RS485.

Nel caso degli uffici il vincolo sarà quello di prevedere un collegamento wireless, con i gateway.

Anche in questo caso collegamenti basati su protocolli standard, come ad esempio, IEEE 802.15.4, sono da preferire. I protocolli e soluzioni offerte non dovranno in alcun modo interferire con le reti e gli apparati di trasmissione dati wireless presenti negli edifici (WiFi standard 802.11.a/b/g/n/ac operanti nelle bande di frequenza dei 2.4 GHz o 5GHz).

Comunicazione tra i livelli 3 e 4

La comunicazione tra questi livelli è basata su protocollo TCP/IP attraverso la rete dati cablata dell'Ateneo

Comunicazione tra i livelli 4 e 5

La comunicazione tra questi livelli è basata su protocollo TCP/IP attraverso la rete dati cablata dell'Ateneo.

3. Funzionalità del sistema di controllo accessi

Funzionalità base Hardware

Il sistema di controllo accessi dovrà utilizzare un sistema di comunicazione tra le sue varie componenti di tipo protetto in modo da tutelare la sicurezza delle comunicazioni e dei dati.

I dati comunicati attraverso la rete da e per il sistema di controllo accessi e le workstation basate sui browser Web dovranno essere protetti almeno con crittografia a 128 bit SSL.

I backup del sistema di controllo accessi dovranno essere crittografati mediante crittografia AES.

Il sistema di controllo accessi dovrà consentire il backup su:

- Dispositivi di archiviazione USB;
- Directory di Windows condivisa o cartella di rete condivisa;
- Server SCP protetti.

Tutte le password di accesso al sistema di controllo accessi dovranno essere crittografate.

Enterprise Controller

L'architettura del sistema di controllo accessi dovrà consentire le decisioni al livello dell'Enterprise Controller. Il sistema di controllo accessi dovrà consentire la funzionalità completa nei momenti in cui la comunicazione tra un'appliance e l'Enterprise Controller ad essa associati si interrompe. In questo caso il controllore locale dovrà mantenere un registro di tutte le attività e dovrà caricare tali dati nel sistema di controllo accessi una volta ripristinate le comunicazioni normali.

Scalabilità

L'architettura del sistema di controllo accessi dovrà assicurare la scalabilità necessaria per supportare l'aggiunta di:

- Lettori schede e/o punti di input/output;
- Server aggiuntivi;
- Hardware Intelligent Enterprise Controller.

Replica e Failover

In caso di distribuzione di più server virtuali, il sistema di controllo accessi dovrà supportare la replica automatica delle informazioni del sistema di controllo accessi. L'architettura di replica dovrà:

- Essere di tipo peer-to-peer
- Consentire la replica di identità e configurazione di tutti i server

La soluzione PACS, dovrà essere in grado di garantire continuità di erogazione del servizio:

- monitorare lo stato dei servizi e riavviandoli in caso di blocco
- se distribuita su più server, deve essere in grado di operare il failover in caso di indisponibilità di uno dei nodi
- la soluzione deve essere resiliente in caso di reset di VM bloccata da parte del Hypervisor

Integrazione terze parti

La soluzione di controllo accesso proposta dovrà supportare l'integrazione con sottosistemi di terze parti attraverso l'utilizzo della propria interfaccia di collaborazione. Questi sistemi dovranno includere, a titolo esemplificativo:

- Sistemi IAM (Integrated Access Management)
- Sistemi SIEM (Security Information and Event Management)
- Sistemi IT e aziendali di terze parti, ivi compresi, a titolo puramente esemplificativo:

- Sistemi che utilizzano Oracle RDBMS come data engine
- Sistemi che utilizzano Microsoft SQL Server come data engine

La soluzione di controllo accesso proposta deve essere in grado di eseguire il pull di informazioni nella propria struttura di directory ed eseguire il push di eventi verso sistemi di terze parti. In particolare saranno messe a disposizione dell'Ateneo da parte della DItta senza alcuna spesa aggiuntiva almeno 30 viste in sola lettura sul database del sistema configurate secondo le specifiche richieste dell'Ateneo.

Licenza

La soluzione di controllo accessi proposta deve offrire una chiave di licenza unica basata su software, residente su ciascun appliance aziendale per controllare le funzioni e/o i componenti concessi in licenza.

Il sistema di controllo accessi deve supportare un minimo di 200 connessioni client contemporaneamente. Le singole chiavi di licenza per workstation client tradizionali e/o le chiavi di licenza per hardware non saranno accettabili.

Aggiornamenti

Gli appliance del sistema di controllo accessi dovranno supportare la perfetta integrazione e compatibilità con le versioni successive degli aggiornamenti del software applicativo.

I dispositivi hardware per il controllo accessi non dovranno richiedere la sostituzione in caso di ampliamento del sistema a livelli superiori

Funzionalità software: Server ed interfaccia operatore

L'interfaccia operatore dovrà essere basata su browser, evitando il ricorso ad installazione di client, base dati o applicativi su PC. L'interfaccia dovrà essere utilizzabile con uno qualunque dei più comuni web-browser esistenti nel mercato (Google, Explorer, Safari, e Mozilla), facile da utilizzare, flessibile, scalabile, convergente ed altamente sicura.

Inoltre, deve essere fornita un'interfaccia semplificata per l'accesso da dispositivi mobili. Questa interfaccia deve essere multipiattaforma (IOS, Android o Windows mobile). Sono accettabili sistemi che presentano un'interfaccia responsive.

L'interfaccia dovrà prevedere configurazioni ed uso di mappe grafiche, pannelli sinottici in formato JPG, PDF, DWG con funzionalità di "drag and drop", icone dinamiche con visualizzazione di stato mediante colori in tempo reale.

Il cambio di stato dei dispositivi dovrà essere visualizzato sulle mappe mediante l'utilizzo di aree con colori configurabili con dati di presenza persone e lista di persone con nome e cognome in area di cosiddette muster semplicemente toccando e facendo click sull'area di interesse.

Funzionalità di controllo degli allarmi

L'interfaccia operatore dovrà prevedere anche le segmenti funzionalità:

1. Attribuzione di allarmi ed eventi

la soluzione di controllo accessi (PACS) deve consentire agli amministratori di configurare la modalità di avviso collegata a ciascun allarme ed evento sui monitor allarmi. Il sistema deve permettere la visualizzazione dell'elenco eventi che deve contenere tutti gli allarmi e gli eventi, ed indicare almeno il tipo di evento ad essi associato e l'oggetto responsabile di aver generato l'allarme o l'evento. Una volta eseguito

l'accesso al monitor allarmi, tutti gli allarmi e gli eventi in coda dovranno essere visualizzati sul monitor per l'intervento dell'operatore.

Per ciascun allarme ed evento del sistema, gli amministratori dovranno avere la possibilità di:

- Modificare il nome dell'allarme o dell'evento impostato in fabbrica.
- Modificare, ove applicabile, il nome di ripristino allo stato normale per l'allarme o evento.
- Assegnare un tipo di evento che imposti la configurazione predefinita per l'allarme o evento.
- Visualizzare l'allarme o evento nel monitor allarmi.
- Impedire la visualizzazione dell'allarme o evento nel monitor allarmi.
- Inserire istruzioni testuali che saranno visualizzate dall'operatore per guidarlo a intervenire in caso di allarme.
- Configurare l'invio in automatico un messaggio e-mail o un SMS a un destinatario.
- Per allarmi o eventi video, avviare automaticamente il riproduttore video per visualizzare i contenuti video live della telecamera associata al dispositivo che ha generato l'allarme o l'evento.
- Creare una pianificazione per l'attivazione/disattivazione degli eventi

2. Registrazione di allarmi ed eventi

per impostazione predefinita, tutti gli allarmi e gli eventi della soluzione PACS devono essere registrati nella struttura di registrazione e memorizzazione dati interna del sistema di controllo accessi.

3. Tipi di allarmi ed eventi

La soluzione PACS dovrà supportare la creazione di tipi di allarmi ed eventi diversi. Nell'ambito dell'installazione del prodotto dovranno essere creati modelli di allarme e di evento. I tipi di evento dovranno contenere parametri di configurazione tra cui, a titolo esemplificativo:

- Priorità
- Istruzioni testuali
- Mascheramento e pianificazione del mascheramento
- Registrazione
- Creazione di rapporti
- Notifiche e-mail

Ciascun tipo di allarme e di evento dovrà essere in grado di supportare più assegnazioni di allarmi ed eventi.

4. Sincronizzazione di allarmi/eventi

La soluzione PACS dovrà supportare la sincronizzazione per allarmi ed eventi con segnalazioni su più monitor allarmi. Quando un allarme viene confermato o cancellato da un operatore del monitor allarmi, deve essere cancellato da tutti gli altri monitor allarmi.

5. Istruzioni testuali per allarmi/eventi

La soluzione PACS deve consentire l'associazione di istruzioni testuali a ciascun allarme ed evento del sistema. La capacità minima delle istruzioni testuali deve essere pari a 200.000 caratteri.

Funzionalità di controllo accessi

I gruppi di accesso dovranno consistere in una combinazione costituita da lettore schede e pianificazione. Non deve essere stabilito un limite nel numero di lettori schede del sistema assegnati a una sola pianificazione. Un lettore schede dovrà poter appartenere a qualsiasi gruppo di accesso ed a più gruppi di accesso.

La soluzione PACS dovrà consentire all'utente dotato di badge l'accesso ad aree protette in base a:

- Lettore schede
- Ora
- Giorno

La soluzione PACS deve supportare la creazione di pianificazioni che dovranno fungere da modelli per l'applicazione ai parametri tra cui, a titolo esemplificativo:

- Gruppi di accesso
- Dispositivi di mascheramento
- Modalità dei dispositivi

La soluzione PACS dovrà supportare un minimo di 200 pianificazioni. Ciascuna pianificazione dovrà essere impostata su una di 3 modalità operative:

- On: la pianificazione è attiva 24 ore su 24, 7 giorni su 7.
- Off: la pianificazione non è mai attiva.
- Intervallo: la pianificazione è attiva durante gli intervalli temporali assegnati.

Ciascuna pianificazione dovrà essere assegnabile a un intervallo temporale predeterminato.

La soluzione PACS dovrà consentire la designazione di date e/o intervalli di date come festività.

- La soluzione PACS dovrà supportare un minimo di 200 festività.
- I seguenti parametri della soluzione PACS possono essere temporaneamente modificati, regolati o sospesi durante le festività:
    - Modalità dei lettori schede
    - Diritti di accesso a un'identità

La soluzione PACS dovrà consentire la definizione delle seguenti opzioni per i lettori schede del sistema:

- Specificare che il lettore schede è attivo.
- Specificare le operazioni in modalità offline in caso di interruzione delle comunicazioni tra il lettore e l'Enterprise Controller.
- Specificare il filtro di forzatura porte che dovrà ridurre i falsi allarmi per le porte che "sbattono". La riapertura della porta entro 3 secondi dalla sua chiusura non deve determinare un allarme di apertura forzata della porta.
- Prolungamento dei tempi di porta tenuta aperta per detentori di schede: la soluzione PACS dovrà consentire per specifici detentori di credenziali il prolungamento dei tempi di porta tenuta aperta di un lettore schede oltre i tempi normali della configurazione.

- Accesso antiaggressione a un lettore schede: la soluzione PACS dovrà supportare l'inserimento dei dati di un utente mediante lettore schede in modalità antiaggressione. Quando l'accesso a un lettore schede avviene sotto aggressione, un allarme dovrà essere inviato al monitor allarmi e registrato nel database di controllo, allo stesso tempo dovrà essere avviata la videoregistrazione ed inviato un SMS a una rubrica di numeri telefonici.

La soluzione PACS dovrà supportare una funzionalità di preallarme in caso di porta tenuta aperta. Quando una porta viene tenuta aperta per un intervallo predeterminato dopo l'autorizzazione di un accesso valido, un avviso sonoro locale dovrà indicare all'utente di chiudere la porta. Il monitor allarmi deve visualizzare un allarme in caso di mancata chiusura della porta tra l'avviso di preallarme e lo scadere del tempo configurato di porta tenuta aperta.

La soluzione PACS dovrà supportare la funzione di override delle modalità del lettore schede nella modalità standard in periodi pianificati. Attraverso la funzione di override la singola serratura potrà essere posta nella modalità bloccata o sbloccata.

Per tutte le porte che hanno associato un tastierino numerico al lettore scheda, la soluzione PACS dovrà supportare un contatore dei tentativi di inserimento PIN non riusciti per ciascun lettore schede. I seguenti eventi dovranno determinare l'azzeramento del contatore:

- Nessun tentativo di accesso non riuscito per X minuti (definiti dall'utente)
- Autorizzazione di accesso a un altro lettore provvisto di scheda e PIN

Quando il conteggio corrente dei tentativi non riusciti raggiunge la soglia configurata per il lettore schede, deve essere segnalata la transazione di superamento del limite di tentativi non riusciti.

La soluzione PACS dovrà supportare una funzionalità macro/trigger quando si verifica la transazione di superamento del limite di tentativi non riusciti. Le azioni dovranno includere, a titolo esemplificativo:

- Il blocco temporaneo del lettore schede
- L'invio via SMS e email di un segnale di allarme

Più azioni complementari possono essere assegnate per ciascun lettore.

Il sistema PACS dovrà essere integrato con l'architettura LDAP dell'Ateneo permettendo la ricerca e il caricamento delle informazioni anagrafiche e di quelle relative alle tessere dal sistema centralizzato di Ateneo. La gestione delle tessere (emissione, blocco, aggiornamento ecc..) sarà a carico dell'ATENEO. Il codice MIFARE sarà caricato su LDAP. Il sistema deve aggiornarsi a partire dai dati contenuti LDAP. Il sistema deve reagire alle modifiche in tempo reale (tramite replica dell'LDAP, oppure tramite un trigger via HTTP gestito dall'ATENEO che segnala in tempo reale quali entry LDAP vengono modificate o tramite webservice).

Il sistema di autenticazione dell'applicazione PACS dovrà essere integrato con l'autenticazione utilizzata in Ateneo basata sul protocollo Shibboleth.

Il modulo di gestione delle identità dell'applicazione non dovrà essere scritto da una terza parte e dovrà essere perfettamente integrato con l'applicazione.

La soluzione PACS dovrà utilizzare autorizzazioni di base per i ruoli. Il ruolo dell'identità ne dovrà determinare i gruppi di accesso:

- I lettori schede a cui ha accesso
- Gli orari in cui può accedere a tali lettori schede

La soluzione dovrà supportare un modulo per la visualizzazione dei gruppi di accesso che consenta agli operatori di visualizzare:

- Tutti i ruoli assegnati a un'identità
- I gruppi di accesso associati al ruolo
- Le porte accessibili a un'identità

La soluzione PACS dovrà supportare una metodologia di autorizzazione basata sui ruoli, da utilizzare unitamente alle identità.

- I ruoli dovranno essere assegnati alle identità per determinare l'accessibilità delle porte e l'accessibilità dell'applicazione di sistema.
- Più ruoli dovranno essere assegnabili a una identità.
- Le identità dovranno aggregare tutti permessi assegnati ai ruoli.
- Per ciascun ruolo dovrà essere definita una data di inizio e una data di fine.

La soluzione PACS dovrà supportare codici PIN fino a 8 cifre.

- Ciascun utente della soluzione PACS dovrà avere la possibilità di scegliere il PIN da associare al proprio record.
- Il PIN di un utente dovrà essere modificabile in qualunque momento direttamente dall'utente stesso attraverso l'APP o attraverso una pagina dedicata.
- La lunghezza minima del pin dovrà essere configurabile

La soluzione PACS dovrà consentire agli operatori di revocare i privilegi di accesso a un utente. In questo caso la revoca dovrà essere immediatamente operativa su tutti i lettori schede.

La soluzione PACS dovrà avere la capacità di eseguire ricerche sulle identità in base a:

- Nome
- Cognome
- Identità

Monitoraggio di allarmi ed eventi

La soluzione PACS dovrà mettere a disposizione "schede" specializzate con funzioni differenti. In particolare, dovranno essere supportate almeno le seguenti schede:

- Monitor eventi: da utilizzare per monitorare gli eventi a livello di sistema, ad esempio l'attività dell'operatore, e gli eventi a livello di Campus.
- Monitoraggio allarmi: da utilizzare per monitorare gli allarmi a livello di Campus, ad esempio l'attività di accesso delle identità, gli allarmi di input e gli allarmi porta, nonché gli eventi a livello di sistema configurati come allarmi.
- Ricerca: da utilizzare per eseguire ricerche sulle transazioni di allarme ed evento memorizzate nella soluzione PACS.
- Stato dell'hardware: da utilizzare per visualizzare in tempo reale lo stato dei dispositivi hardware configurati nel sistema, nonché manipolare/effettuare l'override di tali dispositivi.

Il sistema PACS dovrà consentire agli amministratori di configurare la modalità di segnalazione di allarmi ed eventi. Ciascun allarme ed evento dovrà presentare almeno le seguenti opzioni di configurazione:

- Visualizzazione degli allarmi sul monitor;
- Mascheramento degli allarmi dal monitor;
- Visualizzazione di istruzioni testuali per guidare l'operatore negli interventi in caso di allarme;
- Invio automatico di un messaggio e-mail a uno o più destinatari;
- Invio automatico di un messaggio SMS a uno o più destinatari;
- Per allarmi ed eventi correlati a video, avvio automatico del riproduttore video per visualizzare un feed video live dalla telecamera associata all'allarme o evento scatenante.

Il monitor allarmi della soluzione PACS dovrà fornire un conteggio in tempo reale di tutti gli allarmi e gli eventi presenti sul monitor allarme in attesa di intervento da parte dell'operatore.

La soluzione PACS dovrà supportare la selezione delle seguenti opzioni per la gestione/l'intervento in caso di allarmi ed eventi:

- Conferma allarme;
- Inserimento di note sul motivo di un allarme e/o sull'intervento eseguito in seguito a un allarme;
- Consultazione della cronologia dell'allarme;
- Cancellazione dell'allarme.

La soluzione PACS dovrà supportare la possibilità di gestire più allarmi contemporaneamente offrendo agli operatori la possibilità di cancellare o confermare tutti gli allarmi selezionati con un'unica azione. Inoltre, il sistema dovrà consentire l'indirizzamento degli allarmi in base all'utente, inviando l'allarme all'utente, o al gruppo di utenti, incaricato di monitorare l'applicazione in base almeno a ubicazione e tipo di evento.

Il sistema PACS dovrà consentire il mascheramento di allarmi o tipi di allarme specifici, in base a pianificazioni predefinite o mediante forzature. Gli allarmi mascherati non dovranno essere visualizzati sui monitor allarmi. Il mascheramento non dovrà influenzare la registrazione nel database delle transazioni per la creazione di rapporti e il monitoraggio.

La soluzione PACS dovrà essere in grado di creare un messaggio e-mail da inviare a uno o più destinatari quando viene generato un allarme o evento. La funzione di e-mail dovrà interfacciarsi con un server e-mail che utilizza il protocollo SMTP. Inoltre, specifici allarmi potranno essere inviati tramite SMS per questo motivo la soluzione PACS dovrà essere integrata al servizio sms di Ateneo tramite la chiamata a un webservice HTTP REST.

La soluzione PACS dovrà supportare le immagini di mappe tramite importazione di sfondi di mappe da pacchetti grafici "commerciali" standard almeno nel formato JPEG.

Sulla mappa, gli operatori dovranno essere in grado di:

- Confermare un allarme
- Modificare la modalità di accesso dei lettori
- Applicare/rimuovere una maschera a/da input
- Inviare a impulsi, impostare su ON/OFF gli output relè

- Lanciare una "finestra" video

Configurazione e amministrazione del sistema

Il sistema di controllo accessi dovrà essere integrato con il sistema LDAP di Ateneo per l'identificazione dell'operatore o dell'amministratore che lo sta utilizzando. A ciascun account dovrà essere inoltre assegnato un ruolo che determini il livello di autorizzazione dell'account e controlli in tal modo le funzioni che l'operatore è in grado di svolgere all'interno del sistema.

La soluzione PACS dovrà supportare un numero di account operatore superiore pari almeno a 100 unità.

Gli account locali del sistema PACS dovranno poter essere disabilitati o perlomeno non necessari per le normali attività di utilizzo dei sistemi.

La soluzione PACS dovrà offrire la possibilità di un partizionamento di sistema per potere distinguere la gestione di diversi edifici. Ciascuna partizione dovrà poter disporre di un gruppo di operatori proprio, hardware proprio e parametri propri, ad esempio pianificazioni e gruppi di accesso. Le identità dovranno poter appartenere a una o più partizioni. Il partizionamento dovrà fornire un'architettura flessibile di tipo "tenant/landlord" nella quale gli utenti della partizione possono visualizzare, aggiungere modificare ed eliminare unicamente identità, parametri di sistema e hardware appartenente alle rispettive partizioni. Deve essere possibile assegnare gli operatori PACS a più di una partizione. È possibile assegnare una partizione a più di un operatore.

La soluzione PACS dovrà monitorare tutte le attività correlate a un account operatore e mantenerne un registro completo.

La soluzione PACS dovrà supportare un minimo di 15 rapporti standard.

Dovrà essere possibile creare rapporti nei seguenti formati:

- Documenti PDF
- Documento foglio di calcolo

Una volta generato il rapporto, è possibile:

- Salvarlo come file
- Stamparlo su una stampante locale o di rete

Ciascun rapporto dovrà essere personalizzabile/filtrabile in base ai dati pertinenti per quel rapporto specifico.

I rapporti PACS standard dovranno includere almeno:

- Rapporto di verifica delle autorizzazioni di accesso: il rapporto di verifica delle autorizzazioni di accesso dovrà presentare informazioni su tutte le attività generate manualmente da un operatore e dovranno includere la porta aperta, l'ora e l'operatore che ha autorizzato l'accesso.
- Rapporto dei gruppi di accesso: il rapporto dei gruppi di accesso dovrà presentare le informazioni relative a tutti i gruppi di accesso PACS definiti, tra cui, a titolo esemplificativo:
    - I ruoli assegnati a un gruppo
    - La pianificazione assegnata al gruppo
    - Il numero di porte assegnate al gruppo

    - L'elenco delle porte assegnate al gruppo

- Rapporto degli allarmi: il rapporto degli allarmi dovrà contenere informazioni su tutti gli allarmi che si sono verificati nel sistema, tra cui nome del pannello, intervento eseguito dall'operatore, operatore intervenuto sull'allarme ed eventuali note dell'operatore per l'allarme in questione.
- Rapporto sulle aree: il rapporto sulle aree dovrà presentare le informazioni relative a tutte le aree definite. Per ciascuna area dovranno essere indicati il nome, Il sistema di controllo accessi dislocata presso quell'area e le porte assegnate all'area.
- Rapporto sugli accessi alle porte: il rapporto sugli accessi alle porte dovrà presentare le informazioni relative all'accesso di qualsiasi porta della soluzione PACS da parte di un utente.
- Rapporto di configurazione delle porte: il rapporto di configurazione delle porte dovrà presentare tutte le informazioni di configurazione/impostazione di ciascuna porta configurata nella soluzione PACS.
- Rapporto degli eventi: il rapporto degli eventi dovrà presentare le informazioni relative agli eventi definiti nel sistema, corredate dei relativi attributi, tra cui:
    - Nome evento
    - Tipo di evento
    - Priorità
    - Eventuale configurazione di mascheramento e/o registrazione dell'evento in qualsiasi circostanza
- Rapporto sui gruppi: il rapporto sui gruppi dovrà presentare informazioni su tutti i gruppi definiti, tra cui nome e tipo del gruppo e informazioni sui relativi membri, ad esempio lettori schede e ruoli.
- Rapporto sui diritti di accesso delle identità: il rapporto sui diritti di accesso delle identità dovrà presentare le informazioni relative ai diritti di accesso alle porte di ciascuna identità definita. Il rapporto dovrà includere gli orari pianificati di accesso autorizzato per ciascun lettore, nonché il gruppo di accesso e il ruolo assegnati che consentono l'accesso al lettore.
- Rapporto riepilogativo delle identità: il rapporto riepilogativo delle identità dovrà presentare informazioni su ciascuna identità relative allo stato e al tipo di identità, all'emissione e alla data di scadenza dei token e ai ruoli e gruppi di accesso assegnati all'identità.

.

Integrazione VMS (Video Management System, sistema di gestione video)

La soluzione PACS dovrà supportare l'integrazione video digitale con il server video installato presso il campus scientifico (sistema Omnicast prodotto dalla Siemens).

Nei monitor allarmi della soluzione dovranno essere integrati i server video digitali. Gli allarmi generati dal sistema dovranno collegarsi al video, sia live che registrato, sul sistema di gestione dei video (VMS). Qualsiasi allarme/evento della soluzione PACS dovrà essere associabile a un clip video digitale in tempo reale. Ciascun allarme/evento della soluzione PACS dovrà determinare la memorizzazione da parte del VMS di:

- Una registrazione video di durata predefinita (in secondi) relativa all'arco di tempo precedente all'evento

- Una registrazione video di durata predefinita (in secondi) relativa all'arco di tempo successivo all'evento

Ciascun dispositivo hardware per il controllo accessi configurato nella soluzione PACS dovrà essere associabile a una telecamera del VMS.

- Il numero consentito di associazioni di dispositivi a una telecamera dovrà essere illimitato.
- Una telecamera dovrà essere associabile a più dispositivi hardware per il controllo accessi.
- Un dispositivo per il controllo accessi dovrà essere associabile a più telecamere.
- Laddove più telecamere sono associate a un singolo evento o allarme hardware per il controllo accessi, tutte le telecamere dovranno essere visibili nel riproduttore video con la visualizzazione a matrice appropriata.

Allo scatto di un allarme, la soluzione PACS dovrà comunicare al VMS la lunghezza richiesta per le riprese precedenti e successive al video dell'allarme. La lunghezza delle riprese precedenti è pari ai secondi di contenuti video precedenti all'evento e memorizzati dal VMS. La lunghezza delle riprese successive è pari ai secondi di contenuti video successivi all'evento e memorizzati dal VMS. La lunghezza delle riprese precedenti e successive dovrà essere configurabile fino a 100 secondi.

Il riproduttore video dovrà supportare una visualizzazione a matrice per telecamere online.

La soluzione PACS dovrà consentire l'avvio di più telecamere quando scatta un allarme.

Quando viene generato un allarme associato a più telecamere, una finestra matrice avvia la visualizzazione di tutte le telecamere associate.

Se il dispositivo che ha generato l'evento è associato a più di una telecamera, l'operatore dovrà avere la possibilità di passare con facilità da una telecamera all'altra.

Tutti gli allarmi/eventi generati dovranno essere configurabili per determinare il lancio automatico del riproduttore video nel monitor allarmi della soluzione PACS. La soluzione PACS dovrà supportare i comandi Pan/Tilt/Zoom (PTZ) dal monitor allarmi. Qualora un server VMS o una delle telecamere associate dovesse disconnettersi, un allarme specifico dovrà essere inviato al monitor allarmi della soluzione PACS.

Collaborazione con terze parti

La soluzione PACS dovrà supportare una utility di collaborazione per consentire il trasferimento pianificato o in tempo reale delle informazioni, ad esempio allarmi ed eventi, tra la soluzione PACS e sistemi IT, di sicurezza o di altro tipo di terze parti.

La soluzione PACS dovrà supportare almeno i seguenti tipi di collaborazione:

- Push degli eventi verso XML
- REST

Integrazione con il sistema di rilevazione incendi

Il PACS dovrà integrarsi con il sistema di rilevazione incendio. L'integrazione dovrà consentire lo sblocco di tutte le porte antincendio. Una volta confermata il preallarme e l'allarme di incendio il sistema sbloccherà automaticamente tutte le porte ed i varchi dell'impianto.

L'operatore potrà visualizzare sulle mappe grafiche l'allarme antincendio, e lo status delle porte sbloccate in tempo reale.

Il PACS dovrà inoltre controllare tutte le uscite di sicurezza creando un evento e quindi mostrando un allarme nel caso in cui una porta antincendio venisse aperta in assenza dell'intervento dell'impianto antincendio.

Integrazione con il sistema di antintrusione

Il PACS dovrà integrarsi con il sistema di allarme consentendo mediante l'uso di un badge un lettore e un PIN code personale attribuito al singolo utente delle funzioni di inserimento o disinserimento per l'impianto allarme intrusione, o per le partizioni che il sistema di intrusione avrà attive.

Mediante l'uso di icone, e di mappe grafiche si potrà monitorare sul client nella postazione operatore l'inserimento o disinserimento dell'impianto allarme.

Gestione delle porte degli studi

Per ciascuna porta, incluse le porte degli studi dei docenti dovrà poter essere individuato un "owner" che possa attribuire privilegi sul particolare varco. La figura dell'owner non coincide con quella dell'amministratore di sistema che può controllare ogni porta, né con le figure di gestione applicativa che possono controllare gruppi di porte. L'owner potrebbe essere "proprietario" di una sola porta e potere attribuire privilegi solo su quella.

Attraverso una semplice APP fornita dalla Ditta aggiudicataria l'owner potrà dare accesso anche per un periodo di tempo limitato ad un altro utente alla porta di cui è proprietario. L'APP consentirà la gestione del privilegio di accesso alla porta e di visualizzare la lista dei privilegi attribuiti (sia attivi che non). Il privilegio di accesso per delega potrà avere un tempo limitato o indefinito.

Cablaggio ed installazione

Il sistema PACS deve essere fornito chiavi in mano. La Ditta aggiudicataria dovrà occuparsi dell'installazione e del cablaggio di tutti i dispositivi incluse le modifiche agli impianti elettrici che dovrebbero rendersi necessarie inclusa l'eventuale progettazione delle modifiche e l'aggiornamento della certificazione dell'impianto. La Ditta fornitrice dovrà anche occuparsi lì dove necessario di realizzare le tracce, installare il tubo corrugato per il passaggio dei cavi, chiudere le tracce e rifinire le pareti (rasatura e verniciatura inclusa) di modo che non resti traccia visibile dell'intervento ed inoltre di eseguire il passaggio dei cavi e i collegamenti necessari di modo da offrire un'installazione completamente chiavi in mano.

Tutto il software necessario per il funzionamento dell'intero sistema deve poter essere installato su una o più' macchine virtuali, indipendentemente dal tipo di hypervisor usato (vmware vsphere, HyperV etc). Il sistema non deve aver bisogno di schede di tipo proprietario che, inevitabilmente, non potrebbero essere utilizzate in ambienti virtualizzati. Le virtual machine verranno create, dai tecnici ASIT sull'infrastruttura esistente, in base alle specifiche che ci verranno fornite dalla ditta aggiudicataria (n. Cpu, ram, disco, sistema operativo, db etc). Le licenze software e degli eventuali database a supporto devono essere comprese nell'offerta e il software deve essere certificato su sistemi operativi di ultima generazione (es. minimo windows 2012, oracle 11, sqlserver 2016).

Varchi esistenti

La Ditta fornitrice dovrà occuparsi di riadattare i 14 varchi attualmente controllati attraverso il sistema SIPASS della SIEMENS di modo che possano funzionare con il sistema offerto. Resta inteso che per i 14 varchi attualmente attivi e funzionanti con il sistema SIPASS la Ditta fornitrice dovrà occuparsi anche della disattivazione e dello smontaggio di ogni apparato non più necessario e della risistemazione architettonica delle pareti a seguito dello smontaggio (stuccatura e riverniciatura delle pareti oggetto dell'intervento).

4. Manutenzione e assistenza tecnica

I servizi di manutenzione ed assistenza hanno lo scopo di garantire l'assistenza da parte di personale tecnico specializzato dell'Impresa e la conservazione in efficienza del prodotto installato presso l'Ateneo nei termini e con le modalità più avanti descritti.

I servizi che saranno erogati sono i seguenti:

- Manutenzione ordinaria;
- Assistenza all'utente: telefonica, teleassistenza e/o Help Desk;
- Assistenza on-site;
- Manutenzione evolutiva.

L'Impresa provvede ad erogare all'Ateneo i servizi di manutenzione ed assistenza tramite il proprio Centro di Assistenza Tecnica, sulla base delle condizioni generali fissate nel presente capitolato.

Manutenzione ordinaria

Il Servizio di manutenzione ordinaria comprende le seguenti prestazioni:

- rilascio di nuove release del sistema PACS (APP utente incluse) in sostituzione di quelle già rilasciate a seguito di:
    - modifiche ed aggiornamenti apportate dal produttore del software per il miglioramento del software;
    - eliminazione dei malfunzionamenti di procedura segnalati dagli utenti e verificatisi nell'ambito del corretto utilizzo del software fornito;
- allineamenti a nuove release del software di base di riferimento;
- allineamenti a nuove release di OS per le piattaforme mobili utente;
- istruzioni per il temporaneo superamento di eventuali malfunzionamenti (work-around), in attesa di una soluzione definitiva;
- distribuzione di informazioni relative al software quali: schema del Database e documentazione di tutte le tabelle dello stesso, livelli di aggiornamento; nuove funzioni offerte; evoluzioni del software.

<u>Assistenza all'Utente</u>

Si intende per assistenza all'utente il complesso delle attività di supporto all'utente nell'utilizzo del software.

<u>Assistenza telefonica</u>

Il servizio consiste nella trasmissione di istruzioni verbali al fine di guidare il personale dell'Azienda alla soluzione del problema denunciato e comunicato con le modalità di seguito riportate.

L'intervento si conclude solo dopo verifica telefonica che le istruzioni fornite abbiano consentito la soluzione del problema.

Nel caso che l'assistenza verbale non sia sufficiente a risolvere il problema si procederà con altri tipi di intervento: intervento in tele assistenza e nel caso in cui il malfunzionamento persista attraverso assistenza on-site. Tali modalità d'intervento saranno specificati successivamente nel presente capitolato.

Tele assistenza

Il servizio consiste nell'assistenza tecnica erogata tramite collegamento con il sistema dell'Ateneo in modo da consentire all'Impresa di operare sul sistema stesso.

Le modalità di espletamento della connessione alla rete telematica dovranno avvenire secondo gli standard di comunicazione dell'Ateneo. Le regole tecniche per la connessione remota verranno stabilite con l'Area Sistemi informatici e Telecomunicazioni.

Assistenza on-site

L'Assistenza on-site prevede interventi di tecnici specialisti dell'Impresa presso l'Ateneo per il numero massimo di giornate/uomo sotto prestabilito al fine di:

- risolvere problemi denunciati dall'Ateneo non risolvibili con assistenza telefonica e/o teleassistenza;
- effettuare interventi preventivi atti a migliorare l'utilizzo, a mantenere il sistema ed ottimizzare il DataBase;
- installare nuove release e/o personalizzazioni del software con eventuale conseguente riallineamento degli archivi.

Sono inclusi nell'offerta 25 giorni anno di manutenzione on-site.

Manutenzione evolutiva

Sulla base delle specifiche esigenze dell'Ateneo (in particolare in caso di personalizzazioni) la manutenzione evolutiva viene fornita concordando con l'Ateneo gli interventi. Sono inclusi nell'offerta almeno 20 giorni di manutenzione evolutiva complessivi al fine di consentire:

- nuove personalizzazioni (nuove funzionalità, stampe, export, ecc.) o integrazioni con i Sistemi Informativi di Ateneo ed in modo compatibile con il software e le sue evoluzioni;
- produzione di programmi aggiuntivi e/o APP atti a risolvere specifiche esigenze dell'Ateneo;
- personalizzazioni, integrazioni e sviluppi ad hoc effettuate con la fornitura iniziale o successivamente alla stessa;
- attività di formazione del personale dell'Ateneo all'uso delle eventuali nuove funzionalità derivanti dalle personalizzazioni o dai nuovi programmi forniti nell'ambito del presente servizio.

Tutte le attività inerenti il servizio di manutenzione evolutiva dovranno essere concordate preventivamente, mediante sottoscrizione congiunta di apposito documento dal quale dovranno risultare le eventuali specifiche funzionali per personalizzazioni richieste, il numero delle giornate lavorative occorrenti e i tempi di consegna.

Si precisa che l'assistenza on-site (almeno 25 giornate/uomo annue da 8 ore esclusi i tempi di spostamento dei tecnici) e la manutenzione evolutiva (almeno 20 giornate/uomo complessive da 8 ore) fornite all'Ateneo saranno incluse nella fornitura. Le giornate di assistenza si intendono di otto ore lavorative.

Modalità di erogazione dei servizi di manutenzione.

L'Ateneo provvederà a nominare uno o più responsabili software quali interfaccia permanente con l'Impresa.

L'Impresa mette a disposizione dell'Ateneo il Call Center a cui si devono rivolgere i responsabili software. Il personale di supporto della Ditta provvede all'accoglimento delle richieste di intervento, effettua una prima azione di filtro e supporta l'Ateneo nella risoluzione dei problemi di carattere più operativo richiamandolo entro quattro ore lavorative dall'accoglimento della chiamata, qualora l'intervento non possa essere concluso contestualmente alla chiamata dell'Ateneo.

La comunicazione del problema al Call Center può essere effettuata via telefono, per mezzo di posta elettronica, o per mezzo dell'inserimento di una richiesta su di un apposito sistema messo a disposizione dalla Ditta.

Il Call Center dovrà essere attivo dalle ore 8.00 alle ore 18.00 nei giorni dal lunedì al venerdì festivi esclusi. Negli altri orari, qualora si optasse per il contatto telefonico, dovrà essere attiva una segreteria telefonica a disposizione dei System Administrator dell'Ateneo per registrare messaggi che saranno ascoltati ed accolti all'inizio della prima giornata lavorativa utile.

Sulla base degli elementi raccolti il Call Center stabilisce con azione di filtro, entro le suddette quattro ore lavorative, le modalità con cui la soluzione del problema denunciato può essere perseguita:

- fornendo direttamente informazioni sulla soluzione se il problema si è già presentato;
- comunicando la presenza di patch, work-around o la risoluzione tramite azioni di Manutenzione ordinaria e, eventualmente, con distribuzione di nuove release;
- fornendo direttamente Assistenza telefonica (Assistenza di I^ livello) ai System Administrator nella risoluzione dei problemi di carattere più operativo;
- attivando l'Assistenza di II^ livello che interviene in una delle seguenti forme:
    - tramite assistenza telefonica specialistica
    - tramite collegamento diretto del sistema di elaborazione dell'Azienda (Tele assistenza).

Se l'assistenza all'Ateneo non si rivela conclusiva viene predisposto l'intervento di Assistenza on-site.

Tempi di Intervento (Livelli di Servizio)

La risoluzione positiva dell'intervento richiesto deve comunque avvenire:

- entro otto ore lavorative in caso di blocco della procedura;
- in cinque giorni lavorativi negli altri casi, salvo diversi accordi scritti ed accettati tra l'Impresa ed il System Administrator dell'Ateneo che ne ha richiesto l'intervento.

In particolare dovranno essere garantiti i livelli di servizio sopra definiti sulla base delle due seguenti tipologie:

A. Problemi bloccanti

A fronte del ricevimento di una segnalazione di blocco del Software, tale da interrompere l'operatività dello specifico reparto e/o ufficio dell'Ateneo l'Impresa interverrà in teleassistenza con la massima celerità e comunque entro otto ore lavorative dall'apertura della chiamata da parte del personale dell'Ateneo all'operatore del Call Center dell'impresa.

Si definisce work-around una qualsiasi modalità di intervento da parte dei tecnici dell'Impresa atta ad ottenere lo sblocco del Software, anche se non completamente risolutivo del problema, ma che abbia l'effetto di rendere comunque operativo il Software stesso senza alterare alcune delle funzionalità applicative precedenti il blocco dello stesso.

L'intervento dei tecnici dell'Impresa, per la risoluzione del problema o comunque per l'individuazione di un work-around, attraverso teleassistenza, avverrà al più presto e comunque entro e non oltre le otto ore lavorative.

Nel caso di work-around l'Impresa dovrà garantire la risoluzione completa del problema entro cinque giorni lavorativi successivi, anche attraverso intervento on-site dei tecnici dell'Impresa se necessario. La risoluzione del problema dovrà essere certificata dal responsabile software dell'Ateneo eventualmente in accordo con il Direttore della struttura operativa che utilizza il Software oggetto del presente capitolato.

B. Problemi non bloccanti

A fronte del ricevimento di una segnalazione di malfunzionamento non bloccante del Software da parte dei responsabili software dell'Ateneo, l'Impresa interverrà in teleassistenza con la massima celerità e comunque entro cinque giorni lavorativi dall'apertura della chiamata da parte del personale dell'Ateneo all'operatore del Call Center dell'impresa.

La risoluzione del problema, secondo le modalità descritte nel punto precedente, per questo tipologia di problema dovrà comunque avvenire entro e non oltre cinque giorni lavorativi (riferendosi comunque al primo giorno lavorativo successivo o "next business day").

Si definiscono di sotto, per ogni singola tipologia di servizio le particolarità che differiscono e/o specificano in dettaglio le norme generali di erogazione dei servizi sopra definiti. Per ciò che non è sotto descritto, valgono le norme e le tempistiche di intervento sopra citate:

Manutenzione ordinaria

L'Impresa stabilisce il contenuto ed i tempi delle nuove release la cui distribuzione viene effettuata in modo concordato con il System Administrator dell'Ateneo. L'installazione può essere effettuata dall'Impresa nell'ambito del servizio di teleassistenza o di assistenza on-site, se richiesto dall'Ateneo.

Assistenza on-site

Il Servizio di assistenza on-site è attivato tramite Call Center ed è erogato presso l'Ateneo.

Il numero delle ore/uomo necessarie per ogni singolo intervento richiesto dall'Ateneo, con l'indicazione del tipo di attività da erogare, dovrà essere concordato preventivamente tra l'Impresa e la Area Sistemi Informatici e Telefonici (ASIT) dell'Ateneo. Eventuali giornate di assistenza on-site svolte e non preventivamente approvate dalla ASIT non saranno conteggiate tra quelle a messe a disposizione dalla ditta aggiudicataria.

Gli interventi che hanno come obiettivo la risoluzione di problemi denunciati dall'Ateneo non risolvibili con assistenza telefonica e/o teleassistenza dovranno essere effettuati entro cinque giorni lavorativi dal momento di accoglimento della richiesta di intervento, fatte salve le disposizioni precedenti di tempi di risoluzione interventi.

Gli altri interventi (interventi preventivi, manutenzione del sistema e ottimizzazione del data base, installazione nuove release, personalizzazioni e riallineamento archivi) saranno effettuati previa pianificazione concordata con l'Ateneo.

Manutenzione evolutiva

Avviene su richiesta diretta dell'Ateneo all'Impresa. Il numero delle ore/uomo necessarie per ogni singola attività richiesta dall'Ateneo, con l'indicazione del tipo di attività da erogare e tempi di consegna dovrà essere concordato preventivamente tra l'Impresa e ASIT.

Eventuali giornate di manutenzione evolutiva svolte e non preventivamente approvate dall'ASIT non saranno conteggiate nel novero di quelle erogate dall'azienda.

Documentazione dell'attività eseguita

Tutte le attività di assistenza on-site e manutenzione evolutiva dovranno essere documentate da un Rapporto di Intervento.

Il Responsabile Unico del Procedimento

Ing. Tommaso Piazza