

**Accordo Quadro**

**Capitolato Tecnico**

## Sommario

Art. 1 – Oggetto dell'appalto .....	3
Art. 2 – Obblighi della Ditta aggiudicataria .....	3
Art. 3 – Norme di Sicurezza .....	4
Art. 4 – Condizioni particolari per l'esecuzione del servizio .....	5
Art. 4.1 – Attuale consistenza dell'archivio .....	5
Art. 4.2 - Attività di sopralluogo e analisi.....	5
4.2.1 - Redazione di un piano di lavoro .....	5
4.2.2 - Ricognizione del patrimonio documentario .....	5
Art. 4.3 - Attività di presa in carico .....	6
Art. 4.4 – Riordino e catalogazione.....	7
Art. 4.5 - Attività di custodia e gestione .....	7
Art. 4.6 – Attività di digitalizzazione .....	8
Art. 4.6.1 - Indicizzazione dei documenti.....	10
Art. 4.7 - Attività di scarto.....	10
Art. 5 – Software a supporto della realizzazione del servizio .....	11
Art. 6 –Data Center .....	18
Art. 7 – Sito di lavorazione e conservazione archivi cartacei.....	19
Art.8 -Riconsegna della documentazione al termine del contratto.....	20
8.3 Livelli di qualità dei servizi .....	21

## **1 Premessa**

### **Art. 1 – Oggetto dell'appalto**

Il presente appalto ha per oggetto la stipula di un Accordo Quadro per la fornitura di servizi archivistici e di digitalizzazione documentale

L'affidamento avverrà con procedura aperta in modalità telematica secondo il criterio dell'offerta più vantaggiosa, ai sensi dell'art. 60 del D.Lgs 50/2016 e s.m.i..

I servizi, ricompresi nell'Accordo Quadro, sono i seguenti:

1. Attività di sopralluogo e analisi di archivi cartacei
2. Attività di presa in carico e trasferimento di documenti
3. Attività di riordino e classificazione
4. Attività di custodia e gestione
5. Attività di digitalizzazione
6. Attività di scarto

Inoltre, AID (AGENZIA INDUSTRIE DIFESA) si riserva la facoltà di affidare, dietro esplicita richiesta scritta, i seguenti servizi opzionali:

1. inventariazione della documentazione storica;
2. catalogazione del materiale librario.

Nel corso della esecuzione del contratto la stazione appaltante comunicherà le diverse sedi interessate ai servizi oggetto dell'appalto.

Nei paragrafi successivi verrà fornita una descrizione dettagliata delle modalità di esecuzione dei servizi sopra elencati.

### **Art. 2 – Obblighi della Ditta aggiudicataria**

La Ditta aggiudicataria è tenuta a svolgere il servizio nel rispetto del presente Capitolato.

La Ditta aggiudicataria è tenuta ad eseguire tutte le prestazioni oggetto dell'appalto con la debita cura e diligenza.

La Ditta aggiudicataria deve attenersi agli ordini di servizio del Direttore dell'esecuzione del contratto ed è tenuta a rispettare ed applicare tutte le leggi ed i regolamenti vigenti e ad assicurarne il rispetto anche da parte del proprio personale.

La Ditta aggiudicataria deve altresì garantire l'Amministrazione appaltante contro ricorsi ed azioni per danni a terzi risultanti da eventuali violazioni di leggi e/o regolamenti da parte sua o dei suoi dipendenti e riconosce essere di sua esclusiva competenza e spettanza l'iniziativa dell'adozione di tutti i mezzi opportuni per evitare qualsiasi danno che possa colpire cose o persone.

La Ditta aggiudicataria, pertanto, esonera l'Amministrazione appaltante da ogni responsabilità, facendosi carico anche verso terzi, per infortuni e/o danni che possano verificarsi in dipendenza diretta o indiretta dell'appalto. In specie la Ditta aggiudicataria è considerata terzo responsabile per l'attività appaltatagli.

Qualora la Ditta aggiudicataria sia un'associazione temporanea d'impresa o un consorzio, tutti i soggetti sono tenuti ad adempiere le specifiche obbligazioni del contratto d'appalto conformemente alla legislazione in vigore nello Stato italiano; l'impresa capogruppo funge comunque da responsabile con potere di vincolare l'associazione temporanea o il consorzio. La composizione dell'associazione temporanea o del consorzio non può essere modificata in corso di contratto.

In caso di fallimento del mandatario ovvero, qualora si tratti di imprenditore individuale, in caso di morte, interdizione, inabilitazione o fallimento del medesimo, l'Amministrazione appaltante può proseguire il rapporto di appalto con altro operatore economico che sia costituito mandatario nei modi previsti dal codice dei contratti pubblici purché abbia i requisiti di qualificazione adeguati ai servizi ancora da eseguire; non sussistendo tali condizioni la stazione appaltante può recedere dal contratto.

I danni eventualmente provocati ai beni dell'Ente dalla Ditta aggiudicataria nel corso delle operazioni restano a carico della Ditta aggiudicataria stessa.

La Ditta aggiudicataria dovrà impiegare un numero di addetti adeguato alle prestazioni di cui al presente Capitolato, così da garantire l'espletamento del servizio a regola d'arte.

Dovrà essere impiegato esclusivamente personale di sicura moralità e in possesso dei requisiti di idoneità sanitaria.

L'impresa aggiudicataria deve altresì provvedere alla formazione professionale del proprio personale e al suo costante aggiornamento.

### **Art. 3 – Norme di Sicurezza**

Le attività oggetto del presente appalto sono disciplinate dalla normativa, sia statale che regionale, vigente in materia che deve intendersi integralmente richiamata ai fini del presente capitolato.

Inoltre le attività oggetto del presente appalto sono disciplinate dalle norme regolamentari di emanazione locale inerenti alle attività medesime, che si intendono anch'esse integralmente richiamate al fine del presente capitolato.

In particolare, l'Appaltatore dovrà eseguire le attività oggetto del presente appalto nella piena osservanza di leggi e regolamenti anche locali vigenti in materia di:

- gestione dei servizi affidati;
- smaltimento dei rifiuti;
- prevenzione incendi;
- sicurezza e salute dei lavoratori sui luoghi di lavoro;
- costi della sicurezza di cui al DLgs. 81/08
- assunzioni obbligatorie e patti sindacali,
- prevenzione della criminalità mafiosa.

L'Ente promuove la cooperazione ed il coordinamento per la gestione della sicurezza durante le attività oggetto del l'affidamento e in tale contesto rende disponibile, richiedendola al Responsabile del Procedimento, copia del Documento Unico di Valutazione dei Rischi Interferenziali (di seguito DUVRI) per le attività oggetto del presente capitolato.

Tutte le attività descritte nei documenti di gara verranno svolte dalla Ditta Aggiudicataria nel pieno rispetto delle vigenti norme di sicurezza e igiene del lavoro ed osservando quanto specificato nei predetti documenti di valutazione dei rischi interferenziali che verranno redatti ed allegati al contratto.

Per le attività cui fa riferimento il DUVRI, i relativi oneri per la sicurezza sono stati stimati ed indicati dall'Ente e non possono essere soggetti al ribasso.

## **Art. 4 – Condizioni particolari per l'esecuzione del servizio**

### **Art. 4.1 – Attuale consistenza dell'archivio**

Il servizio richiesto ha per oggetto la documentazione che l'Ente dovrà gestire per le attività archivistiche e di digitalizzazione. Le attività verranno attivate a seguito di emissione di specifico ordine, indicante le attività da eseguire e la quantità di documentazione oggetto del servizio

### **Art. 4.2 - Attività di sopralluogo e analisi**

#### **4.2.1 - Redazione di un piano di lavoro**

Per la redazione del Piano di lavoro, che dovrà contenere anche un cronoprogramma finalizzato all'illustrazione della sequenza temporale e della durata delle attività da svolgere nel servizio, la Ditta aggiudicataria dovrà effettuare un sopralluogo presso la sede di custodia della documentazione.

Il Piano di lavoro dovrà contenere almeno i seguenti elementi:

- a) descrizione delle modalità di erogazione del servizio e delle attività relative al trasferimento del patrimonio documentario nel locale di conservazione della Ditta aggiudicataria (tenuto conto dell'eventuale necessaria sanificazione) e delle attività per il macero;
- b) cronoprogramma relativo alle attività del servizio (inclusa l'organizzazione del trasferimento e la consulenza per la redazione dei relativi elenchi);
- c) prodotti (deliverable) di ciascuna attività;
- d) termini di consegna dei deliverable;
- e) periodicità degli stati di avanzamento lavori (SAL) per le attività del servizio.

Il Piano sarà concordato con il Responsabile dell'Ente e, una volta formalmente approvato, costituirà il documento di riferimento per lo svolgimento del servizio

Il Piano potrà subire varianti nel corso dell'esecuzione del contratto, su richiesta del Responsabile della gestione del servizio dell'Ente o su richiesta della Ditta aggiudicataria che dovrà, comunque, essere soggetta ad approvazione da parte dell'Ente.

#### **4.2.2 - Ricognizione del patrimonio documentario**

Definito il Piano di lavoro, la Ditta aggiudicataria dovrà effettuare una puntuale ricognizione dell'archivio oggetto di intervento, al fine di:

- effettuare un'analisi della documentazione presente, inclusa l'eventuale apertura delle scatole, per:
- quantificare la documentazione e individuarne la collocazione fisica;
- verificare lo stato dell'archivio valutandone lo stato di ordinamento e di conservazione;
- rilevare la frequenza di consultazione della documentazione (con il supporto del personale dell'Ente);
- verificare la presenza di materiale di pregio e/o fuori formato;
- inscatolare ed effettuare gli interventi di trasferimento
- stilare gli elenchi di consistenza

Gli Elenchi potranno essere prodotti a livello di serie archivistica o di singola unità archivistica; per la loro redazione, saranno individuati e accolti tutti, o in parte, i seguenti dati:

- sede di provenienza della documentazione;
- collocazione topografica;

- denominazione del fondo;
- denominazione della serie archivistica in base ai soggetti produttori/UOR;
- descrizione della serie archivistica;
- stato di ordinamento della serie archivistica;
- numero di unità archivistiche di cui si compone la serie archivistica (in alcuni casi, questo dato potrà essere fornito a livello indicativo ed in ogni caso dovrà essere fornito il corrispondente volume in metri lineari);
- estremi cronologici (solo se di immediata rilevazione);
- macero - Sì/No - (su indicazione e approvazione dell'Ente);
- tipologia di archivio (corrente, di deposito e storico)

Tali Elenchi saranno approvati dal Responsabile della gestione del servizio dell'Ente congiuntamente al Responsabile unico di contratto per la Ditta aggiudicataria.

#### **Art. 4.3 - Attività di presa in carico**

La Ditta aggiudicataria dovrà garantire, con mezzi adeguati alle quantità documentali e con proprio personale:

- La presa in carico, con modalità controllate grazie al supporto di tecnologie digitali, del patrimonio documentario esistente presso le strutture indicate dall'Ente;
- Il trasferimento del patrimonio documentario nei nuovi impianti di lavorazione;
- Sanificazione del materiale depositato, finalizzata all'eliminazione di polvere, umidità ed altri agenti patogeni, ivi inclusa, se del caso, la sostituzione dei supporti deteriorati;
- Riordino della documentazione in fondi o serie archivistiche e classificazione della stessa;
- Inventariazione informatica del materiale, tramite apposito software con descrizione delle singole unità archivistiche, attraverso la rilevazione degli elementi identificativi e delle caratteristiche prevalenti delle tipologie documentarie individuate;
- Collocazione fisica della documentazione.

La ditta aggiudicataria ha la totale responsabilità della presa in carico, custodia, gestione e conservazione degli archivi suddetti. La responsabilità dell'impresa decorre dall'inizio di ciascun ritiro.

All'atto della presa in carico, l'impresa aggiudicataria dovrà redigere un verbale nel quale sia specificato un elenco di consistenza delle unità documentali movimentate con apposita dichiarazione di presa in carico. Tale elenco sarà debitamente compilato e sottoscritto congiuntamente dai referenti dell'Ente e della Ditta aggiudicataria.

Nella fase di "presa in carico" dovrà essere garantita la sistematica rintracciabilità delle unità di archiviazione.

La Ditta dovrà descrivere nel progetto tecnico come intende assicurare la tracciabilità e la rintracciabilità dei documenti.

L'Appaltatore dovrà utilizzare mezzi idonei a garantire la corretta conservazione e protezione da agenti esterni durante le fasi di trasporto fino al luogo di deposito usando contenitori adeguati.

La Ditta concorrente dovrà descrivere nel progetto, le modalità tecniche e organizzative con cui intende effettuare questa importante e delicata operazione con l'indicazione del livello di analiticità della presa in carico.

#### **Art. 4.4 – Riordino e catalogazione**

Una volta ritirata, la documentazione dovrà essere classificata e conservata secondo la normativa vigente. In altre parole, la classificazione consente di costituire, mantenere nel tempo o ricostruire i legami logici e funzionali tra documenti formati, pervenuti e gestiti su supporti diversi, che attengano allo svolgimento di una medesima attività amministrativa.

Laddove presente, potrà essere conservata la catalogazione utilizzata dall'Amministrazione.

Ove non fossero presenti criteri di catalogazione, la ditta applicherà il criterio di classificazione definito in sede di sopralluogo e concordato con l'Ente.

La catalogazione dovrà essere effettuata da personale competente e dovrà prevedere le seguenti fasi:

- Riordino e bonifica dei documenti secondo il progetto proposto, di concerto con il personale all'uopo incaricato dall'Ente e secondo quanto rilevato in sede di ricognizione del patrimonio documentario;
- Codifica e catalogazione con idonei campi descrittivi: ciascun campo dovrà poter costituire un indice di ricerca (da solo o in associazione con altri indici);

#### **Art. 4.5 - Attività di custodia e gestione**

È prevista la possibilità di fornire un servizio di conservazione fisica e di gestione di materiale cartaceo costituente il patrimonio documentale dell'Ente

Durante lo svolgimento del servizio, deve essere prevista la custodia sia di quello preso in carico che di quello che nel tempo verrà fornito, nel rispetto delle serie archivistiche, secondo criteri che ne garantiscano l'integrità logica e fisica e nel rispetto dei criteri di sicurezza fisica, logica e di protezione della riservatezza.

La documentazione dovrà essere custodita in contenitori idonei alla conservazione illimitata, identificabili per mezzo dell'etichettatura con codici in chiaro e/o barre; i contenitori utilizzati dovranno essere tali da assicurare la movimentabilità e portabilità in termini di dimensioni e peso ai sensi della normativa vigente.

Le scatole contenenti la documentazione dovranno essere allocate in idonee scaffalature.

La ditta dovrà garantire la corretta conservazione della documentazione, provvedendo periodicamente alla spolveratura o disinfestazione della stessa.

Dovrà essere erogato, con cadenza periodica, un servizio di spolveratura dei documenti e verifica dell'assenza di agenti patogeni ed eventuale intervento risanante.

In caso di richiesta di consultazione, la ditta affidataria dovrà attivare tutte le procedure necessarie per la ricerca, la consegna del materiale richiesto in consultazione e la sua riarchiviazione. Restano a carico della ditta tutte le attività necessarie alla corretta conservazione.

Il progetto dovrà descrivere tutto il processo di archiviazione, conservazione e consultazione ponendo l'accento sull'interoperabilità e sulla tracciabilità delle movimentazioni e degli accessi e, come generalmente richiesto, sulla rispondenza alle linee guida e norme tecniche.

## **Art. 4.6 – Attività di digitalizzazione**

### **Servizio di digitalizzazione**

Nel corso del contratto, AID (AGENZIA INDUSTRIE DIFESA) richiederà alla Ditta aggiudicataria di sviluppare il servizio di digitalizzazione dei documenti analogici anche sulla base della normativa vigente, D. Lgs. 82/2005, Codice dell'amministrazione digitale, aggiornato con D. Lgs. 217/2017 e relative Regole tecniche, per la parte ancora in vigore, per garantire la leggibilità del contenuto dei documenti nel lungo periodo e la conformità degli stessi agli originali analogici. Ai fini della conservazione a norma la Ditta dovrà fornire i metadati e i documenti secondo il tracciato concordato con AID (AGENZIA INDUSTRIE DIFESA) per il caricamento nel sistema di gestione documentale. Il trasferimento delle immagini acquisite verso il sistema di gestione documentale, quindi verso il sistema di conservazione a norma, avverrà tramite sftp o tramite servizi web.

Sarà cura di AID (AGENZIA INDUSTRIE DIFESA) fornire alla Ditta aggiudicataria tutte le informazioni necessarie all'attivazione del servizio (tipologie documentarie, formati, tipologie di supporti cartacei, numero di unità da digitalizzare, modalità di trattamento). Se ritenuto opportuno AID (AGENZIA INDUSTRIE DIFESA) potrà fornire alla Ditta aggiudicataria un campione della documentazione da digitalizzare, che costituirà il campione tecnico da sottoporre a validazione di AID (AGENZIA INDUSTRIE DIFESA) preliminarmente all'attivazione del servizio.

Sarà cura della Ditta aggiudicataria strutturare un Piano di lavoro completo di cronoprogramma delle attività da svolgere, nei casi in cui sia richiesta da AID (AGENZIA INDUSTRIE DIFESA) la digitalizzazione di diverse unità archivistiche. Il Piano di lavoro dovrà essere approvato da AID (AGENZIA INDUSTRIE DIFESA). Attraverso l'interfaccia *web* del sistema informatico utilizzato dalla Ditta aggiudicataria, AID (AGENZIA INDUSTRIE DIFESA) potrà inoltrare la richiesta di digitalizzazione e il relativo elenco dei documenti e potrà inoltre richiedere la digitalizzazione di una o più unità archivistiche durante la consultazione delle stesse in loco, ossia durante la consultazione presso il locale di conservazione.

La digitalizzazione dovrà essere eseguita con strumenti e personale forniti dalla Ditta aggiudicataria e sarà svolta presso la Ditta medesima.

Si precisa che per la lavorazione della documentazione e dei fascicoli sono previste tre tipologie di lavorazione:

- una lavorazione che non comporta un'attività di analisi;
- una lavorazione che prevede l'analisi semplice;
- una lavorazione che prevede l'analisi complessa;

ciò in quanto:

- i fascicoli oggetto di lavorazione potrebbero non essere interamente da digitalizzare e pertanto risulta necessaria un'attività preventiva di selezione dei documenti che devono essere poi sottoposti al processo di scansione;
- l'attività di selezione non sempre comporta l'analisi complessa dei caratteri intrinseci dei documenti e pertanto risulta necessario prevedere anche l'analisi semplice dei caratteri estrinseci dei documenti volta al riconoscimento di specifiche tipologie documentali;
- l'attività di selezione potrebbe portare come risultato alla non digitalizzazione di nessun documento del fascicolo e pertanto risulta necessario distinguere l'attività di scansione da quella di analisi dei documenti.

Anche per quanto riguarda la scansione si potranno avere 3 diverse tipologie:

- scansione semplice: documentazione sciolta o separabile; formati da A4 ad A1; risoluzione minima 300 dpi;
- scansione complessa: documentazione rilegata, non divisibile (es. libri, riviste, registri di grandi dimensioni); formati da A4 ad A1; risoluzione da 300 a 400 dpi o superiore;
- scansione documenti fotografici a colori: risoluzione da 600 a 3200 dpi o superiore.

Di seguito si elenca la sequenza delle attività che generalmente verranno eseguite nell'ambito del servizio di digitalizzazione:

- **selezione** della documentazione cartacea da digitalizzare. Sulla base dell'elenco fornito da AID (AGENZIA INDUSTRIE DIFESA), formulato in modo tale da consentire l'identificazione univoca delle unità archivistiche, il personale della Ditta aggiudicataria individuerà e preleverà le unità da digitalizzare. Il prelievo potrà essere organizzato per lotti (ove richiesta una digitalizzazione massiva), la cui successione sarà stabilita nel Piano di lavoro suddetto;
- **registrazione** delle unità prelevate per la digitalizzazione nel sistema informatico utilizzato dalla Ditta aggiudicataria per la gestione degli archivi. Sullo stesso sistema sarà registrata la ricollocazione delle unità negli impianti di archiviazione successivamente all'avvenuta digitalizzazione;
- **ordinamento** della documentazione all'interno delle singole unità archivistiche secondo modalità concordate preventivamente con AID (AGENZIA INDUSTRIE DIFESA) al fine di renderla più adatta a una gestione di tipo elettronico (es. suddivisione di fascicoli in sotto fascicoli);
- **preparazione fisica dei documenti**: eliminazione di punti metallici e fermagli, rimozione di piegature, ricomposizione di strappi, rimozione *post-it*, ecc.;
- **digitalizzazione dei documenti**: gli scanner utilizzati dovranno essere in grado di generare *file* in formato PDF/A multi pagina, contenenti la riproduzione in digitale del documento nello stesso ordine sequenziale in cui è disposto nella versione cartacea. AID (AGENZIA INDUSTRIE DIFESA) può richiedere la conversione in OCR; in ogni caso i *file* prodotti dovranno avere una qualità adeguata tale da consentire anche l'eventuale conversione in OCR in una fase successiva. I *file* prodotti dalla digitalizzazione dovranno avere un'estensione PDF. In fase di digitalizzazione dovranno inoltre essere rispettati i seguenti elementi:
  - **inquadratura e rifilatura**: i *file* immagine dovranno essere privi delle zone estese al di fuori della pagina (zone prive di parti scritte) e dovranno essere eliminate eventuali pagine bianche;
  - **valore di profondità immagine richiesto**: non meno di 1bit/pixel. Consentita la scala di grigi per garantire la corretta leggibilità dell'immagine (invece della scala colore);
  - **risoluzione**: a seconda della tipologia di scansione;
  - **raddrizzamento e rotazione automatica delle immagini**: le immagini dovranno essere allineate e orientate secondo il senso di lettura del documento;
- **indicizzazione dei documenti**: ad ogni *file* immagine dovrà essere associato un set di metadati tale da consentire, in un momento successivo, l'associazione tra l'immagine e i relativi dati descrittivi, al fine della memorizzazione nel sistema informatico di gestione documentale in uso presso AID (AGENZIA INDUSTRIE DIFESA); i suddetti metadati<sup>4</sup> da memorizzare saranno reperibili direttamente dalla documentazione da digitalizzare o saranno forniti da AID (AGENZIA INDUSTRIE DIFESA) stessa;
- **trasferimento dei documenti**: la fornitura prevede che i file immagine con i relativi metadati siano consegnati a AID (AGENZIA INDUSTRIE DIFESA) per ciascun lotto di lavorazione; lo scambio potrà avvenire via sftp o tramite servizi web.
- **riposizionamento in archivio**: completate le attività di digitalizzazione, l'unità archivistica dovrà essere ricostituita e ricollocata nella corretta sede di conservazione della Ditta aggiudicataria.

Le attività andranno eseguite presso la sede messa a disposizione della ditta o, qualora espressamente indicato, presso la sede indicata dalla committente, con attrezzatura adeguata sia in termini quantitativi che qualitativi

Al fine di supportare le attività di digitalizzazione, si valuta la presenza di sw di intelligenza artificiale per:

1. Il rilevamento in tempo reale degli errori e delle inaccurately che potrebbero incorrere durante il processo di scansione,
2. la post correzione automatica degli errori non rilevati o ignorati durante il processo di scansione
3. il post-processamento della documentazione in maniera flessibile e accurata modellata intorno alle specifiche richieste dalle singole classi documentali.

#### **Art. 4.6.1 - Indicizzazione dei documenti**

Ad ogni file immagine dovrà essere associato un set di metadati tale da consentire, in un momento successivo, l'associazione tra l'immagine e i relativi dati descrittivi, al fine della memorizzazione nel sistema informatico di gestione documentale; i suddetti metadati da memorizzare saranno reperibili direttamente dalla documentazione da digitalizzare o saranno forniti dall'Ente.

Le immagini prodotte dal processo di digitalizzazione dovranno essere sottoposte ad un processo di verifica: le immagini che non rispetteranno i requisiti qualitativi richiesti andranno scartate e gli originali cartacei andranno sottoposti ad un nuovo processo di digitalizzazione.

La ditta offerente dovrà descrivere nella propria offerta tecnica come intende erogare il servizio di digitalizzazione: andranno descritte tutte le fasi del processo di acquisizione ottica, tutta la attrezzatura hardware messa a disposizione per lo svolgimento del servizio e le metodologie utilizzate per la verifica qualitativa dei file immagine prodotti.

#### **Art. 4.7 - Attività di scarto**

La selezione della documentazione archivistica che si propone per lo scarto, è un intervento che presuppone una decisione consapevole e non arbitraria regolata da specifica procedura. Sia i criteri che la modulistica relativa alla proposta di scarto dovranno essere concordati con l'Ente. La Ditta aggiudicataria, acquisite le disposizioni in merito, dovrà provvedere alle seguenti attività:

- a) selezione puntuale della documentazione proposta per lo scarto per la quale sono decorsi i termini di conservazione obbligatoria;
- b) consegna di una proposta di scarto con allegata la lista specifica dei documenti;
- c) estrazione dall'archivio della documentazione per la quale la Soprintendenza Archivistica competente ha autorizzato lo smaltimento;
- d) compilazione della documentazione di supporto necessaria al corretto svolgimento delle operazioni di smaltimento, secondo quanto prescritto dalla normativa in vigore;
- e) consegna del materiale cartaceo destinato allo smaltimento a ditta specializzata, secondo quanto prescritto dalla normativa in vigore;
- f) comunicazione all'Ente dell'avvenuta conclusione dell'attività di sfoltimento e rilascio della documentazione attestante l'avvenuto macero;
- g) attività di macero della documentazione secondo la normativa vigente, nelle modalità idonee seconda la tipologia di documento trattato.

La ditta aggiudicataria dovrà provvedere all'aggiornamento del massimario di scarto secondo la normativa vigente, alle indicazioni della Soprintendenza Archivistica e dell'Ente. Tutte le modifiche introdotte al massimario di scarto e al piano di conservazione dovranno essere concordate con l'Ente.

## **Art. 5 – Software a supporto della realizzazione del servizio**

Le fasi necessarie alla realizzazione dei servizi relativi alla lavorazione della documentazione dovranno essere svolte con l'ausilio di un sistema software web based, ospitato presso l'infrastruttura tecnologica dell'Azienda aggiudicataria, ovvero presso l'infrastruttura di AID, accessibile attraverso connessione sicura (protocollo HTTPS) e attraverso l'unica modalità di accesso Single Sign On. Dovrà quindi essere utilizzabile senza la necessità di installare componenti dello stesso presso le postazioni degli utilizzatori, ovvero accessibile da remoto. La fruibilità del sistema dovrà dunque avvenire utilizzando gli Internet Browser più diffusi (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, etc), Il sistema deve, inoltre, basarsi esclusivamente su tecnologie Open Source (DBMS, Server Applicativi, etc) ed avere caratteristiche di portabilità, ovvero tutta la componente server deve poter essere installata sui sistemi operativi più diffusi (Microsoft, Linux, Unix, etc.).

La Ditta Appaltatrice deve avere piena disponibilità dei codici sorgenti della soluzione proposta.

Il sistema informatizzato web based dovrà presentare le seguenti funzioni di base:

- Gestione di Profili di utenza differenziati: il Sistema deve caratterizzare gli utenti con specifici permessi di accesso ai documenti (consultazione, stampa, richieste di movimentazione, etc,) e prevedere, inoltre, meccanismi per la gestione degli account a norma Privacy e Sicurezza;
- Il sistema dovrà prevedere delle funzionalità specifiche in merito al controllo della lunghezza delle password, cambio della password al primo accesso, scadenza password e meccanismi proattivi inerenti il controllo delle utenze inattive. L'amministrazione degli utenti, ruoli e profili deve avvenire mediante un'interfaccia web;
- Il sistema dovrà fornire una soluzione che consenta di limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e quindi al modulo di dati) indispensabili;
- Acquisizione dei documenti nel formato elettronico e loro codifica, catalogazione e indicizzazione;
- Acquisizione eventuale dei documenti da altri sistemi informativi, eventuale consolidamento, codifica, catalogazione e indicizzazione;
- Gestione presa in carico della documentazione con meccanismi che consentano la tracciabilità della documentazione a partire dalla fase di prelievo della documentazione c/o gli archivi dell'Ente;
- Gestione della metadattazione: il Sistema deve consentire una definizione flessibile dei metadati associabili ad una unità archivistica;
- Gestione della fascicolazione e sottofascicolazione dei documenti;
- Gestione logistica di deposito: il Sistema deve consentire l'immediata rintracciabilità della documentazione custodita attraverso la memorizzazione e successiva fruizione delle informazioni relative alla collocazione fisica dei documenti, al loro stato di consultazione nonché alle coordinate per una rapida ricerca in archivio;
- Gestione barcode: il sistema deve permettere l'identificazione univoca di ciascuna unità archivistica attraverso l'apposizione di una barcode che contenga informazioni relative al cliente di riferimento ed alla tipologia documentale in questione;
- Elenchi di consistenza d'archivio: Il sistema deve consentire di effettuare richieste di consistenza per organizzazione, domini e serie;
- Ricerca ordinata: Deve essere data la possibilità di poter indicare quale sia il campo di ordinamento secondo cui effettuare la ricerca;
- Esportazione del risultato di ricerca: Deve essere data la possibilità di poter effettuare un'esportazione dell'intero set di risultati con indicazione del formato per l'esportazione;

- Sistema di trasmissione dei dati: il Sistema deve disporre di funzioni atte a trasmettere i documenti ed assicurare il pieno rispetto delle norme e misure di sicurezza e privacy;
- Ricerca e consultazione dei documenti elettronici: il Sistema deve disporre di un'interfaccia web che consenta al personale abilitato la ricerca per categoria, full-text, per parola chiave e criteri booleani dei documenti presenti nel sistema, nonché la successiva consultazione. Le funzioni di consultazione devono essere profilate per consentire l'accesso differenziato alle categorie di utenza (definibili dall'amministratore);
- Gestione archivio: il sistema deve consentire la creazione di archivi attraverso i più noti criteri di classificazione archivistici (gestione serie e gestione titolare) e permetterne inoltre la gestione dello scarto con relativo massimario, proposta di scarto e scarto effettivo;
- Modellazione della struttura organizzativa dell'Ente: il Sistema deve consentire la modellazione della struttura organizzativa dell'Ente in modo da attribuire le categorie di utenza ai domini organizzativi di appartenenza;
- Dashboard da condividere con l'Ente sull'andamento in tempo reale dei livelli di servizio della fornitura, degli indicatori di qualità e dello stato di avanzamento delle attività relative ai diversi servizi;
- Produzione di report sull'andamento della fornitura, sulle richieste di consultazione, sui documenti digitalizzati, sulle movimentazioni, ecc. ecc.
- Gestione delle movimentazioni d'archivio: il software deve gestire le movimentazioni in modo puntuale al fine di garantire la tracciabilità degli spostamenti della documentazione stessa. In particolare, esso deve essere in grado di fornire almeno le seguenti informazioni:
  - stato del documento ("in archivio" o "in consultazione");
  - posizione (coordinate archivistiche o informazioni relative all'ufficio richiedente);
  - data di richiesta del documento;
  - estremi del richiedente;
  - data di consegna del documento;
  - data di rientro previsto;

Inoltre:

- Dovrà essere possibile condurre il "trace" di quanto accade nel sistema e di produrre i necessari "log" di dettaglio muniti di "time stamping";
- Il Sistema di consultazione, oltre alla visualizzazione del documento, dovrà consentire il download dello stesso in un unico file in formato PDF per la stampa;
- Il Sistema dovrà supportare la classificazione e la registrazione della documentazione.
- Il Sistema dovrà prevedere l'attivazione di procedure per il salvataggio e recupero dei dati;
- Il Sistema dovrà prevedere l'integrazione con sistemi di firma digitale remota massiva e marca temporale;
- Il sistema software dovrà essere munito di un sistema di monitoraggio di tutti gli elementi ritenuti critici per la continuità dei servizi da esso erogati. Oltre al monitoraggio, il sistema deve essere in grado di eseguire azioni correttive mirate al ripristino, senza intervento umano, delle condizioni normali di funzionamento degli asset per cui sia stato rilevato uno stato critico. Per stato critico si intende una condizione di funzionamento che porta o potrebbe portare ad una indisponibilità o inefficienza del servizio che quel particolare asset concorre ad erogare.
- Il sistema informatico dovrà essere sviluppato, aggiornato e reso funzionale alle esigenze dell'Ente nonché mantenuto sempre in efficienza ed adeguato alle normative vigenti in materia di privacy e sicurezza e alle regole tecniche in materia.

## **Requisiti di sicurezza del sistema**

In ottemperanza alle disposizioni in materia di sicurezza di cui alla normativa Banca d'Italia vigente, AID (AGENZIA INDUSTRIE DIFESA) è tenuta a identificare e monitorare nel continuo i presidi di sicurezza informatica relativi all'oggetto di fornitura. A tal fine sono di seguito definiti i requisiti di sicurezza minimi ed i requisiti di sicurezza oggetto di valutazione.

### **Requisiti di sicurezza minimi**

La Ditta aggiudicataria, in coerenza con le politiche di sicurezza AID (AGENZIA INDUSTRIE DIFESA), deve fornire una soluzione tecnologica che soddisfi elevati standard di sicurezza. Di seguito sono riportati, suddivisi per macro ambiti, i requisiti che dovranno essere garantiti considerando aspetti tecnici, organizzativi e procedurali.

### **Architettura e soluzioni di sicurezza:**

- Il Fornitore deve garantire l'applicazione del principio di Segregation of Duties per il personale addetto ai servizi da erogare a AID (AGENZIA INDUSTRIE DIFESA);
- Il Fornitore deve garantire che siano installati, in modo tempestivo e al più con cadenza almeno annuale, gli aggiornamenti del sistema operativo, dei software di middleware e applicativo necessari a correggere difetti e prevenire vulnerabilità, in coerenza con gli standard internazionali (e.g. OWASP);
- Il Fornitore deve prevedere la ridondanza dei supporti di memorizzazione al fine di garantire la tolleranza ai guasti;
- Nel caso di attività di sviluppo evolutivo e manutenzione (e.g. testing delle patch) è necessario garantire la separazione, logica o fisica, degli ambienti di sviluppo, test e produzione in modo da ridurre il rischio di accessi o cambiamenti non autorizzati;
- Per gli ambienti diversi da quello di produzione (e.g. di collaudo/diagnostica) non devono essere utilizzati dati reali di esercizio o, ove strettamente necessario, devono essere adottate tecniche di sicurezza per garantirne la riservatezza prima del trasferimento (e.g. mascheramento);
- I manuali operativi e le configurazioni rilevanti per la sicurezza devono essere forniti ed aggiornati ad ogni rilascio;
- Il Fornitore deve garantire che siano adottate adeguate procedure di backup che prevedano il salvataggio delle informazioni/dei dati di AID (AGENZIA INDUSTRIE DIFESA) per il completo ripristino del sistema con cadenza almeno settimanale. Tali procedure dovranno essere documentate e contenenti almeno l'indicazione: della frequenza, delle modalità di esecuzione, dell'archiviazione e della conservazione dei backup;
- Le misure di backup e ripristino devono essere integrate nell'ambito della pianificazione della continuità operativa e testate di conseguenza per verificarne l'efficacia;
- Le informazioni dovranno essere conservate per la sola durata del periodo contrattuale, e non replicate o riutilizzate dal Fornitore; dopodiché andranno eliminate, oppure ove richiesto da AID (AGENZIA INDUSTRIE DIFESA) andranno consegnate in formati compatibili;
- Il Fornitore deve garantire che siano adottate, nel caso di malfunzionamenti o incidenti ai propri sistemi informatici, specifiche procedure operative per l'esecuzione delle attività di ripristino, le quali devono prevedere tempi di attuazione in linea con gli SLA contrattualizzati;
- Il Fornitore deve garantire che qualsiasi componente sviluppata o installata sui sistemi informatici non basi le sue funzionalità su funzioni, API, librerie o codici non sicuri e che sia legalmente licenziata.

### **Controllo degli accessi:**

- L'accesso al sistema dovrà prevedere il superamento della fase di autenticazione. Il meccanismo di autenticazione deve prevedere almeno l'utilizzo di un identificativo (userid) e della parola chiave (password);
- Ove richiesto, il sistema di autenticazione deve integrarsi con le soluzioni adottate in AID (AGENZIA INDUSTRIE DIFESA) (e.g. IAM, AD);
- La pagina di accesso deve garantire la riservatezza delle credenziali digitate con meccanismi di cifratura;
- Se non prevista l'integrazione con il SSO di AID (AGENZIA INDUSTRIE DIFESA), il sistema di autenticazione deve essere costruito in modo da:
  - assegnare credenziali di autenticazione individuali e nominali, che non devono essere riassegnate ad altri utenti neppure in tempi diversi;
  - garantire che la password risponda alle caratteristiche previste dalle vigenti policy aziendali (AID (AGENZIA INDUSTRIE DIFESA)) e best practices di sicurezza, se più rigorose:
    - lunghezza minima configurabile (almeno di 8 caratteri);
    - complessità (presenza di un carattere speciale, numeri, carattere maiuscolo, carattere minuscolo);
    - memorizzazione storico password;
    - obbligo modifica password al primo utilizzo;
    - impossibilità di riutilizzo di una password precedentemente utilizzata;
    - blocco password dopo un numero configurabile di tentativi di accesso non andati a buon fine.

### **Data protection**

- I dati trattati sui sistemi devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- Deve essere prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi;
- In merito alla memorizzazione dei dati di AID (AGENZIA INDUSTRIE DIFESA), il Fornitore deve prevedere l'utilizzo di strumenti per la cifratura dei dati "at rest", che deve essere eseguita mediante l'utilizzo di algoritmi robusti secondo le best practices di sicurezza;
- Per la trasmissione dei dati di AID (AGENZIA INDUSTRIE DIFESA), "dati in transit", sia internamente a AID (AGENZIA INDUSTRIE DIFESA) che verso l'esterno, il Fornitore deve prevedere l'utilizzo di flussi cifrati mediante utilizzo di algoritmi robusti (e.g. AES 256) secondo le best practices di sicurezza, sfruttando protocolli aggiornati alla loro versione più recente (e.g. TLS 1.2 vs TLS 1.0);
- Il Fornitore deve prevedere meccanismi di pseudonimizzazione dei dati personali affinché le informazioni siano conservate in un formato che ne impedisca l'identificazione senza l'utilizzo di informazioni aggiuntive (e.g. mediante mascheramento o utilizzo dei tag);
- Il Fornitore deve prevedere la cifratura dei dati personali o di AID (AGENZIA INDUSTRIE DIFESA) se presenti sui database, memorizzati in cloud o su dispositivi mobili come:
  - Laptop;
  - Smartphone;
  - Device rimovibili (HD esterni, pendrive);
- Devono essere previsti controlli e soluzioni tecnologiche per garantire l'integrità e la completezza del dato, prevenendo errori di elaborazione e corruzione dei dati.

### **Log management e monitoraggio**

- Il Fornitore deve garantire la possibilità di generazione dei log necessari per la valutazione ed il monitoraggio degli eventi di sicurezza (e.g. registrazione degli accessi, operazioni alle configurazioni di sicurezza, utilizzo dei privilegi, movimentazione di utenze di amministrazione, etc.) da identificare in cooperazione con AID (AGENZIA INDUSTRIE DIFESA);
- Il Fornitore deve prevedere una soluzione tecnologica che garantisca la non ripudiabilità dei log dalla loro generazione nonché la loro conservazione per un periodo di tempo concordato con AID (AGENZIA INDUSTRIE DIFESA) e in linea con le direttive delle normative vigenti;
- Il Fornitore deve prevedere la registrazione dei log degli accessi logici e delle operazioni effettuate su tutte le componenti del sistema da parte delle utenze con profili privilegiati (e.g. amministratori di sistema/DB/applicazione) e la loro conservazione per almeno 6 mesi, in ottemperanza al Provv. "Amministratori di sistema" del 27 novembre 2008. Ove richiesto, il Fornitore deve fornire opportuna reportistica in merito.

### **Malware protection**

- Il Fornitore deve predisporre presidi antimalware (e.g. antivirus locali) continuamente aggiornati atti a rilevare la presenza e bloccare l'esecuzione di malware su tutti i dispositivi che possano direttamente o indirettamente impattare gli asset informativi di AID (AGENZIA INDUSTRIE DIFESA), basati su firme e su comportamento anomalo del codice; le firme dovranno essere aggiornate al massimo ogni 12 ore.

### **Network security**

- Il Fornitore deve garantire che tutte le reti utilizzate per la creazione, l'archiviazione o il processamento di dati o deliverable, relativi ai servizi da erogare a AID (AGENZIA INDUSTRIE DIFESA), siano dotate di controlli di sicurezza (e.g. firewall, cifratura, filtri, intrusion detection e prevention e altre capacità simili);
- In caso di risorse esposte su internet (e.g. Web Application), esse devono essere protette da possibili attacchi mediante Web Application Firewall;
- Il Fornitore è tenuto a verificare che i firewall posti a protezione della rete su cui risiede il sistema siano configurati coerentemente con le politiche e le linee guida fornite da AID (AGENZIA INDUSTRIE DIFESA) (e.g. mantenere aperte solo le porte strettamente necessarie, bloccare utilizzo di protocolli vulnerabili);
- I dispositivi di rete utilizzati (e.g. router, server, proxy) devono eseguire firmware/S.O. aggiornati alle ultime versioni disponibili.

### **Security assessment**

- Il Fornitore deve prevedere periodicamente l'esecuzione di Vulnerability Assessment e Penetration Test che siano eseguite senza impatti sulla disponibilità del sistema e sui livelli di servizio, richiedendo sempre l'approvazione preventiva e vincolante di AID (AGENZIA INDUSTRIE DIFESA); i risultati di tali attività vanno sottoposti a AID (AGENZIA INDUSTRIE DIFESA);
- Il Fornitore deve sottoporre ogni rilascio a verifiche di sicurezza; tali verifiche devono in particolare essere condotte prima del passaggio in produzione ed i risultati condivisi con le strutture preposte in AID (AGENZIA INDUSTRIE DIFESA) per la valutazione di conformità;
- Il Fornitore garantisce l'implementazione di tutte le opportune remediation previste a valle delle attività di Assessment, delle quali si impegna a fornire evidenza a AID (AGENZIA INDUSTRIE DIFESA);

- Il Fornitore deve garantire che con cadenza almeno annuale saranno condotte attività di analisi statica e dinamica del codice (i.e. Code Review) e condividere con AID (AGENZIA INDUSTRIE DIFESA) le risultanze ottenute;
- AID (AGENZIA INDUSTRIE DIFESA) si riserva la facoltà di eseguire attività di Assessment autonome (e.g. Penetration test, Vulnerability Assessment, audit di seconda parte), che verranno concordate e pianificate ed alle quali la Ditta aggiudicataria deve fornire adeguato supporto.

### **Trattamento dei dati personali**

- Il Fornitore deve essere nominato da AID (AGENZIA INDUSTRIE DIFESA) come soggetto terzo a cui il Titolare dei dati (AID (AGENZIA INDUSTRIE DIFESA)) ha affidato il trattamento di dati personali; la nomina può anche essere effettuata internamente al contratto o come allegato/addendum al contratto.
- Deve essere prevista da parte del Fornitore la nomina e il censimento di eventuali subfornitori UE e/o extra-UE, con il ribaltamento delle clausole a tutela dei trattamenti e previa autorizzazione AID (AGENZIA INDUSTRIE DIFESA)
- Il Fornitore si impegna a rispettare ed accettare le indicazioni riportate all'interno dello standard di nomina che AID (AGENZIA INDUSTRIE DIFESA) e le Società del Gruppo AID (AGENZIA INDUSTRIE DIFESA) invieranno successivamente all'aggiudicazione del presente affidamento.
- Il Fornitore e i subfornitori saranno inseriti nell'elenco dei Responsabili del trattamento dei dati personali
- Il Fornitore deve nominare individualmente i propri addetti che gestiscono i sistemi e le applicazioni di AID (AGENZIA INDUSTRIE DIFESA) che trattano dati personali al fine di assicurare la conformità dell'operato degli Amministratori di Sistema alle prescrizioni del Provvedimento del Garante della Privacy del 27/11/2008
- L'elenco contenente gli estremi identificativi degli Amministratori di Sistema del Fornitore, deve essere reso disponibile su richiesta, secondo quanto previsto dal provvedimento stesso
- Il Fornitore deve impegnarsi formalmente a notificare a AID (AGENZIA INDUSTRIE DIFESA) entro 24 ore gli eventi che possono caratterizzarsi come violazioni di dati personali, in ottemperanza agli art. 33 e 34 del Regolamento UE 679/2016 (GDPR).
- In ottemperanza dell'articolo 35 del Regolamento UE 679/2016 (GDPR), la valutazione d'impatto sulla protezione dei dati, il Fornitore dovrà fornire assistenza, anche attraverso invio di specifica documentazione a supporto, a AID (AGENZIA INDUSTRIE DIFESA) e alle Società del Gruppo AID (AGENZIA INDUSTRIE DIFESA), ove ricorrano i presupposti per procedere alla valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali
- Il Fornitore si impegna a fornire soluzioni tecnologiche che adottino gli strumenti ed impostazioni a tutela dei dati personali, in ottemperanza all'art. 25 del Regolamento UE 679/2016 (i.e. principi privacy by design e privacy by default)

### **Servizi di manutenzione e supporto**

Sono da intendersi a totale carico della Ditta aggiudicataria tutte le attività di manutenzione ordinaria, preventiva, correttiva ed adattiva della piattaforma fornita.

Il servizio di manutenzione della piattaforma tecnologica dovrà prevedere gli interventi di manutenzione ordinaria, in termini di:

- gestione ordinaria delle risorse HW e SW, necessarie per il corretto funzionamento della soluzione;
- pianificazione, esecuzione e controllo delle operazioni di salvataggio dei dati, riorganizzazione del database e tutte le altre operazioni periodiche richieste dal sistema applicativo;
- salvataggio e custodia dei log/documenti dell'attività del sistema, che potranno essere oggetto di richiesta specifica di AID (AGENZIA INDUSTRIE DIFESA);
- ripristino delle complete funzionalità del sistema, sia in termini di accesso al sistema che in termini di integrità logico-fisica dei dati, assicurando la ricostruzione dei dati fino all'ultima transazione eseguita;
- il funzionamento della piattaforma informatica 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno, salvo i periodi di interruzione del servizio per attività di manutenzione programmata o concordata con AID (AGENZIA INDUSTRIE DIFESA);
- garanzia dell'attivazione di tutte le procedure tecniche e organizzative a supporto del mantenimento dell'integrità del database;
- garanzia dell'attivazione di tutte le procedure tecniche e organizzative necessarie al ripristino dell'operatività a fronte di malfunzionamenti in tempi tali da non influire sull'operatività di AID (AGENZIA INDUSTRIE DIFESA).

La Ditta aggiudicatrice dovrà fornire:

- a titolo gratuito un numero di accessi/utenti adeguato alle esigenze di AID (AGENZIA INDUSTRIE DIFESA) connesse al servizio nel rispetto dei volumi riportati nel par. 5.1.3 *Configurazione del sistema informatico*;
- l'adeguamento del sistema alle specifiche esigenze di AID (AGENZIA INDUSTRIE DIFESA) espresse nel presente paragrafo;
- la correzione di eventuali errori rilevati dal personale di AID (AGENZIA INDUSTRIE DIFESA) nell'utilizzo del sistema;
- un servizio di assistenza, telefonica e tramite e-mail, dedicato agli utenti di AID (AGENZIA INDUSTRIE DIFESA) sull'utilizzo funzionale del sistema, supportato da opportuni strumenti di tracciamento delle chiamate pervenute;
- in caso di cessazione del servizio per qualunque causa, le banche dati realizzate e aggiornate durante il periodo di erogazione dei servizi devono essere consegnate e documentate a AID (AGENZIA INDUSTRIE DIFESA) per il loro riutilizzo con altri sistemi o servizi.
- Il sistema suddetto sarà sottoposto a collaudo da parte del personale di AID (AGENZIA INDUSTRIE DIFESA), al fine di certificare l'aderenza del sistema ai requisiti richiesti. L'attività potrà considerarsi conclusa con la redazione del Verbale di collaudo con esito positivo firmato dalla Ditta aggiudicataria nella persona del Responsabile unico di contratto, congiuntamente al Responsabile della gestione del servizio di AID (AGENZIA INDUSTRIE DIFESA).

Rispetto delle statuizioni di cui al Codice in materia di protezione dei dati personali – D.Lgs. 196/2003; qualora nell'ambito della presente fornitura il personale della Ditta si trovi a trattare dati personali comuni, sensibili e/o giudiziari, deve agire nel rigoroso rispetto delle vigenti disposizioni in materia di protezione dei dati personali, rispettando senza eccezioni le previsioni del decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali).

In particolare è indispensabile che la Ditta, una volta opportunamente formato e informato il proprio personale dedicato alla presente fornitura, proceda ai sensi e per gli effetti dell'art. 30 del D.Lgs. 30 giugno 2003, n. 196 alla nomina di "incaricati del trattamento" di tali suoi dipendenti per gli ambiti propri di detta fornitura. I soggetti che non intendono accettare tale nomina non potranno essere presi in considerazione per il presente incarico.

A tal fine, la Ditta garantisce la presenza, tra il proprio personale, di un soggetto con adeguate conoscenze sulla privacy, che per esperienza, capacità e affidabilità sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

***Formazione del personale di AID (AGENZIA INDUSTRIE DIFESA) all'utilizzo del software per la gestione degli archivi e Help Desk***

I destinatari della formazione sono nell'ordine di 100 unità; in considerazione dei contenuti della formazione stessa sarà possibile prevedere un approccio "train-the-trainer", al fine di formare un numero limitato di risorse di AID (AGENZIA INDUSTRIE DIFESA) che a loro volta formeranno gli altri destinatari della formazione.

Dovrà, inoltre, essere predisposto un servizio di *Help Desk* appositamente dedicato disponibile in orario di lavoro (indicativamente 8:00 – 16:00).

**Art. 6 –Data Center**

Il sistema informativo dovrà essere disponibile, nella settimana, 24 ore su 24, ad eccezione degli intervalli di tempo, concordati con l'Ente, necessari ad effettuare le operazioni di servizio (salvataggi, allineamenti, elaborazioni, etc.) per garantire le funzionalità del sistema.

Il livello minimo di disponibilità in tale periodo giornaliero dovrà essere maggiore o uguale al 95%.

Le interruzioni programmate dovranno essere concordate ed effettuate fuori dagli orari lavorativi di utilizzo.

L'aggiudicatario avrà la responsabilità di attivare adeguate procedure di backup, in modo da poter ripristinare il sistema in caso di guasti, e di attuare le operazioni di sicurezza sui dati e sui programmi mediante la duplicazione ed il mantenimento di copia dei file attivi dei dati, di registrazioni statistiche e di qualsiasi altra informazione necessaria per la fornitura del servizio e della sua continuità.

Il sistema proposto dovrà garantire un'adeguata sicurezza fisica, quindi i locali adibiti al Data Center dovranno essere:

- protetti da un'adeguata protezione esterna;
- dotati di sistemi di antiscasso, antifurto interno e antincendio con sistema elettronico di rilevazione fumi;
- dotati di sistemi di controllo accessi e di sorveglianza;
- dotati di impianti di continuità e di condizionamento.

Il Data Center dovrà essere dotato di adeguata connettività ad internet e la configurazione hardware e software dovrà essere compatibile con il carico di lavoro presunto.

Il sistema proposto dovrà garantire un'adeguata sicurezza logica dei dati mediante politiche di business continuity e disaster recovery.

L'infrastruttura tecnologica a supporto del servizio offerto andrà garantita, inoltre, contro eventuali danni o manomissioni per garantire una business continuity h24. In particolare, dovrà essere presentato un adeguato piano di sicurezza e di disaster recovery focalizzato su:

- Integrità fisica del sistema informatico;
- Integrità delle infrastrutture necessarie al funzionamento dei sistemi: elettricità, connettività di rete;
- Integrità dei dati contro azioni di cracking, errori umani, virus, guasti hardware ecc.;
- Integrità dei dati;

Il piano di sicurezza dovrà altresì aderire alle linee guida per il Disaster Recovery delle pubbliche amministrazioni ai sensi del comma 3, lett.b, dell'art. 50-bis del D.lgs n.82/2005 e s.m.i. (AgID).

La ditta aggiudicataria dovrà prevedere l'installazione, presso un sito distante almeno 300 Km in linea d'aria, di un sistema di server in cluster analoghi a quelli in dotazione presso il Data Center e collegato con quest'ultimo attraverso adeguata connettività. Il sito di Disaster Recovery dovrà provvedere all'erogazione dei servizi in caso di indisponibilità della sede principale e vi dovranno essere effettuati periodici test di erogazione remota dei servizi e di verifica dell'integrità dei dati.

La ditta Aggiudicataria dovrà porre in essere ogni attività di sua competenza e supportare l'Ente nell'effettuare i test periodici previsti per la verifica della corretta funzionalità delle soluzioni adottate per garantire la continuità del servizio.

Sia il Data Center che il sito di Disaster Recovery dovranno essere di proprietà della ditta partecipante e nella sua piena ed esclusiva disponibilità.

#### **Art. 7 – Sito di lavorazione e conservazione archivi cartacei**

La custodia dei documenti cartacei dovrà essere assicurata in ambienti idonei che garantiscano la perfetta conservazione del materiale: l'Appaltatore deve inoltre assicurare la conservazione dei documenti nello stato di fatto in cui si trovano al momento del ritiro.

A garanzia del materiale preso in consegna, il magazzino dell'Appaltatore, adeguatamente sorvegliato, deve essere munito di sistemi di sicurezza idonei ai sensi di legge.

La struttura ospitante il magazzino dovrà essere in possesso di tutte le certificazioni e degli impianti di sicurezza e sorveglianza per l'espletamento del servizio di custodia e gestione; inoltre, dovrà essere già operativo, alla data di pubblicazione del bando di gara, ed in possesso e piena disponibilità della ditta partecipante.

Il personale di custodia che per qualunque titolo entri in contatto con la documentazione deve essere informato dall'Appaltatore che quanto in essa contenuto ha carattere di massima riservatezza investendo aspetti coperti dalla normativa vigente per la tutela della Privacy.

Il personale individuato dalla Stazione Appaltante può procedere all'ispezione degli archivi in qualunque momento.

L'accesso ai locali d'archivio deve essere sempre monitorato almeno attraverso la tenuta di un registro in cui devono essere riportati i dati relativi al giorno d'accesso, al soggetto che accede, ai documenti consegnati o prelevati o inseriti dopo la consultazione ed ogni altra informazione utile.

L'Appaltatore sarà tenuto, senza oneri a carico della Stazione Appaltante, a conformarsi a tutte le prescrizioni, anche future, in merito a misure di prevenzione, sicurezza ed emergenza, da adottare in relazione alle attività connesse all'appalto.

Per i locali adibiti alle attività di dematerializzazione ed archivio si richiedono le seguenti caratteristiche:

- Dotazione di impianti a norma (antincendio, antintrusione, ecc...) e dotati di adeguato Certificato Prevenzione incendi, categoria archivi cartacei, rilasciato dal Comando Provinciale dei Vigili del Fuoco competenti per il territorio in data anteriore alla pubblicazione della presente gara;
- Che siano già operativi all'espletamento del servizio di custodia e gestione di archivi almeno alla data di pubblicazione del presente bando di gara;
- Che siano locali adibiti all'esclusivo uso di custodia e gestione di archivi e detta attività non deve interagire in alcun modo con altre attività (es. Movimentazione merci, ecc...);

Si valuterà la distanza dalla sede operativa indicata al Centro di Dematerializzazione e Conservazione Unico della Difesa (C.E.D.E.C.U.) di Gaeta secondo il criterio tabellare di seguito riportato:

- Per Distanze Chilometriche Inferiori A 60 KM Punti 5;
- Per Distanze Chilometriche Inferiori Superiori O Uguali A 60 KM Ed Inferiori A 80 Km Punti 4;
- Per Distanze Chilometriche Inferiori Superiori O Uguali A 80 KM Ed Inferiori A 100 Km Punti 3;
- Per Distanze Chilometriche Superiori O Uguali A 100 KM Ed Inferiori A 120 Km Punti 2.
- Per Distanze Chilometriche Superiori O Uguali A 120 Km Punti 1.

La Distanza Verrà Misurata Con Google Maps

Ogni Concorrente Potrà Concorrere Per Un Solo Tipo Di Punteggio Quindi Se Il Concorrente Offre Una Sede

#### **Art.8 -Riconsegna della documentazione al termine del contratto**

Alla scadenza del contratto, o in caso di cessazione anticipata del medesimo per qualsivoglia causa, la Ditta aggiudicataria dovrà:

- fornire a AID (AGENZIA INDUSTRIE DIFESA), o all'eventuale futuro gestore degli archivi, la collaborazione necessaria alla presa in carico degli stessi, in maniera tale da assicurare l'integrità logica e fisica della documentazione e il suo ordinamento, nonché la riconciliazione almeno tra le serie archivistiche da trasferire e gli Elenchi informatici. Garantire l'estrazione dalle strutture di conservazione delle unità di condizionamento della documentazione oggetto della restituzione definitiva, posizionando i materiali a "bocca di magazzino" (piano stradale);
- trasferire **senza oneri per AID (AGENZIA INDUSTRIE DIFESA)** i dati completi e aggiornati degli archivi in un formato elettronico compatibile con il sistema informativo di AID (AGENZIA INDUSTRIE DIFESA); in particolare, dovranno essere forniti su idoneo supporto informatico i *file* contenenti le informazioni per la gestione delle unità archivistiche, ivi comprese le informazioni aggiuntive e le chiavi di ricerca immesse durante l'allestimento dell'archivio elettronico dei documenti.

Le attività richieste dovranno essere portate a termine secondo le modalità di seguito definite:

- dovrà essere predisposto, di concerto tra le parti, un Piano di lavoro relativo alle attività di riconsegna del patrimonio documentario di AID (AGENZIA INDUSTRIE DIFESA);
- all'avvio delle operazioni di restituzione delle unità archivistiche presso ciascuna sede, ovvero al ritiro del subentrante affidatario del servizio, dovrà essere predisposto un Verbale di inizio lavori redatto in contraddittorio tra le parti interessate e firmato dalla Ditta aggiudicataria nella persona del Responsabile unico di contratto, congiuntamente al Responsabile della gestione del servizio di AID (AGENZIA INDUSTRIE DIFESA) e, se del caso, dal Responsabile unico di contratto della Ditta aggiudicataria subentrante;
- dovranno essere assolti dalla Ditta aggiudicataria, per ciò che compete alla stessa, tutti gli obblighi derivanti dalle disposizioni del D. Lgs. 22 gennaio 2004, n. 42;
- dovrà essere assicurata a AID (AGENZIA INDUSTRIE DIFESA) la consultazione della documentazione in custodia, durante tutta la fase di restituzione;
- al termine delle operazioni di spostamento, dovrà essere predisposto un Verbale di chiusura lavori per attestare la corretta e completa esecuzione delle stesse firmato dalla Ditta aggiudicataria nella persona del Responsabile unico di contratto, congiuntamente al Responsabile della gestione del servizio di AID

(AGENZIA INDUSTRIE DIFESA) e, se del caso, dal Responsabile unico di contratto della Ditta aggiudicataria subentrante.

### **8.3 Livelli di qualità dei servizi**

La prestazione prevede, per ciascuna tipologia di servizio, la definizione di specifici livelli di qualità. I livelli di qualità dei servizi (di seguito livelli di servizio), assicurati contrattualmente, dovranno essere rispettati per tutta la durata del contratto medesimo.

La Ditta aggiudicataria, nell'organizzazione dei servizi e nella redazione del Piano di Qualità, dovrà tenere conto dei livelli di servizio di seguito indicati che potranno essere modificati, nel corso della redazione del contratto in accordo tra le parti.

Si riporta una tabella di sintesi dei livelli di servizio previsti per ciascun servizio richiesto; si precisa che il "valore soglia" indica il livello di servizio da rispettare, ossia il valore oltre il quale il livello di servizio non è più rispettato; mentre "Priorità" indica il livello di importanza del livello di servizio.

Le penali applicate per il mancato rispetto dei livelli indicati sono di seguito riportate:

- 2% del corrispettivo dovuto all'Appaltatore (bimestrale nel caso di costi ricorrenti o intero nel caso dei costi "una tantum") al superamento del valore soglia per i servizi che saranno definiti con Priorità 1;
- 1% del corrispettivo dovuto all'Appaltatore (bimestrale nel caso di costi ricorrenti o intero nel caso dei costi "una tantum") al superamento del valore soglia per i servizi che saranno definiti con Priorità 2.