AEROPORTI DI PUGLIA
BARI BRINDISI FOGGIA TARANTO

ADP
ADP-2021-0011340
del 09-09-2021 16:10

Spett.le
Società

Invio a mezzo pec

OGGETTO: Aeroporti di Puglia SpA – Procedura Negoziata per l'affidamento degli Interventi di adeguamento ed ammodernamento dell'Infrastruttura di Controllo Accessi di Aeroporti di Puglia S.p.A.
CIG: 8883514BA7

Premesso che
Aeroporti di Puglia S.p.A., gestore delle infrastrutture e dei servizi aeroportuali pugliesi, ha pianificato l'ampliamento e la diversificazione delle sue attività, con l'obiettivo di incrementare la qualità e quantità dei servizi offerti per una clientela in rapido sviluppo ottimizzandone l'efficienza e l'efficacia;

sussiste la necessità di adeguare i sistemi informativi all'evoluzione normativa e tecnica e nel contempo di accrescere la difesa della infrastruttura aeroportuale ritenuta potenzialmente critica nell'ambito del Quadro Strategico Nazionale e dal relativo Piano nazionale per la protezione cibernetica e la sicurezza informatica;

l'obiettivo dell'intervento è quello di accrescere l'efficienza del sistema di gestione della sicurezza, in termini di prevenzione, deterrenza e risposta, a maggior tutela della protezione del personale e delle infrastrutture salvaguardando la coerenza tecnologica d'insieme nonché il ciclo di vita dei sistemi e degli apparati;

nell'ambito di tale progetto di sviluppo, rivestono particolare importanza le attività necessarie all'adeguamento delle Infrastrutture di Controllo Accessi riferita a tutti gli Scali attualmente gestiti da AdP (Bari, Brindisi, Foggia e Grottaglie) al fine di ottemperare alle Policy By Design By Default del Regolamento (UE) 2016/679 GDPR (General Data Protection Regulation), ovvero al Regolamento di esecuzione UE 1998/2015 così come modificato dal Reg. UE 2019/1583 per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, riguardante le misure di Cybersicurezza.

Aeroporti di Puglia intende pertanto aggiornare i servizi applicativi, sistemistici e di supporto per la gestione, la manutenzione, l'integrazione e lo sviluppo del proprio Sistema di Controllo Accessi.

INFORMAZIONI DI CARATTERE GENERALE
AEROPORTI di PUGLIA S.p.A. – Viale Enzo Ferrari – 70128 BARI-PALESE, ITALIA tel.+39 080.5800258 – fax +39 080.5800225 sito web www.aeroportidipuglia.it

AEROPORTI DI PUGLIA S.P.A.
VIALE ENZO FERRARI - 70128 BARI-PALESE - TEL 080 5800200 - FAX 080 5800225 - WWW.AEROPORTIDIPUGLIA.IT - UFFICIOPROTOCOLLO@PEC.AEROPORTIDIPUGLIA.IT
CAPITALE SOCIALE € 12.950.000,00 INT. VERS. - R.T. BARI 15742 C.C.I.A.A. BARI 243199 - CODICE FISCALE E PARTITA IVA 03094610726

Punti di contatto: Ufficio Acquisti Gare e Contratti
Responsabile del Procedimento: Sig. Valerio Gadaleta
Pec: ufficioprotocollo@pec.aeroportidipuglia.it

ART. 1 - OGGETTO E DURATA

L'appalto ha ad oggetto l'insieme dei servizi e delle attività volte all'upgrade dell'infrastruttura di Controllo Accesi di Aeroporti di Puglia S.p.A. al fine di adeguare l'attuale infrastruttura logica e fisica, riferita a tutti gli Scali (Bari, Brindisi, Foggia e Grottaglie), alle normative citate e dotare la stessa, di tecnologie e servizi avanzati necessari per affrontare i piani di crescita e le future innovazioni.

L'Appalto ha per oggetto la fornitura di Licenze Software e relativa gestione, manutenzione e conduzione dell'intero sistema di controllo accessi dei quattro scali pugliesi per il periodo di 24 mesi dalla stipula del contratto.
Aeroporti di Puglia SpA. si riserva la facoltà di rinnovare il contratto, alle medesime condizioni, per una durata pari ad ulteriori 12 mesi.
La stazione appaltante esercita tale facoltà comunicandola all'appaltatore mediante posta elettronica certificata almeno 30 giorni prima della scadenza del contratto originario.

Al netto degli apparati Hardware (non oggetto della presente Procedura), gli interventi in appalto consistono nelle seguenti attività di servizi e fornitura:

- Fornitura Software Applicativi;
- Upgrade, Installazione, Sviluppo e Manutenzione Evolutiva del software applicativo;
- Upgrade, Installazione, Sviluppo e Manutenzione Evolutiva dell'hardware;
- Gestione, Manutenzione e Conduzione della Infrastruttura di Controllo Accessi;
- Supporto Specialistico e Sistemistico;
- Censimento Hardware e Software;
- Manutenzione Evolutiva del software applicativo;
- Gestione Applicativa;
- Help Desk;
- Assistenza Tecnica OnSite.

La prestazione principale è quella relativa al Servizio di Gestione, Manutenzione e Conduzione della Infrastruttura di Controllo Accessi.

Il concorrente, dovrà dichiarare (All. A - ATTO DI IMPEGNO ALLA RISERVATEZZA E NON DIVULGAZIONE) di impegnarsi, alla riservatezza e alla non divulgazione di tutte le informazioni e la documentazione di natura non pubblica e riservata riferita alla presente procedura.

La presente procedura, ai sensi dell'art. 51, comma 1, del D.Lgs. 50/2016 e s.m.i., comprenderà un unico lotto per ragioni di coerenza e complementarità tra le singole prestazioni tecniche in quanto trattasi di sistemi/apparati tra loro interconnessi e funzionali alla realizzazione dell'intervento di adeguamento ed upgrade del Sistema Controllo Accessi;

ART. 2 – IMPORTO

L'importo complessivo a base di gara è pari a €uro 350.000,00 di cui €uro 853,00 per oneri della sicurezza, non assoggettabili a ribasso - I.V.A. non imponibile ai sensi dell'Art. 9 comma 1 punto 6 del D.P.R. 633/72, come da seguente dettaglio:

€uro 170.000,00 per Fornitura Software (una tantum);
€uro 60.000,00/anno per Servizio di Gestione, Manutenzione e Conduzione della Infrastruttura di Controllo Accessi.
Ai sensi dell'art. 23 comma 16 del Codice, l'importo posto a base di gara comprende i costi della manodopera che la stazione appaltante ha stimato con incidenza del 30%.

ART. 3 - PROCEDURA E CRITERIO DI SELEZIONE DELLE OFFERTE

L'appalto verrà aggiudicato all'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo di cui ai commi 2 e 3 lett. b bis dell'art. 95 del D.Lgs. 50/2016 e ss.mm.ii..

Ai sensi del comma 6 dell'art. 95 del D.Lgs. 50/2016, l'offerta recante il miglior rapporto qualità/prezzo sarà individuata applicando i criteri di valutazione e ponderazione di seguito esposti.
Stabilito in 100 il punteggio massimo, esso viene ripartito come segue:
prezzo: max punti 30;
qualità: max punti 70.

ART. 4 - TEMPI E MODI DI REALIZZAZIONE DEGLI INTERVENTI – PENALI

Data la urgente necessità sottesa a rendere disponibile la struttura in tempi congrui, il tempo per ultimare gli Interventi di sostituzione e upgrade hardware (fornito da AdP) e software (oggetto della presente procedura) è fissato in **giorni 90 naturali e consecutivi** dalla data del verbale di avvio degli stessi e per ogni Scalo da parte del RUP.

Per ogni giorno di ritardo per cause imputabili all'appaltatore, sarà applicata la penale di Euro 500/per ogni giorno di ritardo.

ART. 5 - SOGGETTI AMMESSI ALLA GARA – CONDIZIONI DI PARTECIPAZIONE

Sono esclusi dalla gara gli operatori economici per i quali sussistono cause di esclusione di cui all'art. 80 del Codice.

Gli operatori economici invitati alla presente procedura dovranno essere in possesso dei requisiti di seguito elencati; tali requisiti, a pena esclusione, devono essere posseduti dall'operatore economico al momento della scadenza del termine di presentazione delle offerte e dovranno perdurare per tutto lo svolgimento della procedura di gara fino alla stipula del contratto.

5.1 Requisiti di ordine generale

Il concorrente non deve trovarsi, a pena di esclusione, in alcuna delle situazioni di esclusione dalla partecipazione alla procedura di affidamento previste dall'art. 80 del D.Lgs 50/2016 e ss.mm.ii. come novellato dal D.L. 76/2020 e successiva L. 120/20.
Sono comunque esclusi gli operatori economici che abbiano affidato incarichi in violazione dell'art. 53, comma 16-ter, del d.lgs. del 2001 n. 165.

5.2 Requisiti di idoneità professionale
Il concorrente deve
- essere iscritto nel registro delle Imprese della Camera di Commercio, Industria, Artigianato e Agricoltura da cui risulti che l'impresa svolge attività pertinente con quella cui l'appalto si riferisce.

Il concorrente (VAR della Soc. LenelS2 Carrier), a pena di esclusione, deve
- essere in possesso del requisito di Certificazione per i Sistemi Facility Commander Wnx® e OnGuard Pro Architecture® in corso di validità del summenzionato Produttore.

In caso di raggruppamento temporaneo di Imprese o consorzio, il requisito dovrà essere posseduto dall'Impresa designata quale capogruppo mandataria.

5.3. Requisiti di capacità economico – finanziaria
Il concorrente deve aver conseguito un fatturato globale d'impresa riferito agli ultimi tre esercizi chiusi alla data di scadenza della presente procedura, non inferiore all'importo dell'appalto, Iva esclusa.

In caso di raggruppamento temporaneo di Imprese o consorzio, il requisito dovrà essere posseduto dall'Impresa capogruppo in misura maggioritaria e la restante percentuale dovrà essere posseduta cumulativamente dalle imprese mandanti o consorziate, ogni impresa dovrà possedere almeno il 10% del requisito.

5.4. Requisiti di capacità tecnica
Il concorrente deve aver eseguito nell'ultimo triennio la data di scadenza della presente procedura, almeno un contratto analogo, intendendosi per contratto analogo servizi di upgrade, installazione e gestione di sistemi controllo accessi " LenelS2 Carrier".
In caso di raggruppamento temporaneo di Imprese o consorzio, il requisito dovrà essere posseduto dall'Impresa designata quale capogruppo mandataria.

ART. 6 – SUBAPPALTO

In considerazione della peculiarità dell'affidamento, il subappalto è vietato.

ART. 7 - RICHIESTA CHIARIMENTI – SOPRALLUOGO

E' possibile ottenere informazioni complementari e/o chiarimenti sulla presente procedura mediante la proposizione di quesiti scritti da inoltrare all'indirizzo pec ufficioprotocollo@pec.aeroportidipuglia.it entro le ore 12:00 del **04.10.2021** all'attenzione del Rup.
Le risposte alle richieste di chiarimenti e/o eventuali ulteriori informazioni sostanziali in merito alla presente procedura saranno pubblicate in forma anonima sul sito di AdP – sezione bandi di gara e contratti nello spazio appositamente dedicato alla presente procedura, ove è possibile altresì reperire il presente avviso.

Gli operatori economici interessati al presente invito dovranno obbligatoriamente effettuare il sopralluogo presso l'Aeroporto di Bari ed a seguire, nella medesima giornata, presso l'Aeroporto di Brindisi.
La relativa richiesta, che dovrà pervenire ad Aeroporti di Puglia tramite posta certificata all'indirizzo ufficioprotocollo@pec.aeroportidipuglia.it **entro e non oltre le ore 12:00 del giorno 04.10.2021.** La stessa dovrà riportare l'indicazione di massimo due nominativi di delegati per ciascun operatore economico, con i relativi dati anagrafici e di residenza, ed essere accompagnata da copia dei loro documenti di identità in corso di validità.
Si precisa che il Sopralluogo a titolo oneroso è obbligatorio ai fini della partecipazione alla procedura di gara.
I sopralluoghi dovranno essere eseguiti con le modalità e nei termini temporali concordati con il RUP. L'accesso ai siti sopraindicati è soggetto a rilascio di pass aeroportuali a pagamento.
Il sopralluogo viene effettuato nei soli giorni stabiliti da AdP garantendo un distinto sopralluogo al giorno per ciascuna impresa richiedente.

ART. 8 - DOCUMENTAZIONE DA PRODURRE PER LA PARTECIPAZIONE ALLA PROCEDURA - MODALITÀ DI PRESENTAZIONE DELL'OFFERTA

A pena di esclusione, l'offerta dovrà pervenire a questa Società al seguente indirizzo: "Aeroporti di Puglia S.p.A., Aeroporto Civile di Bari – Palese – 70128 Bari", per mezzo del servizio delle Poste Italiane S.p.A., agenzie di recapito ovvero mediante consegna a mano (e in tal caso la Aeroporti di Puglia rilascerà apposita ricevuta) in busta chiusa, sigillata e controfirmata sui lembi di chiusura **entro e non oltre le ore 12:00 del giorno 07.10.2021.**

Su tale plico dovrà chiaramente apporsi oltre il nominativo del mittente, la seguente dicitura:
"Aeroporti di Puglia – Procedura Negoziata per l'affidamento degli Interventi di adeguamento ed ammodernamento dell'Infrastruttura di Controllo Accessi di Aeroporti di Puglia S.p.A."

Ai fini della partecipazione faranno fede la data e l'ora di ricezione del plico. Il recapito tempestivo del plico rimane ad esclusivo rischio dei mittenti.

Detto plico dovrà contenere **Nr. 3 buste opache**, o plichi, che dovranno essere debitamente chiuse e sigillate, nonché controfirmate su tutti i lembi di chiusura, pena l'esclusione. Sul frontespizio di ciascuna busta dovrà, inoltre, essere chiaramente indicato il relativo contenuto e precisamente:

- **Busta "A": Documentazione Amministrativa;**
- **Busta "B": Documentazione Tecnica;**
- **Busta "C": Offerta Economica.**

Tutte le dichiarazioni sostitutive richieste ai fini della partecipazione alla presente procedura di gara:

a) devono essere rilasciate ai sensi degli artt. 46 e 47 del D.P.R. 28 dicembre 2000, n. 445 e ss.mm. ii. in carta semplice, con la sottoscrizione del dichiarante (rappresentante legale del candidato o altro soggetto dotato del potere di impegnare contrattualmente il candidato stesso); al tale fine le stesse devono essere corredate dalla copia fotostatica di un documento

di riconoscimento del dichiarante, in corso di validità; per ciascun dichiarante è sufficiente una sola copia del documento di riconoscimento anche in presenza di più dichiarazioni su più fogli distinti;

b) potranno essere sottoscritte anche da procuratori dei legali rappresentati e, in tal caso, alle dichiarazioni dovrà essere allegata copia conforme all'originale della relativa procura;

c) devono essere rese e sottoscritte dai concorrenti, in qualsiasi forma di partecipazione, singoli, raggruppati, consorziati, aggregati in rete di imprese, ancorché appartenenti alle eventuali imprese ausiliarie, ognuno per quanto di propria competenza;

Nella busta "A – Documentazione Amministrativa" devono essere contenuti i seguenti documenti:

A. **Dichiarazione sostitutiva** resa ai sensi degli artt. 46 e 47 del D.P.R. 28 dicembre 2000, n. 445 e ss.mm.ii., con la quale il concorrente formula istanza di partecipazione e dichiara di non trovarsi in alcuna delle condizioni di esclusione previste dall'art.80 del Codice e ss.mm.ii.
Con la citata istanza e dichiarazione il soggetto che la sottoscrive può rendere la dichiarazione di insussistenza delle clausole di esclusione ex art. 80 del D.L.gs 50/2016 e s.m.i. oltre che per sé stesso anche per i soggetti sottoelencati – se presenti - per quanto a propria conoscenza:
   - i titolari ed i direttori tecnici, ove presenti (se si tratta di impresa individuale);
   - i soci ed i direttori tecnici, ove presenti (se si tratta di società in nome collettivo);
   - i soci accomandatari ed i direttori tecnici, ove presenti (se si tratta di società in accomandita semplice);
   - gli amministratori muniti di potere di rappresentanza ed i direttori tecnici, ove presenti (se si tratta di ogni altro tipo di società o consorzio);
   - il socio unico o il socio di maggioranza in caso di società con un numero di soci pari od inferiori a quattro soci nelle società di capitali;
   - gli institori, i procuratori dotati di poteri decisionali rilevanti e sostanziali nei rapporti con la pubblica amministrazione che non siano di sola rappresentanza esterna (ove presenti);
   - i sopra citati soggetti cessati dalla carica nell'anno antecedente l'indizione della presente procedura ai sensi dell'art. 80 comma 3 del D.Lgs 50/2016 e s.m.i.

B. **DGUE** debitamente compilato;

C. Dichiarazione resa dal legale rappresentante ai sensi degli artt. 38, 47 e 48 del D.P.R. 445/2000, accompagnata da fotocopia di documento di identità in corso di validità, recante la dicitura di "essere consapevole delle sanzioni penali previste dall'articolo 76 del d.P.R. n. 445/00, per le ipotesi di falsità in atti e affermazioni mendaci ivi indicate", e attestante:
che l'impresa è iscritta nel registro delle imprese della Camera di Commercio di .....per la seguente attività.....ed attesta i seguenti dati (N.B.: per le ditte con sede in uno stato straniero, indicare i dati di iscrizione nell'Albo o Lista ufficiale dello Stato di appartenenza ovvero indicare i motivi per i quali non è richiesta l'iscrizione alla C.C.I.A.A.):

numero di iscrizione.....data di iscrizione.....
durata della ditta / data termine.....forma giuridica.....

D. **Copia della Certificazione per i Sistemi Facility Commander** Wnx® e OnGuard Pro Architecture® in corso di validità del Produttore LenelS2 Carrier;

E. **Allegato A – Atto di Impegno alla riservatezza** e non divulgazione sottoscritto dal Legale rappresentante dell'operatore economico;

F. **Dichiarazione** resa dal legale rappresentante ai sensi degli artt. 38, 47 e 48 del D.P.R. 445/2000, accompagnata da fotocopia di documento di identità in corso di validità, recante la dicitura di "essere consapevole delle sanzioni penali previste dall'articolo 76 del d.P.R. n. 445/00, per le ipotesi di falsità in atti e affermazioni mendaci ivi indicate", e attestante:
   - di aver conseguito un fatturato globale di impresa riferito agli ultimi tre esercizi chiusi alla data di scadenza della presente procedura non inferiore all'importo dell'appalto Iva esclusa;

G. **Dichiarazione** resa dal legale rappresentante ai sensi degli artt. 38, 47 e 48 del D.P.R. 445/2000, accompagnata da fotocopia di documento di identità in corso di validità, recante la dicitura di "essere consapevole delle sanzioni penali previste dall'articolo 76 del d.P.R. n. 445/00, per le ipotesi di falsità in atti e affermazioni mendaci ivi indicate", e attestante:
   - di aver eseguito nell'ultimo triennio almeno un contratto analogo;

H. **Garanzia provvisoria** pari al 2% dell'importo stimato dei lavori, da prestare nelle forme di cui all'art. 93 del D.Lgs 50/2016 e s.m.i.. Tale garanzia copre la mancata sottoscrizione del contratto dovuta ad ogni fatto riconducibile all'affidatario e sarà svincolata automaticamente al momento della sottoscrizione del contratto. La garanzia dovrà prevedere espressamente:

   - operatività entro quindici giorni a semplice richiesta scritta della stazione appaltante senza eccezione alcuna;
   - rinuncia al beneficio della preventive escussione del debitore principale e rinuncia all'eccezione di cui all'art. 1957 secondo comma del Cod. Civ.;
   - validità di almeno 180 giorni dalla data di scadenza stabilita per la presentazione delle offerte, con impegno da parte del garante, al rinnovo nel caso in cui al momento della scadenza non sia ancora intervenuta l'aggiudicazione.

La cauzione dovrà essere accompagnata dall'impegno di un fideiussore, anche diverso da quello che ha rilasciato la garanzia provvisoria, a rilasciare la garanzia fideiussoria per l'esecuzione del contratto, qualora l'offerente risultasse affidatario.

Avvertenze:

Ai sensi dell'art. 93 co. 8 del D.Lgs 50/2016 e s.m.i., in caso di microimprese, piccole o medie imprese, e raggruppamenti temporanei o consorzi ordinari costituiti esclusivamente da microimprese, piccole e medie imprese, non è richiesto l'impegno di cui sopra.

In caso di raggruppamenti temporanei le garanzie fideiussorie e le garanzie assicurative sono presentate, su mandato irrevocabile, dalla mandataria in nome e per conto di tutti i concorrenti ferma restando la responsabilità solidale tra gli operatori economici, prevista dall'art. 45, comma 5 del D. Lgs. 50/2016.

Ai sensi dell'art. 93 comma 7 del D. Lgs n. 50/2016, l'importo della garanzia, è ridotto nelle misure ivi indicate per gli operatori economici in possesso delle certificazioni previste.

I. **Ricevuta di pagamento della contribuzione a favore dell'Autorità Nazionale AntiCorruzione** per il **CIG: 8883514BA7**. Il versamento dovrà essere effettuato con le modalità previste sul Sito dell'Autorità https://www.anticorruzione.it/portal/public/classic/Servizi/ServiziOnline/ServizioRiscossioneContributi;

J. **Dichiarazione** resa dal legale rappresentante ai sensi degli artt. 38, 47 e 48 del D.P.R. 445/2000, accompagnata da fotocopia di documento di identità in corso di validità, attestante, con preciso riferimento all'oggetto della gara:

"di conoscere e rispettare i principi contenuti nel Piano aziendale Anticorruzione disponibile sul sito www.aeroportidipuglia.it alla sezione "Società Trasparente";

"che non sussistono relazioni di parentela o affinità tra i titolari, gli amministratori, i soci, e i dipendenti dell'impresa, e i dirigenti e i dipendenti della Società committente, ai sensi del combinato disposto dell'art. 1, comma 9, lett. e) della L. 190/2012 e dell'art. 6 del D.P.R. n. 62/2013";

"di conoscere e di impegnarsi a rispettare le disposizioni di cui al Codice etico – Modello ex D.Lgs. n.231/01di AdP, disponibile sul sito www.aerroportidipuglia.it nella sezione "Anticorruzione e trasparenza".
"che non ha concluso contratti di lavoro subordinato o autonomo e comunque non ha attribuito incarichi ad ex dipendenti di Adp che hanno esercitato poteri autoritativi o negoziali per conto di Adp nei propri confronti nel triennio successivo alla cessazione del rapporto di lavoro con Adp (Pantouflage).

Si precisa, a pena di esclusione, che:

in caso di R.T.P. già costituito, la mandataria dovrà allegare il mandato collettivo irrevocabile, munito di poteri di rappresentanza, di cui all'art. 48, comma 12 del D.Lgs. 50/2016 e s.m.i., in alternativa potrà essere allegata una dichiarazione sostitutiva di certificazione resa ai sensi del D.P.R. 445/2000 contenente gli estremi dell'atto costitutivo e del mandato;

in caso di R.T.P. non ancora costituito si dovranno allegare le dichiarazioni - firmate dal legale rappresentante di ciascun operatore economico raggruppando o da persona munita di comprovati poteri di firma - attestanti:

l'operatore economico al quale sarà conferito mandato speciale con rappresentanza, in caso di aggiudicazione;

l'impegno, in caso di aggiudicazione, ad uniformarsi alla disciplina prevista dall'art. 48 del D.Lgs. n. 50/2016 e ss.mm.ii.;

le parti del servizio che saranno eseguite dai singoli operatori economici;

in caso di Consorzio già costituito, si dovrà trasmettere copia autenticata nei modi di legge firmata dal legale rappresentante del Consorzio o da persona munita di comprovati poteri di firma - dell'atto costitutivo e del verbale dell'organo deliberativo nel quale siano indicate le imprese consorziate per le quali il consorzio medesimo concorre alla presente gara;

in caso di Consorzio ordinario non ancora costituito si dovranno allegare le dichiarazioni firmate dal legale rappresentante di ogni operatore economico consorziando o da persona munita di comprovati poteri - attestanti:

l'impegno, in caso di aggiudicazione, ad uniformarsi alla disciplina prevista dall'art. 48 del D.Lgs. n. 50/2016 e ss.mm.ii.;

Fermo restando il diritto di Aeroporti di Puglia S.p.A di procedere alle verifiche di ufficio, si rammenta che la falsa dichiarazione:

comporta responsabilità e sanzioni, civili e penali, ai sensi dell'art. 76 D.P.R. 445/2000;

induce la Stazione Appaltante a darne segnalazione all'ANAC ai sensi dell'art. 80, comma 12 del Codice.

Le carenze di qualsiasi elemento formale della domanda, e in particolare, la mancanza, l'incompletezza e ogni altra irregolarità essenziale degli elementi e del DGUE, con esclusione di quelle afferenti all'offerta tecnica ed economica, possono essere sanate attraverso la procedura di soccorso istruttorio di cui all'art. 83, comma 9 del Codice.

Busta B - Documentazione Tecnica

Nella busta "**Busta B - Documentazione Tecnica**" dovrà essere inserita una **Relazione Tecnica** sottoscritta dal legale rappresentante dell'operatore economico su fogli singoli di formato A4 (**max 50** pagine solo fronte), redatta secondo quanto di seguito indicato e coerente con le prescrizioni di cui al Capitolato Tecnico - Evoluzione Sistema Controllo Accessi:

1) **Introduzione** - Presentazione generale del concorrente e della sua organizzazione, con esplicito riferimento alle principali esperienze maturate in campo di installazione, upgrade e gestione dei medesimi Sistemi di Controllo Accessi e con una descrizione di tali pregresse esperienze in relazione all'organizzazione che il concorrente metterà in campo per realizzare quanto previsto nel Capitolato Tecnico - **Max Punti 10;**
2) **Upgrade Hardware** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza le attività da svolgersi coerentemente con le esigenze espresse nel presente Capitolato Tecnico. Essa dovrà contenere limitatamente alla componente hardware almeno le seguenti informazioni:
   a) Descrizione delle modalità e tipologia di intervento proposto afferiti alla sostituzione Hardware di cui al Capitolato Tecnico, Capitoli 4.3 - Elenco degli apparati di Controllo Accessi e Capitoli 6.7 Installazione di apparati hardware di cui al Capitolato Tecnico; Diagramma di Gantt - **Max Punti** 7;
3) **Upgrade Software** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza le attività da svolgersi relativamente all'Upgrade della componente software coerentemente con le esigenze espresse nel presente Capitolato Tecnico - **Max Punti 8**
   Essa dovrà contenere limitatamente alla componente hardware almeno le seguenti informazioni:
   a) Descrizione delle modalità e tipologia di intervento proposto afferiti alla sostituzione e installazione Software di cui al Capitolo 6.8 Fornitura e Installazione Software;
   b) Diagramma di Gantt;

c) Descrizione sintetica dei sistemi che il concorrente utilizzerà per gestire i servizi di assistenza e manutenzione e di tutti i sistemi di nuova introduzione.

4) **Servizio di Assistenza Hardware** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza il tipo di figura/e a che intende mettere a disposizione per le attività previste nel presente Capitolato e il periodo contrattuale - **Max Punti 20**
Essa dovrà contenere almeno le seguenti informazioni:
   a) Numero di personale impiegato e a disposizione per le attività di Upgrade Hardware e Software;
   b) Modalità di erogazione del Servizio di assistenza tecnica OnSite (SPOC);
   c) Certificazioni in corso di validità o maturate attinenti alla componente Hardware;
   d) Diagramma di Gantt afferito alla presenza di personale e coerente con le attività e le tempistiche da svolgersi.

5) **Servizio di Assistenza Software** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza il tipo di figura/e a che intende mettere a disposizione per le attività previste nel Capitolato e il periodo contrattuale - **Max Punti 20**
Essa dovrà contenere almeno le seguenti informazioni:
   a) Numero di personale impiegato e a disposizione per le attività di Upgrade Hardware e Software;
   b) Modalità di erogazione del Servizio di assistenza tecnica OnSite (SPOC);
   c) Certificazioni in corso di validità o maturate attinenti alla componente Software;
   d) Diagramma di Gantt afferito alla presenza di personale e coerente con le attività e le tempistiche da svolgersi.

6) **Interventi Migliorativi** - Eventuali Migliorie offerte dal concorrente rispetto a quelle indicate nel Capitolato tecnico e che lo stesso ritiene utili e strategiche alla evoluzione e alla manutenzione complessiva dell'infrastruttura di Controllo Accessi - **Max Punti 5**

***Avvertenze**: Eventuali pagine eccedenti quelle sopraindicate non saranno prese in considerazione ai fini dell'attribuzione del punteggio.*

In calce all'offerta tecnica, i concorrenti hanno l'obbligo di indicare con estrema precisione e dettaglio, fornendone adeguata motivazione, che sarà in ogni caso soggetta a valutazione da parte di Aeroporti di Puglia SpA, quali parti dell'offerta tecnica contengano informazioni che, ove divulgate, possano ledere il legittimo interesse della tutela della proprietà intellettuale della società concorrente; non saranno prese in considerazione motivazioni generiche circa il know out aziendale

Busta C – Offerta Economica

Nella busta "**C – Offerta Economica**" dovrà essere inserita la migliore offerta in termini di ribasso sull'importo stimato complessivo della procedura al netto degli oneri della sicurezza non soggetti a ribasso d'asta.
L'importo a base d'asta sul quale dovrà essere esplicitata l'offerta economica è di €uro 350.000,00 al netto degli oneri della sicurezza - IVA non imponibile ex art. 9.6 del D.P.R. 633/72.

Ai sensi del comma 10 dell'art 95 del Codice dei contratti l'operatore deve indicare, pena l'esclusione, i propri costi della manodopera e gli oneri aziendali concernenti l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro.

Nella formulazione dell'offerta il concorrente dovrà tenere conto della complessiva congruità economica, dell'inderogabilità delle norme a tutela della sicurezza dei lavoratori, previdenziali e assicurative, nonché dell'obbligo di rispettare i minimi salariali previsti dai contratti nazionali e locali di lavoro.
L'offerta deve essere sottoscritta dal concorrente con allegata copia di idoneo documento di riconoscimento del sottoscrittore. In caso di Raggruppamento temporaneo, l'offerta economica deve essere sottoscritta da tutti i soggetti facenti parte del raggruppamento.

L'offerta economica sarà dichiarata inammissibile, determinando conseguentemente l'esclusione dalla gara:

- se parziale;
- se condizionata;
- se indeterminata;
- se superiore al prezzo complessivo posto a base di gara.

La validità dell'offerta è di 360 giorni dalla data di scadenza per la presentazione dell'offerta.
L'offerta economica si intende fissa ed invariata per tutta la durata dell'affidamento e non vincolerà in alcun modo la Stazione appaltante.

Per l'assegnazione del punteggio relativa all'offerta tecnica si utilizzerà la seguente formula:

$C(a) = \Sigma n \, [\, Wi * V(a) \, i \,]$

dove:

$C(a)$ = indice di valutazione dell'offerta (a);

n = numero totale dei requisiti;

Wi = peso o punteggio attribuito al requisito (i);

$V(a)i$ = coefficiente della prestazione dell'offerta (a) rispetto al requisito (i) variabile tra zero e uno;

Σn = sommatoria.

I coefficienti $V(a)i$ sono determinati attraverso la media dei coefficienti attribuiti discrezionalmente dai singoli commissari.

Non saranno ammesse offerte tecniche che abbiano totalizzato un punteggio per l'offerta tecnica inferiore **a 45 punti**.

Elemento Quantitativo "OFFERTA ECONOMICA" (max. punti 30/100).

Il punteggio sull'elemento economico verrà attribuito con le seguenti modalità.

Il Concorrente dovrà esprimere l'importo economico offerto in ribasso rispetto all'importo posto a base di gara.

Il punteggio sarà attribuito applicando la seguente formula ai singoli ribassi offerti:

P(i) = 30*Prmin /Pro(i)

Dove:

P(i) è il punteggio attribuito al concorrente iesimo per singolo importo offerto;

Pro (i) è il Prezzo offerto dal concorrente iesimo per singolo importo offerto;

Prmin è il Minor Prezzo proposto in gara.

L'offerta economicamente più vantaggiosa per l'Ente Aggiudicatore è determinata dalla sommatoria del punteggio ottenuto per i singoli Elementi (Qualitativo e Quantitativo) e, pertanto, l'offerta economicamente più vantaggiosa sarà quella che avrà ottenuto il punteggio più alto nella graduatoria redatta dalla Commissione Aggiudicatrice.

ART. 9 - MODALITÀ DI APERTURA DELLE OFFERTE E PROCEDURA DI AGGIUDICAZIONE

Della seduta pubblica si darà comunicazione a mezzo pec.
Nella prima seduta la Commissione procederà

1. all'ammissione dei plichi pervenuti regolarmente entro il termine di scadenza della gara;
2. all'apertura delle BUSTE DOCUMENTAZIONE di tutte le offerte ammesse;
3. a verificare la correttezza formale della documentazione contenuta nella predetta busta contenente la documentazione amministrativa.

Ogni comunicazione inerente la presente procedura di gara sarà notificata a mezzo posta certificata.
Al ricorrere dei presupposti trova applicazione l'art 97 comma 3 del Codice.
Si procederà all'aggiudicazione anche in presenza di una sola offerta valida, sempre che sia ritenuta congrua e conveniente.
Ai sensi dell'art. 95 comma 12 del D.Lgs. 50/2016 e s.m.i., la Stazione Appaltante si riserva la facoltà di non procedere all'aggiudicazione nel caso in cui nessuna offerta risulti conveniente o idonea all'oggetto del contratto.

Dell'esito del procedimento verrà data comunicazione a tutti i partecipanti a mezzo PEC.

ART. 10 - VINCOLO DELL'OFFERTA

L'offerta si riterrà vincolante per 360 giorni dalla presentazione della stessa.

ART. 11 - ULTERIORI INDICAZIONI

La Stazione Appaltante resterà proprietaria di tutta la documentazione tecnica prodotta dai concorrenti in sede di gara senza che nulla possa dagli stessi essere preteso.
A garanzia degli impegni contrattuali l'affidataria dovrà prestare cauzione definitiva di cui all'art. 103 del D.Lgs. n. 50/2016 e s.m.i.. prima della sottoscrizione del contratto; l'affidataria dovrà sottoporre copia della fideiussione bancaria o assicurativa ad AdP S.p.A., la quale potrà richiedere le modifiche necessarie a renderla, ove difforme, conforme alle specifiche richieste.

L'affidataria dovrà essere munita, a far data dalla stipula del contratto di idonea polizza assicurativa di Responsabilità Professionale che abbia tra le specifiche la garanzia per Servizi e Prodotti Tecnologici non conformi a quanto previsto contrattualmente e/o malfunzionanti (cd. PI Tech) con un massimale di € 5mln.
Copia della suddetta polizza dovrà essere sottoposta ad AdP S.p.A., che potrà richiedere le modifiche necessarie a renderla, ove difforme, conforme alle specifiche richieste.
I contratti, previo accertamento ex D.P.R. 445/2000 dell'effettivo possesso dei requisiti morali in capo all'aggiudicatario, saranno stipulati a mezzo di scrittura privata, fiscalmente registrata ex D.P.R. 131/86.
Fermo restando le previsioni della normativa antimafia ed i relativi adempimenti la stazione appaltante, nel pubblico interesse, si riserva di non procedere alla stipulazione del contratto, ovvero di recedere dallo stesso in corso di esecuzione, ove venga a conoscenza, in sede di informative di cui all'art. 4 del D.Lgs. 490/1994 di elementi e circostanze tali da comportare il venir meno del rapporto fiduciario.

ART. 12 - TRATTAMENTO DEI DATI (ART. 12 GDPR 2016/679).

Agli effetti e per le finalità di cui al presente atto e come prescritto dalla vigente normativa, si dà atto che il titolare del trattamento dei dati personali è "Aeroporti di Puglia S.p.A." con sede in Viale Enzo Ferrari, 70128 Bari, e che l'indirizzo di contatto del responsabile per la protezione dei dati personali è dpo@aeroportidipuglia.it .
I dati personali saranno raccolti in modo lecito, corretto e trasparente, utilizzati per le finalità di cui all'articolo 6, comma 1, lettera b) del GDPR, e trattati esclusivamente da personale all'uopo istruito ed autorizzato o da responsabili del trattamento all'uopo designati. I dati non saranno trasferiti al di fuori dell'Unione Europea e saranno conservati coerentemente alle finalità di trattamento (10 anni, ovvero un tempo maggiore in caso di necessità, per il Titolare, di far valere un proprio diritto in giudizio). Il Regolamento riconosce diritti che la parte può esercitare nei confronti di e contro ciascun contitolare, un estratto completo dei quali, come tutte le altre ulteriori e necessarie informazioni, è disponibile sul nostro sito all'indirizzo http://www.aeroportidipuglia.it/privacy-zone.

IL DIRETTORE GENERALE
Arch. Marco CATAMERO'

Il RUP
Valerio GADALETA

AEROPORTI DI PUGLIA

BARI BRINDISI FOGGIA TARANTO

ALLEGATO A – ATTO DI IMPEGNO ALLA RISERVATEZZA E NON DIVULGAZIONE

PREMESSO CHE

Aeroporti di Puglia S.p.A., Gestore delle infrastrutture e dei servizi aeroportuali pugliesi, mediante la presente procedura , intende aggiornare i servizi applicativi, sistemistici e di supporto per la gestione, la manutenzione, l'integrazione e lo sviluppo del proprio Sistema di Controllo Accessi.

Per l'espletamento della procedura, Aeroporti di Puglia S.p.A., rende disponibile, ai soggetti che intendono partecipare alla procedura stessa, il Capitolato Tecnico, il cui contenuto è considerato "*Limited Distribution*":

Per "*Limited Distribution*" si intendono tutte le informazioni e la documentazione di natura non pubblica e confidenziale riferita alla procedura aperta per l'affidamento del servizio di cui alla premessa, che siano state fornite da Aeroporti di Puglia S.p.A., a tutti i soggetti interessati, in relazione e per l'espletamento della predetta procedura.

In relazione alla procedura per l'affidamento degli Interventi in oggetto, con il presente atto si intendono regolamentare gli impegni alla riservatezza conseguenti all'accesso ai documenti e/o alle informazioni di AdP S.p.A. ed, in generale, gli impegni alla riservatezza riguardanti le informazioni anche tecniche e/o commerciali comunque acquisite dal Fornitore _____, con riferimento alla Procedura nonché all'aggiudicazione.

Il sottoscritto si impegna a porre in essere ogni comportamento ed azione che assicuri la segretezza delle informazioni del Capitolato Tecnico e delle informazioni di natura confidenziale, segretata o riservata di cui venga in possesso, che includono, a titolo esemplificativo ma non esaustivo:

i) qualsiasi informazione tecnica e/o commerciale, ivi incluse conoscenze pratiche brevettate o anche non brevettate ma derivanti da esperienze e da prove, comprendente ma non esclusivamente riferita a qualsiasi documento, disegno, bozza o progetto, materiale, nota tecnica, protocollo, modulistica, campione o prototipo di prodotto, rivelata o consegnata da AdP s.p.A. e che al tempo della rivelazione o consegna sia identificata come di natura confidenziale e riservata.

AEROPORTI DI PUGLIA

BARI BRINDISI FOGGIA TARANTO

TUTTO QUANTO SOPRA PREMESSO

Il sottoscritto _____, nato a _____il _____, C.F._____ residente in _____ nella sua qualità di_____ della Società/Consorzio _____, con sede in _____, Via _____ iscritta per attività inerenti all'oggetto dell'appalto nel Registro delle Imprese della Camera di Commercio di _____ N._____ Codice Fiscale_____ Partita IVA_____

*Facente parte del costituendo/costituito RTI /Consorzio_____

ed in relazione alla partecipazione alla gara in premessa, sottoscrive il presente impegno di riservatezza, accettandone integralmente il contenuto.

Il sottoscritto si impegna a considerare le informazioni "Limited Distribution" come strettamente private e confidenziali e ad adottare tutte le misure opportune per non pregiudicarne la loro riservatezza, a non utilizzarle fuori dalla predetta procedura, a non cederle a terzi, a non divulgarle e/o diffonderle in tutto o in parte, direttamente o indirettamente e a non utilizzare tali informazioni per fini diversi da quanto previsto dalla procedura.

Il sottoscritto si impegna, inoltre, in relazione alle informazioni riservate, a tenere Aeroporti di Puglia S.p.A. manlevata da qualsiasi danno e pregiudizio che dovesse derivare, quale conseguenza della violazione della predetta procedura.

AdP S.p.A. ha facoltà di escludere dalla Procedura e di risolvere l'eventuale contratto di affidamento, salvo il risarcimento del danno, nel caso in cui l'operatore economico non rispetti gli obblighi con lo stesso assunti.

Il presente impegno è soggetto alla legge italiana, così come ogni fase della procedura.

Il Foro di Bari è competente, in via esclusiva, a giudicare in ordine a qualunque controversia nascente dal presente impegno, nonché da ogni altro atto presupposto, connesso e/o dipendente.

**In caso di RTI/ Consorzio ordinario/GEIE, sia costituiti che costituendi, la sottoscrizione dell'"Atto di Impegno" potrà essere effettuato anche da una sola Società costituente il RTI/ Consorzio/GEIE, mentre in caso di Consorzio di cui alle lettere b) e c) dell'art. 45, comma 2, del D.Lgs. n.50/2016 e s.m.i., dal Consorzio.*

Lì, (data) Timbro e Firma

si allega*:*

fotocopia di un documento di identità in corso di validità del Rappresentante Legale

(in caso di sottoscrizione da parte di un procuratore)
si allega:

copia dell'atto di procura (corredato della fotocopia di un documento di identità in corso di validità del sottoscrittore)

ADEGUAMENTO E AMMODERNAMENTO INFRASTRUTTURA CONTROLLO ACCESSI AEROPORTI DI PUGLIA

CAPITOLATO TECNICO

Sommario

1. TERMINOLOGIA 4

2. PREMESSA 5

3. OGGETTO DELLA PROCEDURA 5

4. INFRASTRUTTURA 7

4.1 Introduzione 7

4.2 Rete Security 7

4.3 Elenco degli apparati di Controllo Accessi 8

4.4 Apparati Server 9

5. OBIETTIVI DELL'ADEGUAMENTO DELL'INFRASTRUTTURA DI CONTROLLO ACCESSI 9

5.1 Categorie di Utenza 9

5.2 Obiettivi della Infrastruttura di Controllo Accessi 10

6. COMPONENTI DELLA INFRASTRUTTURA DI CONTROLLO ACCESSI 11

6.1 Infrastruttura Controllo Accessi di base 12

6.1.1 Evoluzione dei Sistemi 12

6.1.2 Database 13

6.1.3 Assistenza Sistemistica 13

6.1.4 Business Continuity Aeroporto di Bari 13

6.1.5 Policy Disaster Recovery 14

6.1.7 Licenze Software 14

6.1.8 Piano operativo della continuità 15

6.2 Adeguamento dell'infrastruttura ICT in tema di normativa GDPR e Cybersecurity 15

6.3 Presa in carico del Sistema Software di Controllo Accessi 16

6.4 Servizi di gestione dell'infrastruttura ICT 16

6.5 Servizio di Assistenza Hardware e Sistemi Operativi 16

6.6 Servizio di Manutenzione e Assistenza 19

6.7 Servizio Help Desk (SPOC) 23

6.8 Formazione 25

6.9 Installazione di apparati hardware 26

6.8 Fornitura e Installazione Software 28

6.9 Monitoraggio della Qualità del servizio 29

7. INDICAZIONI PER LA REDAZIONE DEL PROGETTO 30

8. CONDIZIONI GENERALI DI FORNITURA 32

8.1 Sostituzione personale impiegato 32

8.2 Fatturazione e modalità di pagamento 33

8.3 PENALITÀ 34

8.4 CODICE ETICO – ANTICORRUZIONE 35

8.5 CAUZIONE DEFINITIVA - POLIZZA ASSICURATIVA 35

1. TERMINOLOGIA

Nel seguito del documento deve intendersi:

- per **Azienda** o **Committente o AdP** la Aeroporti di Puglia S.p.A. (società di gestione del Sistema Aeroportuale Pugliese);
- per **Capitolato Tecnico** o **CT** il presente documento;
- per **Concorrente** o **Appaltatore o Proponente o Concorrente** la *società*, o il *Raggruppamento Temporaneo di Imprese*, aggiudicatario della fornitura e responsabile di tutte le forniture (hardware e software), nonché di tutte le altre attività necessarie a rendere operativo, fruibile e utilizzabile l'infrastruttura ICT e i relativi servizi oggetto della gara;
- per **CA** il Sistema di Controllo Accessi;
- per **RSIS** (Responsabile dei Servizi Informatici di Security);
- per **Progetto** la proposta tecnica presentata per la fornitura oggetto del presente Capitolato Tecnico;
- per **Documentazione di Gara** l'insieme costituito dai seguenti documenti:
    - **Bando;**
    - **Disciplinare di gara;**
    - **Capitolato Tecnico;**
    - **Schema Contratto di Fornitura.**

  che congiuntamente e complessivamente forniscono le informazioni per la gara, definiscono condizioni, termini e modalità di espletamento e contrattualizzazione.

2. PREMESSA

AdP, Gestore delle infrastrutture e dei servizi aeroportuali pugliesi, ha pianificato l'ampliamento e la diversificazione delle sue attività, con l'obiettivo di incrementare la qualità e quantità dei servizi offerti per una clientela in rapido sviluppo ottimizzandone l'efficienza e l'efficacia.

Nell'ambito di tale progetto di sviluppo, rivestono particolare importanza le attività necessarie all'adeguamento delle Infrastrutture di Controllo Accessi riferita a tutti gli Scali attualmente gestiti da AdP (Bari, Brindisi, Foggia e Grottaglie) al fine di ottemperare alle Policy By Design By Default del Regolamento (UE) 2016/679 GDPR (General Data Protection Regulation), ovvero al Regolamento di esecuzione UE 1998/2015 così come modificato dal Reg. UE 2019/1583 per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, riguardante le misure di Cybersicurezza. Tenuto conto della necessità di aumentare la difesa della infrastruttura aeroportuale ritenuta potenzialmente critica nell'ambito del Quadro Strategico Nazionale e dal relativo Piano nazionale per la protezione cibernetica e la sicurezza informatica. In tale ambito AdP, intende aggiornare i servizi applicativi, sistemistici e di supporto per la gestione, la manutenzione, l'integrazione e lo sviluppo del proprio Sistema di Controllo Accessi. Il presente Capitolato Tecnico ha lo scopo di descrivere i servizi e requisiti tecnico-operativi previsti per l'upgrade dei sistemi hardware e software, in termini di quantità, qualità e normativa, necessari per affrontare i piani di crescita e le future innovazioni.

AdP, al fine di contemperare le esigenze normative con quelle tecnico/economiche, di concerto con la Soc. LenelS2 Carrier, Produttore dell'attuale software del Sistema di Controllo Accessi, ha svolto una analisi volta alla identificazione delle necessità in termini di Hardware e Software occorrenti per l'evoluzione di tale Sistema, e con analogo affidamento ha provveduto, coerentemente con l'analisi svolta, all'approvvigionamento dell'Hardware necessario per l'evoluzione del Software in uso Facility Commander Wnx®, con la versione attuale OnGuard Pro Architecture®.

AdP mediante la presente procedura intende razionalizzare, potenziare e migliorare i Servizi legati all'infrastruttura Security di Controllo Accessi degli aeroporti pugliesi affidando a Società specializzata e altamente qualificata le attività di upgrade hardware, upgrade software, conduzione tecnica, operativa, di sviluppo e integrazione del proprio Sistema Informatico di Security.

Nel seguito si forniscono elementi informativi, quantitativi e qualitativi che caratterizzano l'attuale situazione tecnico/operativa e gli aspetti tecnologici e funzionali ritenuti critici ed essenziali a cui il concorrente dovrà attenersi.

3. OGGETTO DELLA PROCEDURA

L'appalto ha ad oggetto l'insieme dei servizi e delle attività volte all'upgrade dell'infrastruttura di Controllo Accesi di Aeroporti di Puglia S.p.A. al fine di adeguare l'attuale infrastruttura logica e fisica, riferita a tutti gli Scali (Bari, Brindisi, Foggia e Grottaglie), alle normative citate e di dotare la stessa di tecnologie e servizi avanzati necessari per affrontare i piani di crescita e le future innovazioni.

L'obiettivo del progetto è quello di accrescere l'efficienza del sistema di gestione della sicurezza, in termini di prevenzione, deterrenza e risposta, a maggior tutela della protezione del personale e delle infrastrutture salvaguardando la coerenza tecnologica d'insieme nonché il ciclo di vita dei sistemi e degli apparati.
Al netto degli apparati Hardware (non oggetto della Procedura), le componenti dell'Appalto sono costituite dai seguenti servizi:

1. Fornitura Software Applicativi;
2. Upgrade, Installazione, Sviluppo e Manutenzione Evolutiva del software applicativo;
3. Upgrade, Installazione, Sviluppo e Manutenzione Evolutiva dell'hardware;
4. Gestione, Manutenzione e Conduzione della Infrastruttura di Controllo Accessi (anni due + uno);
5. Supporto Specialistico e Sistemistico;
6. Censimento Hardware e Software;
7. Manutenzione Evolutiva del software applicativo;
8. Gestione Applicativa;
9. Help Desk;
10. Assistenza Tecnica OnSite.

L'innalzamento del grado di Security relativo all'Appalto sarà realizzato mediante l'installazione e la configurazione delle nuove Schede di Controllo Accessi riepilogate nel successivo Capitolo 6.9 - Installazione di apparati hardware.
Pertanto, la fattibilità dell'esecuzione degli interventi previsti è vincolata alla scelta di operatori economici (VAR della Soc. LenelS2 Carrier) in possesso del requisito di Certificazione per i Sistemi Facility Commander Wnx® e OnGuard Pro Architecture® del summenzionato Produttore.

La nuova infrastruttura di Controllo Accessi dovrà avere la capacità di coprire le esigenze di automazione di tutti gli Scali Pugliesi, garantendo, al contempo, una possibile diversificazione delle modalità operative o delle funzionalità per specifiche esigenze dello Scalo o dei soggetti in esso attivi (Gestore, Handler, Enti di Stato, Operatori Aeroportuali, Sub-concessionari, ecc.).
L'operatore economico Concorrente dovrà formulare e attuare, un piano di ristrutturazione complessivo della infrastruttura Security, al fine di innalzare i livelli di sicurezza complessivi, nonché le integrazioni e gli upgrade riferiti al Sistema Informativo di Security, prendendo in carico la gestione dell'infrastruttura come manutentore di riferimento.

L'Appaltatore dovrà pertanto:

1. Provvedere alla installazione di apparati hardware, forniti da AdP, necessari per l'upgrade Sistemi di Controllo Accessi;
2. Gestire il Sistema Software di Controllo Accessi integrando i necessari Upgrade Software, le relative personalizzazioni e integrazioni indicate dal committente, al fine di migliorare i processi e gli adeguamenti di cui in premessa;
3. Procedere alla sostituzione e, ove necessario, all'aggiornamento e ristrutturazione degli apparati Hardware del Sistema di Controllo Accessi ormai obsoleti e non più disponibili sul mercato.

4. Implementare nel nuovo Sistema Software OnGuarde alcuni applicativi esistenti e per i quali è necessaria l'integrazione con soluzioni o sviluppo di Software personalizzato per AdP.
5. Fornire i servizi di gestione di tutta l'infrastruttura di Controllo Accessi ristrutturata, al fine di garantire la necessaria operatività e sicurezza H24 nel suo complesso;
6. Provvedere ai servizi di gestione straordinaria della infrastruttura di Controllo Accessi ristrutturata, necessari per:
    - implementare nuove funzionalità;
    - migliorare i processi esistenti;
    - personalizzare i sistemi software che compongono il Sistema Security.

4. INFRASTRUTTURA SECURITY

4.1 Introduzione

L'attuale infrastruttura di Security di AdP è volta a soddisfare le esigenze interne aziendali, degli Enti di Stato, delle Compagnie Aeree, degli Operatori Aeroportuali. Essa si articola sia geograficamente che funzionalmente come di seguito descritto.

L'articolazione geografica è costituita da una rete estesa per le quattro sedi aeroportuali (Bari, Brindisi, Foggia e Grottaglie.

La sede di Bari costituisce il polo geografico principale in cui sono ubicati la maggior parte dei Server e apparati attivi attraverso cui i servizi e gli accessi vengono abilitati.

4.2 Rete Security

La rete Security di AdP copre le quattro sedi aeroportuali la cui interconnessione viene garantita dalla tecnologia MPLS, in funzione delle esigenze di traffico delle singole sedi.

Nella sede di Bari, polo geografico principale, risiedono la maggior parte degli applicativi e, mediante indirizzamenti IP opportunamente impostati, l'instradamento del flusso dei dati mantiene la coerenza logica tra nodo di origine e quello di destinazione.
La rete locale LAN è dotata di cablaggio strutturato in cat.6 nella distribuzione orizzontale e in fibra multimodale 50/125 nella distribuzione verticale, con una banda da 1GB;

Attualmente le linee che interconnettono Bari, Brindisi, Foggia e Grottaglie sono le seguenti:

1) Bari – Brindisi: Primario MPLS full fibra 10Mbps, Secondario Accesso a 8 Mbps BMG 2 Mbps;
2) Bari – Foggia: Primario MPLS full fibra 10Mbps, Secondario Accesso a 2 Mbps BMG 512 Kbps;
3) Bari – Grottaglie: Primario MPLS full fibra 10Mbps, Secondario Accesso a 2 Mbps BMG 512 Kbps, Accesso Full fibra 100Mbps.

4.3 Elenco degli apparati di Controllo Accessi

Di seguito l'elenco degli Armadi Concentratori e degli apparati di Controllo Accessi attualmente installati distinti per sede:

	AEROPORTO BARI						
	ARM. CONCENTRATORI	LOCALE TECN.	MICRO5	8RP	20DI	16DO	DDR
	1	AZPI1	3	5	4		
	1	AZPI2	1	2	1		
	1	AZPM1	1	2	1		
	1	AZPM2	1	2	1		
	1	AZPP1	1	2	1		
	1	AZPP2	1	1	1		
	1	AZPP3	1	1	1		
	1	AZPP4	1	1	1		1
	1	AZPS1	2	3	1		
	1	AZPS2	1	2	1		
	1	AZPS3	1	1	1		
	1	AZPS4	1	1	1		
	1	AZPS5	1	1	1		
	1	AZPT1	1	2	1		
	1	AZPT2	1	2	1		
	1	AZPT3	1	1	1		
	1	AZPT4	1	1	1		1
	1	AZPT5	1	1	1		2
	1	AZPT6	1	1	1		
	1	AZPT7	1	1	1		
	1	Q1A-ISS	1	2	1	1	
	1	Q1B-ISS	1	2	1	1	
	1	QIA-ISS	1	2	1	1	
	1	QIB-ISS	1	1	1	1	
	1	QVD-ISS	1	2	1	1	
TOTALE	**25**	**25**	**28**	**42**	**28**	**5**	**4**

	AEROPORTO BRINDISI						
	ARM. CONCENTRATORI	LOCALE TECN.	MICRO5	8RP	20DI	16DO	DDR
	1	TDO	3	6	3	3	
	1	TD1	1	2	1		
	1	TD2	1	2	1	1	
	1	TD3	1	2	1		
	1	TD4	1	1	1	1	
TOTALE	**5**	**5**	**7**	**13**	**7**	**5**	**0**

	AEROPORTO GROTTAGLIE						
	ARM. CONCENTRATORI	LOCALE TECN.	MICRO5	8RP	20DI	16DO	DDR
	1	TDO	1	1			
TOTALE	**1**	**1**	**1**	**1**	**0**	**0**	**0**

	AEROPORTO FOGGIA						
	ARM. CONCENTRATORI	LOCALE TECN.	MICRO5	8RP	20DI	16DO	DDR
	1	TDO	1	1			
		VDO					1
TOTALE	**1**	**2**	**1**	**1**	**0**	**0**	**1**

4.4 Apparati Server

Gli apparati Server, sono attualmente installati presso la sala CED Security di Bari a servizio dell'intera infrastruttura Security. In occasione dell'Upgrade Hardware e Software, oggetto dell'affidamento, AdP intende rendere disponibili al Concorrente, due o più Server Virtuali, quest'ultimo entro 15 giorni dalla stipula del Contratto dovrà fornire indicazioni propedeutiche alla predisposizione dell'ambiente virtuale necessario all'installazione della componente software.

5. OBIETTIVI DELL'ADEGUAMENTO DELL'INFRASTRUTTURA DI CONTROLLO ACCESSI

5.1 Categorie di Utenza

In questo capitolo si riassumono le tipologie di utenza interessate dal Sistema Informatico di Security aeroportuale, per meglio chiarire le esigenze per il nuovo sistema di controllo accessi.

I soggetti a cui primariamente è rivolta, come fruitori diretti o indiretti, la sezione di Controllo Accessi, sono i seguenti:

- Aeroporti di Puglia S.p.A. (Società di Gestione Aeroportuale);
- Soggetti istituzionali (ad esempio: ENAC, ENAV, Polizia di Stato, GdF, Vigili del Fuoco, GPG, ecc.);
- Società di manutenzione (General Contractor);
- Vettori e società di Handling;
- Operatori aeroportuali;

L'infrastruttura di Controllo Accessi rappresenta l'elemento primario attraverso cui le interazioni tra le varie categorie di utenza devono essere intermediate o censite in modo da garantire e gestire in maniera ottimale gli accessi verso le differenti aree Air Side e Land Side aeroportuali.

Aeroporti di Puglia, dispone inoltre di una propria Sala Controllo affidata ad Istituto di Vigilanza che, tramite suo personale GPG, effettua attività di monitoraggio, anche degli allarmi provenienti dal Sistema di controllo accessi, integrato con l'attuale Sistema di Video Sorveglianza.

In occasione dell'evoluzione del Sistema il concorrente dovrà redigere adeguato piano formativo da estendere anche agli operatori GPG.

5.2 Obiettivi della Infrastruttura di Controllo Accessi

Il Sistema di Controllo Accessi è parte integrante della infrastruttura di Security di Aeroporti di Puglia S.p.A. Il Responsabile dei Sistemi Informativi di Security (RSIS) è deputato alla gestione tecnica e amministrativa dei Sistemi, delle Applicazioni e dell'Infrastruttura tecnologica ed informatica di Security a cui è assegnato anche il personale informatico interno funzionalmente dipendente dal Security Manager.
Considerate le contenute dimensioni in termini di risorse professionali a disposizione della funzione RSIS, si è ritenuto necessario procedere con l'individuazione di un operatore economico in grado di garantire attività di installazione, manutenzione e gestione del Software nonché alla supervisione e al supporto degli interventi di installazione e configurazione dell'Hardware del nuovo Sistema di Controllo Accessi.

L'ammodernamento del Sistema di CA assumendo un ruolo centrale inteso anche come framework aeroportuale dovrà garantire adeguati livelli di Cybersecurity e fornire idoneo supporto alle attività e alle procedure di autorizzazione all'accesso del sistema e assicurare elevata adattabilità, scalabilità, facilità di attivazione di nuovi varchi o di riconfigurazione di quelli esistenti e fornire reportistiche atte ad individuare eventuali criticità operative.

Dal punto di vista tecnologico la nuova infrastruttura, dovrà essere realizzata:

- In alta affidabilità, ossia predisponendo Sistemi software logicamente ridondati, senza Single Point of Failure Software;
- Integrando e garantendo nativamente mediante elevati standard servizi accessibili dall'interno dell'azienda o direttamente su internet, contemperando le esigenze di Cybersecurity;
- Integrando nativamente nuove soluzioni basate su ambienti virtuali e distribuiti prevedendo punti di fault-tolerance minimali o assenti;
- Integrando i sotto-sistemi applicativi, al fine di evitare duplicazioni o reinserimenti di anagrafiche, ovvero il Sistema Security OnLine e il Sistema di Video Sorveglianza;
- Con elevate capacità di integrazione con sistemi esterni, sia per lo scambio di dati, che mediante utilizzo di funzionalità/servizi esterni.
- Attivando processi centralizzati di gestione ordinaria, straordinaria ed evoluta di tutta l'infrastruttura di Controllo Accessi con presa in carico progressiva di servizi e sistemi di seguito dettagliati consentendo ad AdP di usufruire di un Single Point Of Contact di riferimento in grado di gestire, manutenere e far evolvere nel tempo l'intera infrastruttura di Controllo Accessi.
- Adeguando i Sistemi e i Servizi alla normativa GDPR (Privacy by Design) e Cybersecurity implementando quelle funzionalità mancanti, verificando i requisiti secondo le check-list software al GDPR, e attivando servizi altamente specializzati in grado di aumentare il livello complessivo di

sicurezza dell'intera infrastruttura di Controllo Accessi, realizzando dei punti di presidio fondamentali con operatività aeroportuale H24.

6. COMPONENTI DELLA INFRASTRUTTURA DI CONTROLLO ACCESSI

Si riassumono di seguito le componenti hardware, software e i servizi centralizzati a supporto dell'infrastruttura di Controllo Accessi con i requisiti minimi richiesti da AdP a cui il Concorrente dovrà attenersi nella formulazione del progetto tecnico.

Relativamente agli aspetti infrastrutturali il concorrente dovrà progettare e realizzare una ristrutturazione complessiva dell'intero Sistema di Controllo Accessi al fine di realizzarne uno ad alta affidabilità che tenga conto delle seguenti necessità:

1) Predisporre tutte le attività finalizzate al censimento della infrastruttura in essere.
2) Attivare servizi di monitoraggio continuativo, proattivo e tradizionali, dell'intera infrastruttura di Controllo Accessi in grado di prevenire i guasti a tutti gli apparati critici e di diagnosticare tempestivamente eventuali malfunzionamenti.
3) Risolvere le criticità riscontrate da AdP, dettagliate di seguito, salvaguardando quanto più possibile gli investimenti già effettuati da AdP.
4) Predisporre tutte le attività finalizzate al coordinamento del corretto passaggio dal vecchio al nuovo Sistema di Controllo Accessi.

Relativamente al sistema software Security OnLine è richiesta l'integrazione di un brand/modello specifico, poiché trattasi di upgrade di infrastruttura esistente, garantendo la piena compatibilità rispetto all'infrastruttura di rete e dei dispositivi hardware o software esistenti.

COMPLIANCE GDPR

Si precisa che Aeroporti di Puglia ha approvato un proprio documento di conformità al GDPR per i propri sistemi software relativamente al trattamento dei dati personali, pertanto il concorrente relativamente all'applicativo software che proporrà di sviluppare, sostituire o adeguare dovrà obbligatoriamente proporre soluzioni in linea con la check-list dei requisiti software (reperibile al link https://www.aeroportidipuglia.it/privacy-zone) e con la normativa GDPR.

Per quanto sopra l'Aggiudicatario, sarà designato dal Titolare AdP come Responsabile del Trattamento così come previsto nell'Art. 28 del GDPR.

A seguito della stipula del Contratto ADP fornirà l'elenco dei sistemi informatici di AdP interessati dalle lavorazioni previste e con indicazione del livello di sicurezza attribuito a ciascun sistema, pertanto i sistemi che il concorrente andrà a introdurre ovvero mantenere con manutenzione evolutiva, dovranno obbligatoriamente rispettare i principi GDPR contenuti e reperibili al link https://www.aeroportidipuglia.it/privacy-zone. A tal proposito il Concorrente dovrà produrre apposita dichiarazione che qualsiasi sistema software di nuova installazione rispetti i summenzionati requisiti.

DIRITTI DI PROPRIETA' INTELLETTUALE

AdP al netto di Software proprietari avrà la titolarità del SW sviluppato dall'aggiudicatario nel corso dell'appalto per eventuali integrazioni. AdP alla scadenza dell'appalto avrà il diritto all'utilizzo del software sviluppato, per la propria attività e senza scadenza.

Ogni componente software dovrà essere opportunamente documentato, tale documentazione dovrà risiedere in opportuna repository, a disposizione del RSIS, organizzato dall'aggiudicatario in accordo con lo stesso. La documentazione completa dovrà essere realizzata secondo gli standard internazionali di riferimento, e corredata da tutta la manualistica in lingua italiana necessaria agli utenti finali delle componenti software sviluppate. AdP si riserva in ogni momento di richiedere all'aggiudicatario l'adeguamento della documentazione, che dovrà essere manutenuta per tutta la durata contrattuale.

6.1 Infrastruttura Controllo Accessi di base

Il progetto dovrà prevedere la gestione, manutenzione ordinaria e straordinaria, la conduzione della infrastruttura informatica di Controllo Accessi distribuita su tutta la rete geografica aeroportuale pugliese articolata in un insieme di servizi descritti in dettaglio nei successivi paragrafi.

6.1.1 Evoluzione dei Sistemi

La prevista evoluzione dei Sistemi di Controllo Accessi comprende gli adempimenti relativi agli ambienti di test, collaudo ed esercizio da realizzarsi presso i CED Security di AdP dell'aeroporto di Bari Palese. Si precisa che, l'Aggiudicatario avrà la responsabilità della predisposizione della replica dell'ambiente di esercizio. Di seguito gli adempimenti in capo all'Aggiudicatario relativamente all'evoluzione dei Sistemi:

- attività di gestione e installazione dell'hardware relativo al controllo accessi di AdP, comprensive di cablatura (patch), configurazioni di base, installazione di S.O.;
- garantire la disponibilità dei sistemi e l'esecuzione delle attività schedulate in coerenza con le specifiche e secondo le norme ed i criteri di sicurezza indicati da AdP;
- assicurare un presidio continuo al fine di controllare lo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;
- identificare e classificare gli elementi di configurazione relativi all'hardware e software, controllarne lo stato, le modifiche, il livello di aggiornamento, le interdipendenze, gestirne le condizioni di utilizzo, garantirne la rintracciabilità e l'adeguatezza;
- garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software, monitorandone il funzionamento;
- effettuare la gestione e la manutenzione dei sistemi e delle infrastrutture di CA;
- implementare la continuità operativa dei sistemi di CA e definita da AdP;
- verificare e assicurare la continuità operativa delle integrazioni con il Sistema di Video Sorveglianza (INDIGOVISION);
- verificare e integrare il Software Security OnLine.

6.1.2 Database

L'Aggiudicatario dovrà svolgere secondo le indicazioni e i permessi del RSIS attività di gestione delle basi dati del Sistema di Controllo Accessi di AdP. Le attività di gestione dei database comprendono:

- installazione dei prodotti software che implementano il database di CA;
- configurazione di database;
- riorganizzazione e parametrizzazione dei dati;
- analisi di occupazione spazio ed interventi di tuning e di ottimizzazione delle performance;
- manutenzione preventiva e correttiva;
- fornire supporto alla configurazione, nonché allo sviluppo di applicativi relativi alla modifica delle basi dati ai fini di un utilizzo ottimale, per il change e release management delle applicazioni, nonché gestioni di malfunzioni complesse o di interfaccia.

A tal fine si precisa che AdP, per esigenze operative e organizzative si è dotato di un proprio software (Security OnLine) appositamente sviluppato per la gestione delle anagrafiche, pertanto il concorrente dovrà preliminarmente svolgere apposita analisi in concerto con il summenzionato sviluppatore (LM Software), finalizzata all'integrazione del nuovo Sistema di CA con quello di anagrafica.

Il Concorrente dovrà fornire le licenze software intestate ad AdP, relative al DBMS anch'esso progettato in alta affidabilità in grado di essere eseguito all'interno del Cloud Privato di AdP composto da 2 (due) Server dotati di doppio processore da 12 Core cadauno.

6.1.3 Assistenza Sistemistica

Per assistenza sistemistica afferita al Sistema di Controllo Accessi si intende la gestione del software di base e delle licenze software gestite dall'Aggiudicatario per conto di AdP e comprendono i seguenti adempimenti:

- pianificare, sviluppare, collaudare ed applicare tutti gli aggiornamenti infrastrutturali dell'hardware e del software necessari all'upgrade (Server e Client);
- fornire assistenza alla gestione del sistema, dello storage e delle elaborazioni;
- prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio all'utenza;
- controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni esistenti.
- Provvedere alla integrazione di Software complementari (a titolo esemplificativo INDIGOVISION, Security OnLine, ecc.).

6.1.4 Business Continuity Aeroporto di Bari

AdP nel corso dell'appalto, provvederà all'allestimento tecnologico di una doppia Sala Server presso l'aeroporto di Bari, bilanciata per operare in Business Continuity in modo che una sala possa sopperire al carico dell'altra (non oggetto della presente procedura). Ognuna delle due sale sarà equipaggiata con gli stessi apparati di rete, di esecuzione e di storage. Sarà realizzata la medesima configurazione hardware,

pertanto il Concorrente dovrà provvedere senza oneri aggiuntivi a progettare una infrastruttura Software in grado di essere eseguita in ambiente virtuale in alta affidabilità, oltre all'installazione di almeno un ambiente di test.

COMPONENTI DI ESECUZIONE

Ognuna delle due sale server dell'aeroporto di Bari sarà essere equipaggiata con una serie di unità di elaborazione (fornite da AdP e non comprese nel Capitolato) in grado di garantire i requisiti minimi che il Concorrente indicherà ai fini dell'ammodernamento Software.

6.1.5 Policy Disaster Recovery

Si prevede presso l'aeroporto di Grottaglie (TA) l'installazione all'interno di una sala server dedicata l'implementazione in area separata, un ambiente virtuale per attività di test, sviluppo e per l'esecuzione delle copie asincrone di tutti i server virtuali di AdP, da attivare in caso di necessità (cause di disastro presso l'aeroporto di Bari che compromettono la possibilità di utilizzare entrambe le sale server).

A tal proposito qualora la già menzionata infrastruttura fosse disponibile nei termini di validità del Contratto, il Concorrente concorderà con AdP le opportune policy di backup da adottare al fine di disporre di una copia speculare dell'infrastruttura software presso l'aeroporto di Grottaglie.

6.1.7 Licenze Software

Tutti gli strumenti hardware e software che il concorrente necessiterà per realizzare l'ammodernamento del Sistema di CA dovranno essere forniti e dotati di tutte le licenze software necessarie intestate ad Aeroporti di Puglia intese come:

- Nuove licenze;
- Subscription a copertura di tutto il periodo previsto nel successivo Capitolo 6.8 – Fornitura e Installazione Software;
- Integrazioni con Sistemi di Video Sorveglianza e software Security OnLine.

L'Aggiudicatario dovrà provvedere senza costi aggiuntivi alle attività di aggiornamento e installazione delle eventuali nuove release del software di supervisione e controllo Accessi afferiti al nuovo software On Guard Pro Architecture coerentemente ai rilasci che saranno eventualmente resi disponibili dalla Soc. LenelS2 Carrier durante il periodo di vigenza contrattuale.

Al fine di mantenimento in sicurezza dell'intera infrastruttura Hardware e Software, dovranno essere garantiti senza costi aggiuntivi i relativi servizi di Supporto Specialistico.

L'Aggiudicatario dovrà in ogni caso farsi carico del rinnovo delle Subscription di cui al successivo Capitolo 6.8 - Fornitura e Installazione Software.

6.1.8 Piano operativo della continuità

Successivamente alla fase di aggiudicazione, dovranno essere realizzati ad opera del l'Aggiudicatario il Piano di Business Continuity (Business Continuity Plan – BCP), di Disaster Recovery (Disaster Recovery Plan – DRP):

- BCP - deve esplicitare l'insieme delle procedure e delle misure tecnologiche predisposte al fine di ripristinare i sistemi e garantire la funzionalità dei servizi applicativi nel caso di fault del Sistema Primario;
- DRP - deve esplicitare l'insieme delle procedure e delle misure tecnologiche predisposte al fine di garantire la funzionalità dei servizi applicativi nel caso di fault nel caso di fault del Sistema Primario e di quello Secondario;

La summenzionata documentazione dovrà essere sottoposta ad approvazione di AdP e dovrà descrivere nel dettaglio l'architettura predisposta e la sua interazione.

6.2 Adeguamento dell'infrastruttura ICT Security in tema di normativa GDPR e Cybersecurity

Il progetto tecnico che il Concorrente dovrà redigere dovrà tener conto di tutti i sistemi software di seguito specificati ad oggi gestiti da AdP per fornire servizi e sistemi di base a supporto dell'infrastruttura di Security, ovvero alle Policy By Design/Policy By Default del Regolamento (UE) 2016/679 GDPR (General Data Protection Regulation), ovvero al Regolamento di esecuzione UE 1998/2015 così come modificato dal Reg. UE 2019/1583 per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, riguardante le misure di cybersicurezza. Per ognuno di questi sistemi sono indicati gli interventi richiesti da AdP ai quali il Concorrente dovrà rispondere nel progetto tecnico con la sua soluzione proposta in conformità con le Policy by Design del GDPR.

In ogni caso tutti questi sistemi dovranno essere presi in carico dal Concorrente da un punto di vista amministrativo, pertanto nell'offerta presentata lo stesso dovrà farsi carico di:

1) Mettere a disposizione di AdP competenze e skill adeguati a gestire (nell'ambito del servizio di gestione dettagliato successivamente), manutenere e far evolvere il Sistema di CA di Aeroporti di Puglia:

2) Provvedere all'acquisto delle le licenze software afferenti al Sistema di Controllo Accessi indicandone i requisiti software compliant al GDPR (scaricabili dal link https://www.aeroportidipuglia.it/privacy-zone);

3) Provvedere alla sostituzione e al sostanziale aggiornamento del Sistemi di Controllo Accessi;

4) Gestire il processo di deploy ed effettuare la formazione al numero di utenti indicato per i sistemi di nuova introduzione;

6.3 Presa in carico del Sistema Software di Controllo Accessi

Il concorrente dovrà proporre un piano di intervento finalizzato alla:

- Presa in carico del Sistema di Controllo Accessi, provvedendo ad acquistare e rinnovare le licenze software (nel seguito dettagliate), garantire la manutenzione ordinaria, straordinaria e l'evoluzione a far data dalla stipula del Contratto e per tutta la durata contrattualmente prevista.
- Realizzazione delle migliorie e delle integrazioni ove necessario, al fine di promuovere i processi e realizzare i summenzionati adeguamenti normativi.

6.4 Servizi di gestione dell'infrastruttura ICT

Il concorrente nella propria proposta tecnica dovrà illustrare l'organizzazione del team di figure, con relativi skill specializzati in possesso di idonee Certificazioni in corso di validità e rilasciate dal Produttore del Software (LenelS2 Carrier), in grado di gestire i processi di Upgrade Hardware e Software nonché l'intera infrastruttura di Controllo Accessi ristrutturata. Il concorrente dovrà predisporre tutti i servizi necessari a garantire l'operatività H24 dell'infrastruttura di Security nel suo complesso, infrastruttura di base e applicativa (a seconda del sistema software di riferimento), l'ordinaria manutenzione al fine di rimuovere errori o bug di sistemi residui, la manutenzione straordinaria, la normale evoluzione dell'infrastruttura in termini di adeguamento a nuove versioni, l'installazione degli aggiornamenti, patch e quant'altro necessario a garanzia dell'operatività e del mantenimento del livello complessivo di sicurezza dell'infrastruttura di Security (Server e Client).

6.5 Servizio di Assistenza Hardware e Software

Tale servizio comprende le attività necessarie all'acquisto e al mantenimento Software (OnGuard Pro Architecture), nonché al mantenimento dei Sistemi Hardware coerentemente con le più recenti innovazioni rilasciate o che saranno eventualmente rese disponibili dalla Soc. LenelS2 Carrier, per la corretta erogazione dei Sistema di Controllo Accessi, nonché di tutte le attività necessarie al ripristino del funzionamento del Sistema di cui trattasi (Server e Client).

Sono previste le seguenti attività:

- assistenza per i sistemi hardware e software di Controllo Accessi. Per i componenti in garanzia, l'Aggiudicatario si conformerà alle istruzioni del programma di garanzia del costruttore durante il periodo di copertura della stessa gestendo opportuni agreement con i subfornitori al fine di rispettare i livelli di servizio previsti per il servizio. Le informazioni di dettaglio degli apparati in garanzia ed eventuali ulteriori informazioni saranno fornite nella fase di affiancamento di inizio fornitura;
- gestione della manutenzione delle apparecchiature garantendo la riparazione o sostituzione delle parti hardware difettose ovvero effettuare gli interventi sul software necessari a risolvere i malfunzionamenti rilevati al netto dell'hardware aggiuntivo (a carico di AdP) e necessario al servizio;
- manutenzione preventiva periodica ai sistemi hardware e software gestiti;

- Upgrade del software rilasciato dal Produttore (LenelS2 Carrier), fermo restando ove necessario la fornitura dell'hardware necessario da parte di AdP;
- Relazione trimestrale ad AdP relativamente alle linee di evoluzione tecnologica Hardware e Software rilasciate dal Produttore;
- Immediata segnalazione ad AdP relativamente alla cessazione da parte dei fornitori terzi dell'assistenza Hardware e Software delle apparecchiature e dei prodotti in uso per consentire l'adozione delle misure correttive necessarie;
- Gestione delle richieste di intervento in modo efficace, per tutto l'iter operativo, fino alla soluzione del problema secondo i tempi e le modalità di seguito indicate;
- Facilitare la comunicazione con gli utenti per il supporto alla soluzione di tutti quei problemi operativi che non richiedono l'intervento diretto presso i sistemi;
- Gestione delle procedure di Problem Management ed effettuare la diagnosi dei malfunzionamenti delle apparecchiature gestite;
- Minimizzare i tempi di fermo manutentivo, durante le operazioni di aggiornamento tecnologico e di manutenzione preventiva o correttiva;
- Verificare l'esito del ripristino hardware ed effettuare l'eventuale riconfigurazione software dei sistemi gestiti. Tale servizio comprende anche l'aggiornamento periodico dei prodotti che costituiscono l'ambiente software dei sistemi, aggiornamento volto a migliorare la funzionalità, l'affidabilità e l'efficienza dell'ambiente di sistema; ad esso è strettamente correlata la gestione della sicurezza per effetto della continua necessità di aggiornamento dei sistemi. A questo proposito, si dovrà fare ricorso a strumenti di change management per le componenti software di sistema.

AdP necessita di un servizio specializzato per assistenza Hardware e Software afferiti al Sistema di Controllo Accessi presenti presso gli aeroporti di Bari, Brindisi, Foggia e Grottaglie (TA).

Oggetto della Fornitura, sono anche i servizi di presidio presso lo Scalo di Bari e assistenza tecnica per quelli di Brindisi, Foggia e Grottaglie (TA) comprensivi di reperibilità H24 limitatamente allo Scalo di Bari.

Il Concorrente dovrà predispone come servizio minimo il presidio mediante proprio tecnico specializzato e in possesso di idonea certificazione in corso di validità rilasciata dal Produttore per le attività di verifica e ripristino Hardware e Software nelle giornate di lunedì, mercoledì e venerdì (H8/24).

Nelle giornate di presidio previste, dovrà secondo le indicazioni del RSIS, provvedere ai ripristini Hardware e Software, ovvero al manifestarsi di malfunzionamenti Hardware o Software provvedere al loro ripristino e ove praticabile collegandosi dallo Scalo di Bari con sessioni remote, diversamente recarsi presso gli Scali di Brindisi, Foggia e Grottaglie;

Il Concorrente dovrà predisporre idonea figura professionale in grado di provvedere agli interventi in reperibilità durante le ore non presidiate limitatamente a fermi di Sistema con i seguenti parametri di riferimento:

- Tempo di intervento on-site: entro 4 (quattro) ore;
- Tempo di ripristino: entro 60 minuti.

Il Servizio si intende "omnicomprensivo" di:

- tutte le attività di ripristino del Software (Server e Client);
- tutte le attività di ripristino o installazione delle componenti Hardware ivi comprese quelle rese disponibili da AdP;
- tutte le installazioni o nuove installazioni inerenti i software, compresi i service pack, aggiornamento firmware, driver ecc. rilasciati dal Produttore LenelS2 Carrier (Server e Client);
- SPOC (Single Point Of Contact) dedicato;
- tutte le attività di trasporto, trasloco, montaggio, installazione, noleggio nonché nuove attivazioni o implementazioni di hardware e software di base;
- ogni ulteriore elemento connesso alla completa operatività dei sistemi e delle postazioni.

Sono ad esclusivo carico di AdP le parti di ricambio hardware il cui approvvigionamento verrà concordato con il RSIS. AdP si riserva il diritto di mettere a disposizione dell'Aggiudicatario parti Hardware di Spare, intere unità Hardware di Spare o eventualmente richiederne allo stesso la fornitura di nuove da consuntivare a fine mese.

Per SPOC dedicato si intende il servizio verso AdP avente ad oggetto la ricezione, diagnostica, intervento e risoluzione delle richieste e problematiche. Il presidio On-Site presso lo Scalo di Bari, del personale tecnico competente dovrà essere svolto nelle giornate di **lunedì**, **mercoledì** e **venerdì (H8/24) e secondo le indicazioni e gli orari stabiliti dal RSIS**, fermo restando gli interventi in reperibilità che dovranno essere garantiti mediante copertura **H24 sabato, domenica e festività comprese**. Qualora le parti di spare siano disponibili al momento della chiamata il ripristino è garantito entro gli SLA definiti sopra.

Per tempo di intervento si intende il lasso di tempo intercorrente dal momento della ricezione della segnalazione di guasto (telefonate, mail, fax, ecc.) all'arrivo del tecnico in aeroporto. Per il Tempo di Ripristino si intende il lasso di tempo intercorrente dal momento dell'inizio dell'intervento alla sua risoluzione.

AdP può richiedere per particolari esigenze che verranno comunicate almeno con 24H di anticipo che il presidio possa essere effettuato in orari e in uno Scalo differente e/o in quantità differente presso altri scali. In caso di chiamate concorrenti, è di esclusiva competenza dell'RSIS AdP stabilirne la priorità.

La manutenzione correttiva, da intendersi compresa nel Servizio, ha l'obiettivo di ripristinare le funzionalità operative delle apparecchiature, a seguito di un malfunzionamento di qualsiasi dei componenti, sia

hardware sia software, delle stesse. L'utilizzo di risorse tecniche con skill adeguati all'attività richiesta dovranno consentire il raggiungimento di elevate performance in termini di risposta ed efficacia.

La manutenzione preventiva, da intendersi compresa nel Servizio, ha l'obiettivo di prevenire malfunzionamenti di tutte le componenti e periferiche hardware e software dei Sistemi e delle postazioni Client. La manutenzione ordinaria si basa su attività di verifica e pulizia degli apparati ritenuti "sensibili" che il RSIS indicherà alla Società (a titolo esemplificativo e non esaustivo: pulizia programmata di tutti gli apparati Server su base mensile, pulizia programmata degli armadi concentratori su base mensile, verifica dei contatti magnetici su base trimestrale, ecc.). Al termine dovrà essere redatto un verbale di tutte le postazioni coinvolte. Tale servizio dovrà essere pianificato con il RSIS in modo da poter essere effettuato in giornate ed orari distinti presso le varie aerostazioni e per lo stesso dovrà essere in ogni caso prodotto apposito Rapporto di Intervento.

Le figure di presidio dovranno essere figure locali fisicamente vicine allo scalo in cui operano, con profili e skill adeguati a gestire le necessità di intervento di prima necessità e a cooperare con i restanti servizi di seguito descritti al fine di comporre un Team di esperti a servizio della gestione dell'infrastruttura Security di CA nel suo complesso. I profili dovranno essere opportunamente addestrati per gestire gli interventi di prima necessità sulla infrastruttura Security nel suo complesso, pertanto dovranno avere skill di elevato profilo in grado di cooperare con i servizi di seguito descritti per gestire interventi su qualsiasi componente hardware o software che riguarda l'infrastruttura Security in alta affidabilità. A tal fine l'Aggiudicatario, per il personale interessato delle summenzionate attività dovrà produrre apposite Certificazioni rilasciate direttamente dal Produttore Soc. LenelS2 Carrier attestante il livello di qualifica.

L'Aggiudicatario si impegna ad effettuare gli interventi tecnici per riparazione, ripristino, sostituzione di tutto l'Hardware che verrà inventariato post sottoscrizione del contratto e su tutte le future installazioni che dovessero intervenire nel corso dell'esecuzione del contratto stesso, fermo restando la garanzia degli SLA contrattuali e il corrispettivo contrattuale offerto in sede di gara.

6.6 Servizio di Manutenzione e Assistenza

Il Concorrente nel predisporre il progetto tecnico dovrà prevedere tutto il necessario in termini di figure professionali, strumenti tecnologici, attrezzature hardware (qualora quanto già nelle disponibilità di AdP non sia ritenuto sufficiente), ad implementare un servizio di manutenzione proattiva dell'Infrastruttura di Security di CA.

Il servizio dovrà essere orientato alla gestione di ambienti che necessitano di operatività H24. Pertanto, il servizio dovrà essere attivo H24 7 giorni su 7 e dovrà avere come obiettivo quello di:

1) Mantenere attiva H24 l'infrastruttura Hardware e Software sia di base che applicativa del Sistema di Controllo Accessi.

2) Garantire il corretto utilizzo da parte degli utenti dell'infrastruttura di Security;

A titolo puramente indicativo e non esaustivo si riportano i servizi che dovranno essere erogati ai fini di manutenzione proattiva:

- Conduzione operativa degli applicativi;
- Installazione e configurazione del Hardware e del Software di Controllo Accessi(Server e Client);
- Gestione dell'infrastruttura di virtualizzazione (creazione e deployment di una nuova macchina virtuale, gestione del carico sul cluster e ottimizzazione del posizionamento delle macchine virtuali, eventuali operazioni di spostamento delle macchine tra nodi del cluster, ecc.), per la sola parte applicativi software;
- Gestione delle procedure di Backup e Restore e dei piani di Disaster Recovery (per la sola parte applicativi software);
- Gestione Server Applicativi, Web Server (solo componente software);
- Monitoraggio dei sistemi di rilevazione e risoluzione dei malfunzionamenti hardware e software;
- Monitoraggio dei sistemi e dei servizi applicativi;
- Analisi del carico dei sistemi e monitoraggio delle prestazioni.

Tutti gli skill professionali dovranno coordinarsi con il RSIS di AdP, prima dell'attuazione del piano delle attività e in generale ogni qualvolta si renderà necessario, verranno concordate e formalizzate le modalità operative di cooperazione tra Ufficio Security di AdP e personale tecnico dell'Aggiudicatario. In ogni caso il personale tecnico afferente all'Ufficio Security dovrà essere messo in condizione ove necessario di poter intervenire su ogni singola componente in autonomia, nonché essere deputato alle attività di amministrazione, di determinate componenti ICT demandando all'Aggiudicatario solo le attività operative per il corretto funzionamento della singola componente di CA.

Il servizio dovrà essere erogato sia in modalità proattiva che eventualmente ingaggiato dal servizio di assistenza in presidio, che dagli utenti finali direttamente.

Il servizio dovrà essere organizzato per prevedere eventuali fault dovuti a malfunzionamenti hardware, software, logici, riempimento di spazio di dischi o tablespace o degrado delle performance della intera componente Hardware e Software.

Il servizio di manutenzione dovrà occuparsi delle segnalazioni che perverranno dal RSIS o in sua vece da personale tecnico di AdP preposto, su tutte le componenti dell'infrastruttura di CA e dovrà anche occuparsi di mantenere costantemente l'infrastruttura con una serie di piani di attività di manutenzione e aggiornamento programmati. Tali interventi potranno riguardare ad esempio versioni di software o firmare, patch, aggiornamenti vari di una qualunque delle componenti dell'infrastruttura di CA descritta nei paragrafi precedenti (Server e Client).

Tutte le segnalazioni generate, come tutte le manutenzioni programmate o richieste di intervento da parte di AdP dovranno essere registrate in appositi report in formato elettronico al fine di monitorarne i tempi di attivazione e chiusura.

Manutenzione e assistenza

Il Servizio dovrà garantire la manutenzione ed assistenza (Server e Client) per tutta la durata contrattuale di tutta l'infrastruttura di CA Security prevedendo anche le seguenti prestazioni:

- diagnostica e risoluzione di problemi o malfunzionamenti relativi all'infrastruttura di CA (Hardware e Software), consistente nella presa in carico delle segnalazioni effettuate dal RSIS o dagli Uffici Preposti, nell'attivazione delle opportune azioni correttive (apertura guasti, richieste di sostituzione hardware);
- adeguamento tecnologico del prodotto, che a parità di funzionalità consenta di mantenere la coerenza del prodotto con lo sviluppo tecnologico delle sue componenti di base, aggiornando gli applicativi ad esempio in modo che possano operare su una nuova versione di data base relazionale, senza ulteriori costi di installazione;
- esecuzione di interventi migliorativi finalizzati a ottimizzare le prestazioni e la qualità delle procedure esistenti (Es. implementazione nuove regole e/o modifica delle esistenti, creazione nuovi utenti, attivazioni nuovi prodotti su macchine automatiche, ecc.);
- esecuzione delle opportune procedure di backup automatizzato delle configurazioni degli apparati hardware e software necessario al corretto funzionamento dell'infrastruttura di CA;
- predisposizione di un piano di controllo, verifica e produzione di reportistica da inviare al RSIS di AdP che attesti il regolare funzionamento, stato di aggiornamento, interventi effettuati e ogni informazione utile a garantire il controllo sulle attività svolte sull'intera infrastruttura di CA;
- predisposizione di un piano di Test concordato al fine di assicurare che le componenti critiche, come l'alta affidabilità, la correttezza e completezza dei backup siano integre e disponibili in caso di necessità.

In particolare, dovranno essere garantite le seguenti tipologie di attività di manutenzione:

- manutenzione e assistenza correttiva;
- assistenza alla gestione applicativa;
- manutenzione e assistenza adeguativa.

Manutenzione e assistenza correttiva

Il servizio di manutenzione e assistenza correttiva ha per finalità la garanzia del mantenimento della operatività e della funzionalità dell'infrastruttura garantendo il minor tempo di disservizio ad AdP, attuato

attraverso la rimozione di errori residui, non identificati nella fase di produzione, che si manifestano durante la vita operativa dell'infrastruttura. La rimozione degli errori (Server e Client) potrà avvenire secondo la tecnica ritenuta più opportuna in accordo con la prassi consolidata di ingegneria del software e in ogni caso con modalità che non introducano effetti collaterali indesiderati o potenzialmente dannosi per l'operatività e le funzionalità dell'infrastruttura o dei sistemi ad essa collegati. Gli interventi di manutenzione correttiva devono restituire l'infrastruttura in condizioni operative di perfetto funzionamento, con ripristino dello stato informativo precedente al momento in cui si è verificato l'evento che ha richiesto l'intervento manutentivo (con sistemazione, in particolare, di basi di dati corrotte, elaborazioni non effettuate, elaborazioni non volute, ecc.), ed essere coerente con le release rilasciate dal Produttore LenelS2 Carrier.

Assistenza alla gestione Applicativa

Il servizio di assistenza dovrà prevedere secondo gli SLA della manutenzione correttiva, anche eventuali assistenze agli utenti dei vari applicativi che trovano difficoltà nell'utilizzo dei programmi non dovute a malfunzionamenti ma a cause imputabili all'utente che tenta di effettuare operazioni in modo improprio o non consentito.

Il servizio di supporto all'utenza ha come scopo quello di garantire un corretto ed efficiente utilizzo di ogni componente Hardware e Software di CA, supportando gli utenti finali nella soluzione di problemi operativi che possono emergere nell'utilizzo.

Il servizio ha l'obiettivo di agevolare l'utente nella fruizione delle applicazioni, chiarendone le modalità operative di utilizzo, fornendo supporto nella fruizione più efficace delle funzioni disponibili e dei dati gestiti dalle applicazioni.

Manutenzione e assistenza adeguativa

Consiste nelle attività necessarie a rendere operativo e continuo il funzionamento dell'infrastruttura garantendone la continuità, la disponibilità, l'affidabilità, la sicurezza e l'integrità (Server e Client). La manutenzione adeguativa è volta ad assicurare la costante aderenza delle procedure e dei programmi alla evoluzione dell'ambiente tecnologico del sistema informativo, come ad esempio l'innalzamento dei livelli (es. Upgrade, Service Pack) del software di base.

Il servizio di **Manutenzione e assistenza adeguativa** ha lo scopo, quindi, di assicurare il costante, efficace e tempestivo aggiornamento ed evoluzione delle funzionalità del software applicativo, senza costi aggiuntivi e per il quale il Concorrente dovrà fornire assistenza, rispetto a:

- variazioni normative o di regolamenti emessi da Autorità competenti in ambito aeroportuali che comportino interventi di modifica del software;
- evoluzione delle versioni del sistema software di CA che intervengano nel corso del contratto;

- implementazione e/o modifica di configurazioni effettuabile su ogni singola componente hardware o software dell'intera infrastruttura di CA che la componente permette di gestire senza necessità di personalizzazioni software;
- attività di ordinaria amministrazione dei sistemi (Backup, Creazioni profili, Modifica Utenti, Cambio di parametri, Estrazione report, export dei database ecc.);
- esecuzione di periodiche procedure di salvataggio delle componenti software critiche dell'infrastruttura;
- installazione di patch, aggiornamenti di sicurezza e aggiornamenti applicativi necessari.

AdP si riserva coerentemente con la normativa vigente di effettuare delle analisi di sicurezza e vulnerabilità sulla nuova infrastruttura realizzata e gestita dall'Aggiudicataria. Qualora risultassero non conformità rispetto ad essa o nell'ipotesi di vulnerabilità, il Concorrente si impegnerà a proprie spese a porre rimedio ovvero ad adottare misura di mitigazione entro e non oltre 30 giorni dalla formale comunicazione.

AdP si riserva di effettuare attività ispettive, in conformità a quanto previsto nell'Art. 28 lett. h) del GDPR per verificare il rispetto degli obblighi previsti nel Regolamento in virtù della designazione dell'Aggiudicatario a Responsabile del Trattamento e suoi eventuali subresponsabili.

AdP si riserva di richiedere risarcimento danni qualora al verificarsi di avaria hardware il ripristino delle funzionalità del sistema sia compromesso a causa della mancanza di opportuni backup anche automatizzati e opportunamente aggiornati e per danni a terzi.

Il Concorrente senza costi aggiuntivi nel predisporre il progetto tecnico dovrà prevedere relativamente all'infrastruttura di Controllo Accessi e presso una qualunque delle sedi aeroportuali, idonee figure professionali esperte dei sistemi hardware o software di cui trattasi per attività specialistiche non gestibili da remoto.

Si precisa che tutte le attività che necessiteranno di fermi operativi, dovranno essere preventivamente concordate con il RSIS, che valuterà e indicherà la finestra temporale in cui programmare l'attività. Per i sistemi critici e che impattano sulle attività dei passeggeri le attività dovranno essere schedulate in orari notturni.

6.7 Servizio Help Desk (SPOC)

Il concorrente nel predisporre il progetto tecnico dovrà comprendere anche un servizio di Help desk di primo livello di tipo SPOC (Single Point Of Contact), rigorosamente in lingua italiana, per tutta la durata contrattuale che dovrà essere reperibile 24 ore su 24, 7 giorni su 7, festivi compresi.

Il servizio dovrà essere erogato a fronte di specifica richiesta di intervento, tale richiesta dovrà necessariamente pervenire dal RSIS o da personale da esso incaricato. Per garantire il corretto funzionamento dell'apertura delle chiamate il Concorrente dovrà comunicare ad AdP contestualmente alla

stipula del Contratto tutti i recapiti telefonici, a mezzo posta elettronica o fax che AdP dovrà utilizzare per la segnalazione di qualsiasi natura (malfunzionamento, richiesta di assistenza, appuntamento on-site, ecc..).

Il servizio si occuperà di:

- prendere in carico la segnalazione attivando tutte le procedure necessarie ad effettuare eventuale analisi del malfunzionamento e il successivo ripristino o semplicemente a comunicare l'esito al richiedente
- tracciare tutte le chiamate pervenute, in modo da poter redigere con cadenza mensile un apposito report con l'elenco delle chiamate ricevute, le attività intraprese e i tempi per la chiusura dell'attività in modo da controllare gli SLA contrattuali.

Il servizio offerto dovrà garantire i seguenti livelli minimi di servizio:

- Tempo di risposta: Entro 15 MINUTI;
- Apertura del ticket;
- Verifica dello stato dei ticket aperti;
- Chiusura del ticket;

Qualora per qualsivoglia motivo il servizio di assistenza sarà impossibilitato a connettersi e/o a risolvere la problematica segnalata da remoto (esempio: guasto a hardware del varco o lettore ottico), dovrà sempre e comunque garantire l'intervento on-site (presso una qualunque delle sedi aeroportuali) al fine di rispettare gli SLA contrattuali del servizio di gestione e monitoraggio proattivo dell'infrastruttura, di cui al precedente Punto 6.5 - Servizio di Assistenza Hardware e Software.

Il servizio di Help desk offerto dovrà avere caratteristiche di un servizio Single Point Of Contact (SPOC) pertanto il Concorrente si impegna ad interfacciarsi, se necessario, con aziende terze fornitrici di servizi (fornitori terzi, subfornitori, aziende esterne) fino alla completa risoluzione delle problematiche.

Il concorrente dovrà prevedere nel progetto tecnico e senza necessità di rinnovo di licenze, la fornitura di un Software ad hoc di trouble ticketing, in grado di gestire il servizio, il magazzino, e realizzare i rapportini di intervento. Tale sistema al termine del periodo contrattuale dovrà rimanere di proprietà di AdP.

Ad ogni richiesta di intervento di qualsiasi natura, dovrà essere attivato un rapportino che ne riporti tutti i dettagli, il rapportino dovrà essere firmato dal richiedente o da suo delegato ad attestazione della chiusura dell'intervento.

Il Concorrente dovrà predisporre, come precedentemente indicato anche tutto l'inventario hardware del Sistema di CA e per tutti gli Scali. Eventuali necessità di sostituzione di apparati o reintegro degli stessi, dovrà essere formalizzata in modo da consentire ad AdP di disporre sempre di una situazione aggiornata

dell'inventario hardware e software, della corretta collocazione dei beni aziendali, nonché delle eventuali Spare Parts necessarie a magazzino.

Il servizio di Help Desk dovrà avere contezza delle componenti facenti parte dell'infrastruttura di CA nel suo complesso, e provvederà a fornire assistenza anche a eventuali Fornitori esterni che AdP indicherà, ai quali verranno concessi gli accessi alla piattaforma software. Il monitoraggio degli SLA degli interventi di tali Fornitori dovrà essere consultabile e gestibile separatamente non essendo sotto la responsabilità del Concorrente.

Eventuali proposte di Sistemi per la Gestione del Trouble Ticketing dovranno essere fornite nel rispetto delle normative in tema di GDPR.

Per la gestione amministrativa del contratto, AdP, richiede lo SPOC (Single Point Of Contact) pertanto il Concorrente dovrà indicare nell'offerta tecnica il nome (o i nomi nel caso sia un team di responsabili per area) del proprio Referente inteso come "Responsabile del Servizio", del quale dovrà essere fornito il telefono fisso, mobile, FAX e indirizzo di posta elettronica, che sarà il punto di riferimento per il RUP o l'RSIS per dare seguito relativamente alla gestione del contratto, nonché alla presa in carico delle problematiche tecniche e amministrative che dovessero insorgere durate la durata dello stesso. Lo SPOC dovrà essere messo a disposizione di AdP prevedendo una visita mensile presso la Sede di Bari, propedeutica alla verifica dell'andamento del servizio, alla gestione del contratto nonché alla emissione dei certificati di regolare esecuzione in qualsiasi fase propedeutici alla liquidazione delle fatture.

6.8 Formazione

L'aggiudicatario dovrà contestualmente all'upgrade dei Sistemi, prevedere apposite sessioni formative On-Site periodiche e per tutta la durata contrattuale. L'attività di formazione dovrà essere effettuata presso la sede di Bari per gli utenti non Amministratori di Sistema. Il concorrente indicherà nel progetto tecnico per ogni intervento che impatta sugli utenti finali il numero di giornate di formazione preventivate necessarie alla messa in produzione della nuova componente di CA.

In ogni caso, l'aggiudicatario si impegna a effettuare l'attività formativa durante tutta la durata contrattuale anche in occasione di modifiche software che impattano sulle normali attività degli utenti. I piani dell'attività formativa dovranno essere preventivamente concordati con il RSIS di AdP, che inoltre si riserva di richiedere eventuali sessioni di training aggiuntive e/o integrative da svolgersi presso la Sede di Bari.

A tal fine e per tutta la durata contrattuale l'Aggiudicatario dovrà produrre ad ogni cambio release la relativa manualistica.

L'aggiudicatario dovrà predisporre inoltre dei piani formativi durante tutta la durata contrattuale necessari alla formazione di personale tecnico di AdP in modo da renderlo autonomo nelle operazioni di gestione e utilizzo del Sistema (ad esempio: la consultazione di log, modifica di utenti, la modifica di profili, la gestione di policy, ecc.). Ove possibile l'Aggiudicatario valuterà la partecipazione di personale indicato dal RUP o dal RSIS e afferente l'Ufficio Security a corsi di certificazione organizzati direttamente dai vendor e/o provider di specifiche tecnologie.

Le sessioni formative dovranno essere distinte per le seguenti tipologie di utenti finali:

- Sessione di Training per Amministratore di Sistema (max 2 partecipanti);
- Sessione di Training per personale Tecnico Ufficio Security (max 3 partecipanti);
- Sessione di Training per personale impiegato presso la Sala Controllo (max 15 partecipanti).

Al termine di ogni sessione formativa, sarà cura dell'appaltatore rilasciare apposito Certificato di Formazione.

6.9 Installazione di apparati hardware

Il concorrente dovrà includere nell'offerta presentata l'installazione dell'hardware fornito da AdP necessario alla ristrutturazione dell'intera infrastruttura di Controllo Accessi e per tutte le Sedi AdP.

L'Aggiudicatario dovrà provvedere a costo zero e per tutta la durata contrattuale alla gestione delle sostituzioni in Garanzia, al ripristino o sostituzione dell'Hardware fornito da AdP. Per tutte le componenti di nuova fornitura (che AdP metterà a disposizione) il concorrente dovrà analogamente prevedere all'installazione a costo zero per qualsiasi nuova componente hardware riferita al CA (fatta eccezione per eventuali cablaggi).

L'Aggiudicatario dovrà farsi carico senza costi aggiuntivi delle installazioni da effettuarsi in anche orari notturni (relativamente all'hardware in aree operative), e di tutti gli oneri derivanti dall'adeguamento secondo le indicazioni di AdP. Tutto l'hardware dismesso dovrà essere dislocato, in apposito magazzino reso disponibile presso l'aerostazione di Bari.

Ogni ulteriore e nuova fornitura di apparati che l'Aggiudicatario andrà ad installare presso una delle aerostazioni, dovrà essere resa disponibile secondo i seguenti parametri:

- Prodotti originali recanti il marchio di fabbrica del costruttore;
- Prodotti nuovi nel loro packaging originale, e saranno acquistati e licenziati tramite Canali Autorizzati dal Produttore e specificatamente per il cliente Aeroporti di Puglia S.p.A., che sarà il primo acquirente dei prodotti e primo licenziatario di qualsiasi copia di Software, compreso quello incluso dei prodotti;
- L'aggiudicatario si impegna a fornire licenze software originali rilasciate per Aeroporti di Puglia S.p.A. ed apparati idonei allo scopo;
- L'aggiudicatario non potrà fornire materiali di provenienza illegale, o prodotti usati e rigenerati;
- In relazione ai prodotti che verranno acquistati per il progetto Aeroporti di Puglia S.p.A. non dovrà essere messa in condizioni di dover pagare:
    - Tariffe di ispezione dei prodotti del costruttore;
    - Tariffe di relicenziamento del software aggiuntive, che in ogni caso dovranno essere pagate dall'Aggiudcatario, fatto salvo il diritto di maggior danno di Aeroporti di Puglia S.p.A. nei confronti dell'aggiudicatario;

Aeroporti di Puglia S.p.A., a tutela dei propri interessi, si riserva comunque di effettuare verifiche dirette con l'azienda costruttrice e di richiedere all'aggiudicatario conferma scritta di quanto sopra e/o dichiarazione scritta dalla casa madre.

Tutte le apparecchiature hardware dovranno rispettare le norme sugli standard tecnici, sugli standard di qualità, sicurezza, ergonomia e sugli standard di comunicazione indicati nella normativa italiana ed europea in vigore.

Il Concorrente deve garantire che le apparecchiature siano state progettate e costruite in conformità delle norme CEI 110-5 (EN 55022) per i limiti di emissione radio disturbi e EN50082-1 per quelli di immunità. Inoltre, devono essere provviste di marcatura CE in ottemperanza con la direttiva CEE sulla compatibilità elettromagnetica.

Si riepiloga di seguito tutto l'hardware già nella disponibilità di AdP e comprensivo di Spare Parts che l'Aggiudicatario dovrà installare senza oneri aggiuntivi presso tutte le Sedi di AdP:

- N° 42 - Codice Prodotto LNL-3300-M5 - Intelligent System Controller, 12 VDC, Size (4 in. W x 10.25 in. L) RoHS;
- N° 42 – Codice Prodotto LNL-8000-MCOM - Power/ Communications Module-Provides RS485 comm & Power to enclosure; Size (4 in. W x 10.25 in. L);
- N° 67 – Codice Prodotto LNL-1380-8RP - Eight Reader Interface Module (Supports SF2F Rdr) 12/VDC; 8 Rdr interface;
- N° 37 – Codice Prodotto LNL-1100-20DI - Input Control Module, 12 VDC; 20 zone input module;
- N° 12 – Codice Prodotto LNL-1200-16DOR - Output Control Module, 12 VDC; 16 relay output control module;

Pertanto, prima dell'erogazioni di tali servizi on-site, il RSIS di AdP dovrà dare formale autorizzazione secondo le modalità descritte nel Piano delle Attività fornito dal Concorrente e formalizzate in sede contrattuale.
Le rendicontazioni verranno effettuate mensilmente previa sottoscrizione di apposito verbale di regolare esecuzione del servizio a firma del RUP in contradittorio con lo SPOC.
L'Aggiudicatario dovrà preventivare la possibilità da parte di AdP di richiedere la fornitura di parti di ricambio aggiuntive degli apparati oggetto del servizio di manutenzione hardware descritto in precedenza che dovessero rendersi necessarie dopo la presa in carico del servizio. Tali forniture dovranno preventivamente essere autorizzate dal RUP, il quale esprimerà il proprio benestare nelle quantità e congruità dei prezzi oggetto della richiesta di autorizzazione. Qualora AdP, non ritenga conveniente, potrà autonomamente provvedere ad approvvigionarsi di fornitura equivalente al fine di garantire l'operatività del Sistema, nonché all'eventuale reintegro delle scorte a magazzino. Con cadenza mensile, inoltre il RUP e

lo SPOC, in contraddittorio durante la verifica di regolare esecuzione del servizio, rendiconteranno eventuali forniture aggiuntive che implicano la necessità di sostituzioni di apparati hardware, nel mese di riferimento, con le relative quantificazioni economiche.

6.8 Fornitura e Installazione Software

Nell'ambito delle preliminari analisi di evoluzione del Sistema di Controllo Accessi svolte con il Produttore LenelS2 Carrier, al fine del mantenimento della coerenza evolutiva e tecnica, AdP ha inteso mediante la procedura di che trattasi, di approvvigionarsi anche di alcune componenti software afferite al Sistema di Controllo Accessi.

Il Concorrente pertanto dovrà provvedere a proprie spese all'acquisto, alla installazione, nonché all'adeguamento delle componenti software senza oneri aggiuntivi presso le Sedi di AdP interessate da adeguamento evolutivo e di seguito elencate:

- N° 1 – Codice Prodotto SWS-PRO – OnGuarde PRO Server Software Licence;
- N° 3 – Codice Prodotto PRO-64RUP – 64 Access Readers upgrade for all PRO Systems;
- N° 5 – Codice Prodotto SWC-ADV – OnGuarde ADV Client Software Licence;
- N° 5 – Codice Prodotto SWC-IDADV – OnGuarde IDADV Client Software Licence;
- N° 5 – Codice Prodotto OCB-A-PROENT-1 – Non-expiring license for one seat of OnGuard Credentials Client and one seat of OnGuard Monitor client for OnGuard PRO client;
- N° 1 – Codice Prodotto SWG-1225 – DataExchange - Global Data Import/Export Utility;
- N° 1 – Codice Prodotto SWG-1210 – OnGuard FormsDesigner (User definable Fields);
- N° 1 – Codice Prodotto SWG-1240 – Database Segmentation;
- N° 1 – Codice Prodotto SWG-1360 – OnGuard support for Remote Desktop Protocol;
- N° 1 – Codice Prodotto SWG-1140 – DataConduIT included one connection license;
- N° 1 – Codice Prodotto SWG-1635 – Enable Support for Lenel M Series Hardware;
- N° 1 – Codice Prodotto SWG-LP – Language Pack Module;
- N° 3 – Codice Prodotto SUSP-PRO-TR2;
- N° 1 – Codice Prodotto SWC-VIEW5 – View Only Client Workstation Software License - Five (5) License Pack;

- N° 1 – Codice Prodotto SWG-RAM5 – OnGuard Area Access Manager Software License - included 5 concurrent User Licenses;
- N° 1 – Codice Prodotto LSM-3PA-PRO-B – Non-expiring License for a single OnGuard 3rd Party Authentication (OIDC);
- N° 1 – Codice Prodotto LSM-CSS-PRO-A –Non-expiring License for OnGuard Cardholder Self Service module.
- N° 5 – Codice Prodotto LNL-X2220 - Intelligent Dual Reader Controller;

L'Aggiudicatario dovrà preventivare la possibilità da parte di AdP di richiedere la fornitura, nonché l'installazione di licenze software aggiuntive rispetto a quanto sopra menzionato che dovessero rendersi necessarie dopo la presa in carico del servizio. Tali forniture dovranno preventivamente essere autorizzate dal RUP, il quale esprimerà il proprio benestare nelle quantità e congruità dei prezzi oggetto della richiesta di autorizzazione. Qualora AdP, non ritenga conveniente, potrà autonomamente provvedere ad approvvigionarsi di fornitura equivalente al fine di garantire l'operatività del Sistema. Con cadenza mensile, inoltre l'RUP e lo SPOC, in contraddittorio durante la verifica di regolare esecuzione del servizio, rendiconteranno eventuali forniture aggiuntive che implicano la necessità di sostituzioni di implementazioni software, nel mese di riferimento, con le relative quantificazioni economiche.

6.9 Monitoraggio della Qualità del servizio

I processi e le attività che l'Aggiudicatario indicherà, devono derivare dagli standard e dalle metodologie di gestione della Qualità proprie della Società medesima, al fine di garantire che le risposte siano in linea con le esigenze e richieste di AdP SpA. L'Aggiudicatario dovrà incorporare la qualità stessa in tutti i processi che sono alla base dell'attività e della vita aziendale di AdP SpA mediante la definizione preliminare delle specifiche fino al controllo, manutenzione, sicurezza, affidabilità e manutenibilità delle soluzioni proposte e della conduzione del servizio. La Società deve assumere come obiettivo prioritario la Customer Satisfaction di AdP SpA, al cui perseguimento è orientato l'impegno congiunto di tutte le unità operative, in armonia con tutto lo staff Security di AdP SpA.

Con cadenza mensile dovrà essere firmato in contraddittorio con il RUP un verbale di andamento attività e di regolare esecuzione del servizio che riporti (a titolo esemplificativo e non esaustivo):

- l'elenco degli interventi effettuati distinti per sede con indicazione dei tempi di attivazione, intervento e risoluzione delle anomalie segnalate;
- l'elenco degli interventi effettuati dal servizio di monitoraggio proattivo con indicazione dei tempi di rilevazione dell'anomalia, i tempi di intervento e i tempi di risoluzione;
- l'eventuale necessità di parti di ricambio necessarie al corretto funzionamento dell'infrastruttura di CA per tutte le componenti non coperte da garanzia;

- indicazione di tutti gli interventi che non rispettano gli SLA contrattuali con motivazione degli scostamenti;
- indicazione di tutte le giornate di assistenza on-site erogate nel mese di riferimento, con evidenza dell'iter di autorizzazione all'erogazione;

AdP si riserverà la possibilità di applicare le penali previste contrattualmente ogni qual volta verranno individuate delle non conformità valutando nel merito eventuali danni diretti o indiretti subiti da AdP a seguito dell'inadempienza dell'Aggiudicatario.

In ogni momento AdP si riserverà la possibilità di recedere dal contratto qualora:

- l'inadempienza contrattuale del concorrente comporti dei gravi danni diretti o indiretti all'operatività degli aeroporti, o all'immagine di AdP indipendentemente dalla quantificazione economica derivante dal calcolo economico;
- in caso di reiterati comportamenti dell'Aggiudicatario ripetutamente segnalati ai quali non sono seguite le azioni di rimedio concordate;

7. INDICAZIONI PER LA REDAZIONE DEL PROGETTO

Il concorrente dovrà predisporre un progetto tecnico che preveda tutti gli interventi che il concorrente metterà in atto al fine di soddisfare tutte le esigenze espresse nel presente Capitolato Tecnico.

Tutte le installazioni dovranno essere eseguite garantendo la continuità di servizio, pertanto, in funzione delle esigenze operative di AdP alcune delle attività necessarie all'avvio di nuovi impianti o sistemi che impatteranno sull'operatività aeroportuale, dovranno essere eseguite, senza oneri aggiuntivi, anche in orari notturni. A tal fine nella propria Offerta Tecnica, il Concorrente, dovrà fornire ad AdP un CRONOPROGRAMMA dettagliato delle attività, indicante i tempi di esecuzione delle attività di Upgrade dei Sistemi Hardware e Software, nonché di eventuali migliorie aggiuntive che il concorrente riterrà opportuno introdurre. Una volta approvato, il Piano potrà subire modifiche solo per necessità di AdP, il concorrente dovrà impegnarsi al fine di completare le attività nei tempi stabiliti.

Si precisa che l'Aggiudicatario dovrà garantire tutto il supporto necessario con figure professionali idonee in loco per controllare e garantire il livello di funzionalità dell'infrastruttura nei primi giorni di avvio di nuovi impianti o sistemi, in modo da garantire la massima tempestività dell'intervento.

Tutta l'attività dovrà essere descritta sia sul piano dei contenuti tecnici, che sul piano delle modalità operative e dell'utilizzo delle risorse ed informazioni messe a disposizione da AdP.

Si precisa che i lavori dovranno essere in tutto conformi alla proposta tecnico economica offerta, alle indicazioni ivi contenute e a tutte le normative di realizzazione degli impianti/sistemi a regola d'arte che fanno parte integrante del presente Capitolato Tecnico. Si precisa che qualsiasi incombenza non prevista nel presente Capitolato Tecnico e nell'offerta proposta è da intendersi completamente a carico della

Società vincitrice dell'appalto, ad eccezione dell'Hardware o del Software necessario a nuove attivazioni afferite al Sistema di Controllo Accessi.

Il Progetto da presentare come proposta tecnica per la fornitura oggetto del presente Capitolato Tecnico dovrà essere redatto:

- in lingua italiana, in maniera che possano evincersi, in modo completo e dettagliato, tutti gli elementi che il concorrente riterrà utile fornire ai fini della valutazione dell'offerta, con riferimento ai criteri (tecnici) di valutazione stabiliti nel Disciplinare di gara ed alla descrizione delle caratteristiche illustrate nel presente Capitolato Tecnico;
- su fogli singoli di formato A4, con una numerazione progressiva e univoca delle pagine;
- specificando e motivando, nelle premesse, se e quale parte della documentazione presentata, il concorrente ritiene coperta da riservatezza, con riferimento a marchi, know-how, brevetti, ecc.

Il ***Progetto*** dovrà, pertanto, essere strutturato in moduli (Max 50 pagine solo fronte per ogni capitolo), e contenere le seguenti informazioni:

1) **Introduzione** - Presentazione generale del concorrente e della sua organizzazione, con esplicito riferimento alle principali esperienze maturate in campo di installazione, upgrade e gestione dei medesimi Sistemi di Controllo Accessi. e con una descrizione di tali pregresse esperienze in relazione all'organizzazione che il concorrente metterà in campo per realizzare quanto previsto nel Capitolato Tecnico.

2) **Upgrade Hardware** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza le attività da svolgersi coerentemente con le esigenze espresse nel presente Capitolato Tecnico. Essa dovrà contenere limitatamente alla componente hardware almeno le seguenti informazioni:

    a. Descrizione delle modalità e tipologia di intervento proposto afferiti alla sostituzione Hardware di cui ai Capitoli 4.3 - Elenco degli apparati di Controllo Accessi e 6.7 Installazione di apparati hardware;

    b. Diagramma di Gantt.

3) **Upgrade Software** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza le attività da svolgersi relativamente all'Upgrade della componente software coerentemente con le esigenze espresse nel presente Capitolato Tecnico. Essa dovrà contenere limitatamente alla componente hardware almeno le seguenti informazioni:

    a. Descrizione delle modalità e tipologia di intervento proposto afferiti alla sostituzione e installazione Software di cui al Capitolo 6.8 Fornitura e Installazione Software;

    b. Diagramma di Gantt.

c. Descrizione sintetica dei sistemi che il concorrente utilizzerà per gestire i servizi di assistenza e manutenzione e di tutti i sistemi di nuova introduzione.

4) **Servizio di Assistenza Hardware** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza il tipo di figura/e a che intende mettere a disposizione per le attività previste nel presente Capitolato e il periodo contrattuale. Essa dovrà contenere almeno le seguenti informazioni:

   a. Numero di personale impiegato e a disposizione per le attività di Upgrade Hardware e Software;

   b. Modalità di erogazione del Servizio di assistenza tecnica OnSite (SPOC);

   c. Certificazioni in corso di validità o maturate attinenti alla componente Hardware;

   d. Diagramma di Gantt afferito alla presenza di personale e coerente con le attività e le tempistiche da svolgersi.

5) **Servizio di Assistenza Software** – Il Concorrente dovrà predisporre una relazione dettagliata che metta in evidenza il tipo di figura/e a che intende mettere a disposizione per le attività previste nel presente Capitolato e il periodo contrattuale. Essa dovrà contenere almeno le seguenti informazioni:

   a. Numero di personale impiegato e a disposizione per le attività di Upgrade Hardware e Software;

   b. Modalità di erogazione del Servizio di assistenza tecnica OnSite (SPOC);

   c. Certificazioni in corso di validità o maturate attinenti alla componente Software;

   d. Diagramma di Gantt afferito alla presenza di personale e coerente con le attività e le tempistiche da svolgersi.

6) **Interventi Migliorativi** - Eventuali Migliorie offerte dal concorrente rispetto a quelle indicate nel Capitolato tecnico e che lo stesso ritiene utili e strategiche alla evoluzione e alla manutenzione complessiva dell'infrastruttura di Controllo Accessi.

8. CONDIZIONI GENERALI DI FORNITURA

Si riepilogano di seguito le condizioni generali di fornitura che verranno riportate nel Contratto che si andrà a stipulare con l'Aggiudicatario.

8.1 Sostituzione personale impiegato

AdP si riserva insindacabilmente di richiedere la sostituzione del personale impiegato dall'Aggiudicatario, nel caso di gravi o reiterati inadempimenti del personale stesso, di chiedere l'allontanamento del personale

che si sia reso inadempiente agli obblighi del Contratto o che abbia dimostrato scarse qualità tecniche, morali e disciplinari. AdP comunicherà formalmente tale decisione e l'Appaltatore si impegna entro un periodo di 30 giorni solari a rendere operative le sostituzioni richieste da AdP.

8.2 Fatturazione e modalità di pagamento

Relativamente ai costi di avviamento e fornitura, l'Aggiudicatario dovrà prevedere la fatturazione totale al collaudo della singola componente di CA effettivamente installata. Il pagamento avverrà in rate mensili posticipate dal mese successivo al collaudo fino alla scadenza del Contratto (pertanto varieranno a seconda della data effettiva di collaudo della componente di CA).

Con cadenza mensile verranno redatti come specificato al Capitolo "6.9 - Monitoraggio della Qualità del servizio" del presente Capitolato i verbali di andamento attività e di regolare esecuzione riepilogativi di:

- Elenco dei sistemi che il concorrente è riuscito a prendere in carico/mettere in produzione (i canoni mensili per ognuna delle componenti hardware o software di Controllo Accessi verranno riconosciuti nel mese successivo a quello di ingresso in esercizio del sistema, ossia la prima mensilità di canoni decorrerà dal mese successivo, in caso di attivazioni di componenti nella prima metà del mese in corso verranno riconosciuti per tale mese la metà dei canoni previsti nell'offerta economica);
- Elenco degli interventi svolti;
- Le rendicontazioni di eventuali attività extra di cui al Capitolo Capitolo "6.9 - Monitoraggio della Qualità del servizio" del presente Capitolato
- Le rendicontazioni di eventuali parti di ricambio di cui al Capitolo "6.9 - Monitoraggio della Qualità del servizio" del presente Capitolato

Tale documento sarà propedeutico alla fatturazione mensile dei canoni mensili (pertanto varieranno a seconda della data effettiva dell'entrata in esercizio o presa in carico delle componenti il Sistema di Ca), ed eventuali rendiconti extra.

I pagamenti saranno effettuati nei termini di legge, previa verifica di regolarità contributiva e su ogni fattura sarà operata la ritenuta dello 0,50%, così come previsto dall'art. 4, comma 3, del D.P.R. 207/2010; le ritenute saranno svincolate solo in sede di liquidazione finale (alla scadenza contrattuale). Tale ritenuta dovrà comparire in forma esplicita nel dettaglio della fattura, gli importi dovrà essere emessi al netto di tale ritenuta che verrà recuperata in un'unica soluzione con l'ultima fattura utile.

Si precisa che la fatturazione è soggetta agli obblighi di cui all'art. 17 ter del DPR 633/72 e pertanto alla scissione dei pagamenti (cd Split — Payment).

Da ogni pagamento verranno inoltre trattenute le somme eventualmente dovute dall'Appaltatrice ad AdP S.p.A. per penalità (come di seguito specificato), per le quali l'Aggiudicatario rilascerà relativa nota di accredito che verrà compensata al primo pagamento utile.

Ogni fattura dovrà riportare il n. di CIG riferito alla procedura di gara.

Ai sensi dell'articolo 3, comma 8, della legge n. 136/2010 e s.m.i., con la stipula del Contratto, le Parti assumeranno irrevocabilmente tutti gli obblighi di tracciabilità dei flussi finanziari di cui alla legge n. 136/2010 e s.m.i.. In ottemperanza a tali obblighi, la Ditta è tenuta a comunicare, in conformità al disposto di cui all'art. 3, comma 7 della L. 136/2010, e s.m.i., gli estremi identificativi del conto corrente dedicato e le generalità ed il codice fiscale delle persone delegate ad operare su tale conto.

8.3 PENALITÀ

Relativamente alle attività progettuali, AdP e l'Aggiudicatario, concorderanno un piano di attività per la realizzazione degli interventi durante il periodo contrattuale. Concordato il Piano, l'Aggiudicatario si impegnerà a rispettarlo, salvo esigenze di modifiche su richiesta della Stazione Appaltante; pertanto in caso di ritardi nella realizzazione degli interventi previsti e concordati per cause imputabili all'Aggiudicatario, lo stesso sarà sottoposto ad una penale per mancato rispetto dei termini di fornitura/realizzazione degli Interventi nella misura di:

- Euro 500 (cinquecento) per ogni giorno di ritardo rispetto a quello programmato nel piano di attività di progetto condiviso.

La stessa penale di cui sopra si applicherà per eventuali interventi di adeguamento/modifica richiesti durante il corso del contratto la cui tempistica di realizzazione sarà stata comunque concordata preventivamente con AdP.

Relativamente ai servizi effettivamente contrattualizzati, l'Aggiudicatario sarà soggetto alle seguenti penalità qualora gli SLA contrattualizzati per il Sistema di Controllo Accessi, non dovessero essere rispettati:

- Euro 100 (cento) per ogni ora, o frazione di ora, di ritardo tra la ricezione della chiamata ed il tempo di intervento previsto per la componente Hardware di Controllo Accessi;
- Euro 100 (cento) per ogni ora, o frazione di ora, di ritardo tra l'inizio dell'intervento e il tempo di ripristino per la componente Software di Controllo Accessi;

Tali scostamenti di SLA verranno costantemente monitorati durante l'esecuzione del contratto; verrà calcolata un KPI per il monitoraggio sia dei tempi di intervento, che dei tempi di ripristino. Il KPI misurerà in termini percentuali il numero di interventi fuori SLA, rispetto a quelli totali del mese in corso.

Relativamente alle figure in presidio on-site nelle giornate indicate ed in considerazione di eventuali giornate di assistenza concordate e non rispettate, l'Aggiudicatario sarà soggetto alle seguenti penalità:

- Euro 500 (cinquecento) per assenza giornaliera della figura di presidio;

Le Penalità verranno formalizzate da AdP all'Aggiudicatario e trattenute alla prima fatturazione utile.

È fatta salva in ogni caso l'azione per il risarcimento del maggior danno ed ogni altra azione che AdP S.p.A. ritenesse opportuno intraprendere a tutela dei propri diritti. AdP potrà in ogni caso ricorrere a terzi per l'effettuazione del ripristino, addebitando alla Società i relativi costi.

8.4 CODICE ETICO – ANTICORRUZIONE

L'Aggiudicatario dichiara di essere edotto degli obblighi derivanti dal Codice di Comportamento adottato dalla stazione appaltante e pubblicato sul sito internet della stessa alla pagina "Società Trasparente" e si impegna, in caso di aggiudicazione, ad osservare e a far osservare ai propri dipendenti e collaboratori il suddetto codice, pena la risoluzione del contratto.

8.5 CAUZIONE DEFINITIVA - POLIZZA ASSICURATIVA

Ai fini della stipulazione del contratto l'Aggiudicatario dovrà presentare una cauzione definitiva esclusivamente bancaria o polizza assicurativa fideiussoria rilasciata da Compagnia assicurativa di comprovata stabilità finanziaria, riconosciuta dalla Stazione Appaltante, pari al 10 per cento dell'importo contrattuale. In caso di aggiudicazione con ribassi superiori al dieci per cento, la garanzia da costituire è aumentata di tanti punti percentuali quanti sono quelli eccedenti il 10 per cento. Ove il ribasso sia superiore al venti per cento, l'aumento è di due punti percentuali per ogni punto di ribasso superiore al venti per cento. La cauzione è prestata a garanzia dell'adempimento di tutte le obbligazioni del contratto e del risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, nonché a garanzia del rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'Appaltatore. La Stazione appaltante potrà richiedere al soggetto aggiudicatario la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte; in caso di inottemperanza, la reintegrazione si effettuerà a valere sui ratei di prezzo da corrispondere all'esecutore. Alla garanzia di cui al presente punto si applicheranno le riduzioni previste dall'articolo 93, comma 7 del Codice per la garanzia provvisoria.

L'affidataria dovrà essere munita, a far data dalla stipula del contratto di idonea polizza assicurativa di Responsabilità Professionale che abbia tra le specifiche la garanzia per Servizi e Prodotti Tecnologici non conformi a quanto previsto contrattualmente e/o malfunzionanti (cd. PI Tech) con un massimale di € 5mln.

Copia della suddetta polizza dovrà essere sottoposta ad AdP S.p.A., che potrà richiedere le modifiche necessarie a renderla, ove difforme, conforme alle specifiche richieste e dovrà intendersi operante oltre che per i casi di errori, negligenze, omissioni e imperizie, anche per i danni subiti in conseguenza di interruzione di esercizio, perdita di documenti e dati digitali, e violazioni della riservatezza ai sensi del GDPR del 25/05/2018.

Il Responsabile del Procedimento

Valerio GADALETA