Procedura aperta per l'affidamento dei servizi Hosting, Gestione e Manutenzione del Registro elettronico delle presenze per le attività d'aula e FAD sincrona per i piani formativi finanziati da Fondimpresa

Capitolato Tecnico

Sommario

Introduzione

FONDIMPRESA (d'ora in avanti anche il "Fondo") è un Fondo paritetico interprofessionale nazionale per la formazione continua costituito, a seguito dell'accordo interconfederale del 18 gennaio 2002, tra la Confederazione Generale dell'Industria Italiana — Confindustria e la Confederazione Generale Italiana del Lavoro — Cgil e la Confederazione Italiana Sindacati Lavoratori — Cisl e l'Unione Italiana del Lavoro - Uil che assumono la qualifica di soci, in base a quanto previsto dall'art. 118, Legge 23 dicembre 2000, n.388, e successive modificazioni.
FONDIMPRESA, istituito come Associazione ai sensi del capo II, titolo II - Libro primo del codice civile, non ha fini di lucro ed opera a favore di tutte le aziende che ad essa decidano di versare il contributo dello 0,30% istituito dall'articolo 25, quarto comma, della legge 21 dicembre 1978, n. 845, e successive modificazioni. Ai sensi del comma 1 dell'art. 118, Legge 23 dicembre 2000, n. 388, e successive modificazioni, il Fondo finanzia Piani formativi concordati tra le parti sociali in coerenza con la programmazione regionale e con le funzioni di indirizzo attribuite in materia al Ministero del Lavoro. Missione, statuto, regolamento, accordo istitutivo, normativa di riferimento, organi e struttura di FONDIMPRESA sono pubblicati sul sito web www.fondimpresa.it. L'attività del Fondo si esplica attraverso due principali strumenti di intervento:

1. il *Conto Formazione*, che consente a ciascuna azienda aderente di utilizzare il 70% o l'80%, in ragione della scelta effettuata per la singola matricola aderente, dei contributi versati e trasferiti dall'Inps al Fondo per il finanziamento e la realizzazione dei propri Piani formativi, condivisi fra le parti sociali;
2. il *Conto di Sistema*, pari alla sommatoria del 26% o del 16%, in ragione della scelta effettuata per la singola matricola aderente, dei contributi versati dalle aziende aderenti, per finanziare i Piani formativi condivisi su base territoriale, settoriale o ad iniziativa di più aziende.

FONDIMPRESA si è dotata di un Sistema Informativo (denominato Sistema FPF) per la gestione dei Piani formativi (d'ora in avanti, anche semplicemente "Piani") del *Conto Formazione* e del *Conto di Sistema*, per la comunicazione fra FONDIMPRESA, le proprie Articolazioni Territoriali (Organismi Bilaterali Regionali) e le aziende aderenti, per l'acquisizione e la gestione dei dati delle adesioni e dei contributi trasmessi dall'INPS, nonché delle informazioni di monitoraggio da inviare periodicamente al Ministero del Lavoro e delle Politiche Sociali e all'Agenzia Nazionale per le Politiche Attive del Lavoro (ANPAL), istituita dal decreto legislativo 14 settembre 2015, n. 150.
Il Fondo si è poi dotato di un registro elettronico (REF – Registro Elettronico di Fondimpresa) in versione prototipale, in sostituzione di quello cartaceo, sul quale sono presenti tutti i dati relativi alle azioni formative: il luogo, il giorno e l'ora di svolgimento delle azioni formative e le anagrafiche dei partecipanti. Tale registro è utile per verificare le presenze dei partecipanti alle giornate formative. La crescita costante delle adesioni e l'evoluzione delle specifiche di monitoraggio richieste dall'Autorità di indirizzo e vigilanza comportano la necessità di garantire:

- la gestione dei servizi di Hosting, conduzione e manutenzione hardware e software, con particolare attenzione alle attività di monitoraggio dei sistemi e di verifica degli aspetti di sicurezza (pen-test, vulnerability assessment, ecc.);
- la Manutenzione Adeguativa (MAD) e Correttiva (MAC) del registro elettronico e Help Desk di secondo livello;
- lo Sviluppo Software e la Manutenzione Evolutiva (MEV) del registro elettronico.

Tutti i servizi devono essere assicurati per una durata di 36 mesi con decorrenza dalla data di inizio dell'attività indicata in un apposito verbale, e deve essere garantito un periodo di affiancamento al nuovo Aggiudicatario che subentrerà a fine contratto (o risoluzione anticipata dello stesso per qualsiasi motivo), della durata di almeno di un mese.

1 Oggetto del Capitolato

Il presente Capitolato Tecnico si articola nei seguenti gruppi di attività che dovranno essere svolte dall'Affidatario per un periodo di 36 mesi, con decorrenza dalla data di inizio dell'attività indicata in un apposito verbale.

1.1 Presa in carico del registro e sua messa in esercizio

Rientrano nel seguente servizio tutte le attività propedeutiche e necessarie alla presa in carico del prototipo realizzato, ivi compresa la revisione dell'applicazione e la predisposizione degli ambienti necessari all'esercizio della stessa – come meglio specificato al paragrafo 4.1.

1.2 Sviluppo software e MEV

Rientrano nel presente servizio sia gli interventi di sviluppo software e manutenzione evolutiva sia la personalizzazione di prodotti di mercato.
Tale attività, come specificato nel successivo paragrafo 4.2, include tutto lo sviluppo del software applicativo necessario alla digitalizzazione del registro delle presenze e delle attività formative di Fondimpresa che integra i componenti di cui al successivo paragrafo 3, nonché l'eventuale integrazione di nuovi componenti applicativi. In particolare, si richiede lo svolgimento di tutte le attività necessarie per l'analisi e l'implementazione, all'interno del registro delle presenze, delle sezioni Piani Formativi, Azioni formative e Attività formative secondo le specifiche dei requisiti che saranno fornite da Fondimpresa e nel rispetto dei principi di *privacy and security by design and by default*.

1.3 MAD/MAC e Help Desk di secondo livello

Manutenzione correttiva, adeguativa, migliorativa del registro REF (attuale sistema e tutti i futuri sviluppi) come specificata nel successivo paragrafo 4.3.

1.4 Hosting, conduzione e manutenzione hardware e software

Servizio di Hosting, di conduzione tecnica, gestione della sicurezza e manutenzione preventiva, correttiva e adeguativa dell'infrastruttura HW e SW di base e , compresi eventuali virtualizzatori, se applicabili, dbms, di rete e di sicurezza dei sistemi gestiti nell'ambito del presente affidamento, ivi comprese le VPN client-to-lan e lan-to-lan che si rendono necessarie all'operatività del registro REF.

Tale servizio, specificato nel successivo paragrafo 4.4, deve comprendere l'installazione del sistema REF negli ambienti messi a disposizione dall'Affidatario.

2 Responsabile di Progetto dell'affidatario e Gruppo di progetto

L'Affidatario dovrà nominare un proprio Responsabile di Progetto al quale verranno affidate le mansioni di supervisione e coordinamento delle attività svolte dall'Affidatario stesso nell'esecuzione del contratto di cui alla presente procedura.
Il Responsabile di Progetto dell'Affidatario (Capo Progetto) rappresenterà il referente unico del Direttore dell'Esecuzione del Contratto (di seguito DEC) nominato da FONDIMPRESA ed assicurerà, tra l'altro, la necessaria assistenza consulenziale a FONDIMPRESA, anche al fine di definire le interazioni con sistemi di organizzazioni sociali, enti ed istituzioni.
Per tutte le attività di gestione e conduzione del progetto, il Capo progetto e il DEC si incontreranno almeno con cadenza trimestrale, anche con modalità smart, salvo richiesta esplicita di incontri ulteriori da parte di una delle due parti. Di tali incontri si redigerà un verbale, con stato avanzamento lavori, evidenza degli scostamenti rispetto alla pianificazione ed eventuali criticità, sottoscritto dalle parti e messo agli atti del progetto.

Per tutte le attività di conduzione tecnica del progetto, monitoraggio attività, controllo costi, e rispetto dei livelli di servizio definiti, dovrà essere nominato un Responsabile Operativo dell'affidatario che si incontrerà, anche con modalità smart, con il DEC di Fondimpresa con cadenza mensile. Di tali incontri si redigerà un verbale, con stato avanzamento lavori di tipo operativo, criticità, azioni e piani correttivi, sottoscritto dalle parti e messo agli atti del progetto.
Inoltre, per tutte le attività di MEV e/o di evoluzione architetturale dell'infrastruttura o in generale di modifiche ai servizi oggetto dell'affidamento, dovrà essere operativo, per l'intera durata contrattuale, un gruppo di progetto misto, composto dal Capo Progetto e dal Responsabile Operativo nominato dall'affidatario, supportati adeguatamente dai referenti tecnici o di servizio coinvolti nel progetto, dal DEC nominato da FONDIMPRESA, eventualmente coadiuvato dai referenti delle varie aree operative.
Fondimpresa si riserva in ogni caso di modulare la propria organizzazione interna a suo insindacabile giudizio, dandone comunicazione all'Affidatario.
Tale gruppo dovrà coordinare tutte le attività oggetto del presente Capitolato verificandone lo stato di avanzamento e l'adeguatezza delle soluzioni tecniche implementate e valuterà l'esigenza di eventuali modifiche o variazioni rispetto alle specifiche tecniche contrattuali.
Inoltre, il gruppo, nella fase di analisi dei requisiti, dovrà approvare, mediante sottoscrizione, tutti i documenti di specifica delle funzionalità prima dell'avvio della fase implementativa. Tale gruppo di lavoro potrà riunirsi, a discrezione di FONDIMPRESA o su richiesta formale dell'Aggiudicatario, presso la sede indicata da FONDIMPRESA o in modalità smart.
L'Aggiudicatario dovrà predisporre, concordandolo con il gruppo di progetto, un repository digitale, interrogabile tramite interfaccia web, in cui rendere disponibile al Fondo tutta la documentazione di progetto e d'utente. Tale repository dovrà essere inizializzato con la documentazione di progetto del prototipo disponibile.

Per le attività del gruppo di progetto **non** vi sarà alcun tipo di compenso aggiuntivo rispetto a quanto previsto per i singoli servizi dell'affidamento.

3 Architettura del Sistema esistente

Di seguito verrà descritta l'architettura del prototipo del REF.

3.1 Architettura software

L'applicazione web è realizzata sotto forma di PWA (Progressive Web App).

Tale architettura prevede un back-end che espone servizi REST al front-end.

Il back-end è scritto in C# su Net Core 6 (o successiva) e dovrà essere ospitato su Web Server IIS con supporto al Net Core. I dati sono salvati su database relazionale Microsoft Sql Server, compatibile con la versione Express 2019. Il front-end è scritto in Typescript su Angular 14.

Come servizi esterni sono utilizzati:

- Server SMTP di posta
- Provider per invio di SMS
- Integrazione con SPID (o eventuale altro sistema pubblico di identità digitale alternativo)

La figura seguente illustra il modello indicativo dell'architettura del REF.

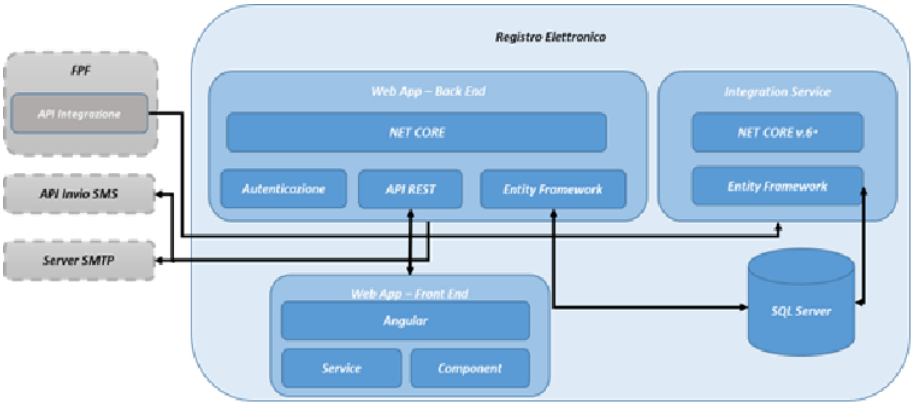

Figura 1 – Schema Logico

Authentication & Authorization

Il sistema di autenticazione e autorizzazione si basa sul sistema di autenticazione di Fondimpresa, sviluppato con OpenLDAP.

3.2 Software applicativo REF

Fondimpresa si è dotata di una piattaforma, al momento in fase prototipale, per l'efficientamento del processo di monitoraggio delle attività formative finanziate, la riduzione degli oneri amministrativi per le aziende aderenti e la semplificazione dell'accesso ai servizi del Fondo.
A tal fine Fondimpresa ha deciso la digitalizzazione del registro di rilevazione delle presenze alle attività formative, in modo da renderlo unico, sempre accessibile.
Nel registro elettronico (REF) sono presenti tutti i dati relativi alle azioni formative: il luogo, il giorno e l'ora di svolgimento dell'azione formativa e le anagrafiche dei partecipanti.
Il Referente di piano inserisce a sistema i dati che riguardano tutta la parte di anagrafica dei docenti/ codocenti, tutor e coordinatori (ove previsti) e l'associazione ai calendari delle azioni formative.

Formazione in presenza
L'inizio della lezione è dichiarato quando il docente o il tutor raggiunge l'aula che ospita l'azione formativa da svolgere, si identifica sul sistema con utenza e password ed inserisce la sua firma. Solo dopo tale attività è possibile acquisire le presenze in entrata di ogni partecipante alla giornata formativa e a sistema è consentita la registrazione degli orari di ingresso. La presenza di ogni singolo partecipante è rilevata tramite l'acquisizione della sua firma elettronica (tratto grafico con georeferenziazione) direttamente su un dispositivo elettronico dotato di touch screen, in possesso del soggetto attuatore o dell'azienda aderente titolare del Piano formativo. Il sistema a tal punto acquisisce il dato della presenza del partecipante. In questa fase gli utenti che utilizzano l'applicazione possono avere una sola sessione attiva per garantire l'univocità della loro presenza all'azione formativa.
Il docente, alla fine della lezione, ha la possibilità di descrivere sul sistema gli argomenti trattati e può caricare eventuali file aggiuntivi, ai fini dell'esecuzione della verifica.
Infine, è possibile rilevare l'inizio e la conclusione dell'eventuale pausa-pranzo e la conclusione della giornata formativa, sempre tramite l'acquisizione della firma elettronica.
Tutte le firme elettroniche incorporano il sistema di Global Positioning System ("GPS").

Formazione a Distanza Sincrona (MODULO DA SVILUPPARE)
Tale modulo non è attualmente presente nel prototipo e sarà la prima MEV da implementare dopo la presa in carico; le indicazioni ivi presenti sono una traccia di requisito suscettibile di modifiche e/o ampliamenti in fase di analisi.

Il docente invia tramite applicazione un invito alla partecipazione alla sessione formativa. All'interno della comunicazione è indicata la modalità di identificazione del discente che può avvenire tramite sistemi forti, come ad esempio OTP o SPID (o eventuale altro sistema pubblico di identità digitale alternativo). Una volta ricevuta la comunicazione, tramite una pagina dedicata sul sito, i partecipanti alla formazione possono effettuare la registrazione per segnalare l'entrata e l'uscita dall'aula virtuale. Il sistema, quindi, acquisisce il dato della presenza dei singoli partecipanti registrando, per ognuno di essi, le informazioni di inizio e fine di ogni specifica lezione e di inizio e fine delle eventuali pause-pranzo.

3.3 Software applicativo FPF (Fondimpresa Piani Formativi)

Il Fondo ha realizzato un'architettura informatica, denominata sistema FPF (Fondimpresa Piani Formativi), basata su tre livelli (livello base di dati, applicativo e web per l'interfaccia), su un potente motore BPM in grado di "coordinare" le transazioni generate dalle diverse applicazioni sviluppate, che interagiscono mediante una logica SOA (Service Oriented Architecture), e su un sistema di gestione documentale e protocollo informatico. Il sistema FPF è lo strumento di supporto allo svolgimento dei processi di Fondimpresa, ed è utilizzato dalle aziende aderenti, dai soggetti proponenti dei piani del conto sistema e da tutte le Aree/Unità di Fondimpresa e dalle sue Articolazioni Territoriali.
Il ruolo della piattaforma all'interno della struttura di Fondimpresa, oltre a supportare le Aree/Unità nello svolgimento delle proprie mansioni, regola e gestisce gli scambi di flussi di informazioni inter-area e con altri sistemi informatizzati al fine di mantenere il controllo su tutti i processi e migliorare l'iter di presentazione, gestione e rendicontazione dei Piani formativi.

Tramite l'utilizzo di servizi REST bidirezionali, REF e FPF comunicano sincronizzando in FPF i dati di riepilogo delle giornate formative comprendenti le ore di presenza e i partecipanti. REF riceve in automatico, da FPF, le informazioni riguardanti: piani, azioni, giornate, docenti e referenti.

4 Descrizione dei Servizi oggetto della procedura

Nei paragrafi seguenti sono dettagliate le specifiche tecniche di tutti i servizi oggetto della presente procedura e di seguito riepilogati.

1. Presa in carico del registro e sua messa in esercizio
2. Sviluppo software e MEV.
3. MAD/MAC e Help Desk di secondo livello.
4. Hosting, conduzione e manutenzione hardware e software.

I predetti servizi dovranno essere svolti per un periodo di 36 mesi con decorrenza dalla data di inizio dell'attività indicata in un apposito verbale.

4.1 Presa in carico del registro e sua messa in esercizio

Il servizio deve essere espletato in accordo con il ***"Piano di presa in carico e messa in esercizio"*** e il ***"Piano della qualità"***, da prodursi come parte integrante dell'offerta tecnica.
Il ***"Piano di presa in carico e messa in esercizio"*** dovrà contenere una dettagliata descrizione delle attività di presa in carico del REF e delle attività per la messa in esercizio dello stesso, in aderenza ai requisiti richiesti nel presente capitolato in termini di qualità, sicurezza, affidabilità e prestazioni, con particolare riferimento a:

- presa in carico e integrazione della documentazione dell'applicazione;
- creazione della baseline di progetto in coerenza con quanto previsto al punto 4.2 del presente capitolato;
- revisione/evoluzione del Registro preso in carico, con realizzazione di un prototipo navigabile che evidenzi le migliorie funzionali e di interfaccia proposte, prima della messa in esercizio;

- definizione dell'architettura fisica o virtualizzata che ospiterà l'ambiente di esercizio e di test/collaudo in coerenza con quanto previsto al punto 4.4 del presente capitolato;
- assessment iniziale della sicurezza dell'infrastruttura, comprensivo di analisi statica del codice, vulnerability assessment e penetration test (anche applicativi) - generando una baseline della sicurezza - e conseguente produzione di un dettagliato documento di remediation delle eventuali criticità evidenziate;
- messa in esercizio.

L'attività di presa in carico, che si conclude con la messa in esercizio, deve essere svolta entro 60 giorni solari dalla data di avvio delle attività (indicata in un apposito verbale).

4.2 Sviluppo software e MEV

Il servizio deve essere espletato in accordo con il ***"Piano di Sviluppo software e MEV"*** e il ***"Piano della qualità"***, da prodursi come parte integrante dell'offerta tecnica. Il *"**Piano di Sviluppo software e MEV"*** dovrà contenere una dettagliata descrizione delle metodologie di sviluppo adottate, in aderenza a quanto richiesto nel presente capitolato, con particolare riferimento a:

- gestione complessiva del ciclo di vita del software;
- metodologie e strumenti adottati per garantire la qualità del software da rilasciare e una bassa difettosità in esercizio;
- metodologie e strumenti adottati per garantire la sicurezza del codice prodotto;
- processo di certificazione e test, nonché del passaggio in produzione del software sviluppato;
- **esempio di attività di manutenzione** evolutiva, con concreta evidenza dell'applicazione delle metodologie e degli strumenti utilizzati;
- proposte migliorative dei livelli di servizio.

Il presente servizio riguarda l'intera applicazione REF descritta dal presente capitolato.
Dovrà essere svolta un'attività di sviluppo per un totale **massimo** stimato di **3.300 PF** (Punti Funzione – cfr. paragrafo 4.2.7) a cui corrispondono, ipotizzando una produttività di 2,2 PF per giorno/uomo, circa **1.500 giorni/uomo**.
Fondimpresa si impegna a garantire l'impiego di 1.000 PF nell'arco del periodo contrattuale; superata tale soglia la fruizione dei Punti Funzione non sarà vincolante, in quanto soggetta alle effettive necessità di Fondimpresa sulla base di suo insindacabile giudizio. Il numero massimo di Punti Funzione (3.300) non vincola, pertanto, in alcun modo Fondimpresa in quanto è da considerarsi solo indicativo e valido ai soli fini della formulazione dell'offerta; il corrispettivo erogato all'aggiudicatario sarà determinato sulla base delle giornate/uomo effettivamente richieste.
Nell'ambito del servizio di *Sviluppo software e MEV* si possono individuare i seguenti sottoservizi.

- Sviluppo e manutenzione evolutiva:
  - analisi, progettazione, implementazione, testing e deployment di nuove funzionalità e/o moduli applicativi;
  - analisi, progettazione, implementazione, testing e deployment per la modifica di funzionalità già esistenti;
  - servizio di manutenzione correttiva delle nuove funzionalità e delle modifiche (ivi compresi gli errori di regressione); tale attività è compresa nel corrispettivo del servizio entro i termini di legge per la garanzia (cfr. par. 4.3);
  - formazione del personale del Fondo e suoi incaricati sulle nuove funzionalità e sulle modifiche;
  - eventuali procedure di migrazione dati e/o gestione del pregresso;
  - documentazione tecnica di progetto e manualistica d'utente.
- Personalizzazione di prodotti di mercato:
  - analisi dei requisiti;
  - realizzazione delle procedure non coperte dall'applicativo nativo (personalizzazioni, adeguamenti del software ed eventuali altre realizzazioni ad hoc);
  - parametrizzazioni ed integrazioni;

- testing;
- manutenzione correttiva del prodotto software "personalizzato" (ivi compresi gli errori di regressione); tale attività è compresa nel corrispettivo del servizio entro i termini di legge per la garanzia (cfr. par. 4.3);
- formazione del personale del Fondo e suoi incaricati sulle nuove funzionalità e sulle modifiche;
- eventuali procedure di migrazione dati e/o gestione del pregresso;
- documentazione tecnica di progetto e manualistica d'utente.

Gli interventi di manutenzione evolutiva di dimensione inferiore o uguale a 25 Punti Funzione (PF) sono da considerarsi MAD o MAC, rientranti nel *Servizio di MAD/MAC e Help Desk di secondo livello* e non in quello di *Sviluppo software e MEV*.

Lo sviluppo e la manutenzione evolutiva rilasciano applicazioni o funzionalità che modificano la consistenza dimensionale del parco applicativo, il cui volume è misurato in Punti Funzione (PF). L'elenco delle applicazioni che costituiscono il patrimonio applicativo con la corrispondente indicazione della dimensione espressa in Punti Funzione viene denominata "baseline delle applicazioni". La baseline delle applicazioni di norma nel tempo subisce variazioni (incremento o decremento) per effetto:

- del rilascio in esercizio di nuove applicazioni;
- dell'eliminazione di applicazioni obsolete;
- delle modifiche alle applicazioni in esercizio introdotte dagli interventi di manutenzione evolutiva, che possono aggiungere nuove funzionalità o eliminare funzionalità esistenti.

Il Fornitore **ha l'obbligo** di fornire gli elementi di misurazione sul patrimonio software gestito del Fondo. All'atto dell'avvio del contratto, il Fornitore **dovrà** realizzare una nuova baseline, provvedendo poi al suo continuo aggiornamento, dopo ogni intervento che modifica la baseline, durante l'intera durata del contratto.
I record di gestione della *baseline* dovranno contenere almeno le seguenti informazioni:

a. codice dell'applicazione;
b. descrizione dell'applicazione;
c. data di collaudo;
d. data di rilascio in esercizio;
e. interventi di Manutenzione evolutiva;
f. n. di Punti Funzione alla data del collaudo;
g. n. di PF aggiunti;
h. n. di PF eliminati;
i. n. di PF dell'applicazione dopo l'intervento di manutenzione.

A oggi, la *baseline* non è presente; la baseline dovrà essere realizzata ex-novo nell'ambito del servizio di presa in carico (cfr. par. 4.1).

I servizi realizzativi (Sviluppo e Manutenzione evolutiva) dovranno assicurare l'esecuzione dei test manuali o automatizzati, di cui deve essere data opportuna evidenza in appositi documenti, il supporto al collaudo, la migrazione dei dati e l'avvio in esercizio del software realizzato comprensivo di eventuali procedure di gestione dei dati pregressi.
Dovranno essere, dunque, ricomprese senza oneri aggiuntivi nei servizi realizzativi le attività indicate al paragrafo 12 (Modalità di collaudo) del presente Capitolato.

I cicli di sviluppo e il profilo di qualità, sicurezza e riservatezza del software e delle informazioni, espresse secondo le caratteristiche indicate dalle norme ISO relative alla qualità del prodotto software (ISO/IEC 25000) e dalle norme che regolano gli aspetti di sicurezza e riservatezza (ISO/IEC 27001, OWASP, Linee guida AGID, Reg. EU 2016/679 GDPR), **dovranno** essere documentati nel ***"Piano di Sviluppo software e MEV"*** e nel ***"Piano della qualità"***.

I servizi di cui sopra, organizzati in lotti funzionali, verranno attivati a richiesta di FONDIMPRESA e dovranno prevedere l'intero ciclo di sviluppo (analisi, implementazione, testing, deployment, collaudo, manutenzione, formazione e documentazione) secondo quanto indicato nei successivi paragrafi.
Per la realizzazione del servizio, l'Affidatario dovrà utilizzare un **proprio** ambiente di sviluppo e un **proprio** ambiente di collaudo conformi all'architettura di esercizio dell'applicazione (anche mediante meccanismi di virtualizzazione delle risorse) senza che per questo venga riconosciuto alcun corrispettivo ulteriore rispetto a quanto previsto per l'espletamento del servizio. Si richiede che l'ambiente di collaudo possa essere messo a disposizione di Fondimpresa per attività formative nei periodi in cui non sono previste attività di collaudo e comunque con reciproco accordo tra l'affidatario e il Fondo. L'ambiente deve contenere le componenti applicative utilizzate per lo svolgimento delle attività di collaudo e formative (*un'istanza della componente elaborativa, un'istanza del* ***server SQL****)*.
Il fornitore ha la facoltà di proporre ambienti separati, uno per il collaudo e uno per la formazione; tale proposta sarà valutata come elemento migliorativo secondo quanto riportato nell'apposito criterio nella Lettera d'invito.

4.2.1 Processo di sviluppo

L'Affidatario deve predisporre un processo di sviluppo software documentato che dovrà contemplare tutte le attività previste nel ciclo di vita del software, conformemente a quanto previsto dalla norma ISO/IEC 12207 in vigore *Systems and software engineering — Software life cycle processes*.
Tale processo, pertanto, deve includere le attività descritte nella successiva tabella. Queste possono sovrapporsi, essere applicate in modo iterativo o in modo differente a seconda del software sviluppato, e non devono necessariamente essere eseguite nell'ordine in cui sono presentate.
Nella seconda colonna della tabella viene fornita una descrizione di massima degli obiettivi che deve avere la corrispondente attività.
Le effettive modalità di realizzazione della stessa possono, ovviamente, essere scelte dall'Affidatario in base al proprio know-how, al proprio sistema di qualità e alle proprie metodologie di lavoro, ai tool di condivisione degli stati di avanzamento e relativi esiti messi a disposizione dei referenti FONDIMPRESA, purché venga garantita l'esecuzione di tutte le attività di interesse di FONDIMPRESA ed il raggiungimento degli obiettivi indicati.

Attività	Descrizione
Organizzazione, pianificazione e supervisione del progetto	L'Affidatario deve eseguire attività di pianificazione e supervisione per: • sviluppo software; • test funzionale e di integrazione; • system test; • installazione del software; • SAL intermedi per gli sviluppi complessi; • eventuali prototipi.
Predisposizione dell'ambiente di sviluppo	L'Affidatario deve predisporre gli ambienti necessari per lo sviluppo e la manutenzione dei prodotti software, garantendone l'adeguatezza, la funzionalità, la sicurezza e l'affidabilità necessarie allo scopo riguardo a: • software engineering; • software test; • gestione della configurazione.
Analisi dei requisiti del sistema	L'Affidatario deve eseguire l'analisi dei requisiti (impliciti ed espliciti) del sistema in conformità con le procedure e le metodologie del proprio ***Piano della qualità***. È richiesto all'Affidatario di utilizzare strumenti informatici di supporto (ad es. CASE tools), che, tra l'altro, consentano di mantenere la tracciabilità tra i requisiti formalizzati ed i casi di test progettati, facilitando così la verifica della piena aderenza delle funzionalità sviluppate ai requisiti. La tracciabilità dei requisiti deve inoltre consentire la piena visibilità degli impatti che eventuali modifiche ai requisiti possono comportare allo sviluppo del sistema. In questa fase dovrà essere prodotta una prima stima della dimensione in PF o, ove non possibile, in gg/uomo.
Progettazione del sistema	L'Affidatario deve eseguire la progettazione del sistema in conformità con le procedure e le metodologie del proprio ***Piano della qualità***. In questa fase dovrà essere aggiornata la stima della dimensione in PF o, ove non possibile, in gg/uomo e **dovrà essere realizzato il prototipo delle interfacce.**

Realizzazione e Unit Test del software	L'Affidatario deve: • eseguire test specifici su ogni unità di software realizzata; • effettuare tutte le necessarie modifiche al software e rieseguire tutti i test necessari in base ai risultati dei test.
Test funzionali e di integrazione	L'Affidatario deve: • predisporre opportuni casi di test (in termini di input, risultati attesi e criteri di valutazione), procedure e dati per l'effettuazione di test funzionali e di integrazione. I casi di test devono coprire tutti gli aspetti funzionali e qualitativi considerati nella progettazione del software; • eseguire i test funzionali e di integrazione in modo conforme a quanto stabilito dai casi di test e dalle relative procedure; • effettuare le modifiche al software e rieseguire tutti i test necessari in base ai risultati dei test; • registrare e analizzare i risultati dei test e le anomalie eventualmente riscontrate.
Test di sistema (collaudo)	Per la pianificazione ed esecuzione del collaudo l'Affidatario deve conformarsi a quanto indicato nella Procedura di collaudo (paragrafo 12 del presente Capitolato). In sede di collaudo dovrà inoltre essere rendicontata la dimensione finale effettiva di quanto realizzato in PF.
Installazione software	L'Affidatario deve: • preparare il software eseguibile, inclusi i file batch, i file di comandi, i file di dati e ogni altro oggetto necessario per installare e far funzionare il sistema nell'ambiente operativo previsto; • identificare e registrare la versione esatta del software predisposto per ogni ambiente operativo; • predisporre i manuali utente e operativi; • installare e controllare il software eseguibile sulle macchine destinatarie secondo quanto concordato caso per caso con FONDIMPRESA interfacciandosi e fornendo supporto ai servizi di gestione operativa sia condotti dall'Affidatario stesso sia da altri Fornitori. L'installazione avverrà preliminarmente nell'ambiente di Test (tale ambiente riproduce quello di esercizio) e successivamente, dopo l'eventuale periodo di pre-esercizio e a seguito di positivo collaudo ed esplicita richiesta di FONDIMPRESA, nell'ambiente finale di esercizio, con eventuali interruzioni programmate, con almeno una settimana di anticipo, al di fuori del normale orario di lavoro (dopo le ore 24 o in giorni festivi).

Gestione della manutenzione Software	L'Affidatario deve: • identificare le entità da mettere sotto controllo di configurazione e deve assegnare a ciascuna una codifica univoca; • predisporre e implementare procedure per individuare i livelli di controllo per ciascuna entità in configurazione (ad esempio controllo dell'autore, del capo progetto, del cliente ecc.); • individuare le persone o i gruppi con l'autorità per autorizzare ed effettuare modifiche ad ogni livello; • definire i passi da seguire per richiedere l'autorizzazione per modifiche, elaborare richieste di modifica, tracciare e distribuire le modifiche e mantenere le precedenti versioni del software. Devono essere mantenute le registrazioni dello stato della configurazione di tutte le entità poste sotto controllo. Queste registrazioni devono essere mantenute per tutta la durata del contratto e devono contenere, a seconda dei casi, la corrente versione di ogni entità, informazioni su tutte le modifiche che hanno subito da quando sono state inserite sotto controllo di configurazione e sullo stato in cui si trovano.
Assicurazione sulla qualità e sicurezza del software	L'Affidatario deve effettuare, in modo continuativo, verifiche sulle attività di sviluppo software e sui prodotti risultanti da queste, al fine di: • assicurare che ogni attività sia stata eseguita in conformità con il contratto e con le procedure previste nel ***Piano della qualità***; • assicurare che ogni prodotto software sia stato sottoposto a verifiche, test e azioni correttive necessarie; • assicurare che ogni sviluppo software non introduca vulnerabilità né comprometta in alcun modo la sicurezza dell'applicativo; • assicurare che ogni sviluppo software venga effettuato sulla base del principio di *privacy by design* e *privacy by default*. Ogni attività di sviluppo software deve prevedere una attenta analisi in termini di efficienza che consenta di massimizzare le prestazioni, rispetto all'architettura esistente e alle funzionalità già implementate/previste. L'Affidatario deve effettuare registrazioni di tutte le attività di assicurazione qualità e sicurezza svolte e deve conservarle per tutta la durata del contratto.
Azioni correttive	L'Affidatario deve produrre un rapporto di rilevazione anomalia ogni qualvolta siano rilevati problemi concernenti i prodotti software e le loro componenti poste sotto controllo di configurazione, e svolgere le attività richieste da FONDIMPRESA o descritte nel ***Piano della qualità***. Tali rapporti devono descrivere il problema, le azioni correttive richieste e quelle svolte alla data.

4.2.2 Linee Guida per le attività di sviluppo e documentazione

L'Affidatario deve utilizzare, per tutte le attività di sviluppo software, metodologie documentate, sistematiche ed efficaci. Queste metodologie devono essere descritte nel ***"Piano di Sviluppo software e MEV".***

La metodologia scelta dovrà comunque prevedere l'utilizzo di strumenti/linguaggi formali secondo *best practice* per la produzione dei casi d'uso e di tutta la documentazione tecnica e di progetto, e schemi ER e dizionari dei dati per la documentazione relativa alle basi dati.

L'Affidatario deve quindi prevedere tutte le attività necessarie a presidiare il rilascio di nuove componenti o di aggiornamenti di componenti già distribuite in produzione, secondo controlli e verifiche di coerenza con

l'architettura del Sistema. La necessità di adottare nuove componenti architetturali o di aggiornare elementi già in produzione dovrà essere evidenziata nelle fasi di analisi del prodotto e sottoposta ad esplicita approvazione da parte di FONDIMPRESA.

Per la realizzazione del presente servizio, l'Affidatario dovrà garantire l'impiego di figure professionali adeguate in termini di competenze e numerosità per la realizzazione delle attività progettuali (Curricula). Tali figure devono essere scelte nell'ambito dei seguenti profili professionali:

- Capo Progetto
- Analista Funzionale/UI Designer/BP Analyst
- Analista Programmatore/Tester Senior
- Application security specialist
- Programmatore/Tester
- Specialista di Prodotto/Tecnologia
- Data Base Administrator
- Sistemista Senior

L'Affidatario deve dichiarare nel *"Piano dell'organizzazione dei gruppi di lavoro"*, fornendo i relativi curricula professionali, il numero di risorse professionali, comunque non inferiore a *otto*, che compongono il team di sviluppo, fermo restando che tali risorse possono essere impiegate in tutto o in parte in relazione alle esigenze di sviluppo ed alla pianificazione condivisa con FONDIMPRESA.
Eventuali sostituzioni di risorse dovranno **essere preventivamente autorizzate** da FONDIMPRESA e comunque sostituite con profili professionali uguali o superiori. Il mancato rispetto della preventiva autorizzazione verrà sanzionato sulla base degli indicatori previsti al paragrafo 9.5.3. ***Il suddetto team, a richiesta di Fondimpresa, dovrà essere rafforzato fino al 50% senza alcun aggravio economico per il Fondo. Incrementi del gruppo di lavoro richiesti da Fondimpresa e superiori al 50%, fino al 100%, comporteranno un aumento della tariffa contrattuale (espressa in PF) di una percentuale del 5% ogni 10 punti percentuali (o frazioni) di incremento eccedente il 50%, fino ad un massimo del 25% di incremento della tariffa (es. se il gruppo di lavoro viene aumentato del 60% la tariffa sarà incrementata del 5% se l'incremento è del 100% la tariffa sarà incrementata del 25%)".***

Per lo svolgimento delle attività di sviluppo e manutenzione evolutiva dovranno essere utilizzate risorse specialistiche con il mix di professionalità di seguito riportate.

In fase di offerta tecnica, il fornitore dovrà dichiarare la composizione del gruppo di lavoro, indicando le percentuali di utilizzo, per ognuna delle figure professionali, che dovranno rientrare nei valori indicati in tabella; in ogni caso la somma delle percentuali di utilizzo proposte deve essere pari a 100.

Figura Professionale	**Percentuale Minima**	**Percentuale Massima**
Capo Progetto	5%	15%
Analista Funzionale/UI Designer/BP Analyst	15%	35%
Analista Programmatore/Tester Senior	20%	40%
Application security specialist	5%	10%
Programmatore/Tester	10%	30%
Specialista di Prodotto/Tecnologia	10%	20%
Data Base Administrator	5%	10%
Sistemista Senior	5%	10%
Totale	**100%**	

Le attività di sviluppo, svolte a richiesta di Fondimpresa, saranno raggruppate in “lotti applicativi” e per ognuno di essi andrà realizzato un ciclo completo di sviluppo in conformità alle presenti linee guida. Pertanto, per “lotto applicativo”, si intende l’unità minima che contiene un insieme di funzionalità e a cui si applica l’intero ciclo di sviluppo fino al rilascio in produzione.

L'esecuzione delle attività previste per il singolo “lotto applicativo” è espressamente subordinata alla approvazione da parte di Fondimpresa del documento di progettazione esecutiva contenente la pianificazione ed il dettaglio delle attività e delle risorse impegnate (PF o, ove non possibile, gg/uomo) predisposto dall'affidatario sulla base delle specifiche indicate dal Fondo. Pertanto, in caso di mancata approvazione dei documenti di pianificazione e dettaglio da parte di Fondimpresa, l'affidatario non avrà nulla a pretendere per lo svolgimento delle attività necessarie alla loro elaborazione e non si darà luogo alla realizzazione delle attività ivi previste. Qualsiasi modifica del documento di progettazione esecutiva approvato, anche in riferimento ai componenti del gruppo di lavoro previsto, deve essere preventivamente autorizzata da Fondimpresa.

Il flusso di Analisi viene svolto principalmente nelle fasi di evoluzione dell'Architettura e di evoluzione delle Funzionalità e mira a definire in modo completo ed esaustivo la struttura generale del sistema (fuoco dell'analisi nella fase di *Architettura*) e le funzioni da realizzare e/o modificare (fuoco dell'analisi nella fase di *Funzionalità*), con riferimento ai processi individuati e alle modalità con cui tali processi risulteranno visibili all'utente.
Le attività svolte all'interno di questo flusso portano a:

- descrivere formalmente l'applicazione e/o le funzioni da sviluppare in termini di esigenze funzionali dell'utenza e di esigenze non funzionali, in modo chiaro, esaustivo e sistematizzato, compresa la descrizione logica delle interconnessioni con altri sistemi/applicazioni/apparati/aree applicative;
- dove necessario, predisporre un documento di mappatura fra il prodotto del ridisegno dei processi e i requisiti dell'applicazione;
- individuare e documentare dettagliatamente la soluzione applicativa e tecnologica adeguata al soddisfacimento delle esigenze funzionali di cui sopra;
- validare e dettagliare la pianificazione e la stima dello sforzo motivando eventuali scostamenti;
- progettare il piano di test con particolare attenzione all'individuazione delle tipologie di test (es. stress test, test accessibilità ecc.), dei criteri di scelta dei test da automatizzare, l'individuazione della base dati necessaria per il test, eventuali criticità note;
- individuare i rischi di progetto e definire le opportune azioni correttive;
- realizzare i documenti di progetto e d'utente e aggiornarli in caso di modifiche intercorse rispetto a precedenti versioni degli stessi;
- produrre la progettazione esecutiva del lotto applicativo.

Qualora tecnicamente possibile e ritenuto utile da Fondimpresa, le specifiche funzionali dovranno essere corredate dalla realizzazione di un prototipo delle interfacce (*mockup*) che rappresenti almeno le modalità di navigazione e il layout delle interfacce.

Le attività di Disegno, ovviamente, hanno come prerequisito la descrizione delle relative specifiche funzionali.
Il *Disegno* traduce le caratteristiche della soluzione in specifiche tecniche di dettaglio necessarie alla generazione dei prodotti finali.
Gli obiettivi principali dell'attività di *Disegno* sono:

- descrivere ogni elemento da realizzare, le modalità di integrazione con gli altri elementi, i vincoli e i controlli cui devono essere sottoposti gli elementi;
- descrivere tutti i dati trattati raggruppati per insiemi logici (schema logico e fisico dei dati), e rappresentare il mapping con lo schema concettuale;
- applicare i principi di *privacy by design* e *by default* e *security by design* e *by default;*
- dettagliare le modalità di interconnessione con altri sistemi / applicazioni /aree applicative / apparati;

- progettare i test (anche con riferimento alla sicurezza del software, alla protezione dei dati e alle prestazioni);
- validare e dettagliare la pianificazione motivando eventuali scostamenti;
- aggiornare, in caso di modifiche intercorse, precedenti versioni di prodotti.

Le attività di *Realizzazione* sono finalizzate a generare i componenti software e la base dati che costituiscono il lotto applicativo, verificando inoltre la loro correttezza e funzionalità. I componenti dovranno essere realizzati coerentemente con il disegno di dettaglio.
Per quanto riguarda gli aspetti inerenti all'Architettura, la *Realizzazione* garantirà che le diverse componenti dell'architettura possano comunicare correttamente e soddisfino i requisiti non funzionali per il sistema complessivo. Per quanto attiene alle Funzionalità, la *Realizzazione* dovrà garantire la soddisfazione dei requisiti utente, anche per aspetti non funzionali, quali usabilità, accessibilità, disponibilità ecc.

L'attività prevede tra l'altro di:
- effettuare l'implementazione del sistema, producendo il codice sorgente;
- utilizzare *best practice* di *secure coding*;
- eseguire i test e relativo codice di test, verificando anche l'impatto prestazionale del codice generato e la sua sicurezza;
- consegnare alla gestione della configurazione i componenti realizzati e la relativa documentazione;
- aggiornare, in caso di modifiche intercorse, precedenti versioni di prodotti;
- **realizzare, su richiesta di Fondimpresa, un prototipo <u>funzionante</u>** per consentire una fase di pre-esercizio di durata concordata (di norma 30-60 giorni solari), che rappresenterà parte integrante delle attività di collaudo.

4.2.2.1 Documentazione

Durante tutto il ciclo di sviluppo si rende necessaria la creazione e/o l'aggiornamento dei documenti di progetto e dei manuali utente. Il flusso di documentazione si svolge in continuità lungo tutte le fasi, venendo finalizzato durante la fase di Messa in esercizio mediante una standardizzazione di quanto prodotto nelle fasi precedenti per produrre i documenti ufficiali finali del progetto.
Nell'offerta tecnica dovranno essere dettagliatamente descritte le modalità di documentazione proposte dal fornitore, in accordo alle presenti indicazioni e a quelle presenti al paragrafo 8 del presente capitolato (contenente alcune linee guida allo schema di documentazione), in un apposito ***"Piano della documentazione di progetto"***.
Si richiede che la documentazione tecnica venga prodotta per quanto possibile utilizzando linguaggi di modellazione diagrammatici di uso comune, per quanto riguarda sia aspetti strutturali sia dinamici. Nel caso i diagrammi siano stati prodotti mediante tool proprietari, il fornitore dovrà **permettere** anche **alla direzione dei lavori l'accesso al tool.**

4.2.2.2 Avvio in esercizio

Il flusso di avvio in esercizio e/o in pre-esercizio inizia a partire dal positivo collaudo e dall'accettazione del prodotto realizzato da parte del DEC di Fondimpresa. L'attività comprende:
- la predisposizione dell'ambiente di esercizio,
- il rilascio della versione software sviluppata o reingegnerizzata e, ove necessario, la migrazione dei dati e/o processi e la gestione del pregresso;
- il monitoraggio del software realizzato e/o modificato per poterne verificare l'affidabilità nei primi tre mesi di esercizio e/o pre-esercizio o in altro periodo definito nella **"Progettazione esecutiva"** del lotto funzionale approvato. Nel corso di tale fase il Fornitore dovrà garantire adeguato supporto al DEC.

La durata del flusso sarà definita nella **"Progettazione esecutiva"** del lotto funzionale.

4.2.3 Standard per i prodotti software

L'Affidatario dovrà garantire che tutte le attività di sviluppo software siano effettuate rispettando i seguenti standard generali che dovranno essere documentati da opportune linee guida:

- standard di programmazione che dovranno dare, tra le altre cose, regole precise per la scrittura e la documentazione dei moduli software realizzati e modificati, anche in merito al rispetto di specifiche e opportune metriche statiche. Quando applicabile, gli standard dovranno fare riferimento anche a standard già esistenti in letteratura per linguaggi specifici (es. Standard Oracle per linguaggio JAVA);
- standard di interfaccia utente con particolare riferimento alle problematiche di accessibilità (orientati all'usabilità, accessibilità ecc.). Quando applicabile, gli standard dovranno fare riferimento anche a standard già esistenti in letteratura per linguaggi/ambienti specifici (e.g. WCAG);
- standard di nomenclatura degli *item* software;
- standard di documentazione tecnica del software applicativo.

I requisiti, di cui al precedente elenco, dovranno trovare riscontro anche nel ***"Piano della qualità"*** predisposto dall'Affidatario nel quale dovranno essere previste adeguate verifiche in corso d'opera che assicurino la qualità di quanto fornito.
I documenti prodotti all'inizio delle attività, dovranno essere tenuti aggiornati per tutta la durata del contratto sia per l'attivazione di nuovi ambienti applicativi, sia per variazioni nelle Tecnologie.

Per garantire la sicurezza delle applicazioni l'affidatario dovrà rispettare le linee guida per lo sviluppo di software sicuro dell'AGID e garantire livelli di sicurezza **Application Risk (AR%)**, condivisi con Fondimpresa, valutati secondo il metodo Application Security Verification Standard 4.0 (ASVS) indicato al paragrafo 4.2.10 (Linee guida per il calcolo dell'Application Risk) del presente capitolato.

Lo sviluppo delle applicazioni deve essere effettuato conformemente a quanto previsto nel paragrafo 14 del presente capitolato, con riferimento alla protezione dei dati personali.

4.2.4 Accessibilità del software

L'Affidatario deve essere in grado di sviluppare il software rispettando la normativa concernente l'accessibilità (c.d. legge Stanca) e garantendo la conformità alle direttive AgID e le linee guida WCAG 2.1 per lo sviluppo di software accessibile. Pertanto, nei nuovi sviluppi devono esser tenuti presenti i criteri di accessibilità.

Annualmente dovrà essere eseguito un'analisi dello stato di accessibilità del REF (tramite la piattaforma Mauve++ del CNR o analogo strumento alternativo previo consenso del DEC dell'affidamento) ai fini della predisposizione, da parte di Fondimpresa, della "Dichiarazione di accessibilità" secondo normativa vigente.

4.2.5 Accesso per ispezioni di FONDIMPRESA

L'Affidatario deve consentire l'accesso a personale di FONDIMPRESA, o a soggetti terzi da questa espressamente autorizzati, con vincoli di riservatezza, al sistema di *versioning*, gestione e monitoraggio e controllo del servizio utilizzato dall'Affidatario.

4.2.6 Accettazione dei prodotti sviluppati

L'accettazione dei prodotti da parte di FONDIMPRESA avverrà al positivo completamento dell'esecuzione delle attività di collaudo per la cui esecuzione l'Affidatario si deve conformare a quanto previsto per la procedura di Collaudo al paragrafo 12 del presente Capitolato.

4.2.7 Linee guida per il conteggio della dimensione funzionale

Per la determinazione dell'effort di sviluppo, all'Affidatario è richiesto per ogni intervento:

- il conteggio dei Punti Funzione (PF) quale misura del volume dell'intervento erogato e un'analoga quantificazione in giorni uomo del mix di figure professionali sopra indicate (secondo quanto indicato in offerta);
- di fornire un documento di dettaglio sulla misurazione (stimata ed effettiva), che contenga i l'individuazione delle entità concettuali (associabili ai requisiti funzionali e informativi espressi dall'utente) previste dalla metodica PF e la loro complessità.

Entità di tipo transazionale:
- EI (External Input): Input esterni;
- EO (External Output): Output esterni;
- EQ (External inQuiry): Interrogazioni esterne;

Entità di tipo dati:
- ILF (Internal Logic File): File Logici Interni;
- EIF (External Interface File): File di Interfaccia Esterni.

Di ogni entità individuata (dati o transazionale), deve essere riportata la sua complessità (data da una scala nominale a tre valori: bassa, media, alta) e il numero di attributi (campi o DET – Data Element Type) individuati per ciascuna entità, nonché il numero di file logici (EIF e/o ILF) referenziati (FTR) – per le entità di tipo dati dovranno essere riportati invece il numero di tipi record logici (RET, Record Element Type).

La tabella seguente riporta il numero di ogni *unadjusted* PF per ognuna delle summenzionate entità in base al livello di complessità[1].
Si precisa che ovunque nel presente documento si trovi l'indicazione PF essa è da intendersi come *unadjusted* Function Point.

Complessità	EI	EO	EQ	ILF	EIF
Bassa	3	4	3	7	5
Media	4	5	4	10	7
Alta	6	7	6	15	10

Per le personalizzazioni di prodotti di mercato si dovrà utilizzare una metrica espressa esclusivamente in giorni uomo, documentando la previsione con un dettagliato piano di lavoro che descriva le attività (task) necessarie e le figure professionali impegnate con il relativo effort.

Il Fondo si riserva di adottare una procedura periodica, affidata a un'entità terza, di controllo a consuntivo degli effort proposti dal fornitore rispetto a quanto effettivamente consumato, in modo da poter mettere a punto eventuali correttivi. Eventuali discrepanze tra la valutazione del soggetto terzo e quelle fatturate dall'Affidatario saranno compensate a seguito di tale verifica.

4.2.8 Gestione dei lotti funzionali di SVILUPPO/MEV

Lo sviluppo e la manutenzione evolutiva sono suddivisi in Lotti funzionali, ognuno dei quali può essere assimilato, dal punto di vista del Fornitore, a un "progetto", la cui esecuzione è suddivisa in fasi, secondo il ciclo di sviluppo adottato.
L'esecuzione delle attività previste per il singolo lotto applicativo è espressamente subordinata alla approvazione da parte di Fondimpresa del documento di progettazione esecutiva contenente la

[1] "Linee guida sulla qualità dei beni e dei servizi ICT per la definizione e il governo dei contratti della PA", i Quaderni numero 11 anno II - gennaio 2005 a cura del CNIPA (Centro Nazionale per l'informatica nella Pubblica Amministrazione)

pianificazione ed il dettaglio delle attività e delle risorse impegnate (Punti Funzione) predisposto dal Fornitore sulla base delle specifiche indicate dal Fondo. Pertanto, in caso di mancata approvazione dei documenti di pianificazione e dettaglio da parte di Fondimpresa, il Fornitore non avrà nulla a pretendere per lo svolgimento delle attività necessarie alla loro elaborazione e non si darà luogo alla realizzazione delle attività ivi previste.

Il dimensionamento dei Lotti funzionali (sviluppo e manutenzione evolutiva) in termini di impegno progettuale dovrà essere effettuato, ove possibile, utilizzando la metrica dei Punti Funzione IFPUG **nella versione corrente,** e ricavando l'impegno in Giorni Uomo, ove richiesto, in base alla produttività stabilita nel presente capitolato (cfr. paragrafo 4.2). Laddove la metrica dei Punti Funzione **non risulti applicabile,** il dimensionamento degli Obiettivi sarà effettuato direttamente in Giorni Uomo.
Gli Obiettivi relativi a prodotti software di mercato, da integrare nel REF ed eventualmente personalizzare e/o adattare in termini di funzionalità, che non si prestano ad essere quantificati e conteggiati in Punti Funzione, in quanto non introducono funzionalità aggiuntive percepibili dall'utente, saranno dimensionati direttamente in Giorni Uomo a corpo, previo calcolo a priori del corrispettivo sulla base della stima delle figure professionali da impiegare.

Un cambiamento dei requisiti funzionali in corso d'opera (cioè sopraggiunti dopo l'approvazione del documento di analisi funzionale e della progettazione esecutiva) per un progetto di sviluppo o di manutenzione evolutiva può ripercuotersi in più modi sulle dimensioni del progetto: può richiedere di creare nuove funzionalità logiche o strutture dati e/o può avere ripercussioni sul modo in cui altre funzionalità logiche o strutture dati devono essere trasformate o cancellate. In particolare:

- nel caso di nuovi requisiti che richiedano lo sviluppo di nuove funzionalità, saranno contate in PF le funzionalità aggiunte;
- nel caso di modifica dei requisiti, in qualsiasi fase dell'obiettivo, se questa rientra nel volume di PF delle funzionalità realizzate indipendentemente dall'entità del cambiamento, non sarà riconosciuto alcun corrispettivo aggiuntivo. Se invece il volume di PF risulta aumentato, il corrispettivo sarà ricalcolato sulla base del nuovo dimensionamento;
- nel caso di requisiti cancellati in corso di progetto, saranno riconosciuti i PF ottenuti utilizzando la seguente formula: *PF riconosciuti = PF del requisito cancellato* x *% avanzamento cumulativo* dove la *% avanzamento cumulativo* da utilizzare è quella relativa all'ultima fase completata al momento della cancellazione **(NB: La mancata approvazione della progettazione esecutiva non ricade in tale casistica).**

Si precisa che il cambiamento dei requisiti nel corso del flusso di definizione è considerato **fisiologico.**

4.2.9 Modalità di valorizzazione e pagamento

Il pagamento, con le modalità previste nello schema di contratto, avverrà dopo il positivo collaudo, con le modalità previste nel paragrafo 12, e all'approvazione da parte del DEC della stima, qualificata in PF (**Unadjusted Function Point) ove possibile o in alternativa in gg/uomo**, effettiva a consuntivo. La mancata approvazione della stima a consuntivo comporta il mancato pagamento delle attività di sviluppo. Dovrà essere fornita una rendicontazione in merito alle attività svolte che dovrà contenere almeno le seguenti informazioni (tutti i parametri dovranno avere il dettaglio per il singolo progetto di sviluppo, manutenzione, personalizzazione o verifica cui si riferiscono):

- numero di interventi di sviluppo/manutenzione evolutiva totali richiesti;
- numero di interventi di sviluppo/manutenzione evolutiva totali;
- numero di interventi di sviluppo/manutenzione evolutiva totali residui (richiesti e non ancora completati) a fine periodo;
- numero totale di interventi di sviluppo/manutenzione evolutiva richiesti per area applicativa;
- numero totale di interventi di sviluppo/manutenzione evolutiva chiusi per area applicativa;
- volume totale in PF (e gg/uomo) degli interventi di sviluppo/manutenzione evolutiva completati nel periodo;

- volume totale in PF (e gg/uomo) degli interventi di sviluppo/manutenzione evolutiva completati da inizio contratto;
- volume totale stimato in PF (e gg/uomo) degli interventi di sviluppo/manutenzione evolutiva avviati e non ancora completati a fine periodo;
- risorse impiegate (numero, effort e tipologia).

Dovranno essere fornite le suddette informazioni e tutti i dati elementari relativi alle misure effettuate sul prodotto (ad es. dati relativi alla qualità degli oggetti realizzati rilevata nelle fasi di realizzazione e collaudo) e sul servizio erogato (ad es. numero di persone impegnate, effort speso ecc.).
Per le attività accessorie a quelle di sviluppo si applicherà una quantificazione in gg/uomo per un ammontare di PF (Unadjusted Function Point) calcolati come gg/uomo*2,2. Tali attività consistono a titolo esemplificativo e non esaustivo in:

- testing;
- collaudo;
- redazione della manualistica tecnica e manualistica d'utente;
- formazione.

Tali attività accessorie di **norma dovranno avere un effort non superiore** a quello di sviluppo determinato, ove possibile, secondo il metodo IFPUG. Importi superiori **dovranno essere dettagliatamente motivati e documentati** nella progettazione esecutiva.
Nel caso di realizzazione - su richiesta - di un prototipo funzionante, l'importo dei PF verrà maggiorato del 10%.

4.2.10 Linee guida per il calcolo dell'Application Risk

Per valutare il livello di sicurezza del software prodotto viene utilizzato l'*Application Risk percentuale* (AR%). L'AR% rappresenta la soglia massima attesa o accettata per il codice prodotto, e nel lungo periodo deve tendere a 0. Per calcolare l'AR% si utilizzano i 286 punti del metodo Application Security Verification Standard 4.0 (ASVS).

Section		Control	L1	L2	L3
V1: Architecture, Design and Threat Modeling Requirements					
V1.1 Secure Software Development Lifecycle Requirements					
V1	1.1.1	Verify the use of a secure software development lifecycle that addresses security in all stages of development.		x	x
V1	1.1.2	Verify the use of threat modeling for every design change or sprint planning to identify threats, plan for countermeasures, facilitate appropriate risk responses, and guide security testing.		x	x
V1	1.1.3	Verify that all user stories and features contain functional security constraints, such as "As a user, I should be able to view and edit my profile. I should not be able to view or edit anyone else's profile"		x	x
V1	1.1.4	Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.		x	x
V1	1.1.5	Verify definition and security analysis of the application's high-level architecture and all connected remote services.		x	x
V1	1.1.6	Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls.		x	x
V1	1.1.7	Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.		x	x
V1.2 Authentication Architectural Requirements					
V1	1.2.1	Verify the use of unique or special low-privilege operating system accounts for all application components, services, and servers.		x	x

V1	1.2.2	Verify that communications between application components, including APIs, middleware and data layers, are authenticated. Components should have the least necessary privileges needed.		x	x
V1	1.2.3	Verify that the application uses a single vetted authentication mechanism that is known to be secure, can be extended to include strong authentication, and has sufficient logging and monitoring to detect account abuse or breaches.		x	x
V1	1.2.4	Verify that all authentication pathways and identity management APIs implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.		x	x
V1.4 Access Control Architectural Requirements					
V1	1.4.1	Verify that trusted enforcement points such as at access control gateways, servers, and serverless functions enforce access controls. Never enforce access controls on the client.		x	x
V1	1.4.2	Verify that the chosen access control solution is flexible enough to meet the application's needs.		x	x
V1	1.4.3	Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.		x	x
V1	1.4.4	Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.		x	x
V1	1.4.5	Verify that attribute or feature-based access control is used whereby the code checks the user's authorization for a feature/data item rather than just their role. Permissions should still be allocated using roles.		x	x
V1.5 Input and Output Architectural Requirements					
V1	1.5.1	Verify that input and output requirements clearly define how to handle and process data based on type, content, and applicable laws, regulations, and other policy compliance.		x	x
V1	1.5.2	Verify that serialization is not used when communicating with untrusted clients. If this is not possible, ensure that adequate integrity controls (and possibly encryption if sensitive data is sent) are enforced to prevent deserialization attacks including object injection.		x	x
V1	1.5.3	Verify that input validation is enforced on a trusted service layer.		x	x
V1	1.5.4	Verify that output encoding occurs close to or by the interpreter for which it is intended.		x	x
V1.6 Cryptographic Architectural Requirements					
V1	1.6.1	Verify that there is an explicit policy for management of cryptographic keys and that a cryptographic key lifecycle follows a key management standard such as NIST SP 800-57.		x	x
V1	1.6.2	Verify that consumers of cryptographic services protect key material and other secrets by using key vaults or API based alternatives.		x	x
V1	1.6.3	Verify that all keys and passwords are replaceable and are part of a well-defined process to re-encrypt sensitive data.		x	x
V1	1.6.4	Verify that symmetric keys, passwords, or API secrets generated by or shared with clients are used only in protecting low risk secrets, such as encrypting local storage, or temporary ephemeral uses such as parameter obfuscation. Sharing secrets with clients is clear-text equivalent and architecturally should be treated as such.		x	x
V1.7 Errors, Logging and Auditing Architectural Requirements					
V1	1.7.1	Verify that a common logging format and approach is used across the system.		x	x

V1	1.7.2	Verify that logs are securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation.		x	x
V1.8 Data Protection and Privacy Architectural Requirements					
V1	1.8.1	Verify that all sensitive data is identified and classified into protection levels.		x	x
V1	1.8.2	Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.		x	x
V1.9 Communications Architectural Requirements					
V1	1.9.1	Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers.		x	x
V1	1.9.2	Verify that application components verify the authenticity of each side in a communication link to prevent person-in-the-middle attacks. For example, application components should validate TLS certificates and chains.		x	x
V1.10 Malicious Software Architectural Requirements					
V1	1.10.1	Verify that a source code control system is in use, with procedures to ensure that check-ins are accompanied by issues or change tickets. The source code control system should have access control and identifiable users to allow traceability of any changes.		x	x
V1.11 Business Logic Architectural Requirements					
V1	1.11.1	Verify the definition and documentation of all application components in terms of the business or security functions they provide.		x	x
V1	1.11.2	Verify that all high-value business logic flows, including authentication, session management and access control, do not share unsynchronized state.		x	x
V1	1.11.3	Verify that all high-value business logic flows, including authentication, session management and access control are thread safe and resistant to time-of-check and time-of-use race conditions.			x
V1.12 Secure File Upload Architectural Requirements					
V1	1.12.1	Verify that user-uploaded files are stored outside of the web root.		x	x
V1	1.12.2	Verify that user-uploaded files - if required to be displayed or downloaded from the application - are served by either octet stream downloads, or from an unrelated domain, such as a cloud file storage bucket. Implement a suitable content security policy to reduce the risk from XSS vectors or other attacks from the uploaded file.		x	x
V1.13 API Architectural Requirements					
This is a placeholder for future requirements.					
V1.14 Configuration Architectural Requirements					
V1	1.14.1	Verify the segregation of components of differing trust levels through well-defined security controls, firewall rules, API gateways, reverse proxies, cloud-based security groups, or similar mechanisms.		x	x
V1	1.14.2	Verify that if deploying binaries to untrusted devices makes use of binary signatures, trusted connections, and verified endpoints.		x	x
V1	1.14.3	Verify that the build pipeline warns of out-of-date or insecure components and takes appropriate actions.		x	x
V1	1.14.4	Verify that the build pipeline contains a build step to automatically build and verify the secure deployment of the application, particularly if the application infrastructure is software defined, such as cloud environment build scripts.		x	x
V1	1.14.5	Verify that application deployments adequately sandbox, containerize and/or isolate at the network level to delay and deter attackers from attacking other applications, especially when they are performing sensitive or dangerous actions such as deserialization.		x	x

V1	1.14.6	Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.		x	x
V2: Authentication Verification Requirements					
V2.1 Password Security Requirements					
V2	2.1.1	Verify that user set passwords are at least 12 characters in length.	x	x	x
V2	2.1.2	Verify that passwords 64 characters or longer are permitted.	x	x	x
V2	2.1.3	Verify that passwords can contain spaces and truncation is not performed. Consecutive multiple spaces MAY optionally be coalesced.	x	x	x
V2	2.1.4	Verify that Unicode characters are permitted in passwords. A single Unicode code point is considered a character, so 12 emoji or 64 kanji characters should be valid and permitted.	x	x	x
V2	2.1.5	Verify users can change their password.	x	x	x
V2	2.1.6	Verify that password change functionality requires the user's current and new password.	x	x	x
V2	2.1.7	Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password.	x	x	x
V2	2.1.8	Verify that a password strength meter is provided to help users set a stronger password.	x	x	x
V2	2.1.9	Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters.	x	x	x
V2	2.1.10	Verify that there are no periodic credential rotation or password history requirements.	x	x	x
V2	2.1.11	Verify that "paste" functionality, browser password helpers, and external password managers are permitted.	x	x	x
V2	2.1.12	Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as native functionality.	x	x	x
V2.2 General Authenticator Requirements					
V2	2.2.1	Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.	x	x	x
V2	2.2.2	Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.	x	x	x
V2	2.2.3	Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.	x	x	x

V2	2.2.4	Verify impersonation resistance against phishing, such as the use of multi-factor authentication, cryptographic devices with intent (such as connected keys with a push to authenticate), or at higher AAL levels, client-side certificates.			x
V2	2.2.5	Verify that where a credential service provider (CSP) and the application verifying authentication are separated, mutually authenticated TLS is in place between the two endpoints.			x
V2	2.2.6	Verify replay resistance through the mandated use of OTP devices, cryptographic authenticators, or lookup codes.			x
V2	2.2.7	Verify intent to authenticate by requiring the entry of an OTP token or user-initiated action such as a button press on a FIDO hardware key.			x
V2.3 Authenticator Lifecycle Requirements					
V2	2.3.1	Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.	x	x	x
V2	2.3.2	Verify that enrollment and use of subscriber-provided authentication devices are supported, such as a U2F or FIDO tokens.		x	x
V2	2.3.3	Verify that renewal instructions are sent with sufficient time to renew time bound authenticators.		x	x
V2.4 Credential Storage Requirements					
V2	2.4.1	Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.		x	x
V2	2.4.2	Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored.		x	x
V2	2.4.3	Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations.		x	x
V2	2.4.4	Verify that if bcrypt is used, the work factor SHOULD be as large as verification server performance will allow, typically at least 13.		x	x
V2	2.4.5	Verify that an additional iteration of a key derivation function is performed, using a salt value that is secret and known only to the verifier. Generate the salt value using an approved random bit generator [SP 800-90Ar1] and provide at least the minimum security strength specified in the latest revision of SP 800-131A. The secret salt value SHALL be stored separately from the hashed passwords (e.g., in a specialized device like a hardware security module).		x	x
V2.5 Credential Recovery Requirements					
V2	2.5.1	Verify that a system generated initial activation or recovery secret is not sent in clear text to the user.	x	x	x
V2	2.5.2	Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.	x	x	x
V2	2.5.3	Verify password credential recovery does not reveal the current password in any way.	x	x	x
V2	2.5.4	Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").	x	x	x
V2	2.5.5	Verify that if an authentication factor is changed or replaced, that the user is notified of this event.	x	x	x

V2	2.5.6	Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as TOTP or other soft token, mobile push, or another offline recovery mechanism.	x	x	x
V2	2.5.7	Verify that if OTP or multi-factor authentication factors are lost, that evidence of identity proofing is performed at the same level as during enrollment.		x	x
V2.6 Look-up Secret Verifier Requirements					
V2	2.6.1	Verify that lookup secrets can be used only once.		x	x
V2	2.6.2	Verify that lookup secrets have sufficient randomness (112 bits of entropy), or if less than 112 bits of entropy, salted with a unique and random 32-bit salt and hashed with an approved one-way hash.		x	x
V2	2.6.3	Verify that lookup secrets are resistant to offline attacks, such as predictable values.		x	x
V2.7 Out of Band Verifier Requirements					
V2	2.7.1	Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.	x	x	x
V2	2.7.2	Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.	x	x	x
V2	2.7.3	Verify that the out of band verifier authentication requests, codes, or tokens are only usable once, and only for the original authentication request.	x	x	x
V2	2.7.4	Verify that the out of band authenticator and verifier communicates over a secure independent channel.	x	x	x
V2	2.7.5	Verify that the out of band verifier retains only a hashed version of the authentication code.		x	x
V2	2.7.6	Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).		x	x
V2.8 Single or Multi Factor One Time Verifier Requirements					
V2	2.8.1	Verify that time-based OTPs have a defined lifetime before expiring.	x	x	x
V2	2.8.2	Verify that symmetric keys used to verify submitted OTPs are highly protected, such as by using a hardware security module or secure operating system based key storage.		x	x
V2	2.8.3	Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.		x	x
V2	2.8.4	Verify that time-based OTP can be used only once within the validity period.		x	x
V2	2.8.5	Verify that if a time-based multi factor OTP token is re-used during the validity period, it is logged and rejected with secure notifications being sent to the holder of the device.		x	x
V2	2.8.6	Verify physical single factor OTP generator can be revoked in case of theft or other loss. Ensure that revocation is immediately effective across logged in sessions, regardless of location.		x	x
V2	2.8.7	Verify that biometric authenticators are limited to use only as secondary factors in conjunction with either something you have and something you know.		o	x
V2.9 Cryptographic Software and Devices Verifier Requirements					
V2	2.9.1	Verify that cryptographic keys used in verification are stored securely and protected against disclosure, such as using a TPM or HSM, or an OS service that can use this secure storage.		x	x
V2	2.9.2	Verify that the challenge nonce is at least 64 bits in length, and statistically unique or unique over the lifetime of the cryptographic device.		x	x
V2	2.9.3	Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.		x	x
V2.10 Service Authentication Requirements					
V2	2.10.1	Verify that integration secrets do not rely on unchanging passwords, such as API keys or shared privileged accounts.		OS	HSM
V2	2.10.2	Verify that if passwords are required, the credentials are not a default account.		OS	HSM

V2	2.10.3	Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.		OS	HSM
V2	2.10.4	Verify passwords, integrations with databases and third-party systems, seeds and internal secrets, and API keys are managed securely and not included in the source code or stored within source code repositories. Such storage SHOULD resist offline attacks. The use of a secure software key store (L1), hardware trusted platform module (TPM), or a hardware security module (L3) is recommended for password storage.		OS	HSM
V3: Session Management Verification Requirements					
V3.1 Fundamental Session Management Requirements					
V3	3.1.1	Verify the application never reveals session tokens in URL parameters or error messages.	x	x	x
V3.2 Session Binding Requirements					
V3	3.2.1	Verify the application generates a new session token on user authentication.	x	x	x
V3	3.2.2	Verify that session tokens possess at least 64 bits of entropy.	x	x	x
V3	3.2.3	Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.	x	x	x
V3	3.2.4	Verify that session token are generated using approved cryptographic algorithms.		x	x
V3.3 Session Logout and Timeout Requirements					
V3	3.3.1	Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties.	x	x	x
V3	3.3.2	If authenticators permit users to remain logged in, verify that re-authentication occurs periodically both when actively used or after an idle period.	x	x	x
V3	3.3.3	Verify that the application terminates all other active sessions after a successful password change, and that this is effective across the application, federated login (if present), and any relying parties.		x	x
V3	3.3.4	Verify that users are able to view and log out of any or all currently active sessions and devices.		x	x
V3.4 Cookie-based Session Management					
V3	3.4.1	Verify that cookie-based session tokens have the 'Secure' attribute set.	x	x	x
V3	3.4.2	Verify that cookie-based session tokens have the 'HttpOnly' attribute set.	x	x	x
V3	3.4.3	Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks.	x	x	x
V3	3.4.4	Verify that cookie-based session tokens use "__Host-" prefix (see references) to provide session cookie confidentiality.	x	x	x
V3	3.4.5	Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible.	x	x	x
V3.5 Token-based Session Management					
V3	3.5.1	Verify the application does not treat OAuth and refresh tokens - on their own - as the presence of the subscriber and allows users to terminate trust relationships with linked applications.		x	x
V3	3.5.2	Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.		x	x

V3	3.5.3	Verify that stateless session tokens use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.		x	x
V3.6 Re-authentication from a Federation or Assertion					
V3	3.6.1	Verify that relying parties specify the maximum authentication time to CSPs and that CSPs re-authenticate the subscriber if they haven't used a session within that period.			x
V3	3.6.2	Verify that CSPs inform relying parties of the last authentication event, to allow RPs to determine if they need to re-authenticate the user.			x
V3.7 Defenses Against Session Management Exploits					
V3	3.7.1	Verify the application ensures a valid login session or requires re-authentication or secondary verification before allowing any sensitive transactions or account modifications.	x	x	x
V4: Access Control Verification Requirements					
V4.1 General Access Control Design					
V4	4.1.1	Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.	x	x	x
V4	4.1.2	Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.	x	x	x
V4	4.1.3	Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.	x	x	x
V4	4.1.4	Verify that the principle of deny by default exists whereby new users/roles start with minimal or no permissions and users/roles do not receive access to new features until access is explicitly assigned.	x	x	x
V4	4.1.5	Verify that access controls fail securely including when an exception occurs.	x	x	x
V4.2 Operation Level Access Control					
V4	4.2.1	Verify that sensitive data and APIs are protected against direct object attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	x	x	x
V4	4.2.2	Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.	x	x	x
V4.3 Other Access Control Considerations					
V4	4.3.1	Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.	x	x	x
V4	4.3.2	Verify that directory browsing is disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of file or directory metadata, such as Thumbs.db, .DS_Store, .git or .svn folders.	x	x	x
V4	4.3.3	Verify the application has additional authorization (such as step up or adaptive authentication) for lower value systems, and / or segregation of duties for high value applications to enforce anti-fraud controls as per the risk of application and past fraud.		x	x
V5: Validation, Sanitization and Encoding Verification Requirements					
V5.1 Input Validation Requirements					
V5	5.1.1	Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	x	x	x

V5	5.1.2	Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.	x	x	x
V5	5.1.3	Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (whitelisting).	x	x	x
V5	5.1.4	Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).	x	x	x
V5	5.1.5	Verify that URL redirects and forwards only allow whitelisted destinations, or show a warning when redirecting to potentially untrusted content.	x	x	x
V5.2 Sanitization and Sandboxing Requirements					
V5	5.2.1	Verify that all untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature.	x	x	x
V5	5.2.2	Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.		x	x
V5	5.2.3	Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.	x	x	x
V5	5.2.4	Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.	x	x	x
V5	5.2.5	Verify that the application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.	x	x	x
V5	5.2.6	Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, use whitelisting of protocols, domains, paths and ports.	x	x	x
V5	5.2.7	Verify that the application sanitizes, disables, or sandboxes user-supplied SVG scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.	x	x	x
V5	5.2.8	Verify that the application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.	x	x	x
V5.3 Output encoding and Injection Prevention Requirements					
V5	5.3.1	Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL Parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ã•ã•“ or O'Hara).	x	x	x
V5	5.3.2	Verify that output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled.	x	x	x
V5	5.3.3	Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.	x	x	x
V5	5.3.4	Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.	x	x	x
V5	5.3.5	Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.	x	x	x
V5	5.3.6	Verify that the application projects against JavaScript or JSON injection attacks, including for eval attacks, remote JavaScript includes, CSP bypasses, DOM XSS, and JavaScript expression evaluation.	x	x	x

V5	5.3.7	Verify that the application protects against LDAP Injection vulnerabilities, or that specific security controls to prevent LDAP Injection have been implemented.	x	x	x
V5	5.3.8	Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.	x	x	x
V5	5.3.9	Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.	x	x	x
V5	5.3.10	Verify that the application protects against XPath injection or XML injection attacks.	x	x	x
V5.4 Memory, String, and Unmanaged Code Requirements					
V5	5.4.1	Verify that the application uses memory-safe string, safer memory copy and pointer arithmetic to detect or prevent stack, buffer, or heap overflows.		x	x
V5	5.4.2	Verify that format strings do not take potentially hostile input, and are constant.		x	x
V5	5.4.3	Verify that sign, range, and input validation techniques are used to prevent integer overflows.		x	x
V5.5 Deserialization Prevention Requirements					
V5	5.5.1	Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering.	x	x	x
V5	5.5.2	Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XXE.	x	x	x
V5	5.5.3	Verify that deserialization of untrusted data is avoided or is protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).	x	x	x
V5	5.5.4	Verify that when parsing JSON in browsers or JavaScript-based back-ends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.	x	x	x
V6: Stored Cryptography Verification Requirements					
V6.1 Data Classification					
V6	6.1.1	Verify that regulated private data is stored encrypted while at rest, such as personally identifiable information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.		x	x
V6	6.1.2	Verify that regulated health data is stored encrypted while at rest, such as medical records, medical device details, or de-anonymized research records.		x	x
V6	6.1.3	Verify that regulated financial data is stored encrypted while at rest, such as financial accounts, defaults or credit history, tax records, pay history, beneficiaries, or de-anonymized market or research records.		x	x
V6.2 Algorithms					
V6	6.2.1	Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.	x	x	x
V6	6.2.2	Verify that industry proven or government approved cryptographic algorithms, modes, and libraries are used, instead of custom coded cryptography.		x	x
V6	6.2.3	Verify that encryption initialization vector, cipher configuration, and block modes are configured securely using the latest advice.		x	x
V6	6.2.4	Verify that random number, encryption or hashing algorithms, key lengths, rounds, ciphers or modes, can be reconfigured, upgraded, or swapped at any time, to protect against cryptographic breaks.		x	x
V6	6.2.5	Verify that known insecure block modes (i.e. ECB, etc.), padding modes (i.e. PKCS#1 v1.5, etc.), ciphers with small block sizes (i.e. Triple-DES, Blowfish, etc.), and weak hashing algorithms (i.e. MD5, SHA1, etc.) are not used unless required for backwards compatibility.		x	x

V6	6.2.6	Verify that nonces, initialization vectors, and other single use numbers must not be used more than once with a given encryption key. The method of generation must be appropriate for the algorithm being used.		x	x
V6	6.2.7	Verify that encrypted data is authenticated via signatures, authenticated cipher modes, or HMAC to ensure that ciphertext is not altered by an unauthorized party.			x
V6	6.2.8	Verify that all cryptographic operations are constant-time, with no 'short-circuit' operations in comparisons, calculations, or returns, to avoid leaking information.			x
V6.3 Random Values					
V6	6.3.1	Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved cryptographically secure random number generator when these random values are intended to be not guessable by an attacker.		x	x
V6	6.3.2	Verify that random GUIDs are created using the GUID v4 algorithm, and a cryptographically-secure pseudo-random number generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.		x	x
V6	6.3.3	Verify that random numbers are created with proper entropy even when the application is under heavy load, or that the application degrades gracefully in such circumstances.			x
V6.4 Secret Management					
V6	6.4.1	Verify that a secrets management solution such as a key vault is used to securely create, store, control access to and destroy secrets.		x	x
V6	6.4.2	Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations.		x	x
V7: Error Handling and Logging Verification Requirements					
V7.1 Log Content Requirements					
V7	7.1.1	Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form.	x	x	x
V7	7.1.2	Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy.	x	x	x
V7	7.1.3	Verify that the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures.		x	x
V7	7.1.4	Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens.		x	x
V7.2 Log Processing Requirements					
V7	7.2.1	Verify that all authentication decisions are logged, without storing sensitive session identifiers or passwords. This should include requests with relevant metadata needed for security investigations.		x	x
V7	7.2.2	Verify that all access control decisions can be logged and all failed decisions are logged. This should include requests with relevant metadata needed for security investigations.		x	x
V7.3 Log Protection Requirements					
V7	7.3.1	Verify that the application appropriately encodes user-supplied data to prevent log injection.		x	x
V7	7.3.2	Verify that all events are protected from injection when viewed in log viewing software.		x	x
V7	7.3.3	Verify that security logs are protected from unauthorized access and modification.		x	x
V7	7.3.4	Verify that time sources are synchronized to the correct time and time zone. Strongly consider logging only in UTC if systems are global to assist with post-incident forensic analysis.		x	x

V7.4 Error Handling					
V7	7.4.1	Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.	x	x	x
V7	7.4.2	Verify that exception handling (or a functional equivalent) is used across the codebase to account for expected and unexpected error conditions.		x	x
V7	7.4.3	Verify that a "last resort" error handler is defined which will catch all unhandled exceptions.		x	x
V8: Data Protection Verification Requirements					
V8.1 General Data Protection					
V8	8.1.1	Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.		x	x
V8	8.1.2	Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.		x	x
V8	8.1.3	Verify the application minimizes the number of parameters in a request, such as hidden fields, Ajax variables, cookies and header values.		x	x
V8	8.1.4	Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application.		x	x
V8	8.1.5	Verify that regular backups of important data are performed and that test restoration of data is performed.			x
V8	8.1.6	Verify that backups are stored securely to prevent data from being stolen or corrupted.			x
V8.2 Client-side Data Protection					
V8	8.2.1	Verify the application sets sufficient anti-caching headers so that sensitive data is not cached in modern browsers.	x	x	x
V8	8.2.2	Verify that data stored in client side storage (such as HTML5 local storage, session storage, IndexedDB, regular cookies or Flash cookies) does not contain sensitive data or PII.	x	x	x
V8	8.2.3	Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated.	x	x	x
V8.3 Sensitive Private Data					
V8	8.3.1	Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.	x	x	x
V8	8.3.2	Verify that users have a method to remove or export their data on demand.	x	x	x
V8	8.3.3	Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.	x	x	x
V8	8.3.4	Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data.	x	x	x
V8	8.3.5	Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.		x	x
V8	8.3.6	Verify that sensitive information contained in memory is overwritten as soon as it is no longer required to mitigate memory dumping attacks, using zeroes or random data.		x	x
V8	8.3.7	Verify that sensitive or private information that is required to be encrypted, is encrypted using approved algorithms that provide both confidentiality and integrity.		x	x
V8	8.3.8	Verify that sensitive personal information is subject to data retention classification, such that old or out of date data is deleted automatically, on a schedule, or as the situation requires.		x	x
V9: Communications Verification Requirements					
V9.1 Communications Security Requirements					

V9	9.1.1	Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols.	x	x	x
V9	9.1.2	Verify using online or up to date TLS testing tools that only strong algorithms, ciphers, and protocols are enabled, with the strongest algorithms and ciphers set as preferred.	x	x	x
V9	9.1.3	Verify that old versions of SSL and TLS protocols, algorithms, ciphers, and configuration are disabled, such as SSLv2, SSLv3, or TLS 1.0 and TLS 1.1. The latest version of TLS should be the preferred cipher suite.	x	x	x
V9.2 Server Communications Security Requirements					
V9	9.2.1	Verify that connections to and from the server use trusted TLS certificates. Where internally generated or self-signed certificates are used, the server must be configured to only trust specific internal CAs and specific self-signed certificates. All others should be rejected.		x	x
V9	9.2.2	Verify that encrypted communications such as TLS is used for all inbound and outbound connections, including for management ports, monitoring, authentication, API, or web service calls, database, cloud, serverless, mainframe, external, and partner connections. The server must not fall back to insecure or unencrypted protocols.		x	x
V9	9.2.3	Verify that all encrypted connections to external systems that involve sensitive information or functions are authenticated.		x	x
V9	9.2.4	Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.		x	x
V9	9.2.5	Verify that back-end TLS connection failures are logged.			x
V10: Malicious Code Verification Requirements					
V10.1 Code Integrity Controls					
V10	10.1.1	Verify that a code analysis tool is in use that can detect potentially malicious code, such as time functions, unsafe file operations and network connections.			x
V10.2 Malicious Code Search					
V10	10.2.1	Verify that the application source code and third party libraries do not contain unauthorized phone home or data collection capabilities. Where such functionality exists, obtain the user's permission for it to operate before collecting any data.		x	x
V10	10.2.2	Verify that the application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.		x	x
V10	10.2.3	Verify that the application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered.			x
V10	10.2.4	Verify that the application source code and third party libraries does not contain time bombs by searching for date and time related functions.			x
V10	10.2.5	Verify that the application source code and third party libraries does not contain malicious code, such as salami attacks, logic bypasses, or logic bombs.			x
V10	10.2.6	Verify that the application source code and third party libraries do not contain Easter eggs or any other potentially unwanted functionality.			x
V10.3 Deployed Application Integrity Controls					
V10	10.3.1	Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.	x	x	x
V10	10.3.2	Verify that the application employs integrity protections, such as code signing or sub-resource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.	x	x	x

V10	10.3.3	Verify that the application has protection from sub-domain takeovers if the application relies upon DNS entries or DNS sub-domains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (autogen-bucket-id.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.	x	x	x
V11: Business Logic Verification Requirements					
V11.1 Business Logic Security Requirements					
V11	11.1.1	Verify the application will only process business logic flows for the same user in sequential step order and without skipping steps.	x	x	x
V11	11.1.2	Verify the application will only process business logic flows with all steps being processed in realistic human time, i.e. transactions are not submitted too quickly.	x	x	x
V11	11.1.3	Verify the application has appropriate limits for specific business actions or transactions which are correctly enforced on a per user basis.	x	x	x
V11	11.1.4	Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.	x	x	x
V11	11.1.5	Verify the application has business logic limits or validation to protect against likely business risks or threats, identified using threat modelling or similar methodologies.	x	x	x
V11	11.1.6	Verify the application does not suffer from "time of check to time of use" (TOCTOU) issues or other race conditions for sensitive operations.		x	x
V11	11.1.7	Verify the application monitors for unusual events or activity from a business logic perspective. For example, attempts to perform actions out of order or actions which a normal user would never attempt.		x	x
V11	11.1.8	Verify the application has configurable alerting when automated attacks or unusual activity is detected.		x	x
V12: File and Resources Verification Requirements					
V12.1 File Upload Requirements					
V12	12.1.1	Verify that the application will not accept large files that could fill up storage or cause a denial of service attack.	x	x	x
V12	12.1.2	Verify that compressed files are checked for "zip bombs" - small input files that will decompress into huge files thus exhausting file storage limits.		x	x
V12	12.1.3	Verify that a file size quota and maximum number of files per user is enforced to ensure that a single user cannot fill up the storage with too many files, or excessively large files.		x	x
V12.2 File Integrity Requirements					
V12	12.2.1	Verify that files obtained from untrusted sources are validated to be of expected type based on the file's content.		x	x
V12.3 File execution Requirements					
V12	12.3.1	Verify that user-submitted filename metadata is not used directly with system or framework file and URL API to protect against path traversal.	x	x	x
V12	12.3.2	Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure, creation, updating or removal of local files (LFI).	x	x	x
V12	12.3.3	Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure or execution of remote files (RFI), which may also lead to SSRF.	x	x	x
V12	12.3.4	Verify that the application protects against reflective file download (RFD) by validating or ignoring user-submitted filenames in a JSON, JSONP, or URL parameter, the response Content-Type header should be set to text/plain, and the Content-Disposition header should have a fixed filename.	x	x	x

V12	12.3.5	Verify that untrusted file metadata is not used directly with system API or libraries, to protect against OS command injection.	x	x	x
V12	12.3.6	Verify that the application does not include and execute functionality from untrusted sources, such as unverified content distribution networks, JavaScript libraries, node npm libraries, or server-side DLLs.		x	x
V12.4 File Storage Requirements					
V12	12.4.1	Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions, preferably with strong validation.	x	x	x
V12	12.4.2	Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload of known malicious content.	x	x	x
V12.5 File Download Requirements					
V12	12.5.1	Verify that the web tier is configured to serve only files with specific file extensions to prevent unintentional information and source code leakage. For example, backup files (e.g. .bak), temporary working files (e.g. .swp), compressed files (.zip, .tar.gz, etc) and other extensions commonly used by editors should be blocked unless required.	x	x	x
V12	12.5.2	Verify that direct requests to uploaded files will never be executed as HTML/JavaScript content.	x	x	x
V12.6 SSRF Protection Requirements					
V12	12.6.1	Verify that the web or application server is configured with a whitelist of resources or systems to which the server can send requests or load data/files from.	x	x	x
V13: API and Web Service Verification Requirements					
V13.1 Generic Web Service Security Verification Requirements					
V13	13.1.1	Verify that all application components use the same encodings and parsers to avoid parsing attacks that exploit different URI or file parsing behavior that could be used in SSRF and RFI attacks.	x	x	x
V13	13.1.2	Verify that access to administration and management functions is limited to authorized administrators.	x	x	x
V13	13.1.3	Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.	x	x	x
V13	13.1.4	Verify that authorization decisions are made at both the URI, enforced by programmatic or declarative security at the controller or router, and at the resource level, enforced by model-based permissions.		x	x
V13	13.1.5	Verify that requests containing unexpected or missing content types are rejected with appropriate headers (HTTP response status 406 Unacceptable or 415 Unsupported Media Type).		x	x
V13.2 RESTful Web Service Verification Requirements					
V13	13.2.1	Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.	x	x	x
V13	13.2.2	Verify that JSON schema validation is in place and verified before accepting input.	x	x	x
V13	13.2.3	Verify that RESTful web services that utilize cookies are protected from Cross-Site Request Forgery via the use of at least one or more of the following: triple or double submit cookie pattern (see references), CSRF nonces, or ORIGIN request header checks.	x	x	x
V13	13.2.4	Verify that REST services have anti-automation controls to protect against excessive calls, especially if the API is unauthenticated.		x	x
V13	13.2.5	Verify that REST services explicitly check the incoming Content-Type to be the expected one, such as application/xml or application/JSON.		x	x

V13	13.2.6	Verify that the message headers and payload are trustworthy and not modified in transit. Requiring strong encryption for transport (TLS only) may be sufficient in many cases as it provides both confidentiality and integrity protection. Per-message digital signatures can provide additional assurance on top of the transport protections for high-security applications but bring with them additional complexity and risks to weigh against the benefits.		x	x
V13.3 SOAP Web Service Verification Requirements					
V13	13.3.1	Verify that XSD schema validation takes place to ensure a properly formed XML document, followed by validation of each input field before any processing of that data takes place.	x	x	x
V13	13.3.2	Verify that the message payload is signed using WS-Security to ensure reliable transport between client and service.		x	x
V13.4 GraphQL and other Web Service Data Layer Security Requirements					
V13	13.4.1	Verify that query whitelisting or a combination of depth limiting and amount limiting should be used to prevent GraphQL or data layer expression denial of service (DoS) as a result of expensive, nested queries. For more advanced scenarios, query cost analysis should be used.		x	x
V13	13.4.2	Verify that GraphQL or other data layer authorization logic should be implemented at the business logic layer instead of the GraphQL layer.		x	x
V14: Configuration Verification Requirements					
V14.1 Build					
V14	14.1.1	Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.		x	x
V14	14.1.2	Verify that compiler flags are configured to enable all available buffer overflow protections and warnings, including stack randomization, data execution prevention, and to break the build if an unsafe pointer, memory, format string, integer, or string operations are found.		x	x
V14	14.1.3	Verify that server configuration is hardened as per the recommendations of the application server and frameworks in use.		x	x
V14	14.1.4	Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.		x	x
V14	14.1.5	Verify that authorized administrators can verify the integrity of all security-relevant configurations to detect tampering.			x
V14.2 Dependency					
V14	14.2.1	Verify that all components are up to date, preferably using a dependency checker during build or compile time.	x	x	x
V14	14.2.2	Verify that all unneeded features, documentation, samples, configurations are removed, such as sample applications, platform documentation, and default or example users.	x	x	x
V14	14.2.3	Verify that if application assets, such as JavaScript libraries, CSS stylesheets or web fonts, are hosted externally on a content delivery network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.	x	x	x
V14	14.2.4	Verify that third party components come from pre-defined, trusted and continually maintained repositories.		x	x
V14	14.2.5	Verify that an inventory catalog is maintained of all third party libraries in use.		x	x
V14	14.2.6	Verify that the attack surface is reduced by sandboxing or encapsulating third party libraries to expose only the required behaviour into the application.		x	x
V14.3 Unintended Security Disclosure Requirements					

V14	14.3.1	Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures.	x	x	x
V14	14.3.2	Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.	x	x	x
V14	14.3.3	Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.	x	x	x
V14.4 HTTP Security Headers Requirements					
V14	14.4.1	Verify that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8, ISO 8859-1).	x	x	x
V14	14.4.2	Verify that all API responses contain Content-Disposition: attachment; filename="api.json" (or other appropriate filename for the content type).	x	x	x
V14	14.4.3	Verify that a content security policy (CSPv2) is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.	x	x	x
V14	14.4.4	Verify that all responses contain X-Content-Type-Options: nosniff.	x	x	x
V14	14.4.5	Verify that HTTP Strict Transport Security headers are included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.	x	x	x
V14	14.4.6	Verify that a suitable "Referrer-Policy" header is included, such as "no-referrer" or "same-origin".	x	x	x
V14	14.4.7	Verify that a suitable X-Frame-Options or Content-Security-Policy: frame-ancestors header is in use for sites where content should not be embedded in a third-party site.	x	x	x
V14.5 Validate HTTP Request Header Requirements					
V14	14.5.1	Verify that the application server only accepts the HTTP methods in use by the application or API, including pre-flight OPTIONS.	x	x	x
V14	14.5.2	Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.	x	x	x
V14	14.5.3	Verify that the cross-domain resource sharing (CORS) Access-Control-Allow-Origin header uses a strict white-list of trusted domains to match against and does not support the "null" origin.	x	x	x
V14	14.5.4	Verify that HTTP headers added by a trusted proxy or SSO devices, such as a bearer token, are authenticated by the application.		x	x

Ogni sviluppo viene classificato in base al livello di sicurezza:

- Level 1 - low assurance levels;
- Level 2 - applications that contain sensitive data, which requires protection, recommended level for most apps;
- Level 3 - critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.

Per ogni punto che si decide di applicare al codice da sviluppare viene definito uno stato iniziale (*Maturity current*) e un target (*Maturity target*), con punteggio da 0 a 5.

Level	Maturity	Description
0	Non-existing	Requirement is not selected. We do not believe this is a problem that needs to be solved in our application.
1	Initial	We are aware of the existence of the requirement and the need to study it. However, there is no implementation, and further consideration is needed before going into development.
2	Defined	Implementation has been developed, but relies heavily on individual knowledge, and where a probability of omission exists.
3	Standardised	A standard for implementation and procedures has been documented and communicated across teams, including awareness and training where needed.
4	Verified	Implementation of control has been tested and verified across entire application. The processes are constantly improved and correspond to good practice. Automation and the use of tools are still limited or partial.
5	Automated	The implementation is verified at all times through automated testing and integration with development workflow, and has reached the recommended level of best practices.

La differenza tra *Maturity current* e *Maturity target* rappresenta il Rischio residuo (*Residual Risk*). L'AR% si calcola come il rapporto tra il rischio residuo totale e il punteggio target totale (*Total target maturity*).
L'affidatario in fase di valutazione dell'effort e di analisi delle specifiche funzionali deve produrre la classificazione (L1, L2, L3), l'elenco dei check da attivare e il *Total target maturity* concordati con Fondimpresa. L'affidatario potrà dare evidenza della corretta applicazione delle best practice di sicurezza e coding mediante l'utilizzo di software per l'analisi statica del codice e dell'application security.
Periodicamente Fondimpresa definisce degli standard, che dovranno essere rispettati per gli sviluppi che iniziano da quel momento. Inoltre, prima del collaudo di accettazione, il fornitore deve dare evidenza del rispetto dell'*AR%* definito minimo. Fondimpresa si riserva di effettuare verifiche sul rispetto di tale parametro, anche facendo ricorso a consulenti esterni e/o a strumenti software per l'Application Security Testing.

4.3 MAD/MAC e Help Desk di secondo livello

Il servizio qui descritto si applica al software REF, sia quello sviluppato precedentemente al contratto sia ogni sua successiva modifica dovuta alle attività svolte nell'ambito dell'intero affidamento, senza che ciò comporti, per questo servizio, alcuna variazione nel corrispettivo economico riconosciuto all'Affidatario che si considera invariabile e omnicomprensivo. All'interno di tale servizio si devono ritenere **interamente ricompresi, a carico dell'affidatario, i canoni di manutenzione** (maintenance del relativo produttore) di tutte le applicazioni facenti parte dell'architettura descritta al punto 3 del presente Capitolato.

La manutenzione correttiva comprende le attività necessarie per la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti delle procedure e dei programmi che impediscono o che potrebbero impedire la normale operatività dei servizi erogati, comprese le attività necessarie per il ripristino dei livelli minimi di operatività anche attraverso il ricorso a soluzioni temporanee.
Per "difetto" si intende un errore presente nel software, latente finché non rilevato, in quanto dà luogo ad un malfunzionamento. La manutenzione correttiva è, quindi, attivata con lo scopo di rimuovere i difetti del software e di conseguenza i malfunzionamenti rilevati.
Tutto il software su cui sono stati effettuati interventi di sviluppo e/o manutenzione deve essere consegnato a Fondimpresa in formato sorgente e si intende di piena proprietà del Fondo, oltre che coperto da garanzia per l'intera durata contrattuale e per almeno 12 mesi successivi, a far data dal collaudo positivo con accettazione da parte del DEC, anche se questi ricadono oltre la fine del contratto.
Le attività di manutenzione correttiva, svolte in periodo di validità della garanzia, sono da intendersi a totale carico del Fornitore, compresi gli interventi di aggiornamento e di allineamento della documentazione e delle componenti a corredo impattate dall'intervento.
I malfunzionamenti le cui cause non sono imputabili a difetti presenti nel software applicativo, ma ad errori tecnici, operativi o d'integrazione con altri sistemi (ad esempio interruzione di rete, uso improprio delle funzioni ecc.), non rientrano nel servizio di manutenzione correttiva, ma nel Servizio di Hosting e conduzione tecnica.
Gli interventi di MAC, di norma, non comportano la modifica della baseline delle applicazioni; nei casi di eccezione, il Fornitore è tenuto a fornire tutti gli elementi di misurazione necessari a mantenere aggiornata la baseline delle applicazioni.

Gli interventi di **manutenzione evolutiva di dimensione inferiore o uguale a 25 PF** rientrano nel presente servizio essendo da considerarsi come MAD e non in quello di *Sviluppo software e MEV*.

Il servizio riguarda le attività di manutenzione[2] correttiva, adeguativa e migliorativa del registro REF (attuale sistema e futuri sviluppi) da applicarsi:

- all'infrastruttura SW di base, di comunicazione e middleware costituente il sistema;
- a tutto il software applicativo realizzato dall'Affidatario, nonché a tutti i pacchetti software forniti per l'erogazione di tutti i servizi richiesti;
- al patrimonio informativo del sistema;
- al mantenimento e alla verifica della compatibilità della PWA con gli aggiornamenti dei sistemi operativi mobile (iOS e Android) e con i nuovi hardware.

Nell'ambito di tale servizio deve essere garantita l'attività di aggiornamento di tutti i prodotti software e librerie, con cadenza almeno semestrale, eccetto quelli critici per la sicurezza che dovranno essere installati non appena resi disponibili dai produttori.

Nel dimensionamento del servizio, l'Affidatario dovrà prevedere (i documenti ivi richiesti si riferiscono anche alle esigenze dell'infrastruttura di hosting prevista al successivo paragrafo 4.4):

- la predisposizione trimestrale, di "note evolutive" attraverso le quali dovranno essere illustrati gli interventi da apportare al software applicativo ed alle eventuali espansioni hardware che allo scopo si ritenessero necessarie;
- la predisposizione mensile di report statistici finalizzati ad evidenziare:
    - l'elenco delle inoperatività/malfunzionamenti riscontrati e la MEV di riferimento almeno per tutte le modifiche evolutive implementate durante il periodo contrattuale;
    - la rilevazione analitica dell'attività di manutenzione effettuata (sia ordinaria sia straordinaria), con l'evidenza dei tempi di intervento e di ripristino dei malfunzionamenti;

[2] La manutenzione dell'hardware dovrà essere eseguita dall'Aggiudicatario, nell'ambito del servizio di hosting. L'Aggiudicatario dovrà curare gli interventi di ripristino facendo eventualmente ricorso al servizio di assistenza del produttore.

- l'esecuzione periodica degli interventi di manutenzione ordinaria riguardanti tutte le componenti del sistema precedentemente elencate.

Il servizio dovrà essere espletato in accordo con un *"Piano di Manutenzione adeguativa e correttiva"* ed un *"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello"* da prodursi come parte integrante dell'offerta tecnica, indicando il numero di risorse professionali, comunque non inferiore a una, che compongono il team dedicato, **fornendo i relativi curricula professionali,** fermo restando che tali risorse possono essere impiegate in tutto o in parte in relazione alle esigenze di manutenzione e alla pianificazione condivisa con FONDIMPRESA.

Il *"Piano di Manutenzione adeguativa e correttiva"* deve contenere almeno:

- la descrizione delle attività di manutenzione ordinaria, con l'indicazione analitica delle operazioni previste per ciascuna delle componenti indicate e della periodicità di esecuzione di tali operazioni;
- la descrizione delle modalità di aggiornamento di tutti prodotti software e librerie sia per quanto riguarda gli aggiornamenti di sicurezza sia per gli altri aggiornamenti;
- la descrizione delle modalità di gestione delle chiamate di assistenza per interventi di manutenzione straordinaria, nonché gli accorgimenti che l'Affidatario intende adottare per garantire i livelli di servizio indicati nel prosieguo del presente Capitolato;
- la struttura dei report statistici finalizzati a facilitare il controllo e la verifica, da parte di FONDIMPRESA, delle attività svolte dall'Affidatario nonché dei livelli di servizio erogati dal sistema;
- i livelli di servizio offerti, se migliorativi rispetto a quelli di illustrati nel prosieguo del presente Capitolato tecnico.

Nel ***"Piano di Manutenzione adeguativa e correttiva"*** devono essere altresì illustrate le modalità di svolgimento dell'affiancamento per subentro, per una durata non inferiore a un mese, alla conclusione o eventuale risoluzione anticipata del contratto stipulato con la presente procedura.

4.3.1 Help Desk di secondo livello

All'interno del servizio di Manutenzione ed Assistenza è richiesto lo svolgimento delle attività di ***Help Desk di secondo livello,*** come di seguito sinteticamente riportato.

Criteri di attivazione: attraverso il sistema di trouble-ticketing esistente. Fondimpresa, o suoi incaricati, può comunque attivare la comunicazione tramite e-mail, e l'helpdesk provvederà a tracciare tale richiesta sul sistema di trouble ticketing esistente (attualmente VTiger).

L'Help Desk di secondo livello deve:

- raccogliere e registrare le richieste di assistenza assegnando la priorità;
- risolvere problematiche non note e definire *best practice* per soluzioni standardizzate;
- smistare al servizio di Manutenzione HW e SW di base i problemi non risolvibili nell'ambito dell'Help Desk di 2° livello;
- controllare i processi di risoluzione attivati e verificarne gli esiti;
- informare gli utenti interessati e Fondimpresa sullo stato di avanzamento delle richieste;
- analizzare le statistiche sugli interventi, al fine di identificare i fabbisogni e definire azioni di prevenzione dei problemi;
- effettuare interventi per casistiche non gestite dall'interfaccia applicativa;
- garantire supporto sistemistico (database administrator) per attività a supporto delle esigenze di monitoraggio e statistiche del Fondo;
- effettuare fix dati richieste da Fondimpresa;
- gestire le emergenze;
- gestire le procedure di escalation.

Le predette attività di secondo livello dovranno essere svolte secondo un ***"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello"*** che costituirà parte **integrante dell'offerta tecnica,** in accordo con le seguenti indicazioni:

- il servizio offerto dovrà essere comprensivo:

- della reportistica mensile da inviare a Fondimpresa che metta in evidenza le attività complessive erogate dalla struttura di Help Desk:
  - le questioni sollevate dagli utenti sulla base della categorizzazione approvata da Fondimpresa;
  - i ticket ancora aperti e quelli chiusi, con l'oggetto e i relativi **tempi di risoluzione e lavorazione**.

Il servizio dovrà essere eseguito da ***almeno n. 1 operatore di 2° livello.***
Devono essere presenti un numero telefonico e un canale mail dedicati disponibili H24 7/7 per segnalazioni bloccanti e non bloccanti urgenti da parte del DEC del contratto.
Con cadenza trimestrale FONDIMPRESA analizzerà l'andamento del servizio di Help Desk e potrà chiedere l'aumento o la diminuzione degli operatori di secondo livello con la conseguente rimodulazione dei costi previsti. Tale variazione dimensionale:

- potrà essere disposta a insindacabile giudizio di Fondimpresa per un massimo di n. 1 volta ogni n. 3 mesi;
- dovrà avvenire in modo automatico entro 15 giorni solari dalla richiesta di Fondimpresa, salvo diverse richieste del Fondo in senso dilatorio;
- in ogni richiesta, Fondimpresa potrà disporre il dimensionamento dell'Help Desk entro i seguenti margini, senza altri vincoli rispetto al dimensionamento precedente tra un minimo di n. 1 a un massimo di n. 3 operatori.

Il servizio di Help Desk dovrà essere svolto in conformità alle specifiche ITIL V4 ed in accordo con un ***"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello"*** da prodursi in Allegato all'offerta tecnica.
Il ***"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello",*** deve contenere almeno:

- la descrizione delle modalità di "tracing" del problema (apertura, gestione e chiusura del "trouble-ticket");
- la struttura del report statistico e informativo da inserire nel report SAL mensile destinato al personale di FONDIMPRESA per il controllo e la verifica delle attività svolte. Devono essere indicati almeno:
  - produttività degli operatori;
  - tempi medi di risoluzione dei ticket;
  - tasso di risoluzione al primo contatto;
  - tasso di ricorrenza delle diverse casistiche dei ticket sulla base della categorizzazione approvata da Fondimpresa, con relativo commento;
- i livelli di servizio offerti;
- la descrizione del numero degli operatori e dei profili professionali impiegati in relazione all'Help Desk.

Nel ***"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello"*** devono essere altresì illustrate le modalità di svolgimento dell'affiancamento per subentro, per una durata non inferiore a un mese, nel periodo immediatamente successivo alla conclusione del contratto stipulato con la presente procedura.
Nell'ambito della valutazione delle competenze del personale di presidio, costituirà titolo di merito il possesso delle seguenti competenze e certificazioni:

- esperienze specifiche ed anni di esperienza in ruoli analoghi per complessità e tipologia di applicazioni e attività;
- certificazione ITIL Foundation, certificazione ITIL a livello avanzato sui processi di supporto/service management;
- certificazioni sui sistemi operativi/base dati e sulle tecnologie di sviluppo.

4.3.2 Modalità di valorizzazione e pagamento

Per il presente servizio è previsto un canone trimestrale che verrà pagato posticipatamente, all'esito delle verifiche condotte da parte di FONDIMPRESA, secondo le modalità previste dallo schema di contratto.

4.4 Hosting conduzione e manutenzione HW/SW

Il servizio di Hosting include di fatto un insieme di attività che consistono principalmente in:

- messa a disposizione di infrastrutture logistiche appropriate, progettazione e realizzazione di infrastrutture informatiche chiavi in mano per il REF. La fornitura delle componenti architetturali necessarie per l'erogazione del servizio dovrà essere in solo uso, la proprietà rimarrà dell'Affidatario;
- predisposizione di un sistema di backup e ripristino dati;
- predisposizione di un'architettura di Disaster Recovery che dovrà essere dislocata presso un sito secondario, geograficamente separato, mantenendo la stessa struttura logico/fisica e la stessa capacità elaborativa e di connettività del sito principale di Produzione;
- connessioni ad internet garantite con istradamenti diversificati (banda minima garantita di 500Mb/s e con possibilità di picchi fino a 1Gb/s e possibilità di estendere (nell'arco della durata contrattuale) a richiesta di FONDIMPRESA tale connettività ad una banda minima di 1Gb/s con possibilità di picchi fino a 2Gb/s);
- connessioni sicure tramite VPN lan-to-lan e/o VPN client-to-lan per l'accesso all'infrastruttura e/o ai singoli servizi;
- conduzione tecnica e operativa delle piattaforme impiegate (manutenzione HW e SW, backup dei dati, deployment dell'applicazione e relative evoluzioni ecc.);
- gestione dei cambiamenti di configurazione preposti al funzionamento del servizio con possibilità di:
  - definire le politiche e i processi di "change management" e le procedure di ripristino;
  - valutare preliminarmente l'impatto dei "change" sull'operatività dei server in uso suggerendo le soluzioni atte a minimizzare i rischi del piano di modifica;
  - garantire la coerenza dei "change" effettuati;
  - assicurare l'integrità e la tracciabilità di tutti i "change" che modifichino le configurazioni delle piattaforme (di base ed applicative) dei servizi;
  - tener traccia documentale di tutti i "change";
  - fornire assistenza alla conduzione operativa in caso di necessità;
  - esecuzione di test volti a verificare la piena funzionalità dei componenti infrastrutturali (es. ram, storage, cpu ecc.) e applicativi (servizio, pagina e/o applicazione web);
  - monitoraggio dei sistemi, rilevazione e risoluzione di malfunzionamenti hardware e software allo scopo di garantire un'erogazione del servizio corrispondente ai requisiti espressi da Fondimpresa. Tale attività richiede:
    - il monitoraggio costante della disponibilità dei Server;
    - il controllo della stabilità del sistema, dei servizi attivi e delle funzionalità dei componenti del portale (Application server, web server, DB server, applicazioni, ecc.);
    - l'analisi dell'utilizzo dei server;
    - il monitoraggio, la raccolta e la storicizzazione dei valori del carico dei server su base oraria, giornaliera e mensile, allo scopo di garantire l'efficienza di tutte le componenti (CPU, memorie, BUS di sistema e dispositivi di I/O ecc.), al fine di determinare possibili aree di inefficienza e/o colli di bottiglia dell'intera infrastruttura;
- gestione della sicurezza perimetrale e *load balacing* applicativo;
- esecuzione periodica di Vulnerability Assessment, Penetration Test e relative attività di correzione e messa in sicurezza (con periodicità non superiore a un anno);
- configurazione e monitoraggio di eventuali servizi di replica dei DB verso istanze remote collegate in VPN.

4.4.1 Continuità e reportistica del servizio

Le applicazioni in Hosting e i servizi di connettività devono essere attivi, raggiungibili ed utilizzabili 7 gg su 7, h24 senza interruzione, salvo diversa indicazione di Fondimpresa, con un livello di disponibilità del datacenter come indicato nel paragrafo 4.4.6 e con un livello di disponibilità totale come riportato nel paragrafo 9.2.

Il tempo massimo di ripartenza dei Servizi (RTO) in caso di incidente o interruzione è stabilito in 8 ore dalla rilevazione dell'evento di indisponibilità (Indicatori di qualità della fornitura). La soglia di tolleranza per il ripristino dei dati (RPO) è stabilito in 4 ore.
Deve essere fornito un dettagliato piano di Disaster Recovery come parte integrante dell'offerta all'interno del ***"Piano di Hosting, conduzione e manutenzione HW/SW"***.
Ogni richiesta di change, di incident report o di informativa dovrà essere inviata da Fondimpresa attraverso lo strumento di tracciatura degli interventi di Sicurezza e Identity Management segnalando l'oggetto di riferimento, il tipo e il dettaglio della richiesta. Le segnalazioni di change e di incident, che possono essere anticipate in italiano via telefono e/o e-mail, dovranno essere formalizzate e inviate a Fondimpresa dal referente unico indicato dal fornitore; sarà responsabilità del Fornitore aggiornare le informazioni sugli strumenti di supporto degli interventi fino alla chiusura dell'intervento stesso. Il fornitore dovrà tenere aggiornato e rendere disponibile a Fondimpresa un registro degli incidenti la cui struttura, verrà concordata con Fondimpresa entro una settimana lavorativa dall'avvio del contratto.
Il Fornitore dovrà produrre un Report delle attività svolte sugli strumenti di tracciatura e gestione delle richieste di intervento secondo le modalità e tempistiche definite in offerta.
Qualsiasi pianificazione di attività che abbiano impatto sul servizio erogato dovrà essere approvata formalmente da Fondimpresa attraverso verbale o lettera di approvazione.

Il servizio di Hosting, conduzione tecnica e manutenzione preventiva, correttiva ed adeguativa, deve coprire l'intera durata del contratto (36 mesi).
Il servizio si intende comprensivo di tutti gli oneri relativi alla gestione e alla conduzione tecnica ivi compresi tutti i costi di connessione alla rete Internet.

Nel dimensionamento del servizio Hosting si devono tener presenti le stime seguenti, con previsione di crescita del 10-15% annuo:

- Il volume delle sottoscrizioni elettroniche raccolte per ogni anno in funzione della registrazione delle presenze alle attività formative è di circa 15.000.000. Tali sottoscrizioni devono essere conservate per tutta la durata dell'affidamento e trasferite a fine contratto al nuovo affidatario; alla data di pubblicazione non sono presenti sottoscrizioni.

- Numero di accessi simultanei per la segnalazione della presenza pari a 21.000.

Il servizio di conduzione tecnica, relativo a tutta la piattaforma hardware e software descritta in questo Capitolato, deve comprendere anche tutte le operazioni necessarie per la sincronizzazione (bidirezionale) dei dati del registro REF con FPF.
Il servizio di gestione e manutenzione dovrà essere espletato conformemente alle specifiche ITIL V4 e in accordo con un ***"Piano di Housing, conduzione e manutenzione HW/SW"*** e un ***"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello"*** da prodursi come **parte integrante dell'offerta tecnica** fornendo i relativi curricula professionali, **il numero di risorse professionali, comunque non inferiore a due (di cui una allocata a tempo pieno e una allocata almeno al 50%), che compongono il team dedicato al servizio, fermo restando che tali risorse possono essere impiegate in tutto o in parte in relazione alle esigenze e alla pianificazione condivisa con FONDIMPRESA.**

L'installazione dovrà essere conclusa entro 60 giorni dall'avvio del contratto.

Potenziamenti dell'infrastruttura nel limite del 20%, non daranno luogo a nessuna variazione del corrispettivo per il presente servizio; solo eventuali potenziamenti superiori al 20%, per la quota eccedente tale soglia, potranno dar luogo ad un incremento del corrispettivo previsto per il servizio.

4.4.2 Change management

L'affidatario deve prevedere l'utilizzo di metodi e procedure standardizzate per un'efficiente e rapida gestione di tutti i cambiamenti all'infrastruttura.

I maggiori obiettivi del Change Management sono:

- minimizzare l'impatto dei cambiamenti nell'ambiente produttivo;
- ridurre il numero delle emergenze;
- assicurare che tutti i cambiamenti siano documentati, autorizzati e testati;
- assicurare dove possibile un piano di Backup/Recovery;
- fornire un processo di identificazione dei rischi, e minimizzarli.

I principali ruoli coinvolti in queste attività dovranno essere almeno:

- Change Manager (l'owner del processo di Change Management);
- IT staff dell'area relativa;
- Fondimpresa;
- Esperti/Tecnici.

I cambiamenti possono essere classificati secondo le seguenti tipologie:

- cambiamenti software di base: si tratta di modifiche sostanziali e potenzialmente critiche ai software di base;
- cambiamenti di configurazione: si tratta di modifiche che, pur non prevedendo la sostituzione o la modifica di un componente hardware o software utilizzato per l'operatività, ne comportano un cambio di configurazione che ne modifica le modalità operative;
- cambiamenti relativi ai tool di supporto: si tratta di modifiche che riguardano software di proprietà di fornitori terzi;
- cambiamenti hardware: si tratta di modifiche anche di piccola entità relative alla configurazione hardware dell'infrastruttura;
- altro: in questa categoria rientrano tutti i cambiamenti critici che non rientrano nelle categorie precedenti.

In fase di presentazione dell'offerta, dovrà essere provvista opportuna documentazione relativa alle procedure di gestione del Change Management.
Naturalmente, non tutti i cambiamenti devono passare da un workflow complesso. Normalmente si distinguono degli *standard changes*, che prevedono un'approvazione automatica, idonea per cambiamenti molto comuni e ripetitivi (tipo creazione di account, ecc.), e *model changes*, che prevedono dei workflow specifici e/o semplificati che meglio si adattano al tipo di cambiamento (per esempio bug fixing, ecc.).
Il Change Management deve essere fortemente integrato con il project management perché i cambiamenti (almeno quelli più significativi) normalmente sono output di progetto.

Dovranno essere incluse nel Change Management almeno le seguenti attività:

- iniziare il processo di richiesta di cambiamenti (o Request For Change, RFC);
- valutare l'impatto*, costi, benefici e rischi dei cambiamenti proposti;
- sviluppare giustificazioni (dal punto di vista del business) dei cambiamenti proposti ed ottenerne l'approvazione;
- gestire e coordinare l'implementazione delle RFC;
- monitorare e fornire report sulle RFC;
- fare la review e chiudere le RFC.

*Anche nell'ambito del Change Management devono essere tenuti in considerazione gli aspetti legati alla sicurezza e alla privacy (secondo i principi di privacy by design/default e security by design/default), pertanto qualsiasi modifica non deve avere impatti negativi sulla riservatezza, integrità e disponibilità dei dati (cfr. paragrafo 14).

La RFC è l'unico meccanismo previsto da ITIL per richiedere un cambiamento all'infrastruttura. La RFC deve contenere tutte le informazioni necessarie affinché un cambiamento possa essere valutato, approvato e implementato. Tra i motivi per i quali può essere richiesta una RFC, si trovano ad esempio:

- risoluzione di un Incident o di un Problem;
- insoddisfazione di un cliente su un servizio (attraverso il SLM – Service Level Management);
- introduzione, upgrade o rimozione di un CI (Configuration Item);
- cambiamenti in seguito a richieste del business;
- spostamenti di sede;
- cambiamenti legislativi;
- cambiamenti di prodotti o servizi da parte di fornitori.

All'interno del piano della manutenzione deve essere dedicato un paragrafo apposito al Change Management.

Tutta la documentazione inerente al Change Management deve essere depositata nel repository web e disponibile in lettura per Fondimpresa.

4.4.3 Servizio di Backup e restore

Deve essere fornito, in accordo con un dettagliato piano di backup da concordare con Fondimpresa entro 30 giorni dall'avvio del contratto, un sistema di backup e restore con i seguenti requisiti minimi:

- un servizio di backup/restore implementato tramite software di backup di mercato con disponibilità di agent dedicati per i principali applicativi (MS SQL, ecc.) con meccanismi di protezione anti-ransomware(backup immutabili) e con politica di back-up almeno 3-2-1:
  - tre copie dei dati (ad esempio, una copia primaria e due backup),
  - due supporti diversi (ad esempio: una copia principale su un disco rigido interno e una copia di backup su nastro o supporto removibile al termine del backup),
  - una copia off-site.
- monitoraggio dell'esito dei backup con meccanismi di alert e retry anche manuali;
- sistema di conservazione del dato con deduplica e/o compressione del dato;
- remote vaulting del back-up in sito geograficamente distinto (preferibilmente almeno a 10km di distanza) dal principale con backup immutabili.

La soluzione proposta deve garantire la conservazione di almeno 50TB di dati con una policy prevista, per ciascuno dei sistemi gestiti, di:

- un full backup mensile;
- un backup incrementale giornaliero, con retention di un mese.

Per l'implementazione del servizio di backup relativo agli apparati di rete, date le caratteristiche di ridotta volatilità del dato, si può prevedere l'utilizzo dello specifico software proprietario dell'apparato in modalità manuale, cioè il backup del dato verrà effettuato solo in corrispondenza di interventi sulla configurazione.

Al fine di identificare le policy più adatte all'infrastruttura, per evitare la perdita dei dati e consentire la protezione dei dati stessi in modo efficiente, dovrà essere effettuata un'analisi in base alle categorie dei dati della applicazione, considerando la loro criticità, in relazione a quanto la perdita di tali dati possa compromettere il regolare svolgimento delle attività di Fondimpresa e/o una perdita di immagine del Fondo e/o comportare rischi sanzionatori in relazione al trattamento dei dati personali. Si dovrà garantire una policy minima: full giornaliero, incrementale ogni 4 ore.

Quanto sopra indicato si riferisce al backup dei dati. Per quanto riguarda i server (fisici e/o virtuali), in termini di sistemi operativi, ecc. si dovrà effettuare il backup dei file di sistema Full mensile, o comunque ogni qualvolta si procederà a modifiche di configurazione.
Per il dimensionamento si dovrà considerare indicativamente un *volume di dati* nell'ordine di 10 TB. Per tutti i Backup si dovrà considerare una retention di un mese.

L'affidatario deve produrre un report mensile riassuntivo degli esiti di backup e, in caso di completamento con errore, deve contenere almeno le informazioni su quali tipi di backup sono falliti, la numerosità e le cause di errore.

I supporti di backup devono essere sottoposti a test periodici semestrali per assicurare la loro affidabilità in caso di emergenza; questi devono essere associati alla verifica delle procedure di ripristino e confrontati con il tempo di ripristino richiesto. I test di backup e ripristino devono essere eseguiti in un ambiente disgiunto da quello di esercizio. A seguito dei testi periodici dovrà essere fornito un dettagliato report delle attività effettuate e degli esiti delle stesse.

4.4.4 Sistema di Monitoraggio

L'affidatario deve fornire come parte integrante del servizio, un sistema completo di monitoraggio HW/SW di rete, sistemi, middleware ed applicativi (in grado di misurare i tempi di risposta e la disponibilità di specifiche funzioni applicative) che in caso di anomalia di funzionamento, o comunque al superamento delle soglie di attenzione impostate, invii allarmi (all'affidatario e a Fondimpresa) per un tempestivo intervento e, mediante la correlazione di metriche, componenti e relazioni dell'infrastruttura IT, fornisca al team di gestione informazioni utili ad identificare e diagnosticare l'esatta origine del problema. L'affidatario deve provvedere a fornire accesso in sola lettura a Fondimpresa a tale sistema di monitoraggio, compresi anche i sistemi di monitoraggio locali di apparati di rete quali Firewall, ADC, ecc.

Di seguito sono riportate le principali caratteristiche:

- analisi delle prestazioni dei server con opportuni allarmi (livello di occupazione memoria, cpu, accessi disco e spazio disco, accessi alla rete, swap, ecc.);
- monitoraggio e correlazione tra il livello dei servizi di business e le componenti dell'infrastruttura;
- monitoraggio del database;
- monitoraggio dei sistemi operativi;
- rilevazione dei parametri oggetto degli SLA contrattuali, in modalità che garantisca l'affidabilità e non modificabilità dei dati, e restituzione tramite opportuni report automatici senza rielaborazioni umane;
- assegnazione di priorità ai problemi in base alle conseguenze sulle attività di business;
- gestione centralizzata degli allarmi (event console) con notifiche tramite e-mail.

Il sistema offerto deve garantire l'erogazione dei seguenti servizi minimali.

- Monitoraggio Standard:
  - monitoraggio basilare richiesto da Control Room per garantire i servizi di gestione, tipicamente tramite l'attivazione di un agente di monitoraggio standard su ogni elemento dell'infrastruttura;
  - raccolta delle metriche di Disponibilità e Performance dei sistemi e dei servizi applicativi;
  - gestione delle risorse monitorate e delle rispettive configurazioni, effettuata centralmente tramite sistema CMDB (da offrire a carico dell'affidatario) in conformità con quanto previso dall'ITIL V4;
  - gestione delle segnalazioni in modo centralizzato su un'unica console di Event Management;
  - sistema Standard di Reportistica: integra il servizio di Standard Monitoring abilitando anche la Rendicontazione standard di tipo Operazionale e Livelli di Servizio sulle metriche standard di Availability e Performance di Sistemi, Middleware e Applicazioni.

- Monitoraggio avanzato:

- integra il servizio di Standard Monitoring abilitando anche il Monitoraggio e la raccolta di indicatori applicativi non censiti tra quelli standard richiesti per l'erogazione dei servizi, ma necessari al monitoraggio degli SLA ed allo svolgimento di un'analisi in grado di individuare proattivamente potenziali criticità, degrado delle prestazioni ed esigenze di adeguamento dell'infrastruttura;
- sistema di reportistica avanzato, che estenda il servizio di monitoraggio abilitando la Rendicontazione di specifici indicatori applicativi.

4.4.4.1 Monitoraggio integrato

L'integrazione del monitoraggio si realizza attraverso:

- la centralizzazione dei parametri gestiti da ciascuna componente di monitoraggio;
- la centralizzazione delle configurazioni e delle policy di monitoraggio;
- l'omogeneizzazione e normalizzazione delle segnalazioni generate da fonti eterogenee finalizzate alla migliore fruizione da parte del personale dei presidi operativi.

La piattaforma di monitoraggio deve essere in grado di gestire i due tipi eventi, sincroni e asincroni, che generano segnalazioni verso la piattaforma di Event Management.
Deve essere gestito, ove possibile, un meccanismo "Continuos Alarming", con generazione di segnalazioni di tipo ATTIVAZIONE ogni volta che venga rilevata una condizione da segnalare ed una segnalazione di tipo DISATTIVAZIONE allorquando venga rilevato il ritorno alla normalità di una condizione precedentemente segnalata.
Tale meccanismo, prevalentemente realizzato dai controlli di tipo Sincrono, anche se genera un numero elevato di eventi, garantisce la corretta gestione anche in caso di perdita di un evento o di errata chiusura da parte di un operatore.
Le segnalazioni di ATTIVAZIONE e DISATTIVAZIONE per un medesimo evento devono essere classificate e caratterizzate in maniera tale che siano identiche in tutti gli elementi identificativi dell'evento e differiscano esclusivamente per lo stato.

4.4.4.2 Controlli di tipo Sincrono

Sono quei controlli che vengono effettuati con frequenza predefinita (generalmente ogni 5, 10, 15 min) e per i quali è possibile rivelare e valutare una condizione ben precisa.
Generalmente questi controlli, ad ogni ciclo di polling (es.: Controllo Utilizzo File System):

- eseguono un comando (es.: df —k);
- ne analizzano l'output (es.: rileva i valori di %usage di ciascun FS);
- confrontano i valori risultanti con delle soglie o degli stati definiti (es.: 95% critical, 90% Major);
- generano una segnalazione di ATTIVAZIONE se il controllo rileva una condizione da segnalare come Problema (es.: %usage rilevato = 98%);
- generano una segnalazione di DISATTIVAZIONE solo se il controllo rileva una condizione di normalità e nel ciclo precedente era stata generata una segnalazione di ATTIVAZIONE.

Tipici controlli sincroni sono:

- CPU, MEM, SWAP, FS Usage;
- Process Instance;
- Windows Service Status;
- Database Status.

4.4.4.3 Controlli di Tipo Asincrono

Sono quei controlli che rilevano segnalazioni generate da tool di sistema o applicativo senza specifica sollecitazione.
Generalmente tali segnalazioni NON sono subordinate a specifici meccanismi standard di generazione e sono difficilmente riconducibili a qualcosa di analogo al "Continuos Alarming".
Normalmente tali segnalazioni sono di tipo ATTIVAZIONE e difficilmente prevedono la corrispondente DISATTIVAZIONE.

Non essendo pilotabili in termini di numerosità e frequenza di generazione, per tali segnalazioni si cerca di:

- definire criteri precisi di identificazione degli eventi di interesse;
- classificare e caratterizzare le segnalazioni in maniera che siano sovrapponibili a parità di significato.

Esempi tipici di controlli asincroni sono:

- parsing dei log file (system messages, generic application log file, ecc.);
- eventi di Windows.

4.4.4.4 Servizio di Monitoraggio dei Log degli eventi

La registrazione dei log degli eventi, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente.

I log degli eventi possono contenere dati critici e personali. Devono quindi essere applicate adeguate misure per la protezione della privacy.

Dove possibile gli amministratori di sistema non devono poter cancellare o disattivare i log delle proprie attività.

I log di sistema contengono spesso un gran volume di informazioni, molte delle quali sono estranee al monitoraggio della sicurezza delle informazioni. Al fine di agevolare l'individuazione di eventi significativi per il monitoraggio della sicurezza delle informazioni, si deve considerare la copia di appropriati tipi di messaggi su un secondo log o l'uso di adeguate utilità di sistema o strumenti di audit per effettuare l'interrogazione e la razionalizzazione dei file.

È necessario proteggere i log di sistema in quanto, se i dati al loro interno possono essere modificati o cancellati, la loro esistenza potrebbe creare un falso senso di sicurezza. La copia in tempo reale dei log su un sistema al di fuori del controllo dell'amministratore di sistema o dell'operatore può essere utilizzata per salvaguardare i log.

Gli amministratori di sistema devono essere nominati individualmente, con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, e l'elenco degli stessi deve essere comunicato a Fondimpresa entro 5gg. di calendario dalla data di inizio delle attività previste dall'affidamento ed entro 5gg. di calendario da ogni successiva modifica. Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi, nel rispetto del Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 (G.U. N. 300 Del 24 dicembre 2008), così come modificato dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 25 giugno 2009 (G.U. N. 149 Del 30 giugno 2009).

Nel "***Piano di Hosting, conduzione e manutenzione HW/SW"*** devono essere indicate le modalità di monitoraggio dei log degli eventi insieme alla reportistica di analisi fornita trimestralmente.

4.4.5 Risk & Security Assessment, Stress & Penetration Test

Con cadenza almeno annuale devono essere forniti un documento di Risk Assessment, Analisi statica del codice, Vulnerability Assessment, Penetration Test e Stress Test del sistema REF. I documenti, che potranno essere redatti anche in momenti distinti, verranno utilizzati da Fondimpresa per valutare eventuali interventi

infrastrutturali mirati all'elusione, alla mitigazione, al trasferimento o all'accettazione del rischio infrastrutturale. Le modalità di esecuzione devono essere indicate nel "***Piano di Hosting, conduzione e manutenzione HW/SW"***, i tempi e le modalità di attuazione devono essere concordati con Fondimpresa con un preavviso di almeno 15 giorni lavorativi. In particolare, gli stress test, se eseguiti su ambienti diversi da produzione, possono essere eseguiti in scala, altrimenti devono essere effettuati fuori dal normale orario di lavoro, in giorni festivi, in orari notturni e comunque con preavviso autorizzato da Fondimpresa di almeno 15 giorni lavorativi. I risultati di tale attività dovranno essere analizzati dal fornitore per anticipare eventuali problematiche prestazionali e/o di sicurezza, e più in generale per tutti i possibili rischi individuati, proponendo tempestivamente soluzioni attuabili a titolo di contromisura.
All'atto della presa in carico dell'affidamento, l'affidatario deve eseguire un assessment iniziale di Analisi statica del Codice, della sicurezza dell'infrastruttura, con vulnerability assessment e penetration test (anche applicativi) – generando una *baseline* della sicurezza, e deve quindi produrre un dettagliato documento di remediation di eventuali criticità evidenziate.
Fondimpresa si riserva di richiedere una ulteriore attività di assessment/test di cui sopra all'anno.

4.4.6 Server Farm

L'erogazione dei Servizi di Hosting richiede che il Fornitore aggiudicatario disponga di una o più Server Farm che soddisfino i requisiti minimi specificati di seguito:

- la/le Server Farm in cui il Fornitore erogherà il servizio di Hosting potrà/potranno essere dislocata/e su una o più sedi operative, comunque tutte ubicate in un paese dell'Unione Europea;
- ogni sede ed il personale ad essa addetto potranno non essere esclusivamente dedicati alla erogazione dei servizi di Hosting ma dovranno, comunque, rispettare i requisiti sotto riportati;
- tutte le Server Farm in cui il Fornitore erogherà il servizio di Hosting dovranno essere di livello almeno TIER IV della TIA-942 tale da garantire tutti i livelli di sicurezza previsti dalle normative vigenti (certificazione ISO 27001) e in particolar modo:
  - presenza di ambienti sicuri e protetti;
  - riservatezza, integrità e disponibilità su base permanente delle informazioni raccolte;
  - strumenti e processi organizzativi atti al tempestivo ripristino di dati e di servizi interrotti.

I suddetti requisiti dovranno essere dettagliati e presentati come parte integrante della documentazione di gara all'interno dei documenti come di seguito indicato: ***"Documento Organizzativo della Sicurezza"***, il ***"Piano di Continuità Operativa"*** e il ***"Piano della Sicurezza del Data Center"***, per i quali si dovrà garantire, per tutta la durata del contratto, un aggiornamento costante, oltre ad offrire un continuo miglioramento dei processi attuati e delle risorse HW/SW e un utilizzo ottimale delle risorse impiegate.
Il Fornitore dovrà provvedere che le Server Farm siano in un ambiente sicuro e protetto, caratterizzato da:

- un sistema di controllo degli accessi, ad accesso singolo, mediante smart-card personale o dispositivo alternativo (es: generatore codici RSA, biometria ecc.) al fine di garantire l'accesso ai locali relativi a tale ambiente esclusivamente a personale autorizzato;
- sorveglianza armata 24 ore al giorno, per tutti i giorni dell'anno.

Il Fornitore dovrà utilizzare un registro elettronico interno delle visite in grado di gestire una black-list dei visitatori cui non è consentito l'accesso ai locali.
Gli apparati server dislocati presso il Data Center dovranno prevedere dei meccanismi di sicurezza fisica che impediscano il furto locale di dati (es. blocco di tutte le periferiche rimovibili scrivibili quali floppy disk o dispositivi USB, disabilitazione del boot da periferiche rimovibili ecc.).
Il Fornitore dovrà assicurare apparati di continuità dell'Energia Elettrica in grado di garantire un'autonomia di almeno 24h e utilizzare un sistema di segnalazione degli allarmi di tipo locale o remoto.

Le aree destinate a ospitare gli apparati dovranno essere protette contro gli incendi e gli allagamenti mediante idonee misure di rilevazione e intervento, dovrà essere inoltre garantito un impianto di climatizzazione ridondato.
Nel caso i locali si trovino a livello stradale o inferiore, dovranno essere previsti sistemi anti-allagamento dotati di opportune pompe idrauliche.
Gli apparati attivi di rete dovranno essere compartimentati mediante armadi di cablaggio con chiusura a chiave.
È fatto obbligo, inoltre, al Fornitore di trattare, trasferire e conservare le eventuali repliche dei dati, ove autorizzate da Fondimpresa, sempre all'interno del territorio comunitario; tali repliche dei dati dovranno essere conservate con livelli di sicurezza concordati con Fondimpresa.
Si richiede che il Fornitore indichi l'ubicazione dei data center e le principali caratteristiche in termini di logistica e condizioni ambientali (es. almeno: infrastrutture di collegamento, impianto elettrico, dislocazione apparecchiature di rete e server, illuminazione, sicurezza, aerazione e impianto di climatizzazione artificiale).
Per quanto attiene più in particolare all'infrastruttura utilizzata dal Fornitore ai fini dell'erogazione dei servizi oggetto della presente fornitura, si precisa che il/i CED e le relative macchine fisiche potranno essere condivisi in logica di Community Cloud; resta in ogni caso inteso che il Fornitore dovrà garantire la segregazione logica degli ambienti e dei dati (ad esempio attraverso macchine virtuali e VLAN dedicate).
Il sistema operativo dei server che erogano il servizio deve soddisfare i seguenti requisiti (DPCM 31/10/2000, Art. 7, comma 1):

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne la identificazione.

In particolare, i sistemi operativi devono essere pienamente supportati (non in EOL/EOS) e aggiornati con le ultime patch di sicurezza.
Le registrazioni di sicurezza devono essere protette da modifiche non autorizzate (DPCM 31/10/2000, Art. 7, comma 4).
Dovrà essere garantita l'indipendenza e la protezione (isolamento) dei dati di Fondimpresa.
Le patch che risolvano problematiche di sicurezza critiche per i server esposti alla rete dovranno essere installate nel più breve tempo possibile dalla disponibilità delle patch stesse e di norma entro le 48 ore salvo diverse indicazioni di Fondimpresa e/o nel caso i cui l'installazione comporti un'interruzione del servizio.
Ogni attività di *change*, che comporti interruzioni del servizio, deve essere svolta in orario notturno e comunque in finestre temporali concordate con Fondimpresa; per ognuna di esse dovrà essere prodotta una checklist di sicurezza da utilizzarsi in fase di verifica. Tale checklist dovrà essere approvata da Fondimpresa.
Il Fornitore deve garantire che tutti gli apparati necessari all'erogazione dei servizi del presente Capitolato siano gestiti solo da personale univocamente individuato, residente e operante in un paese UE.
Il Fornitore dovrà rendere disponibili al personale interessato istruzioni scritte inerenti ai seguenti aspetti della gestione della sicurezza:

- accesso fisico delle persone agli edifici/locali in cui sono situati gli apparati;
- regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione, visitatori ecc.);
- gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi ecc.);
- gestione di situazioni anomale;
- ripristino dell'interruzione dell'erogazione di energia elettrica;
- procedure di backup e di restore, Disaster Recovery;
- procedure di escalation.

L'infrastruttura tecnologica dei Centri Servizi dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza.
I data center dovranno garantire la continuità di servizio, in coerenza con gli orari di servizio e con gli Indicatori di Qualità. In caso di eventi di disastro che rendono indisponibile l'infrastruttura il fornitore dovrà

comunicare formalmente a Fondimpresa tale evento e garantire la ripartenza di tutti i servizi, anche su un diverso sito (sempre in UE).
I data center del Fornitore, dai quali vengono erogati i servizi del presente capitolato, devono essere interconnessi alla rete Internet in modo da garantire una connettività ai servizi erogati presso i Data Center con almeno due collegamenti distinti su percorsi e apparati differenti anche se del medesimo Carrier.
Il Fornitore dovrà effettuare verifiche interne (audit interno) con cadenza almeno semestrale circa il rispetto delle norme e delle procedure indicate; il Fornitore dovrà fornire i relativi verbali il cui contenuto dovrà essere concordato con Fondimpresa.

L'Affidatario deve consentire l'accesso alla Server Farm a personale di FONDIMPRESA, o a soggetti terzi da questa espressamente autorizzati, con vincoli di riservatezza, con preavviso minimo di 48h solari.

4.4.7 Sicurezza

Il Fornitore dovrà garantire, per la propria interconnessione a internet, la sicurezza delle strutture, dei collegamenti e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno. In particolare, è responsabilità del Fornitore assicurare che le server farm, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete INTERNET siano protette mediante l'adozione di adeguati sistemi e metodologie, nel rispetto di quanto stabilito dallo standard ISO/IEC 27001, oltre che gestite in piena conformità con la normativa vigente.
Devono comunque essere soddisfatti dal Fornitore, almeno i seguenti requisiti minimi:

- utilizzo di dispositivi di tipo Firewall e sistemi di Network Detection ed Event & Log Monitoring, necessari a rilevare e contenere eventuali incidenti di sicurezza ICT;
- devono essere adottate tutte le necessarie misure volte a limitare il rischio di attacchi informatici e a eliminare eventuali vulnerabilità della rete, causate dalla violazione o dall'utilizzo illecito di sistemi o infrastrutture del Fornitore (es. Firewall, antivirus su tutte le macchine ecc.).
- devono essere effettuati periodicamente (cfr. 4.4.5) attività di *vulnerability assessment* e *penetration test* i cui esiti devono essere comunicati a Fondimpresa con indicazione delle azioni di remediation intraprese e/o suggerite.

Le modalità di attuazione dei suddetti requisiti di sicurezza dovranno essere dettagliate all'interno del ***"Piano di Hosting, conduzione e manutenzione HW/SW"*** con particolare attenzione ai dati gestiti dal Sistema Informatico e dalle risorse e strumenti a essi afferenti in capo al Fornitore relativamente all'erogazione dei servizi contrattuali.
I principali obiettivi che il piano di gestione della sicurezza del Fornitore dovrà garantire sono:

- assicurare la continuità dei servizi e delle applicazioni ospitate;
- minimizzare i danni in caso di incidente e/o di avaria del Sistema Informatico;
- garantire la gestione della sicurezza in linea con la normativa e con gli standard nazionali e internazionali applicabili;
- assicurare su base permanente la riservatezza, l'integrità, la disponibilità dei dati;
- normalizzare l'approccio alla gestione della sicurezza, ottimizzando e coordinando le risorse disponibili;
- creare un'organizzazione della sicurezza condivisa, documentata, organica, efficiente e capillare, in grado di testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate;
- consentire un miglioramento continuo del sistema della sicurezza;
- fornire metodologia, politiche e procedure per il sistema di gestione;
- sicurezza logica;
- sicurezza fisica;
- sicurezza delle applicazioni;
- gestione delle utenze (policy per il personale);

- gestione degli incidenti;
- continuità operativa.

4.4.8 Conservazione a norma dei registri

La conservazione dei registri delle presenze della attività formative deve essere effettuata nel rispetto delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agid.
Il sistema informatico di gestione dei registri affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del registro e rispettare i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio. Entro 30 giorni dall'avvio delle attività contrattuali deve essere redatto un **"Manuale di gestione e conservazione documentale"**, dove devono essere indicati, a titolo esemplificativo e non esaustivo, i workflow documentali, i sistemi di Document & Content Management e gli applicativi informatici, che si basino su elevati livelli di automazione e interoperabilità in grado di operare nel web. In un contesto in continua trasformazione, il manuale deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati. I processi e le attività che governano le fasi di formazione, gestione e conservazione dei documenti informatici devono essere sottoposti a un costante lavoro di valutazione, monitoraggio, riprogettazione e reingegnerizzazione.
Il registro di conservazione deve essere online e accessibile, da Fondimpresa, h24 e 7 giorni su 7.
I registri elettronici dovranno essere conservati per tutta la durata dell'affidamento e trasferiti a fine contratto al nuovo affidatario.

4.4.9 Modalità di valorizzazione e pagamento

Per il servizio di Hosting e manutenzione HW/SW è previsto un canone trimestrale che verrà pagato posticipatamente all'esito delle verifiche condotte da parte di FONDIMPRESA, secondo quanto previsto dallo schema di contratto.

5 Piano di continuità operativa

Si richiede, come documento da allegare all'offerta tecnica, un ***"Piano di continuità operativa"***, che deve formalizzare i principi, definire gli obiettivi e descrivere le procedure per la gestione della continuità operativa dei processi gestiti nell'ambito dell'affidamento (indicazione degli strumenti di gestione e monitoraggio dei vari ambienti, modalità backup/ripristino, DR ecc.). Nella redazione del piano deve essere ovviamente svolta un'analisi dei rischi e relativi impatti sulla continuità operativa del sistema oggetto dell'affidamento e le possibili strategie di mitigazione degli stessi. In particolare, dovranno essere identificate le procedure di *escalation,* in caso di eventi che comportino l'interruzione della continuità operativa, i meccanismi di attivazione delle stesse, nonché le figure e i ruoli coinvolti nell'ambito di tale piano.

6 Affiancamento a fine contratto

Alla fine della durata contrattuale o alla eventuale risoluzione anticipata dello stesso per qualsiasi motivo, il fornitore dovrà garantire per il nuovo affidatario un periodo di affiancamento per subentro di almeno un mese. Fino al completamento del passaggio di consegna al nuovo affidatario, attestato da apposito verbale sottoscritto e accettato dalle parti, il fornitore uscente sarà responsabile di tutte le attività di gestione e manutenzione (ivi comprese MAC, MAD e MEV) del sistema.

L'affiancamento per subentro consiste nell'affiancamento al nuovo fornitore per presa in carico del software di base e applicativo del registro REF nonché dei servizi di MEV, MAD/MAC e Help Desk di secondo livello, Hosting, conduzione e manutenzione HW/SW. Le attività di affiancamento per subentro devono partire dalla richiesta di Fondimpresa e devono essere svolte secondo un dettagliato ***"Piano di affiancamento a fine contratto"*** fornito come parte integrante dell'offerta tecnica.
L'Affidatario deve assicurare per il periodo di affiancamento a fine contratto il pieno supporto necessario a garantire il regolare funzionamento dei servizi di Hosting, conduzione e Manutenzione HW/SW del sistema REF, di MAD/MAC e Help Desk di secondo livello, affiancando con proprio personale le risorse professionali del nuovo Affidatario garantendo l'acquisizione delle informazioni tecniche e operative necessarie per realizzare compiutamente il subentro nella conduzione dei servizi.
L'Affidatario dovrà svolgere sessioni di formazione in aula, il cui contenuto deve essere preventivamente approvato da Fondimpresa, propedeutiche all'affiancamento per un ammontare di almeno 16 ore. L'Affidatario dovrà fornire tutto il supporto necessario al trasferimento delle competenze e delle conoscenze e all'operatività del sistema e dei servizi nel periodo di affiancamento.
L'Affidatario dovrà fornire tutto il supporto al nuovo Affidatario anche per quanto concerne il trasferimento dei dati soggetti a conservazione.

7 Gruppi di lavoro

Per tutte le attività previste oggetto del presente Capitolato dovranno essere impiegate figure professionali adeguate in termini di competenze e numerosità per la realizzazione delle attività progettuali. Tali figure devono far parte di uno o più gruppi di lavoro di cui l'Affidatario si impegna a fornire i profili professionali, documentati dai curricula nominativi da allegare all'offerta tecnica, con l'indicazione del numero di unità impiegate per ciascuno di essi. Essendo opportuna la presenza continuativa dello stesso personale per tutta la durata della fornitura, le eventuali sostituzioni di personale durante l'esecuzione della medesima dovranno essere concordate preventivamente con il DEC, dietro presentazione e approvazione dei curricula, nel rispetto dei requisiti indicati per ciascuna figura professionale. La sostituzione richiederà un adeguato periodo di affiancamento per la risorsa entrante, il cui costo sarà interamente a carico dell'Affidatario.
In caso di particolari esigenze FONDIMPRESA potrà richiedere un rafforzamento del suddetto team.
Come parte integrante dell'offerta tecnica, deve essere fornito un ***"Piano dell'organizzazione dei gruppi di lavoro",*** contenente un'accurata descrizione dell'organizzazione delle risorse umane in relazione ai singoli servizi e alla gestione complessiva del progetto, corredata dai curricula delle risorse messe a disposizione.
Tale scenario può cambiare in corso d'opera, in conseguenza dell'evoluzione delle piattaforme utilizzate. Fondimpresa si riserva di specificare il dettaglio del profilo richiesto per ciascuna figura in fase di costituzione dei gruppi di lavoro o di inserimento/sostituzione delle risorse.
Pertanto, in tale fase verranno specificate le esperienze richieste (tra quelle indicate nei profili o comunicate al Fornitore) e i prodotti di cui le risorse devono avere una ottima conoscenza (o, lì dove indicato, essere in possesso di certificazione o cultura equivalente). Inoltre, in conseguenza delle esigenze del servizio, il DEC potrà richiedere in corso di esecuzione del Contratto la conoscenza da parte delle risorse impegnate nell'erogazione dei servizi di ulteriori prodotti, sistemi, linguaggi di programmazione e metodologie e standard rispetto a quelli definiti nel Capitolato. Entro 30 giorni dalla presa in carico del servizio, e successivamente con cadenza semestrale, il fornitore dovrà fornire un elenco di tutte le risorse impiegate sul progetto.

8 Documentazione di progetto e d'utente

Le attività di manutenzione correttive e/o evolutive devono prevedere una ampia documentazione di progetto che comprenda l'analisi, il progetto, l'implementazione e il deployment.

Tale documentazione dovrà essere prodotta utilizzando, preferibilmente, linguaggi formali di uso comune con le informazioni comparabili a quelle contenute nei seguenti diagrammi tipici dell'UML:

- Use Case Diagram (con dettagliato flusso degli eventi per ogni caso d'uso);

- Class diagram;
- Object diagram;
- Statechart diagram;
- Activity diagram;
- Sequence diagram;
- Communication diagram;
- Component diagram;
- Deployment diagram;
- Relazioni fra diagrammi.

Nel caso i diagrammi siano stati prodotti mediante tool proprietari, il fornitore dovrà anche **permettere a Fondimpresa l'accesso al tool.**

Deve essere, inoltre, previsto un dettagliato dizionario dei dati e un completo schema del/dei DB mediante il modello E/R.
Deve essere fornita copia dei sorgenti relativi alle personalizzazioni e al software applicativo sviluppato. Si precisa che il software sviluppato deve contenere un'adeguata documentazione interna, sotto forma di commenti.
La documentazione dovrà essere relativa all'intero sistema e quindi anche alle parti precedentemente implementate; pertanto, l'Affidatario potrà alternativamente decidere di mantenere lo standard di documentazione pre-esistente o di migrare tutta la documentazione in altri formati e standard che verranno successivamente utilizzati durante tutta la durata del contratto.
Deve essere fornita una completa manualistica d'uso personalizzata per ruolo e/o categoria di utenti e una completa guida all'installazione e alla configurazione; le evoluzioni del sistema comportano l'obbligo di adeguare la manualistica.
Devono, inoltre, essere forniti un "***Piano dei Test***" e un "***Piano di collaudo***".
Tale documentazione deve essere redatta in lingua italiana e fornita anche in formato elettronico nel repository di progetto all'uopo predisposto dall'Affidatario, e accessibile in sola lettura a Fondimpresa, che garantisca la profilazione degli utenti e l'accesso sicuro.

8.1 Analisi Preliminare

Il documento di analisi preliminare ha lo scopo di raccogliere le informazioni necessarie alla formulazione del piano di lavoro del lotto funzionale e alla quantificazione delle risorse assegnate e deve pertanto definire:

- ambito e obiettivi generali di progetto;
- finalità dei processi e norme principali di riferimento;
- unità organizzative interessate con le relative dipendenze gerarchiche e referenti per il progetto;
- dettaglio degli obiettivi in relazione alla corretta identificazione delle principali dimensioni di riferimento (esempio: necessità utenti, prestazioni, output, workflow, struttura, attività e relativi strumenti di supporto, risorse);
- strumenti e metodologie da utilizzare per la realizzazione del progetto.

8.2 Specifiche Funzionali e Progettazione esecutiva

Le specifiche contengono in modo completo ed esaustivo l'analisi dei requisiti relativamente:

- ai processi e alle modalità con cui tali processi risulteranno visibili agli utenti finali,
- al disegno logico dei dati secondo il modello relazionale,
- agli aspetti non funzionali (architettura, sicurezza, accessibilità, vincoli, prestazioni ecc.),
- alla documentazione delle interfacce (incluso esempi di layout delle principali schermate utente ecc.),
- ai casi in cui è previsto l'utilizzo di un prototipo.

Il risultato finale deve essere la progettazione esecutiva che riepiloga le specifiche funzionali, la pianificazione delle attività del lotto funzionale e la stima dell'effort in Punti Funzione.

Il livello di completezza richiesto deve essere tale da:

- consentire l'approvazione delle funzionalità da parte del DEC e dei referenti delle Aree/unità di Fondimpresa;
- consentire la produzione del Piano di test senza necessità di ulteriori approfondimenti;
- consentire lo svolgimento della successiva fase di disegno di dettaglio;
- consentire la verifica della stima in Punti Funzione del volume di software da sviluppare e/o da modificare;
- garantire la rispondenza con quanto descritto nel documento dei requisiti.

8.3 Disegno di Dettaglio

I documenti di disegno di dettaglio contengono una specifica in cui le funzionalità sono trasformate e organizzate in moduli elaborativi strutturati. È compresa nel disegno di dettaglio la documentazione del disegno logico e fisico dei dati.
Ad esempio, per i vari moduli, devono essere trattati:

- descrizione delle funzioni svolte;
- tipologia (on-line, batch, ecc.);
- indicazioni sulla riutilizzabilità del componente;
- parametri scambiati con altri componenti;
- parametri di attivazione;
- accessi agli archivi/base dati;
- controlli e diagnostica;
- algoritmi di calcolo per ciascuna entità.

Per quanto riguarda il disegno logico dei dati, la tecnica di rappresentazione può variare in funzione del DBMS utilizzato.
Deve comunque essere garantita la rispondenza rispetto ai documenti di Specifiche funzionali, Specifiche requisiti e Glossario. I dati contenuti nel documento devono essere sempre tenuti aggiornati.
Di seguito viene riportato un elenco di contenuti tipicamente attesi per la documentazione tecnica di dettaglio. Essi sono qui descritti come *deliverable* singoli, ma possono anche essere integrati in documenti complessivi.
Questi *deliverable* sono definiti rispetto alla stratificazione architetturale di riferimento sviluppata e alle singole funzionalità, secondo il seguente schema.

Documentazione relativa alla definizione generale dell'architettura applicativa, con indicazione delle corrispondenze con l'architettura di riferimento. Questa comprende:

1. Documento di analisi concettuale, inclusivo di:
    a. glossario;
    b. diagramma dei package e relativa descrizione testuale;
    c. modello concettuale definito tramite un diagramma delle classi di analisi;
    d. specifica dei protocolli di comunicazione fra le classi, mediante diagrammi di attività o di sequenza;
    e. verifiche di correttezza dei protocolli.
2. Documento di progettazione, inclusivo di:
    a. diagramma delle componenti;
    b. diagramma di disposizione fisica (deployment);
    c. diagramma delle classi di progetto;
    d. specifica dei protocolli di comunicazione fra le componenti, mediante diagrammi di attività o di sequenza;
    e. verifiche di correttezza dei protocolli.
3. Per ogni funzionalità realizzata andrà prodotta la documentazione relativa, comprendente:
    a. diagramma delle classi specifiche alla funzionalità;

b. diagramma di sequenza specifico all'esecuzione della funzionalità, inclusivo della comunicazione con il DB Access Manager;
c. descrizione delle precondizioni e post-condizioni;
d. diagramma delle transizioni di stato delle entità persistenti influenzate dalla funzionalità.
e. modello di test della funzionalità, comprendente:
    i. piano di test;
    ii. specifica dei test;
    iii. rapporto sui test effettuati e sul loro esito.

4. Per ogni interfaccia utente realizzata andrà prodotta documentazione comprendente:
    a. analisi delle tipologie di utenti e dei loro compiti;
    b. descrizione dei casi d'uso degli ambienti;
    c. analisi dell'accessiblità;
    d. manuale utente ed help-online.

8.4 Codice Sorgente

Per codice sorgente si intende genericamente l'insieme degli oggetti software, realizzati o sottoposti a manutenzione, che sono soggetti a esecuzione da parte di un compilatore (o analogo strumento di "program preparation") o di un interprete (es. "job control program", "query manager"), a titolo esemplificativo e non esaustivo quindi:

- programmi;
- tracciati e definizioni dati;
- form di input/output;
- pagine web;
- procedure;
- query;
- script (anche gli script relativi ai test automatizzati);
- utility di modifica/aggiornamento dati.

Fanno parte del codice sorgente le procedure di consegna e trasferimento oggetti per gli ambienti di configuration management, nonché le procedure di creazione e popolamento delle tabelle anche attraverso la migrazione dei dati dai data base esistenti, e i relativi job di caricamento dati (per intero DB e/o porzioni secondo criteri definiti) anche per gli ambienti di sviluppo, manutenzione, collaudo ed esercizio.
Fanno parte del codice sorgente, inoltre, l'help on-line e l'eventuale manualistica online, nonché l'eventuale codice di test e collaudo.
Il codice sorgente di nuova realizzazione (anche nuovo codice all'interno di programmi preesistenti) dovrà essere redatto in conformità agli standard, ove previsti, e comunque sempre secondo le indicazioni presenti nella documentazione ufficiale dei linguaggi utilizzati.
Non è consentito l'uso di istruzioni (o funzioni) proprietarie o caratteristiche di singole piattaforme. I richiami, dall'interno dei programmi, dei vari sottosistemi (transaction monitor, data base, rete ecc.) dovranno avvenire tramite comandi o interfacce standard disponibili nei singoli linguaggi / prodotti utilizzati.
Si richiama inoltre l'attenzione al rispetto, nella stesura del codice, degli standard in vigore, sia per formalismi di redazione, sia per l'adozione dei prodotti proposti dal fornitore e condivisi dal DEC di Fondimpresa, sia per il loro corretto utilizzo, sia per il rispetto dei principi di privacy by design/default e security by design/default.
Gli oggetti software necessari alla predisposizione degli ambienti (collaudo, esercizio, ecc.) dovranno essere consegnati almeno tre giorni prima dello scadere del termine previsto per la consegna del codice sorgente.

8.5 Piano Di Test

Il Piano di Test è un documento che accompagna ogni lotto funzionale in tutto il ciclo di vita ed è pertanto un documento che si evolve nel tempo.

Nel Piano di Test devono essere necessariamente comprese le verifiche della corretta predisposizione dell'ambiente di collaudo messo a disposizione dall'affidatario.
Il documento ha lo scopo di definire test specifici, tramite i quali saranno sottoposti a verifica i prodotti realizzati, con particolare riguardo alla loro validazione rispetto ai requisiti dell'utente e ai requisiti non funzionali (sicurezza, prestazioni etc..), nonché sarà documentato l'esito della verifica.
Devono essere garantiti il riscontro e la corrispondenza con il documento di Specifiche funzionali, Specifiche requisiti e Disegno di dettaglio.
Nel documento deve inoltre essere indicato come vengono generati i dati di test. In caso di utilizzo di una copia dei dati di produzione, deve essere indicata e spiegata la procedura applicata per rendere anonime le informazioni nel rispetto alla normativa sulla protezione dei dati personali.

8.6 Documentazione Utente

La documentazione utente, rivolta all'utente finale delle applicazioni, è composta dal Manuale utente e dall'help on line (ove presente).
Il manuale utente deve fornire una descrizione generale dell'applicazione e una guida operativa all'utilizzo delle singole funzionalità utilizzabili, personalizzata per tipo di utente.

La descrizione deve contemplare:

- la tipologia di utenza cui è destinata e le funzioni abilitate a ciascuna tipologia;
- gli eventuali flussi di dati scambiati con altri sistemi informativi o con specifiche tipologie di utenze;
- le modalità di attivazione e chiusura della "sessione di lavoro";
- la descrizione delle funzioni e della navigazione tra le stesse;
- la spiegazione dettagliata dell'uso delle singole funzioni di interfaccia utente (comprensiva della funzione di richiamo dell'help);
- la descrizione degli algoritmi di calcolo utilizzati;
- la descrizione dei contenuti degli output della applicazione (es. stampe).

Nel caso in cui l'applicazione preveda un utilizzo diretto dei dati da parte dell'utente, deve essere inserita anche la descrizione dettagliata della struttura dei dati interessati.
Tutte le applicazioni interattive devono prevedere, se richiesto da Fondimpresa, le funzioni di help on line.

8.7 Manuale di Gestione Applicativo

Il Manuale di gestione applicativo è lo strumento necessario alle strutture preposte all'installazione e all'esercizio dell'applicazione. È un manuale rivolto al personale tecnico. Tale manuale dovrà essere corredato di uno schema riepilogativo contenente informazioni relative all'applicazione, tra le quali la dimensione e tipologia del DB, la dipendenza da altre applicazioni, i modelli di interfaccia, i tool utilizzati per lo sviluppo ecc.
Per quello che riguarda gli ambienti di collaudo ed esercizio, il documento dovrà esplicitare i parametri di personalizzazione dei prodotti, le modalità di attuazione dei livelli di protezione dei dati, le modalità di accesso al sistema e alle transazioni, le soluzioni tecniche necessarie alla realizzazione di tali modalità. Il documento deve contenere il ***"Piano di adeguamento degli ambienti"***, cioè la documentazione sintetica di supporto alle attività di trasferimento e installazione in ambiente di collaudo, di esercizio e di sviluppo. Viene strutturato in tre sezioni relative rispettivamente all'ambiente di collaudo, all'ambiente di esercizio e all'ambiente di sviluppo e deve contenere tutte le informazioni necessarie alla completa e corretta pianificazione dei ticket di change, quali:

- individuazione del responsabile di adeguamento degli ambienti;
- pianificazione di tutte le attività necessarie alla predisposizione dell'ambiente di collaudo/esercizio/sviluppo con l'evidenza delle date di inizio e di completamento e dei referenti (sia tecnici sia applicativi);
- qualificazione del progetto e degli elementi di configurazione coinvolti (DB, utenze, Application Server, directory ecc.);
- specifica delle istruzioni operative evidenziando i riferimenti ai manuali di gestione dei server;

- documento di Lista Oggetti Software (LOS) che contenga un elenco di tutti gli oggetti software realizzati, modificati o resi obsoleti nell'ambito delle attività riguardanti il lotto funzionale;
- documentazione delle procedure off line (batch, job, stored procedure, script ecc.) destinata ai gruppi di gestione applicativi e basi dati quale supporto alle loro attività ordinarie.

Qualora la documentazione presente all'inizio delle attività contrattuali fosse deficitaria, sarà compito dell'affidatario completarla in modo esaustivo e funzionale.

8.8 Rapporto Indicatori di Qualità degli Obiettivi e della Fornitura

Il Rapporto mensile *indicatori di qualità* (tali indicatori saranno concordati, all'avvio delle attività, con Fondimpresa) deve contenere almeno:

- Il riferimento al contratto, all'area funzionale, all'obiettivo;
- per ciascun indicatore applicabile:
  - il periodo di riferimento della misura,
  - il riferimento agli strumenti di misura utilizzati,
  - i dati rilevati;
- il valore rilevato dell'indicatore di qualità:
  - l'eventuale scostamento dal valore di soglia,
  - l'eventuale razionale di scostamento dai valori di soglia,
  - le eventuali azioni correttive intraprese o proposte per risolvere lo scostamento dai valori di soglia.

Nel caso degli indicatori rilevabili con strumenti specifici, è necessario allegare al documento *Rapporto indicatori di qualità di obiettivo* i report ottenuti tramite tali strumenti, contenenti i risultati della rilevazione. Tali report costituiranno parte integrante ed essenziale del documento. Il DEC di Fondimpresa si riserva di richiedere al Fornitore l'accesso agli strumenti in modo da poter replicare i risultati.

Al fine di consentire ai responsabili di FONDIMPRESA l'accesso in tempo reale alla documentazione di progetto e di utente durante tutte le fasi del progetto, l'Affidatario dovrà predisporre un opportuno repository interrogabile tramite interfaccia web.

8.9 Pianificazione dei documenti di contratto

L'affidatario deve produrre e mantenere aggiornato per tutta la durata del contratto la pianificazione delle date di consegna dei documenti contrattuali. Ogni riga del registro deve contenere in via esemplificativa e non esaustiva, il titolo del documento, la data prevista di emissione e la data reale di approvazione e/o consegna, la modalità cui il documento o la documentazione è stata inviata al Fondo.
Il piano dei documenti deve essere consegnato a Fondimpresa non oltre 10 giorni lavorativi dalla data di inizio attività e deve essere aggiornato mensilmente per tutta la durata del contratto con un periodo di pianificazione di almeno 6 mesi futuri.
Alcuni esempi di documenti che devono essere presenti sono: Piano di Backup, organigramma e matrice delle responsabilità aggiornati corredati di *escalation path*, Baseline, Proposta delle aree di miglioramento, Esiti backup, Definizione dei tempi di retention, Risk assessment, Vulnerability assessment, Penetration test ecc.

Si riporta si seguito un elenco indicativo dei documenti da presentare per i primi sei mesi dall'inizio delle attività contrattuali:

Scadenza	**Contenuto del Documento**	**Riferimento**
15gg	Pianificazione messa in esercizio del Registro REF	4.1
60gg	Nuova Baseline	4.2
5gg	Definizione incident report	4.4.1
30gg	Piano di Backup	4.4.3

6 mesi	Report stato dei supporti di BackUp e Restore	4.4.3
1 mesi	Report stato dei BackUp	4.4.3
3 mesi	Report di analisi dei log	4.4.4
5gg	Elenco degli amministratori di sistema	4.4.4.4
presa in carico	Analisi statica del Codice, vulnerability assessment e penetration test (anche applicativi), baseline della sicurezza, e dettagliato documento di remediation di eventuali criticità evidenziate	4.4.5
30gg	Manuale di gestione e conservazione documentale	4.4.8
30gg	Elenco risorse impiegate sul progetto	7
60gg	Manuale di gestione applicativo	8.10
30gg	Rapporto mensile indicatori di qualità SAL	8.11 - 13
30gg	Aggiornamento Organigramma, matrice responsabilità, escalation path	11
5gg	Struttura mensile Report	13
5gg	Mappatura completa dati trasferiti verso paesi esterni all'UE	14

9 Livelli di servizio e penali

L'Affidatario deve rendere disponibili a Fondimpresa strumenti idonei all'autonoma rilevazione e verifica dei parametri oggetto dei livelli di servizio della fornitura.

I livelli di servizio attesi sono introdotti per la valutazione quantitativa e qualitativa dei servizi sotto l'ipotesi di fruibilità del sistema H24, 7 gg su 7. Le metriche sono raggruppate in base alle seguenti aree:

- Sviluppo Software e MEV – (SW);
- Ambiente di Esercizio e Conduzione tecnica – (EC);
- Manutenzione – (MN);
- Affiancamento per subentro nuovo fornitore – (SB);
- Gruppi di Lavoro – (GL);
- Documentazione – (DC).

La rilevazione e la valorizzazione degli indicatori dovrà essere effettuata dall'Affidatario e approvata da FONDIMPRESA attraverso una costante e puntuale attività di monitoraggio dei livelli quantitativi e qualitativi dei servizi erogati dall'Affidatario.

I momenti di controllo e verifica sono costanti per tutta la durata della fornitura e garantiscono una visibilità completa e dettagliata sull'avanzamento delle attività.

Le attività di verifica e controllo riguardano:

- Verifica dell'andamento operativo della fornitura o della singola attività (SAL Operativo)
- Verifica dell'andamento economico e generale del contratto (SAL Economico – Generale)

Il dettaglio è riportato nella seguente tabella:

Attività di verifica	Oggetto	Finalità	Attori	Frequenza	Output
SAL OPERATIVO	Intero contratto	Monitoraggio attività operative, controllo costi e attestazione di consegna dei rilasci, controllo	DEC e Responsabile operativo dell'affidatario	Mensile o su richiesta di Fondimpresa	Verbale di SAL OPERATIVO

		qualità della fornitura e del rispetto degli SLA definiti			
SAL ECONOMICO GENERALE	Intero contratto	Verifica dei costi, consumi e andamento generale del contratto	DEC e Capo progetto dell'affidatario	Trimestrale o su richiesta di Fondimpresa	Verbale di SAL ECONOMICO GENERALE

Eventuali scostamenti, criticità, anomalie ecc. verranno evidenziate dal DEC tramite comunicazione ufficiale. Per forniture "a corpo" o "a misura", la frequenza delle riunioni sarà almeno in corrispondenza delle Milestone previste. Fondimpresa potrà richiedere l'esecuzione di SAL con frequenza maggiore, soprattutto in presenza di progetti complessi.

Di seguito la mappatura dei controlli previsti.

Responsabile	**A Corpo/A Misura**	**A Canone**
Fornitore	Fornisce evidenza del raggiungimento di quanto previsto e pianificato	
Fondimpresa	Esegue controlli in termini di: • Avanzamento delle attività sulla base dei rilasci raggiunti fasi / funzionalità • Qualità della fornitura erogata in conformità ai requisiti • Aggiornamento delle tempistiche di consegna se necessario	Esegue controllo in termini di: • Qualità della fornitura erogata in conformità ai requisiti
	Esegue il controllo dei Livelli di Servizio	
Fornitore	Consegna i rilasci previsti	Consegna evidenze relative allo svolgimento del servizio
Fondimpresa	Verifica e valida quanto consegnato e segnala al Fornitore le eventuali Criticità	
Fornitore	Gestisce Criticità	
Fondimpresa	Controlla e chiude eventuali Criticità	
	Esegue validazione del rilascio consegnato, verbalizzando	Esegue validazione delle eventuali evidenze, verbalizzando

Le Azioni correttive vengono attivate nel momento in cui si presentano violazioni dei livelli di servizio previsti o in presenza di criticità che pregiudicano il perseguimento degli obiettivi prefissati. Tutte le azioni correttive verranno notificate a FONDIMPRESA nello SLA report e riportate sull'attestazione di regolare esecuzione del periodo di riferimento. Saranno identificate:

1. le violazioni rilevate;
2. le cause che hanno determinato le violazioni;
3. gli effetti delle violazioni;
4. le azioni correttive impiegate;
5. eventuali proposte di modifiche in termini di servizi;
6. costi riconducibili alle violazioni riscontrate.

Se nel corso dello svolgimento delle attività dovessero subentrare situazioni tali da richiedere una modifica delle condizioni precedentemente concordate, Fondimpresa ed il Fornitore devono formalizzare le decisioni assunte all'interno del primo verbale utile di SAL OPERATIVO da predisporre.

L'Attestazione di regolare esecuzione, documento a carico di Fondimpresa, sintetizza le attività oggetto di verifica, segnalando eventuali criticità riscontrate e le azioni concordate per la risoluzione delle criticità.

La firma del documento, apposta dal DEC di Fondimpresa e Capo progetto dell'affidatario, attesta la piena condivisione da parte di entrambi dei contenuti riportati nel verbale e, salvo esplicita dichiarazione, costituisce formale validazione delle consegne descritte nel documento.

9.1 Sviluppo Software e MEV

Per il servizio di *Sviluppo Software e MEV* si prende in considerazione per la valutazione dei Livelli di Servizio la seguente composizione di indicatori e metriche.

SW-COLL: Esito del collaudo

Descrizione	Questo indicatore viene utilizzato per valutare l'esito della fase di collaudo. La metrica utilizzata è l'Esito della fase di Collaudo.
Unità di misura	N/A
Periodo di riferimento	Durata intervento di realizzazione.
Frequenza misurazione	A ogni realizzazione.
Dati da rilevare	Rilevazione esito da verbale di collaudo.
Formula	*SW-COLL = Esito del verbale di collaudo.*
Risultati Attesi (valore soglia)	POSITIVO
Penale	5‰ (cinquepermille) dell'importo previsto, con minimo di 200€.

SW-RTC: Rispetto dei tempi concordati

Descrizione	Questo indicatore viene utilizzato per misurare l'aderenza dei tempi tra la pianificazione dei deliverable e le date effettive di consegna. La metrica utilizzata sono le giornate intercorrenti tra le date di consegna dei deliverable contrattuali (documenti di fine analisi e piano di collaudo) concordate e quelle effettive.
Unità di misura	Giorni
Periodo di riferimento	Durata intervento di realizzazione
Frequenza misurazione	A ogni realizzazione per ogni deliverable contrattuale quando richiesto da Fondimpresa
Dati da rilevare	• Data di consegna prevista deliverable contrattuale i-esima (D_i^P). • Data effettiva deliverable contrattuale i-esima (D_i^E). • Elenco deliverable
Formula	*SW-RTC$_i$* = $D_i^E - D_i^P$
Risultati Attesi (valore soglia)	*SW-RTC$_i$ ≤ 0*
Penale	• *SW-RTC$_i$* ≤ 10 gg, 0,5‰ (zerovirgolacinquepermille) dell'importo previsto, con un minimo di € 200 (duecento). • *SW-RTC$_i$* > 10 gg, ulteriore 0,5‰ (zerovirgolacinquepermille) dell'importo previsto, con un minimo di € 200 (duecento) ogni 10 giorni, o frazioni di questo periodo, di ulteriore ritardo.

SW-TRLS: Tempo di rilascio

Descrizione	Questo indicatore viene utilizzato specificamente per misurare l'aderenza del tempo di rilascio alla pianificazione fatta. Il tempo di rilascio misura le giornate intercorrenti tra la data concordata di fine realizzazione (o fine collaudo) e quella effettiva.

Unità di misura	Giorni
Periodo di riferimento	Durata intervento di realizzazione.
Frequenza misurazione	A ogni realizzazione.
Dati da rilevare	• Data concordata di fine realizzazione (o fine collaudo) (D_p). • Data effettiva di fine realizzazione (o fine collaudo) (D_e). • Tempo di realizzazione previsto (T_R).
Formula	*SW-TRLS* = D_e-D_p
Risultati Attesi (valore soglia)	*SW-TRLS* $\leq \begin{cases} 3\%\ T_R & 3\%\ T_R \geq 5 \\ 5 & 3\%\ T_R < 5 \end{cases}$
Penale	*SW-TRLS* > 5 gg ($3\%\ T_R < 5$) o *SW-TRLS* > $3\%\ T_R$ (se $3\%\ T_R \geq 5$), 1‰ (unopermille) dell'importo previsto, con un minimo di € 200 (duecento) ogni 5 giorni, o frazioni di questo periodo, di ritardo.

SW-DIF: Difettosità del Software

Descrizione	Questo indicatore misura l'accuratezza della fase di codifica e di testing del software realizzato. La Metrica utilizzata è il numero totale N degli errori nel primo anno di esercizio dell'applicazione realizzata. Tale indicatore si applica solo ed esclusivamente ai nuovi sviluppi.
Unità di misura	Numero
Periodo di riferimento	Primo anno di esercizio di ogni nuovo sviluppo
Frequenza misurazione	A ogni realizzazione
Dati da rilevare	N: Numero di errori nel primo anno di esercizio del software per i nuovi sviluppi
Formula	*SW-DIF = N*
Risultati Attesi (valore soglia)	*SW-DIF ≤ 10*
Penale	1‰ (unopermille) dell'importo previsto per il nuovo sviluppo in caso di violazione della soglia prevista.

9.2 Ambiente di Esercizio e Conduzione tecnica

Per ambiente di esercizio si intende il sistema di esercizio REF.

I livelli di servizio per l'ambiente di esercizio e la conduzione tecnica (software di base e hardware) devono essere valutati almeno secondo il rispetto dei tempi di fornitura, la Disponibilità totale, i Tempi di risposta e gli indicatori di Accessibilità.

9.2.1 Fornitura nuovo HW e relativo software a corredo.

Per il servizio di fornitura, installazione e configurazione di nuovo Hardware nell'ambito dell'affidamento si prende in considerazione, per la valutazione dei Livelli di Servizio, la seguente composizione di indicatori e metriche.

EC-RTC: Rispetto dei tempi concordati

Descrizione	Questo indicatore viene utilizzato per misurare l'aderenza dei tempi tra la pianificazione delle date di consegna chiavi in mano di eventuale nuovo HW (e relativo software a corredo) e quelle effettive. La metrica utilizzata sono le giornate intercorrenti tra le date consegna contrattuali concordate e quelle effettive con esito di collaudo positivo.
Unità di misura	Giorni
Periodo di riferimento	Durata intervento di realizzazione

Frequenza misurazione	A ogni fornitura per ogni consegna contrattuale quando richiesto da Fondimpresa.
Dati da rilevare	• Data di consegna prevista contrattuale i-esima (D_i^P) • Data effettiva consegna i-esima (D_i^E) • Elenco deliverable
Formula	*EC-RTC$_i$* = $D_i^E - D_i^P$
Risultati Attesi (valore soglia)	*EC-RTC$_i$ ≤ 7*
Penale	1‰ (unopermille) del corrispettivo totale dell'attività per ogni giorno solare di ritardo superiore al settimo giorno fino al raggiungimento del 10% dell'importo contrattuale.

9.2.2 Livelli di servizio per Change Management

Per quanto riguarda le attività di Change Management viene definito un livello di servizio per la realizzazione delle RFC.

EC-RFC: Rispetto dei tempi concordati

Descrizione	Questo indicatore viene utilizzato per misurare l'aderenza dei tempi pianificati/concordati di change e quelli effettivi. La metrica utilizzata sono le giornate intercorrenti tra le date pianificate/concordate e quelle effettive.
Unità di misura	Giorni
Periodo di riferimento	Durata intervento di realizzazione
Frequenza misurazione	A ogni RFC
Dati da rilevare	• Data di consegna prevista contrattuale i-esima (D_i^P). • Data effettiva consegna i-esima (D_i^E). • Elenco deliverable.
Formula	*EC-RFC$_i$* = $D_i^E - D_i^P$
Risultati Attesi (valore soglia)	*EC-RFC$_i$ ≤ 0*
Penale	Per ogni giorno e/o frazione di giorno superiore al minimo verrà applicata una penale di € 50 (cinquanta).

9.2.3 Disponibilità totale

EC-DTD: Disponibilità totale del datacenter su base annuale durante 36 mesi di conduzione tecnica

Descrizione	Questo indicatore viene utilizzato per valutare quantitativamente e qualitativamente la disponibilità del datacenter (cfr. par 4.4.6)
Unità di misura	Percentuale
Periodo di riferimento	Durata contratto
Frequenza misurazione	Annuale
Dati da rilevare	• ΔT: Periodo di osservazione (anno). • d_i: Durata del disservizio "i-esimo": rappresenta il periodo di tempo, misurato in ore solari e frazioni, compreso tra l'apertura e la chiusura di un determinato disservizio. • $M(\Delta T)$: Numero totale di disservizi in "ΔT". • $T(\Delta T)$: rappresenta il "Periodo di servizio del sistema nel periodo di osservazione", cioè l'intervallo di tempo, continuo e misurato in ore solari nell'arco delle 24 ore giornaliere.

Formula	$$EC - DTD = \left(1 - \frac{\sum_{i=1}^{M(\Delta T)} d_i}{T(\Delta T)}\right) * 100$$
Risultati Attesi (valore soglia)	*EC-DTD ≥ 99,995%*
Penale	Per ogni riduzione di 0,001% rispetto al predetto valore minimo, verrà applicata una penale pari a € 10 (dieci).

EC-DTM: Disponibilità totale del sistema su base mensile durante 36 mesi di conduzione tecnica

Descrizione	Questo indicatore viene utilizzato per valutare quantitativamente e qualitativamente le modalità di impiego di risorse umane e tecnologiche connesse con l'operatività del sistema.
Unità di misura	Percentuale
Periodo di riferimento	Durata contratto
Frequenza misurazione	Mensile
Dati da rilevare	• ΔT: Periodo di osservazione (mese). • d_i: Durata del disservizio "i-esimo": rappresenta il periodo di tempo, misurato in ore solari e frazioni, compreso tra l'apertura e la chiusura di un determinato disservizio. • $M(\Delta T)$: Numero totale di disservizi in "ΔT". • $T(\Delta T)$: periodo di servizio del sistema nel periodo di osservazione: rappresenta il "periodo di servizio del sistema", ovvero l'intervallo di tempo, continuo e misurato in ore solari, nel quale gli utenti devono essere in grado di fruire dei servizi del Sistema.
Formula	$$EC - DTM = \left(1 - \frac{\sum_{i=1}^{M(\Delta T)} d_i}{T(\Delta T)}\right) * 100$$
Risultati Attesi (valore soglia)	*EC-DTM ≥ 99,7%*
Penale	Per ogni riduzione dello 0,1% rispetto al predetto valore minimo, da valutarsi durante il periodo di conduzione tecnica del Sistema, verrà applicata una penale pari a € 30 (trenta).

EC-DTA: Disponibilità totale del sistema base annuale durante 36 mesi di conduzione tecnica

Descrizione	Questo indicatore viene utilizzato per valutare quantitativamente e qualitativamente le modalità di impiego di risorse umane e tecnologiche connesse con l'operatività del sistema.
Unità di misura	Percentuale
Periodo di riferimento	Durata contratto
Frequenza misurazione	Annuale
Dati da rilevare	• ΔT: Periodo di osservazione (12 mesi). • d_i: Durata del disservizio "i-esimo": rappresenta il periodo di tempo, misurato in ore solari e frazioni, compreso tra l'apertura e la chiusura di un determinato disservizio. • $M(\Delta T)$: Numero totale di disservizi in "ΔT". • $T(\Delta T)$: periodo di servizio del sistema nel periodo di osservazione: rappresenta il "periodo di servizio del sistema", ovvero l'intervallo di tempo, continuo e misurato in ore solari, nel quale gli utenti devono essere in grado di fruire dei servizi del Sistema.

Formula	$$EC - DTA = \left(1 - \frac{\sum_{i=1}^{M(\Delta T)} d_i}{T(\Delta T)}\right) * 100$$
Risultati Attesi (valore soglia)	*EC-DTA ≥ 99,5%*
Penale	Per ogni riduzione dello 0,1% rispetto al predetto valore minimo, da valutarsi durante il periodo di conduzione tecnica del Sistema, verrà applicata una penale pari a € 30 (trenta).

9.2.4 Accessibilità del sistema

Il numero di sessioni utente contemporanee supportate dal sistema informatico devono risultare adeguate alla platea di utenti potenziale.
Dovrà essere garantita l'accessibilità per 10.000 sessioni utente contemporanee. Per tale indicatore sono previsti i livelli di servizio riportati nella seguente tabella:

SESSIONI ATTIVE CONTEMPORANEE	PENALE (mancata accessibilità del sistema in base al numero di utenti collegati)
fino a 1500	1‰ dell'importo del servizio di Hosting e conduzione per giorno o frazione di giorno di disservizio
da 1501 a 3000	0,8‰ dell'importo del servizio di Hosting e conduzione per giorno o frazione di giorno di disservizio
da 3001 a 5000	0,5‰ dell'importo del servizio di Hosting e conduzione per giorno o frazione di giorno di disservizio
da 5001 a 10.000	0,3‰ dell'importo del servizio di Hosting e conduzione per giorno o frazione di giorno di disservizio
Oltre le 10.000	Non applicabile

L'affidatario nell'ambito del sistema di monitoraggio dei servizi e sistemi dovrà rendere disponibile un cruscotto di verifica del presente indicatore.
La soluzione proposta deve garantire la possibilità di gestire un numero maggiore di sessioni attive di utenti e servizi registrati, al crescere delle esigenze di FONDIMPRESA; tale requisito deve essere soddisfatto senza modifiche al Software applicativo e all'architettura software di riferimento utilizzata, aggiungendo o potenziando le componenti che costituiscono il sistema.
Per soddisfare il parametro precedentemente definito, la soluzione deve essere dimensionata e realizzata nei termini delle sue componenti hardware e software, dell'architettura e delle tecnologie.

9.3 Manutenzione

La manutenzione dell'intera infrastruttura hardware e software deve essere svolta in accordo con un dettagliato ***"Piano di Manutenzione ed Assistenza e Help Desk di secondo livello"*** da produrre come **parte integrante dell'offerta tecnica** contenente almeno:

- l'organizzazione del servizio di manutenzione hardware e software;
- la descrizione analitica delle infrastrutture logistiche e tecnologiche predisposte per l'erogazione del servizio;
- la descrizione delle modalità con le quali l'Affidatario garantisce l'adeguamento nel tempo della struttura organizzativa e tecnologica prevista;
- i livelli di servizio offerti;
- la descrizione del numero degli operatori e dei profili professionali impiegati.

I livelli di servizio per la manutenzione dovranno essere garantiti in relazione ai seguenti indicatori:

- tempi medi di intervento/ripristino HW, SW di base e di servizio;
- tempi medi di intervento/ripristino SW applicativo.

Tali livelli di servizio comprendono tutte le eventuali attività di salvataggio/ripristino del SW di base, del SW di servizio, del SW applicativo, dei tool software, nonché delle basi di dati, del patrimonio informativo del sistema e di quant'altro, più in generale, costituisca elemento necessario per la corretta operatività. Essi riguardano, anche, quelle eventuali anomalie imputabili a un uso improprio del sistema da parte dell'utente.

9.3.1 Tempi medi di intervento/ripristino HW, SW di base e di servizio

MN-TMI: Tempo medio di intervento (HW/SW di base e di servizio) dalla ricezione della richiesta di assistenza

Descrizione	Questo è un indicatore quantitativo utilizzato per valutare l'efficienza dell'Affidatario, in termini di qualità di distribuzione del lavoro e di supporto alla pianificazione, in merito agli interventi di assistenza e manutenzione effettuati sulle componenti HW e SW di base e di servizio costituenti il sistema, 7 giorni su 7, 24 ore su 24. Il "tempo medio di intervento" (T_m) può essere calcolato, in riferimento a ciascun periodo di osservazione ΔT = 1 mese solare, come media dei singoli tempi di intervento effettuati nel già menzionato periodo di osservazione.
Unità di misura	Ore solari
Periodo di riferimento	Durata contratto
Frequenza misurazione	Mensile
Dati da rilevare	• *ΔT*: Periodo di osservazione (mese). • d_i: Durata del tempo di intervento "i-esimo", calcolato come differenza tra il momento di inizio intervento e il momento di ricezione della richiesta di assistenza. • *N(ΔT)*: Numero totale di interventi in "*ΔT*".
Formula	$$MN-TMI = \frac{\sum_{i=1}^{N(\Delta T)} d_i}{N(\Delta T)}$$
Risultati Attesi (valore soglia)	*MN-TMI ≤ 4 ore*
Penale	Per ogni ora e/o frazione di ora superiore al minimo verrà applicata una penale di € 50 (cinquanta).

MN-TMR: Tempo medio di ripristino (HW/SW di base e di servizio) dall'inizio dell'intervento

Descrizione	Questo è un indicatore quantitativo utilizzato per valutare l'efficienza dell'Affidatario, in termini di qualità di distribuzione del lavoro e di supporto alla pianificazione, in merito agli interventi di assistenza e manutenzione effettuati sulle componenti HW e SW di base, di servizio costituenti il sistema, 7 giorni su 7, 24 ore su 24. Il "tempo medio di intervento/ripristino" (T_m) può essere calcolato, in riferimento a ciascun periodo di osservazione ΔT = 1 mese solare, come media dei singoli tempi di intervento/ripristino effettuati nel già menzionato periodo di osservazione.
Unità di misura	Ore solari
Periodo di riferimento	Durata contratto
Frequenza misurazione	Mensile

Dati da rilevare	• *ΔT*: Periodo di osservazione (mese). • d_i: Durata del ripristino "i-esimo" calcolato come la differenza tra il momento di fine ripristino e l'inizio intervento. • *N(ΔT)*: Numero totale di interventi in "*ΔT*".
Formula	$$MN - TMR = \frac{\sum_{i=1}^{N(\Delta T)} d_i}{N(\Delta T)}$$
Risultati Attesi (valore soglia)	*MN-TMR ≤ 4 ore*
Penale	Per ogni ora e/o frazione di ora superiore al minimo verrà applicata una penale di € 100 (cento).

9.3.2 Tempi medi di intervento/ripristino SW applicativo

MN-TMIA: Tempo medio di intervento (SW applicativo) dalla ricezione della richiesta di assistenza

Descrizione	Questo è un indicatore quantitativo utilizzato per valutare l'efficienza dell'Affidatario, in termini di qualità di distribuzione del lavoro e di supporto alla pianificazione, in merito agli interventi di assistenza e manutenzione effettuati sulle componenti SW dell'applicativo, 7 giorni su 7, 24 ore su 24. Il "tempo medio di intervento" (T_m) può essere calcolato, in riferimento a ciascun periodo di osservazione ΔT = 1 mese solare, come media dei singoli tempi di intervento effettuati nel già menzionato periodo di osservazione.
Unità di misura	Ore solari
Periodo di riferimento	Durata contratto
Frequenza misurazione	Mensile
Dati da rilevare	• *ΔT*: Periodo di osservazione (mese). • d_i: Durata del tempo di intervento "i-esimo", calcolato come differenza tra il momento di inizio intervento e il momento di ricezione della richiesta di assistenza. • *N(ΔT)*: Numero totale di interventi in "*ΔT*".
Formula	$$MN - TMI = \frac{\sum_{i=1}^{N(\Delta T)} d_i}{N(\Delta T)}$$
Risultati Attesi (valore soglia)	*MN-TMI ≤ 2 ore*
Sanzione	Per ogni ora e/o frazione di ora superiore al minimo verrà applicata una penale di € 50 (cinquanta)

MN-TMRB: Tempo medio di ripristino (SW applicativo) dall'inizio dell'intervento per i "malfunzionamenti bloccanti" [3]

Descrizione	Questo è un indicatore quantitativo utilizzato per valutare l'efficienza dell'Affidatario, in termini di qualità di distribuzione del lavoro e di supporto alla pianificazione, in merito agli interventi di assistenza e manutenzione effettuati sulle componenti SW dell'applicativo, 7 giorni su 7, 24 ore su 24. Il "tempo medio di intervento/ripristino" (T_m) può essere calcolato, in riferimento a ciascun periodo di osservazione ΔT = 1

3 Con il termine "***malfunzionamenti bloccanti***" si identificano tutte le eventuali anomalie che direttamente o indirettamente comportano il blocco o la non disponibilità di una o più "***funzionalità o servizi***" rispetto alle esigenze di una qualsiasi delle categorie di utenti.

	mese solare, come media dei singoli tempi di intervento/ripristino effettuati nel già menzionato periodo di osservazione.
Unità di misura	Ore solari
Periodo di riferimento	Durata contratto
Frequenza misurazione	Mensile
Dati da rilevare	• *ΔT*: Periodo di osservazione (mese). • d_i: Durata del ripristino "i-esimo" calcolato come la differenza tra il momento di fine ripristino e l'inizio intervento, per i "malfunzionamenti bloccanti". • *N(ΔT)*: Numero totale di interventi in "*ΔT*".
Formula	$$MN - TMRB = \frac{\sum_{i=1}^{N(\Delta T)} d_i}{N(\Delta T)}$$
Risultati Attesi (valore soglia)	*MN-TMRB ≤ 3 ore*
Sanzione	Per ogni ora e/o frazione di ora superiore al minimo verrà applicata una penale di € 100 (cento)

MN-TMRA: Tempo medio di ripristino (SW applicativo) dall'inizio dell'intervento per i "malfunzionamenti non bloccanti"[4]

Descrizione	Questo è un indicatore quantitativo utilizzato per valutare l'efficienza dell'Affidatario, in termini di qualità di distribuzione del lavoro e di supporto alla pianificazione, in merito agli interventi di assistenza e manutenzione effettuati sulle componenti SW dell'applicativo, 7 giorni su 7, 24 ore su 24. Il "tempo medio di intervento/ripristino" (T_m) può essere calcolato, in riferimento a ciascun periodo di osservazione ΔT = 1 mese solare, come media dei singoli tempi di intervento/ripristino effettuati nel già menzionato periodo di osservazione.
Unità di misura	Ore solari
Periodo di riferimento	Durata contratto
Frequenza misurazione	Mensile
Dati da rilevare	• *ΔT*: Periodo di osservazione (mese). • d_i: Durata del ripristino "i-esimo" calcolato come la differenza tra il momento di fine ripristino e l'inizio intervento, per i "malfunzionamenti non bloccanti". • *N(ΔT)*: Numero totale di interventi in "*ΔT*"
Formula	$$MN - TMRA = \frac{\sum_{i=1}^{N(\Delta T)} d_i}{N(\Delta T)}$$
Risultati Attesi (valore soglia)	*MN-TMRA ≤ 12 ore*
Sanzione	Per ogni ora e/o frazione di ora superiore al minimo verrà applicata una penale di € 50 (cinquanta)

9.4 Affiancamento a fine contratto per subentro nuovo fornitore

Il Fornitore deve garantire al termine della durata contrattuale, o in caso di risoluzione anticipata del contratto per qualsiasi motivo, un periodo di affiancamento per subentro di almeno un mese al nuovo

4 Con il termine *"**malfunzionamenti non bloccanti**"* si identificano, per esclusione rispetto alla nota precedente, tutte le eventuali anomalie che non rientrano nella precedente categoria "***malfunzionamenti bloccanti***".

fornitore, per tutti i servizi oggetto del presente affidamento, in accordo con quanto previsto nel ***"Piano di affiancamento a fine contratto"*** da produrre come **parte integrante dell'offerta tecnica** contenente almeno:

- la modalità di svolgimento dell'affiancamento per subentro;
- la pianificazione temporale delle attività di affiancamento;
- la descrizione analitica delle infrastrutture logistiche e tecnologiche predisposte per l'erogazione del servizio;
- i livelli di servizio offerti;
- la descrizione del numero degli operatori e dei profili professionali impiegati.

I livelli di servizio per l'affiancamento per subentro dovranno essere garantiti in relazione ai seguenti indicatori:

- tempo massimo di attivazione del servizio;
- aderenza alla pianificazione delle attività;
- soddisfazione del cliente.

9.4.1 Tempo massimo di attivazione del servizio

SB-TAS – Tempo massimo di attivazione del servizio

Descrizione	Il tempo massimo di attivazione viene misurato come numero di giorni dalla richiesta di Fondimpresa dell'attivazione del servizio di affiancamento e l'effettiva attivazione.
Unità di misura	Giorni
Periodo di riferimento	Avvio attività di affiancamento per subentro
Frequenza misurazione	N/A
Dati da rilevare	• D_r: Data di richiesta di attivazione del servizio di affiancamento. • D_e: Data di effettiva attivazione del servizio.
Formula	$SB - TAS = D_e - D_r$
Risultati Attesi (valore soglia)	SB-TAS ≤ 5
Penale	1‰ (unopermille) del corrispettivo totale del presente contratto per ogni giorno solare di ritardo.

9.4.2 Aderenza alla pianificazione delle attività

SB-APA: Aderenza alla pianificazione delle attività

Descrizione	Questo indicatore viene utilizzato per misurare l'aderenza dei tempi tra la pianificazione delle attività previste dal piano di affiancamento a fine contratto e quelle effettive. La metrica utilizzata sono le giornate intercorrenti tra le date concordate e quelle effettive.
Unità di misura	Giorni
Periodo di riferimento	Durata di affiancamento
Frequenza misurazione	A ogni realizzazione per ogni attività prevista dal piano di affiancamento a fine contratto.
Dati da rilevare	• Data concordata, prevista per l'attività i-esima (D_i^P). • Data effettiva per l'attività i-esima (D_i^E). • Elenco attività
Formula	*SB-ATA$_i$* = $D_i^E - D_i^P$
Risultati Attesi (valore soglia)	*SB-ATA$_i$ ≤ 1*

Sanzione	1‰ (unopermille) del corrispettivo totale del presente contratto per ogni giorno solare di ritardo.

9.5 Gruppi di Lavoro

Il fornitore deve garantire la qualità e la quantità delle risorse impiegate nell'ambito dei servizi e attività previste dall'affidamento in conformità a quanto previsto nel **"Piano dell'organizzazione dei gruppi di lavoro"** da produrre come **parte integrante dell'offerta tecnica** contenente almeno:

- metodologie e strumenti utilizzati per il management dei gruppi di lavoro;
- management e organizzazione della struttura di coordinamento dei gruppi di lavoro;
- management e organizzazione (processi e struttura organizzativa) dei singoli gruppi di lavoro per ognuno dei servizi oggetto dell'affidamento;
- composizione dei gruppi di lavoro: devono essere forniti i curricula delle persone che compongono i gruppi di lavoro per ognuno dei servizi.

I livelli di servizio per i gruppi di lavoro dovranno essere garantiti in relazione ai seguenti indicatori:

- Tempestività nell'inserimento/sostituzione di personale;
- Personale inadeguato;
- Turnover del personale.

9.5.1 Tempestività nell'inserimento/Sostituzione di Personale

Con questo indicatore si misura la tempestività nell'inserimento/sostituzione di tutte le risorse impiegate nella fornitura compresi i ruoli di interfaccia verso Fondimpresa.
Tale indicatore è misurato in giorni solari dalla richiesta/autorizzazione di inserimento /sostituzione.
Viene rilevato a ogni inserimento/sostituzione.

GL-TISP: Tempestività nell'Inserimento/Sostituzione di Personale

Descrizione	Questo indicatore viene utilizzato per misurare la tempestività nell'inserimento/sostituzione di tutte le risorse impiegate nella fornitura compresi i ruoli di interfaccia verso Fondimpresa. Giornate intercorrenti tra la richiesta del DEC e l'inserimento/sostituzione della risorsa richiesta.
Unità di misura	Giorni
Periodo di riferimento	Durata contratto
Frequenza misurazione	A ogni richiesta di inserimento/sostituzione
Dati da rilevare	• Data Richiesta Risorsa *(Data_rich_risorsa).* • Data Inserimento/Sostituzione Risorsa *(Data_ins_sost_risorsa).* • Tempo necessario al DEC a valutare la risorsa proposta dal Fornitore (*T_assenso*).
Formula	*GL-TISP = Data_ins_sost_risorsa - Data_rich_risorsa - T_assenso*
Risultati Attesi (valore soglia)	*GL-TISP ≤ 4*
Penale	TISP > 4 gg, € 200 (duecento) ogni 5 giorni, o frazioni di questo periodo, di ritardo.

9.5.2 Personale Non Adeguato

GL-PRNA: Personale Non Adeguato

Descrizione	Nella misura dell'indicatore vanno considerate tutte le risorse impiegate nell'erogazione della fornitura. Si deve valutare il numero di risorse sostituite, perché non ritenute adeguate, su richiesta del DEC.
Unità di misura	Numero
Periodo di riferimento	Durata contratto
Frequenza misurazione	Semestrale (a fine semestre).
Dati da rilevare	Numero risorse sostituite su richiesta del DEC $(N_{risorse\_inadeg})$.
Formula	*GL-PRNA* = $N_{risorse\_inadeg}$
Risultati Attesi (valore soglia)	*GL-PRNA = 0*
Penale	*GL-PRNA* > 0, € 500 (cinquecento) ogni unità di personale inadeguata.

9.5.2.1 Turn Over Del Personale

GL-TORS: Turn Over Del Personale

Descrizione	Con questo indicatore si misurano le sostituzioni, su iniziativa dell'Affidatario e senza l'autorizzazione del DEC, delle risorse impiegate nella fornitura, comprensive dei referenti.
Unità di misura	Numero.
Periodo di riferimento	Durata contratto.
Frequenza misurazione	Semestrale (a fine semestre).
Dati da rilevare	Numero risorse sostituite su iniziativa del Fornitore $(N_{risorse\_sostituite})$
Formula	*GL-TORS* = $N_{risorse\_sostituite}$
Risultati Attesi (valore soglia)	*GL-TORS = 0*
Penale	*GL-TORS* > 0, €1000 (mille) per ogni sostituzione non autorizzata.

9.6 Documentazione

DC-TCDR – Tempi di consegna di documentazione e/o report

Descrizione	Con questo indicatore si misura l'aderenza dei tempi effettivi di consegna dei documenti e/o report correttamente formati e completi rispetto ai tempi previsti da contratto.
Unità di misura	Giorni lavorativi
Periodo di riferimento	Durata contratto
Frequenza misurazione	A ogni scadenza contrattualmente prevista dalla tipologia di documento
Dati da rilevare	• Data programmata di consegna del documento/report (previsto o a richiesta) (D_i^p). • Data di effettiva ricezione della documentazione (D_i^e) . • Elenco report e documenti *i.*
Formula	*DC-TCDR* = $D_i^e - D_i^p$
Risultati Attesi (valore soglia)	*DC-TCDR ≤ 6*
Penale	*DC-TCDR* > 6, €200 (duecento) ogni 6 giorni, o frazioni di questo periodo, di ritardo.

10 Formazione del personale

L'Affidatario è tenuto a erogare, a richiesta di FONDIMPRESA, formazione di base e avanzata sull'uso del Registro Elettronico (REF), rivolta al personale del Fondo per un massimo complessivo di 24 ore annue. Tale attività è già remunerata dal corrispettivo complessivo riconosciuto in sede contrattuale.

11 Piano della qualità

Come parte integrante dell'offerta tecnica l'Affidatario deve presentare il ***"Piano della qualità"*** da esso adottato che comprenda ognuno dei servizi oggetto del presente Capitolato con particolare riferimento all'organizzazione del processo e del lavoro.
Nella redazione del Piano della Qualità il Fornitore terrà come guida lo schema di riferimento di seguito descritto.

1. Scopo e Campo di applicazione
   Si chiede di indicare:
   - la finalità del documento;
   - il campo di applicazione (comprese le limitazioni, cioè i casi in cui questo piano non verrà applicato);
   - l'organizzazione del documento e gli eventuali allegati.

2. Documenti applicabili e di riferimento
   2.1. Documenti applicabili
   Si chiede di indicare:
   - il Sistema di Gestione della Qualità (SGQ) adottato per il contratto da applicare ad esempio per:
     - tenuta sotto controllo dei documenti;
     - tenuta sotto controllo delle registrazioni della qualità;
     - azioni correttive;
     - azioni preventive;
     - audit;
     - gestione degli incidenti;
   - altri piani pertinenti (ad esempio: piani di progetto, piani di gestione ambientale, di salute e sicurezza sul lavoro, di sicurezza e di gestione delle informazioni).

   2.2. Documenti di riferimento
   Si chiede di indicare i documenti che costituiscono un riferimento per quanto esposto nel Piano della Qualità.

3. Glossario
   Si chiede di descrivere abbreviazioni, acronimi, definizioni che sono utilizzate all'interno del Piano della Qualità.

4. Organizzazione
   Si chiede di:
   - definire l'organigramma del gruppo di lavoro dell'Affidatario impegnato sul contratto e le interfacce con Fondimpresa;
   - indicare i ruoli e le responsabilità di ciascun soggetto nell'organigramma mediante una matrice delle responsabilità;
   - identificare i responsabili previsti per la fornitura dei servizi oggetto del presente Capitolato.

Entro i primi 30 giorni dall'inizio delle attività contrattuali deve essere fornito un aggiornato organigramma e matrice delle responsabilità corredato di *escalation path* che dovrà essere mantenuto aggiornato durante tutta la durata del contratto (36 mesi).

5. Formazione e Addestramento del personale
   Si chiede di descrivere le attività di formazione necessarie per l'espletamento delle attività contrattuali a cui il Fornitore sottoporrà le proprie risorse.

6. Infrastruttura
   Si chiede di descrivere l'infrastruttura (hardware, software e strumenti) e gli ambienti di lavoro (per quanto non stabilito nella documentazione contrattuale). In particolare, si chiede di indicare:
   - strumenti per la gestione delle attività progettuali;

- strumenti per l'analisi, la progettazione, lo sviluppo, la creazione o la generazione del codice;
- strumenti per la gestione della configurazione e della documentazione;
- strumenti per la progettazione ed esecuzione delle prove del software;
- strumenti per le reti, compresi quelli per la riservatezza, la protezione dai virus, i "firewall", per le copie di salvataggio;
- strumenti di prima assistenza e di manutenzione.

7. Requisiti di qualità

7.1. Obiettivi e Indicatori di qualità

Si chiede identificare, in modo chiaro e non ambiguo, i requisiti di qualità del contratto, eventualmente aggiornati con quanto proposto in Offerta Tecnica. Per questo è necessario definire:

- gli attributi di qualità (caratteristiche e sotto-caratteristiche nella terminologia delle Linee guida sulla qualità dei beni e dei servizi ICT DigitPA) relativi a ciascun prodotto e a ciascun servizio, compresa l'usabilità delle interfacce utente;
- gli indicatori di qualità con cui misurare gli attributi identificati;
- i valori limite ritenuti accettabili con cui confrontare le misure degli attributi di qualità sulla base di indicatori di qualità definiti.

7.2. Indicatori di prestazione

Si chiede di indicare gli indicatori di prestazione del contratto.

7.3. Valutazione della qualità

Si chiede di descrivere le modalità che saranno utilizzate dall'Affidatario per valutare la qualità dei prodotti e dei servizi realizzati (output del contratto) prima che tali prodotti e/o servizi vengano consegnati/erogati. In particolare, si chiede di esplicitare:

- modalità di misura o di rilevamento dei dati;
- modalità di calcolo e di aggregazione delle misure (per il computo di indicatori derivati);
- frequenza delle misure;
- periodi temporali di riferimento;
- le regole con cui si perviene ai giudizi di Approvazione Incondizionata /Approvazione con Riserva / Non Approvazione di un prodotto e/o un servizio considerando i risultati delle misure relative ai singoli attributi di qualità associati al prodotto e/o livelli di servizio associati al servizio.

8. Gestione del Rischio

Si chiede di:

- descrivere le modalità operative di identificazione, valutazione, trattamento e controllo dei rischi;
- pianificare la gestione dei rischi della fornitura.

9. Gestione degli incidenti

Si chiede di descrivere tutte le attività, i ruoli e le responsabilità relative alla gestione delle violazioni di dati (personali e no), con l'obiettivo di:

- ridurre al minimo gli impatti degli incidenti di sicurezza delle informazioni;
- garantire un tempestivo ripristino delle condizioni di normale operatività;
- assicurare l'adeguato coinvolgimento di tutto il personale necessario;
- identificare gli strumenti da utilizzare per documentare gli incidenti (inclusi i "near miss"), con l'analisi delle cause e le soluzioni adottate.

12 Modalità di collaudo

I collaudi per l'accettazione delle attività realizzate nell'espletamento di tutti i servizi oggetto del presente Capitolato saranno eseguiti, in accordo con un ***"Piano dei Test"*** e un ***"Piano di collaudo"*** forniti come parte integrante dell'offerta tecnica, alla presenza di un gruppo di collaudo nominato da FONDIMPRESA.
Scopo delle operazioni di collaudo è accertare che i servizi erogati dal sistema, i prodotti forniti e le prestazioni erogate dall'Affidatario risultino conformi alle specifiche tecniche e ai livelli di qualità e sicurezza riportati nel presente Capitolato.
A seguito di ciascun collaudo dovrà essere redatto apposito verbale, congiuntamente sottoscritto dai Responsabili delle Unità/Direttori delle Aree di Fondimpresa eventualmente coinvolte nel gruppo di collaudo, dal DEC di FONDIMPRESA e dal Responsabile di Progetto per l'Affidatario, nel quale siano almeno indicate le seguenti informazioni:

- l'oggetto del collaudo;
- la tipologia di collaudo (provvisorio o definitivo);
- la data di inizio e di conclusione delle operazioni di collaudo;
- il contesto operativo in cui è stato effettuato il collaudo, con l'indicazione dell'infrastruttura HW, SW di base/di servizio, SW applicativo utilizzata;
- i prodotti, i servizi e le prestazioni esaminate;
- le procedure seguite per l'esecuzione del collaudo;
- i risultati ottenuti;
- l'esito del collaudo.

In caso di collaudo di servizi ripetitivi quali il servizio di Manutenzione adeguativa e correttiva (eccetto gli interventi di maggiore complessità), Hosting, conduzione tecnica e Manutenzione HW, il verbale di collaudo è sostituito da una attestazione di regolare esecuzione redatta dal DEC di FONDIMPRESA e controfirmata dal Responsabile di progetto per l'Affidatario.

In caso di mancato collaudo positivo potranno essere applicate le penali previste nel presente capitolato e inoltre verrà stabilito da FONDIMPRESA un termine inderogabile per la correzione delle anomalie e/o per l'integrazione delle funzionalità mancanti o parziali; si provvederà quindi a un nuovo collaudo. FONDIMPRESA potrà disporre l'effettuazione di uno o più collaudi per ogni attività svolta nell'ambito dei servizi di *Sviluppo Software e MEV*, di *MAD/MAC e Help Desk di secondo livello* (per gli interventi di maggiore complessità), per eventuali ulteriori forniture di SW o altre attività di evoluzione architetturale. Il flusso di collaudo del software realizzato è di responsabilità del DEC di Fondimpresa, che agirà come unica interfaccia nei confronti dell'Affidatario.
Saranno oggetto di verifica durante il collaudo tutti i prodotti risultanti dalle fasi di Architettura e Funzionalità e in particolare:

- software realizzato;
- manuale utente;
- manuale di gestione applicativo;
- modello dati e glossario
- dizionario dati
- file di configurazione;
- manuale di gestione del server;
- eventuali altri documenti.

Il Fornitore dovrà garantire almeno le macro-attività elencate di seguito:

- messa a disposizione e predisposizione dell'ambiente di collaudo e supporto alle attività di collaudo e testing proceduralizzato e automatico nonché agli eventuali test manuali;
- rimozione delle anomalie fino al momento dell'accettazione;
- supporto alla consegna in gestione, volto ad assicurare un corretto passaggio di consegne al Servizio di Gestione, formalizzato nella Progettazione esecutiva del lotto funzionale;
- migrazione dei dati per alimentare/aggiornare le basi dati realizzate/modificate nell'ambito degli interventi di sviluppo e manutenzione;

- supporto alle attività di passaggio in esercizio.

Nel caso in cui Fondimpresa ritenga di operare un periodo di pre-esercizio, mediante l'utilizzo di un prototipo pienamente funzionante, lo stesso sarà ritenuto parte integrante delle attività di collaudo e pertanto il fornitore dovrà garantire tutto il supporto logistico e operativo necessario al suo corretto svolgimento.

Entro sei mesi dall'ultimazione delle prestazioni contrattuali, risultante dal certificato appositamente redatto dal DEC, il gruppo di collaudo nominato dal Committente procederà a effettuare la verifica finale di conformità delle prestazioni complessivamente rese dall'Affidatario nel corso del contratto.

13 Reportistica

Al termine di ogni mese per tutta la durata dell'affidamento, l'Affidatario deve presentare, ***entro una settimana lavorativa***, un documento che racchiuda in modo ordinato tutta la reportistica indicata in Piano di Sviluppo software e MEV, Piano della qualità, Piano dell'organizzazione dei gruppi di lavoro, Piano della documentazione di progetto, Piano di Manutenzione adeguativa e correttiva, Piano di Manutenzione ed Assistenza e Help Desk di secondo livello, Documento Organizzativo della Sicurezza , Piano della Sicurezza del Data Center, Piano di Hosting, conduzione e manutenzione HW/SW, Piano di continuità operativa, Piano di affiancamento a fine contratto, Piano dei Test, Piano di collaudo, Incident Report. *La struttura del documento verrà approvata da Fondimpresa entro due settimane dalla presentazione dell'ultima versione contenente le eventuali correzioni o modifiche richieste dal Fondo*. Una volta consolidato non potrà più essere modificato dall'Affidatario senza il consenso di Fondimpresa.
Dovranno essere presenti almeno le informazioni sulle azioni eseguite nel periodo in esame e quelle pianificate per il periodo successivo, oltre agli indicatori dei livelli di servizio raggiunti (cfr. paragrafo 9).

14 Protezione dei dati personali

Tutte le attività oggetto dell'affidamento dovranno essere svolte conformemente al Regolamento (UE) 2016/679 e alla normativa nazionale applicabile in materia di protezione dei dati personali, con particolare riferimento ai principi della Privacy by design e Privacy by default di cui all'art. 25 del citato Regolamento e a quanto previsto all'articolo 32 ("Sicurezza del trattamento"). Dovrà inoltre essere rispettata la normativa secondaria nonché le eventuali ulteriori disposizioni nazionali o internazionali in materia.
Tutte le attività di sviluppo e di conduzione e manutenzione hardware e software, nonché le misure organizzative e di sicurezza fisica adottate, dovranno tenere in considerazione e documentare gli impatti in termini di protezione dei dati personali, quanto a riservatezza, integrità e disponibilità dei dati, nonché le contromisure adottate per garantire la sicurezza, in applicazione dei principi previsti all'art. 5, all'art. 25 e delle indicazioni di cui all'art. 32.
Eventuali violazioni di dati personali che dovessero verificarsi dovranno essere comunicate al DEC dell'affidamento e al DPO di Fondimpresa, a prescindere da qualsiasi valutazione circa l'impatto e le conseguenze attese della violazione stessa, senza indugio e comunque entro il tempo massimo di 12 ore dal momento in cui l'Affidatario ne sia venuto a conoscenza.
Eventuali richieste di esercizio dei diritti riconosciuti dal Regolamento (UE) 2016/679, avanzate nei confronti dell'Affidatario da parte degli interessati al trattamento, dovranno essere inoltrate immediatamente, e comunque non oltre 72 ore dalla ricezione, al DPO di Fondimpresa.
Con riferimento alle condizioni di cui al Capo V del Regolamento (UE) 2016/679 relative ai trasferimenti di dati personali verso paesi esterni all'Unione Europea (UE) o organizzazioni internazionali, l'attività dovrà essere condotta tenendo conto del quadro normativo e delle evoluzioni dello stesso, con particolare riguardo alle indicazioni fornite dall'EDPB e dal Garante per la Protezione dei Dati Personali quanto all'individuazione di misure di garanzia e protezione dei dati idonee in rapporto all'esistenza di ordinamenti giuridici che prevedono forme di accesso delle autorità statali ai dati personali dei cittadini, che non rispettano il principio di proporzionalità e non garantiscono sufficienti diritti agli interessati.

In ogni caso, l'affidatario dovrà effettuare una mappatura completa e continuamente aggiornata degli eventuali trasferimenti di dati verso paesi esterni all'UE o organizzazioni internazionali e delle relative misure di protezione dei dati adottate, dandone visibilità a Fondimpresa entro 5 giorni dalle modifiche e comunque all'inizio delle attività per le valutazioni di merito e l'eventuale opposizione.
In proposito, si intende inclusa nella nozione di trasferimento di dati qualsiasi forma di trattamento ai sensi dell'art. 4, punto 2, del Regolamento UE 2016/679, svolto in paesi terzi rispetto all'UE o organizzazioni internazionali, compreso il mero accesso a dati conservati nel territorio dell'Unione Europea da parte di personale localizzato in territorio esterno all'Unione Europea.

15 ALLEGATI

1. Manuale d’uso del Registro REF