

Procedura aperta, ai sensi dell'art. 60 del d. lgs. n. 50/2016,
per l'affidamento dei servizi di gestione, conduzione e manutenzione del
sistema informativo PREVENTIVASS

(CIG: 95326385BB)

CAPITOLATO TECNICO

Sommario

1. Premessa	4
1.1. Acronimi e definizioni	4
1.2. Oggetto, finalità, durata e valore dell'appalto	5
1.3. Fasi contrattuali	6
1.3.1 Fase di Presa in carico ed erogazione	7
1.3.2 Fase di erogazione a regime	8
1.3.3 Fase di fine fornitura	8
2. Contesto	9
2.1 Missione, Struttura e Attività dell'IVASS	9
2.2 Contesto Normativo	10
2.3 Contesto Applicativo	11
2.3.1 Portale di preventivazione	11
2.3.2 Portale Imprese	13
2.3.3 Portale Admin/Ivass	14
2.3.4 Portale Intermediari	15
2.3.5 Mobile	15
2.3.6 Flussi di alimentazione del DWH	15
2.3.7 Volumi e dimensionamento dei servizi	16
2.3.8 A2A	17
3 Descrizione dell'oggetto dell'appalto	18
3.1 Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche (CLOUD AWS)	18
3.1.1 Descrizione del Servizio	18
3.1.2 Composizione del team del Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche (CLOUD AWS)	19
3.2 Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database	19
3.2.1 Sviluppo del <i>Software</i> e Manutenzione Evolutiva del <i>Software</i>	19
3.2.2 Manutenzione App Mobile	21
3.2.3 Manutenzione Adeguativa e Correttiva	21
3.2.4 Conduzione Operativa Applicativi e Database	22
3.2.5 Strumenti di <i>Test management</i>	23
3.2.6 Accessibilità	23

3.2.7	Composizione del team dei Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database	24
3.3	Servizio di <i>Backoffice</i> e supporto alle Imprese Assicurative e Intermediari.....	25
3.3.1	Descrizione del Servizio	25
3.3.2	Composizione del team del Servizio di <i>Backoffice</i> e supporto alle Imprese Assicurative.....	26
3.4	Servizi di Supporto Specialistico / Presidio on-site.....	27
3.4.1	Descrizione del Servizio	27
3.4.2	Composizione del team del Servizio di Supporto Specialistico / Presidio on-site.....	28
3.5	Servizio di <i>cyber security</i>	28
3.5.1	<i>Security Assessment</i>	29
3.5.2	<i>Code Review</i>	29
3.5.3	Controllo Accessi Logici	29
3.5.4	Strumenti di <i>Security Incident</i> SIEM	30
3.5.5	Strumenti di <i>Vulnerability Assessment</i>	31
3.5.6	Strumenti di <i>Penetration Test</i>	32
3.5.7	Tool di <i>Log Management</i>	32
3.5.8	Gestione del <i>Web Application Firewall</i> (WAF)	33
3.5.9	<i>Assessment</i> per la protezione dei dati personali.....	33
3.5.10	<i>Hardening</i> dei sistemi.....	34
3.5.11	<i>Advanced Endpoint Protection</i> (AEP) e <i>Virtual Patching</i>	34
3.5.12	Composizione del <i>team</i> del Servizio di <i>cyber security</i>	34
3.6	Servizi trasversali	35
3.6.1	Centro Servizi.....	35
3.6.2	<i>Help Desk</i>	35
3.6.3	Servizio di <i>Incident Management</i> e <i>Trouble Ticketing</i>	36
3.6.4	Strumenti di monitoraggio H24 dei sistemi.....	37
3.6.5	Strumenti per la gestione degli sviluppi <i>DevOps</i>	37
3.6.6	Portale di governo e gestione della fornitura.....	37
3.6.7	Strumenti di <i>Change Management</i>	38
3.6.8	Strumenti di <i>Stress Test</i>	38
3.6.9	Reportistica.....	38
3.6.10	Dimensionamento dei Servizi Trasversali.....	40
3.7	Fornitura Crediti AWS.....	40

4	Modalità di esecuzione della Fornitura	41
4.1	Luogo e orari di erogazione della Fornitura	41
4.2	Tabella riepilogativa di luogo e orari di erogazione della fornitura	41
4.3	<i>Project Manager</i>	41
4.4	Reperibilità	42
4.5	Interventi fuori orario.....	42
5	MODALITA' DI EROGAZIONE	43
6	QUALITÀ DELLA FORNITURA.....	44
6.1	PIANO DELLA QUALITÀ GENERALE	44

1. Premessa

L'IVASS – Istituto per la Vigilanza sulle Assicurazioni – è un ente di diritto pubblico, istituito con legge n. 135/2012 (di conversione, con modifiche, del D.L. 95/12), che opera per garantire la stabilità del mercato assicurativo e la tutela del consumatore.

Nell'ambito delle proprie attività istituzionali l'IVASS provvede alla gestione di un sistema informativo che tramite un sito internet specializzato:

- consente al consumatore, con riferimento al proprio profilo individuale, di comparare le tariffe applicate da ciascun'impresa assicurativa relativamente al contratto base r.c. auto previsto dall'articolo 22 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012;
- offre agli intermediari assicurativi un servizio che permetta di adempiere all'obbligo previsto dall'art. 132-bis del Codice delle Assicurazioni (Obblighi informativi degli intermediari), ai sensi del quale "Gli intermediari, prima della sottoscrizione di un contratto di assicurazione obbligatoria per i veicoli a motore, sono tenuti a informare il consumatore in modo corretto, trasparente ed esaustivo sui premi offerti da tutte le imprese di assicurazione di cui sono mandatari relativamente al contratto base – (...) e, a tal fine, - forniscono l'indicazione dei premi offerti dalle imprese di assicurazione mediante collegamento telematico al preventivatore consultabile nei siti internet dell'IVASS e del Ministero dello sviluppo economico."

Per l'espletamento dei suddetti compiti l'IVASS e il Ministero dello Sviluppo Economico hanno realizzato il Preventivatore pubblico r.c. auto – denominato PREVENTIVASS - ovvero un'applicazione WEB che consente la comparazione dei prezzi delle coperture assicurative relative al contratto base r.c. auto proposte da tutte le imprese di assicurazione operanti in Italia nel ramo r.c. auto.

1.1. Acronimi e definizioni

Definizione Acronimo	Descrizione
A2A	Application to Application
AgID	Agenzia per l'Italia Digitale
ANIA	Associazione Nazionale Imprese Assicuratrici
Banca dati ATRC	Banca dati attestati di rischio, presso ANIA
Banca dati SITA	Servizio Informatico Targhe Assicurate, presso ANIA
Banca dati SIVI	Servizio Informatico Veicoli Immatricolati, tramite ANIA
BdI	Banca d'Italia
CAD	Codice dell'Amministrazione Digitale
CF	Codice Fiscale
DWH	Data Warehouse
Egon	Banca dati indirizzi stradali
GDPR	General Data Protection Regulation
IAM	Identity Access Management
Infobike	Banca dati allestimenti motocicli e ciclomotori
Infocar	Banca dati allestimenti autovetture
MFT	Managed File Transfer
MiSE	Ministero dello Sviluppo Economico
OWASP	Open Web Application Security Project

RCA	Responsabilità civile auto
REST	Representational State Transfer
RUI	Registro Unico Intermediari
SIEM	Security Information and Event Management
SOAP	Service Oriented Architecture Protocol
SPID	Sistema Pubblico di Identità Digitale
Utente non professionale	Consumatore ovvero la persona fisica come definita dall'articolo 3 del decreto legislativo 6 settembre 2005, n. 206 (Codice del consumo)
Utente professionale	Imprese di assicurazione e/o intermediari assicurativi iscritti al Registro Unico degli intermediari
UX	User Experience
WAF	Web Application Firewall

1.2. Oggetto, finalità, durata e valore dell'appalto

L'IVASS (di seguito anche "Istituto") ha indetto una procedura aperta, ai sensi dell'art. 60 del d. lgs. n. 50/2016, per l'affidamento del contratto avente ad oggetto i servizi necessari per la gestione, conduzione e manutenzione del sistema informativo PREVENTIVASS, Preventivatore pubblico r.c. auto ovvero un'applicazione WEB che consente la comparazione dei prezzi delle coperture assicurative relative al contratto base r.c. auto proposte da tutte le imprese di assicurazione operanti in Italia nel ramo r.c. auto.

Il codice CIG attribuito alla procedura è il seguente: 95326385BB.

Obiettivo del contratto è quello di garantire livelli di servizio adeguati alle necessità dell'Istituto, migliorare l'efficacia dei vari sistemi, adeguare i sistemi a eventuali necessità future, assicurare il pieno e continuo funzionamento del sistema informativo e nel contempo limitare e ottimizzare i costi di gestione. Il contratto avrà la durata di 24 mesi dalla data della stipula e comunque fino alla conclusione di tutte le attività che consentano la continuità delle funzionalità del sistema informativo PREVENTIVASS.

Il valore della base d'asta, per la durata di 24 mesi comprensiva della fase iniziale di presa in carico, riferito ai servizi e fornitura di crediti richiesti, che verranno dettagliatamente descritti nei paragrafi a seguire, è pari complessivamente a **euro 2.851.887,76** oltre IVA. Le voci che compongono la base d'asta oggetto d'offerta sono descritte al par. 1.1 del Disciplinare di Gara.

Il contratto avrà la durata di 24 mesi comprensivi della fase iniziale di presa in carico (phase in). Il contratto può essere rinnovato, per una durata pari a 24 mesi, a discrezione dell'Istituto e alle stesse condizioni contrattuali, salvo l'applicazione della clausola di revisione prezzi da applicarsi su richiesta motivata del Fornitore allo scadere del contratto.

Parametri di stima del valore dell'appalto:

RIFERIMENTO: al fine di individuare l'entità del corrispettivo dei servizi richiesti, ci si è avvalsi, per affinità nella tipologia e nella caratteristica dell'oggetto dell'appalto, della impostazione e dei parametri di riferimento mutuati dalla documentazione di Gara di CONSIP (bando pubblicato in GUUE in data 24.05.2013), avente come oggetto il Servizio Cloud Computing, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni, che si è conclusa con l'aggiudicazione del Contratto Quadro SPCL4 (stipulato il 4 agosto 2017).

PREZZI: sono state considerate le tariffe di riferimento per le figure professionali e servizi simili poste come base di gara da CONSIP, in quanto remunerative di tutti gli elementi come l'organizzazione, i mezzi, le persone, che il Fornitore dovrà approntare per la conduzione e la manutenzione del sistema informativo. Le tariffe di riferimento sono state rivalutate del 10% a titolo di recupero forfettario dell'inflazione.

DIMENSIONAMENTO: s'intende la quantificazione dei servizi in giornate/uomo necessaria a supportare la conduzione di PREVENTIVASS nel suo pieno utilizzo, che come indicato nel dettaglio al par. 2.3.7 del Capitolato tecnico, stimato per ogni anno tra i 200 e i 300 milioni di unità di preventivi generati dai sistemi di preventivazione delle imprese assicurative. Presumibilmente, salvo impedimenti non imputabili a questa Amministrazione, tale pieno utilizzo dovrebbe essere raggiunto già da marzo 2023. L'IVASS non garantisce, pertanto, il pieno utilizzo del budget per le voci di spesa a consumo, che verranno impiegate di volta in volta sulla base dell'effettivo fabbisogno.

METODO: il criterio scelto, mutuato da CONSIP, per il dimensionamento dei servizi ha ipotizzato lo svolgimento degli stessi attraverso la composizione di 5 TEAM mix, ciascuno dimensionato per un numero totale di giornate/uomo (anche giornate/team) medie mensili e composto da distinte figure professionali con un diverso peso all'interno del Team a seconda delle attività cui lo stesso è rivolto, al fine di definirne la tipologia e la qualità. Si ipotizza che i servizi siano svolti attraverso detti TEAM, indicati distintamente nei paragrafi successivi, soltanto ai fini della quantificazione economica dell'appalto ed in continuità con l'organizzazione attuale dei servizi; tale criterio non è vincolante per il Fornitore concorrente il quale potrà proporre nella propria offerta tecnica, in linea con la propria organizzazione aziendale, una diversa struttura organizzativa dei servizi che sarà valutata al fine del miglioramento delle stesse prestazioni contrattuali.

Il presente Capitolato Tecnico, unitamente ai relativi allegati che ne costituiscono parte integrante e sostanziale, disciplina gli aspetti tecnico-giuridici ed economici per l'affidamento dei suddetti servizi.

L'appalto è regolato dalla legge italiana. Per tutto quanto non espressamente regolato dalle condizioni del presente Capitolato Tecnico e dello Schema di contratto, valgono le norme di legge.

1.3. Fasi contrattuali

Dopo la stipula del Contratto l'attività dell'aggiudicatario sarà articolata in tre specifiche fasi temporali:

- a) Fase di presa in carico (phase in) (3 mesi): dalla data di firma contrattuale (T0), per un periodo di 90 gg. solari alla data (T1)

- b) Fase di erogazione a regime (24 mesi): dalla data (T0), in parallelo alla fase definita in precedenza, sino alla data di scadenza di 24 mesi di fornitura richiesti (T2) (salvo recesso anticipato da parte dell'Istituto o rinnovo per ulteriori 24 mesi);
- c) Fase di fine fornitura (3 mesi): ultimi 3 mesi di fornitura fino alla data ultima di conclusione contrattuale (T2) al fine di assicurare il passaggio ad un nuovo Fornitore.

Di seguito si riporta una descrizione dettagliata delle fasi temporali.

1.3.1 Fase di Presa in carico ed erogazione

In questa fase l'aggiudicatario dovrà procedere, in stretta collaborazione con l'IVASS e con il Fornitore uscente, alla presa in carico di tutte le attività concernenti la gestione e la conduzione del sistema informativo PREVENTIVASS.

L'Amministrazione si adopererà, in collaborazione con il Fornitore uscente, a garantire il corretto trasferimento della conoscenza sui servizi e sulle applicazioni interessate, nell'ambito dell'erogazione di quanto oggetto della fornitura.

Tale trasferimento si completerà entro i primi 3 mesi dalla stipula del contratto, salvo il protrarsi oltre i 3 mesi per cause eccezionali non dipendenti dal Fornitore subentrante e comunque previo accordo tra le parti.

Gli indici di qualità riscontrati durante la fase di *phase in* terranno conto di eventuali elementi significativi non imputabili al Fornitore che non porteranno all'applicabilità di penali nei confronti dello stesso. Il Fornitore nella fase di presa in carico è comunque tenuto al rispetto degli obblighi previsti dal contratto.

Il dimensionamento dei *team* per la fase di presa in carico dovrà essere lo stesso previsto per la fase di erogazione a regime, dettagliato nei relativi paragrafi dei singoli servizi oggetto di gara.

L'aggiudicatario, in questa fase, dovrà garantire almeno le seguenti attività definite accessorie:

- Migrazione strumenti a supporto dello Sviluppo Software;
- Installazione e configurazione strumenti di Test Automation e Test di Carico;
- Installazione e configurazione agent di sicurezza e integrazione con il SIEM messo a disposizione nel rispetto di quanto riportato nei par. 3.5 Servizio di Cyber Security;
- Installazione e configurazione del sistema di *Event Management* e integrazione con il Centro Servizi del Fornitore messo a disposizione nel rispetto di quanto riportato nel par. 3.6 Servizi Trasversali;
- Presa in carico delle procedure di *Disaster Recovery*;
- Presa in carico della sottoscrizione e fornitura della piattaforma (AWS);
- Attività di *Privacy Assessment*;
- Attività di *Accessibility Assessment*;
- Attività di *Penetration Testing* e *Vulnerability Assessment*, volte all'assunzione di responsabilità da parte del Fornitore del rispetto delle normative e disposizioni vigenti in materia (es. GDPR, Compliance AgID, ...).

Il mancato raggiungimento, da parte del Fornitore, delle attività sopra descritte – entro il termine massimo previsto pari a 3 mesi – costituisce motivo di rescissione del contratto, salvo diversa pattuizione concordata fra le parti.

A conclusione di questa fase, l'IVASS procederà ad effettuare le verifiche sull'effettivo subentro del nuovo Fornitore mediante collaudo funzionale, nel rispetto di quanto prescritto nel presente documento e nell'Offerta tecnica presentata dall'offerente. L'esito favorevole di tali verifiche verrà formalizzato in un apposito verbale sottoscritto dalle parti nel quale verrà indicata la data di inizio della successiva Fase di erogazione a regime.

Il corrispettivo per lo svolgimento di tutte le attività accessorie sopraelencate sarà erogato a corpo sulla base dell'importo specificatamente indicato dal Fornitore nella propria Offerta economica.

1.3.2 Fase di erogazione a regime

Nel corso del periodo di erogazione a regime, il Fornitore dovrà procedere alla completa gestione e conduzione della piattaforma PREVENTIVASS e dei servizi ad essa collegati nel rispetto di quanto indicato nel presente Capitolato, nel contratto, nonché secondo quanto indicato dal Fornitore stesso in sede di Offerta Tecnica.

In questa fase, in ragione degli indici di qualità del servizio riscontrati, saranno imputabili al Fornitore le penali previste dal contratto.

1.3.3 Fase di fine fornitura

Tale fase individua l'ultima parte del rapporto contrattuale; nel corso di questa fase il Fornitore continuerà a mantenere attive le funzionalità della piattaforma PREVENTIVASS fino al completamento di tutte le attività eventualmente ancora in corso

Il Fornitore deve mettere a disposizione le stesse risorse impegnate nell'erogazione a regime del servizio.

Durante tale periodo, il Fornitore dovrà:

- assicurare la continuità della funzionalità del sistema fino al subentro del nuovo Fornitore;
- rendersi disponibile, ove richiesto, ad affiancare il Fornitore subentrante;
- trasferire le competenze necessarie all'erogazione dei servizi;
- fornire tutta la documentazione tecnica, redatta nell'intero periodo contrattuale, descrittiva di tutti gli elementi architetture e applicativi che compongono l'infrastruttura.

I corrispettivi per l'attività svolta sono quelli previsti per la precedente fase di erogazione a regime.

2. Contesto

2.1 Missione, Struttura e Attività dell'IVASS

L'IVASS, Istituto per la Vigilanza sulle Assicurazioni, è un ente dotato di personalità giuridica di diritto pubblico che opera per garantire l'adeguata protezione degli assicurati perseguendo la sana e prudente gestione delle imprese di assicurazione e riassicurazione e la loro trasparenza e correttezza nei confronti della clientela. L'Istituto persegue altresì la stabilità del sistema e dei mercati finanziari. Al fine di assicurare l'esercizio imparziale delle proprie funzioni, l'Istituto gode di autonomia organizzativa, finanziaria e contabile e agisce in base ai principi di trasparenza ed economicità, salvo il controllo della Corte dei Conti sulla gestione finanziaria.

L'IVASS è subentrato in tutte le funzioni, le competenze e i poteri dell'ISVAP a seguito del decreto legge 6 luglio 2012, n. 95 (convertito, con modifiche, dalla legge 7 agosto 2012, n. 135) per realizzare la piena integrazione della vigilanza assicurativa con quella bancaria.

Le funzioni dell'IVASS sono dirette a garantire l'adeguata protezione degli assicurati e degli aventi diritto alle prestazioni assicurative attraverso il perseguimento della sana e prudente gestione delle imprese di assicurazione e riassicurazione e della loro trasparenza e correttezza nei confronti della clientela (condotta di mercato). L'Istituto persegue altresì la stabilità del sistema e dei mercati finanziari.

L'IVASS esercita le funzioni di vigilanza nei confronti delle imprese di assicurazione e riassicurazione, dei gruppi assicurativi, dei conglomerati finanziari nei quali sono incluse le imprese, dei soggetti che svolgono funzioni parzialmente comprese nel ciclo operativo delle imprese nonché degli intermediari assicurativi e riassicurativi.

L'Istituto autorizza le imprese all'esercizio dell'attività assicurativa e riassicurativa, svolge accertamenti ispettivi presso i gruppi e le imprese del mercato assicurativo e riassicurativo e presso gli altri soggetti vigilati, anche in collaborazione con la Banca d'Italia, con altre Autorità pubbliche o con altre Autorità di vigilanza assicurativa dell'Unione europea.

L'Istituto vigila sull'operato degli intermediari assicurativi e riassicurativi. Verifica la conformità dei loro comportamenti alla normativa di settore, con particolare riguardo al rispetto degli obblighi di separazione patrimoniale e d'informativa, alla correttezza e alla trasparenza nelle relazioni con il cliente.

L'IVASS cura la tenuta del Registro unico degli intermediari assicurativi e riassicurativi (RUI) e, nell'ottica di protezione del consumatore, promuove la diffusione di buone prassi tra gli operatori.

Per l'esercizio delle funzioni di vigilanza sulla gestione tecnica, finanziaria e patrimoniale delle imprese e sulla trasparenza e sulla correttezza dei comportamenti degli operatori, l'IVASS adotta regolamenti per l'attuazione del Codice delle assicurazioni e delle disposizioni direttamente applicabili dell'Unione europea nonché regolamenti per l'attuazione delle raccomandazioni, linee guida e altre disposizioni emanate dall'Autorità di vigilanza europea (EIOPA).

Accerta le condotte illecite da parte dei soggetti vigilati e applica sanzioni amministrative-pecuniarie e disciplinari.

L'IVASS vigila sulla correttezza dei comportamenti delle imprese nei confronti del consumatore e sulla trasparenza dei prodotti assicurativi. Stabilisce le regole di comportamento che le imprese e gli intermediari

sono tenuti a osservare nell'offerta e nell'esecuzione dei contratti e ne verifica il puntuale adempimento. Fornisce ai consumatori assistenza telefonica in materia assicurativa mediante il *Contact Center*. I reclami scritti e le segnalazioni al *Contact Center* rappresentano strumenti essenziali per analizzare le cause che sono alla base dei motivi d'insoddisfazione dei consumatori e per intervenire, in presenza di problematiche ricorrenti o di particolare rilievo, con azioni mirate di vigilanza. Cura le relazioni con le Associazioni dei consumatori.

Sviluppa la conoscenza del mercato assicurativo attraverso studi e indagini di natura statistica ed economica.

Le entrate dell'IVASS sono costituite dai contributi a carico dei soggetti vigilati, il cui ammontare è definito annualmente con decreto del Ministro dell'economia e delle finanze adottato, su proposta dell'IVASS, in modo da assicurare la copertura finanziaria degli oneri di funzionamento dell'Istituto.

In sede di predisposizione dei bilanci l'IVASS, sul piano amministrativo-finanziario tiene conto delle norme esterne di riduzione delle uscite oltre che di autonome politiche di contenimento della spesa.

I bilanci dell'Istituto sono sottoposti al controllo della Corte dei Conti; la contabilità viene verificata anche da revisori esterni così come stabilito dall'art. 14 dello Statuto dell'IVASS.

2.2 Contesto Normativo

Nell'ambito delle proprie attività istituzionali l'IVASS si occupa della gestione e della realizzazione del Preventivatore pubblico r.c. auto – PREVENTIVASS – per consentire la comparazione tra le offerte assicurative r.c. Auto, relative al contratto base, schema contrattuale definito con decreto del Ministro dello Sviluppo Economico dell'11 marzo 2020, n. 54.

L'applicazione si interfaccia con i sistemi delle imprese assicurative che esercitano il ramo r.c. auto in Italia alle quali fornisce in input i dati inseriti dagli utenti, integrati mediante consultazione delle Banche Dati pubbliche di settore e di banche Dati commerciali private sulla base del Modello Elettronico definito dal decreto del Ministero dello Sviluppo Economico 4 gennaio 2021.

Ai sensi dell'articolo 132-bis, comma 3, del decreto legislativo 7 settembre 2005 n. 209, (Codice delle Assicurazioni Private), l'IVASS, con regolamento n. 51 del 21 giugno 2022, ha adottato disposizioni attuative per garantire ai consumatori e agli intermediari l'accesso e la risposta per via telematica ai premi applicati dalle imprese di assicurazione per il contratto base, definendo altresì le modalità attraverso le quali, ottenuti i preventivi sulla base delle informazioni inserite nel servizio informativo realizzato, è consentita la conclusione del contratto.

Le imprese assicurative, ai sensi del sopra citato regolamento IVASS n. 51 del 22 giugno 2022, sono obbligate a rispondere ad ogni richiesta di preventivo proveniente da PREVENTIVASS a far data dal 1° novembre 2022.

Ai sensi dello stesso regolamento IVASS n. 51/2022 gli intermediari sono tenuti ad adempiere agli obblighi di cui all'art. 132-bis del Codice delle Assicurazioni a far data dal 1° marzo 2023.

Si rinvia integralmente al regolamento IVASS n. 51/2022, che si allega al presente Capitolato (all. 1), evidenziando, in particolare, le disposizioni relative a:

- Funzionamento di PREVENTIVASS;
- Utenti e funzionalità di PREVENTIVASS;
- Tipologie di Intermediari interessati;

- Modalità di accesso;
- Settori di Uso;
- Esposizione dei risultati;
- Finalizzazione del preventivo;
- Registrazione, tracciatura e conservazione dei preventivi.

Ulteriori previsioni concernenti le condizioni di operatività delle imprese assicurative sono contenute nell'Allegato 1 al sopra citato regolamento IVASS n. 51/2022, in particolare relative a:

- Area riservata d'impresa;
- Nomina e modalità di accesso degli Amministratori di impresa;
- Funzionalità di amministrazione;
- Integrazione tra sistemi di preventivazione di impresa e PREVENTIVASS;
- Reportistica delle richieste di preventivo e dei livelli di servizio di integrazione tra sistemi;
- Procedure di finalizzazione dei preventivi;
- Procedure di aggiornamento versioni di PREVENTIVASS;
- Connessioni *Application to Application* (A2A).

2.3 Contesto Applicativo

In ottemperanza alle disposizioni di cui sopra è stato realizzato un sistema informativo denominato PREVENTIVASS, che necessita di servizi di gestione e di manutenzione, oggetto del presente appalto. I componenti dell'attuale sistema rispondono pienamente a quanto previsto in sede regolamentare, con la possibilità da parte del committente, di modificare l'insieme delle funzionalità di seguito descritte per interventi di Manutenzione Evolutiva o Adeguativa.

PREVENTIVASS consta delle seguenti componenti:

- Portale di preventivazione (rivolto ai consumatori e agli intermediari);
- Portale Imprese;
- Portale Ivass;
- Portale Intermediari;
- Integrazione A2A;
- Applicazione Mobile;
- Integrazione con DWH (presso i sistemi di Banca d'Italia).

2.3.1 Portale di preventivazione

Il portale di preventivazione è accessibile attraverso l'indirizzo <https://www.preventivass.it/>.

Il portale è sviluppato in *Angular* per la componente *Front End* mentre per la componente *Back-End* impiega la tecnologia a microservizi sviluppati sulla piattaforma *Cloud Amazon Web Services* (di seguito anche AWS).

Attraverso il portale, gli utenti inseriscono le informazioni utili alla generazione del Modello Elettronico del preventivo da Contratto Base R.C. Auto. Tale fase è definita come *data entry*.

Il processo di data entry prevede inoltre l'interrogazione da parte del sistema di alcune banche dati di settore, attraverso l'invocazione di servizi SOAP e REST. Tale processo è definito come *data enrichment*. Le banche dati interrogate sono:

- SIVI – Banca dati Veicoli;
- SITA – Banca dati Coperture Assicurative;
- ATRC – Banca dati Attestati di Rischio;
- Infocar / Infobike – Banca dati degli Allestimenti;
- Egon – Banca dati degli indirizzi stradali.

L'interrogazione alle banche dati SIVI, SITA e ATRC avviene attraverso i servizi informatici dell'Associazione Nazionale delle Imprese Assicuratrici (ANIA); il reperimento degli allestimenti viene effettuato impiegando il database Infocar / Infobike (base dati aggiornata con cadenza giornaliera e interrogata su un servizio sviluppato in cloud); la banca dati degli indirizzi stradali, Egon, viene interrogata usando il *web service* fornito dalla società *Ware Places*.

La fase di data entry è soggetta a controlli sintattici e semantici. Questi ultimi sfruttano la fase di data *enrichment* per assolvere al loro compito.

Alla fase di data *enrichment* segue la fase di compilazione delle clausole aggiuntive, previste per legge, che completa la definizione del Modello Elettronico, che è così inviato ai *web service* di preventivazione di tutte le imprese operanti sul territorio nazionale. L'invio del Modello Elettronico ai *web service* delle imprese assicurative avviene utilizzando un formato di interscambio json e viene gestito da un microservizio.

Tali *web service* rispondono con un preventivo da contratto base.

Prima della trasmissione l'oggetto *json* di richiesta viene convertito in base64 e firmato digitalmente, al fine di garantire la tracciabilità dei dati e rispondere alle normative vigenti in termini di *Privacy Protection*.

I *web service* delle imprese devono rispondere entro un tempo limite di 30 secondi. Oltre il predetto termine di 30 secondi il sistema accetta solamente i preventivi trasmessi entro 5 minuti, che tuttavia non vengono esposti all'interno dell'applicazione.

Il sistema tiene traccia di eventuali problemi derivanti dallo scambio intercorrente tra PREVENTIVASS e i sistemi delle imprese assicurative, categorizzando opportunamente gli errori, per poter permettere la rilevazione e l'analisi di eventuali malfunzionamenti.

Le risposte generate dalle imprese assicurative usano altresì il formato *json*, e sono anch'esse codificate in base64 e firmate digitalmente.

Il sistema presenta agli utenti i preventivi validi permettendogli di ordinarli e filtrarli usando un insieme di parametri messi a disposizione dal *Front End*.

Gli utenti hanno la possibilità di recuperare dal portale ogni singolo preventivo generato anche in sessioni successive all'interrogazione effettuata, utilizzando l'identificativo univoco assegnato ad ogni preventivo in sede di generazione per tutta la durata prevista dalle vigenti disposizioni in materia.

Il *Front End* è *compliant* con i requisiti definiti da AgID in materia di accessibilità e usabilità.

Di seguito si riportano alcune delle funzionalità gestite dall'applicativo:

- Acquisizione dall'utenza delle informazioni necessarie per avviare il processo di interrogazione delle imprese (targa veicolo, codice fiscale contraente, data di decorrenza della copertura assicurativa, etc);

- Navigazione guidata al fine di indirizzare l'utente sulle possibili varianti che, in relazione alle specifiche caratteristiche della situazione assicurativa del singolo assicurato, possono verificarsi nell'iter di preventivazione (ad es. prima assicurazione, contratto per veicolo già assicurato, bonus famiglia, acquisto veicolo nuovo, acquisto veicolo usato, etc.) informandolo anche sull'esito dell'interrogazione delle banche dati di settore (SITA, SIVI, ATRC);
- Esposizione automatica di specifiche informative al verificarsi di predefinite fattispecie (ad es. preventivi aventi decorrenza successiva al periodo di validità di 60 giorni, preventivi emessi senza indicazione di targa del veicolo, veicoli radiati, etc.);
- Guida e assistenza nella scelta delle clausole aggiuntive offerte dal mercato assicurativo, fornendo adeguata informazione per agevolare la scelta della copertura assicurativa più aderente alle necessità del consumatore;
- Interfaccia con le banche dati esterne all'Istituto (ATRC, SITA, SIVI, Infocar / Infobike, Egon) per completare il set informativo da fornire alle imprese assicurative;
- Interfaccia con i sistemi di preventivazione delle società assicurative;
- Acquisizione e presentazione in tempi prestabiliti (30 secondi dall'avvio della ricerca) dei risultati della richiesta di preventivo inoltrata.

2.3.2 Portale Imprese

Il portale imprese è un modulo software indipendente raggiungibile all'indirizzo <https://backoffice.PREVENTIVASS.it> attraverso il quale le imprese assicurative accedono all'area funzionale riservata messa a disposizione di ognuna di esse.

Il portale è sviluppato in *Angular* per la componente *Front End* mentre per la componente *Back-End* insiste su alcuni microservizi sviluppati sulla piattaforma Cloud AWS.

Le imprese operano all'interno dell'area riservata di propria competenza (*Backoffice*) per il tramite di uno o più Amministratori abilitati secondo la procedura prevista nell'Allegato 1 al sopra citato regolamento IVASS n. 51/2022 (disposizione n. 2).

Ogni amministratore accede al portale tramite Servizio Pubblico di Identità Digitale (SPID), autenticandosi tramite SPID Professionale, ottenibile presso i c.d. *Identity Provider SPID* riconosciuti dall'Agenzia per l'Italia digitale (AgID), reperibili negli elenchi pubblicati dalla stessa AgID.

Dal proprio *Backoffice* le imprese provvedono all'inserimento, all'aggiornamento e alla modifica dei contenuti informativi di propria competenza. Parte di detti contenuti sono utilizzati dall'applicazione per alimentare il front end rivolto all'utente, come, ad esempio, le formulazioni contrattuali delle clausole aggiuntive che vanno a compilare i singoli preventivi emessi a favore dei richiedenti.

A tal fine il Portale Imprese mette a disposizione le seguenti funzionalità:

- a) Gestione dei parametri identificativi e di configurazione dell'impresa:
Consente di inserire, aggiornare e monitorare una serie di parametri identificativi e di configurazione. A titolo esemplificativo ma non esaustivo si riporta di seguito un elenco dei possibili parametri:
 - Logo impresa;
 - Url del sito internet dell'impresa;
 - Descrizione sintetica dell'impresa;
 - Certificato per la firma dei preventivi;

- URL per l'integrazione con i sistemi di preventivazione d'impresa;
 - URL alla documentazione pre-contrattuale;
 - URL per la finalizzazione del preventivo;
 - URL di informativa sulla Privacy;
 - Adesione alla convenzione Card.
- b) Gestione delle clausole aggiuntive offerte:
Consente di inserire, aggiornare e monitorare le clausole aggiuntive di cui all'art. 7, comma 2, del regolamento IVASS n. 51/2022 offerte dall'impresa.
- c) *Testing* della funzionalità di connessione, di validazione sintattica e di firma dei preventivi:
Consente di verificare il corretto funzionamento della connettività tra PREVENTIVASS e il sistema di preventivazione d'impresa.
- d) Report richieste e livelli di servizio:
Consente ad ogni impresa di monitorare i livelli di servizio conseguiti nell'attività di risposta alle richieste di preventivo pervenute.

2.3.3 Portale Admin/Ivass

Il portale Admin/Ivass (Admin Tool Preventivatore) è la componente dell'applicazione rivolta agli utenti abilitati IVASS ai quali sono rese disponibili diverse funzionalità.

La Funzionalità "Utenti IVASS" consente di abilitare o disabilitare (grazie alla gestione di profili con differenti livelli operativi) gli utenti IVASS autorizzati ad accedere al portale.

Il portale mette a disposizione delle funzionalità avanzate di verifica e gestione delle richieste inserite dalle imprese assicurative per lo svolgimento delle attività autorizzative di competenza dell'IVASS.

Il portale dispone della Funzionalità "*Report*" mediante la quale è possibile visualizzare e scaricare diverse tipologie di resoconti sull'andamento dell'attività di preventivazione svolta da tutte le imprese ("Richieste ricevute", "Errori schema", "Classe di merito", "Provenienza").

In particolare il *report* "Richieste ricevute" fornisce il dettaglio dei risultati di tutte le richieste di preventivo ricevute dall'applicazione e delle risposte ricevute, comprensivo degli esiti dei controlli di validità effettuati e delle segnalazioni di errore o incompletezza trasmesse dalle imprese. Detta reportistica è a disposizione degli utenti IVASS per il monitoraggio e controllo delle attività di preventivazione delle imprese e l'espletamento delle attività istituzionali di vigilanza, studio e statistica.

È altresì messa a disposizione una sezione utile alla verifica dei flussi di alimentazione prodotti per il DWH (par. 2.3.6).

Il portale permette il censimento e la gestione degli utenti di Impresa e degli Intermediari.

Mediante il portale Admin/Ivass è consentito lo svolgimento di attività di monitoraggio e controllo dei parametri identificativi e di configurazione adottati dalle imprese per verificarne la corretta configurazione e il corretto funzionamento.

Il portale consente, infine, di inserire *disclaimer* di comunicazione a vantaggio degli utenti per eventuali interruzioni di servizio programmate.

2.3.4 Portale Intermediari

Il portale Intermediari è la componente dell'applicazione rivolta agli Intermediari assicurativi, per consentire loro un utilizzo semplificato delle funzionalità messe a disposizione dal sistema.

Nello specifico il portale Intermediari consente ad esempio di tracciare efficacemente le richieste di preventivo compilate da uno specifico intermediario assicurativo e di configurare l'integrazione tra i sistemi di preventivazione di ciascun intermediario e Preventivass.

2.3.5 Mobile

Al fine di semplificare la fruizione del sistema in mobilità è stata sviluppata una applicazione "mobile", destinata alle piattaforme Android e iOS, alla cui manutenzione e gestione il Fornitore è tenuto, rendendo fruibili tutte le funzionalità offerte dall'interfaccia web.

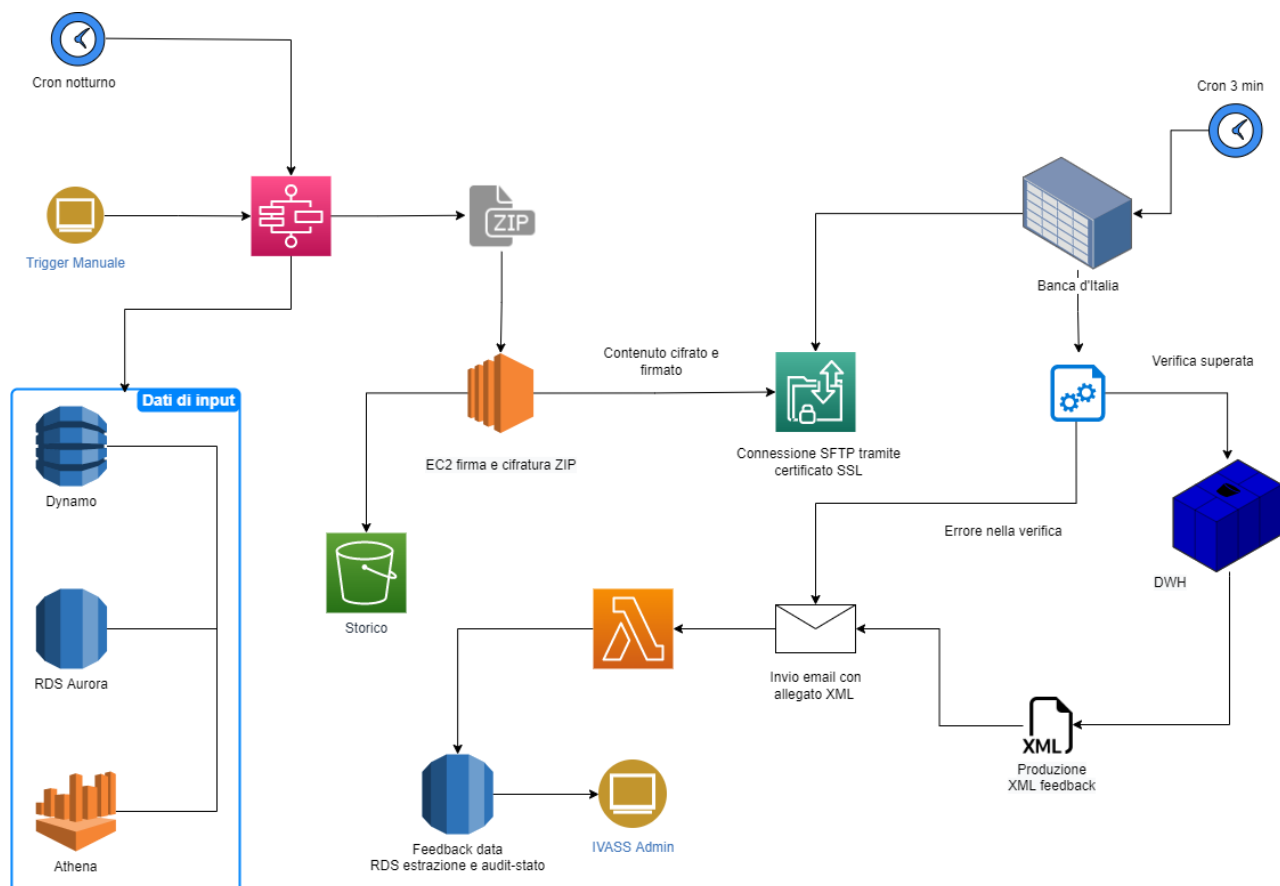
Su richiesta di IVASS il Fornitore è tenuto a svolgere tutte le operazioni necessarie alla gestione delle suddette applicazioni "mobile", compresa la pubblicazione delle stesse all'interno dei servizi impiegati per la loro distribuzione, nello specifico all'interno di *Play Store* e di *App Store*.

2.3.6 Flussi di alimentazione del DWH

L'applicazione gestisce appositi flussi di integrazione con il sistema MFT di Banca d'Italia al fine di alimentare, previa esecuzione degli opportuni controlli di sicurezza e di qualità dei dati raccolti, l'apposito *Data Warehouse* (DWH) ospitato nei sistemi di Banca d'Italia.

Detti flussi vengono generati dall'acquisizione delle informazioni gestite in ambiente cloud da Preventivass e sono periodicamente trasmessi al DWH in Banca d'Italia per archiviare in maniera stabile e duratura i dati trattati dall'applicazione e procedere ad analisi di carattere statistico e di studio.

Si riporta di seguito lo schema architetturale impiegato per l'alimentazione del DWH.



Flussi DWH

Produzione di dataset di supporto all'elaborazione statistica di base in cloud

L'architettura applicativa sfrutta due distinte basi dati, rispettivamente dedicate all' *On-Line Transaction Processing* (OLTP) e all' *On-Line Analytical Processing* (OLAP).

Le informazioni contenute all'interno del sistema OLTP sono periodicamente copiate all'interno del servizio impiegato per l'OLAP. Il Fornitore si impegna a mantenere la periodica alimentazione del sistema OLAP e ad integrare lo stesso con ulteriori *dataset* prodotti dal sistema OLTP tramite eventuali attività di Manutenzione Evolutiva.

2.3.7 Volumi e dimensionamento dei servizi

Il volume che si dovrà gestire è stimabile in 40-50 milioni di richieste di preventivo per singolo anno di esercizio, suddivise tra richieste da piattaforma web e richieste provenienti dai sistemi integrati tramite A2A. Le richieste generate sono inoltrate ai sistemi di preventivazione delle imprese assicurative (circa 50). Ciascuna richiesta comporta la generazione di uno o più preventivi.

La stima del numero di preventivi generati dai sistemi di preventivazione delle imprese assicurative si aggira quindi tra i 200 e i 300 milioni di unità per anno di esercizio.

Sulla base delle esigenze operative l'IVASS potrà richiedere con cadenza trimestrale la revisione del dimensionamento dei team di lavoro. L'ammontare dei relativi canoni verrà ricalcolato sulla base delle mutate necessità gestionali.

L'attuale architettura consente di rispondere in maniera scalabile all'aumento o alla diminuzione dei volumi di richieste di preventivo generate. Ciò si traduce in un'ottimizzazione dei costi di esercizio dei crediti AWS.

Di seguito si riporta un elenco dei servizi AWS utilizzati dall'attuale implementazione: *Api Gateway, Cloud Front, WAF, ELB, EC2, Lambda, DynamoDB, SQS, SES, RDS, Amazon CloudWatch, SFTP, S3, VPN, NAT Gateway, Kinesis Firehose, Athena, Glue, Trusted Advisor.*

[2.3.8 A2A](#)

La funzionalità Application to Application (A2A) consente l'integrazione tra Preventivass e sistemi informativi delle imprese o degli intermediari assicurativi. Nello specifico tale funzionalità permette di generare preventivi senza l'utilizzo dell'interfaccia web.

L'A2A viene erogato secondo due modalità distinte: A2A Online e A2A Massiva.

[2.3.8.1 A2A Online](#)

L'A2A Online replica esattamente le funzionalità messe a disposizione dall'interfaccia web, permettendo la generazione di una singola richiesta di preventivo in *near-real time*, ovvero con tempi di risposta nell'ordine di secondi.

[2.3.8.2 A2A Massiva](#)

L'A2A Massiva mette a disposizione delle API che consentono ai sistemi utilizzatori di generare un elevato numero di preventivi (nell'ordine delle migliaia di unità). In questa modalità di integrazione i termini temporali di risposta ed emissione dei preventivi sono svincolati dai termini regolamentari.

3 Descrizione dell'oggetto dell'appalto

L'appalto è suddiviso in n. 6 servizi e una fornitura, secondo le previsioni descritte dettagliatamente nei paragrafi a seguire, con le migliorie indicate nell'offerta tecnica e remunerati applicando quanto previsto nell'offerta economica.

3.1 Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche (CLOUD AWS)

3.1.1 Descrizione del Servizio

Il servizio comprende tutte le attività necessarie per la gestione in esercizio di quanto sviluppato, gestito e mantenuto in ambiente cloud AWS, ovvero la gestione di tutta l'infrastruttura tecnologica di erogazione, ivi incluse le piattaforme di monitoraggio e analisi delle *operations*, di gestione delle configurazioni e la *knowledge base* con le soluzioni ai problemi noti.

La gestione dei sistemi ha l'obiettivo di:

- garantire la disponibilità dei sistemi e l'esecuzione delle attività schedate in coerenza con le pianificazioni concordate con l'Istituto;
- assicurare un continuo controllo sullo stato dei sistemi e dei collegamenti alle banche dati gestite da ANIA al fine di individuare criticità o malfunzionamenti e intraprendere le conseguenti azioni necessarie;
- assicurare un continuo aggiornamento delle Banche dati Infocar / Infobike;
- prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio all'utenza;
- ottimizzare l'utilizzo dello storage e garantire la disponibilità, la salvaguardia e l'integrità dei dati;
- assicurare l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni esistenti;
- assicurare la corretta produzione e distribuzione della reportistica prevista nel par. 3.6.9;
- assicurare la gestione di procedure di *Disaster Recovery* e l'esecuzione di almeno un test annuale di *Disaster Recovery*;
- garantire attività di provisioning e configurazione delle risorse in linea con le best practice di AWS;
- adottare misure volte alla protezione del dato;
- adottare soluzioni di data encryption;
- adottare soluzioni di data loss prevention;
- garantire la gestione delle regole di routing e configurazione VPN;
- monitorare costantemente e registrare le configurazioni delle risorse ospitate all'interno dell'account AWS dell'Istituto in modo da garantire per tutta la durata del contratto l'accesso allo storico delle attività di change alle configurazioni;
- ripristinare il funzionamento dei sistemi a fronte di errori entro i termini stabiliti nell'APPENDICE 1 – Indicatori di Qualità;
- prendere in carico le richieste di intervento, per tutto l'iter operativo, fino al completamento dell'attività;
- minimizzare i tempi di fermo manutentivo, durante le operazioni di aggiornamento tecnologico;
- garantire l'amministrazione del sistema di *Identity Management* basato su tecnologia WSO2 e integrazione con SPID ad uso Professionale;

- supportare l'Istituto nella gestione dei consumi AWS, mediante costante monitoraggio dei consumi, delle performance e di possibili variazioni architetturali, evidenziate in corso di esercizio, per garantire adeguati standard qualitativi del contesto applicativo e/o ottimizzazioni dei costi sostenuti.

Inoltre nel servizio rientra la manutenzione del SW di sistema mediante l'esecuzione delle operazioni di modifica e upgrade sui sistemi, a seguito del rilascio da parte del produttore degli aggiornamenti e/o correzioni SW.

Le attività di manutenzione sistemi previste sono di due tipi:

1. Manutenzione Preventiva (attività di manutenzione atta a prevenire l'occorrenza di errori, malfunzionamenti e guasti);
2. Manutenzione Correttiva (attività di manutenzione a seguito di malfunzionamenti o guasti).

Le attività sopra elencate, da erogarsi in modalità continuativa, saranno remunerate a canone secondo quanto indicato in offerta economica sulla base del dimensionamento determinato nel seguente paragrafo.

3.1.2 Composizione del team del Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche (CLOUD AWS)

Il Fornitore nell'ambito del servizio deve garantire la disponibilità delle seguenti figure professionali/skill

Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche	Peso % sul servizio	gg/mese
Capo progetto	5%	1,25
Architetto/Progettista IT (AWS)	10%	2,5
Specialista di tecnologia/prodotto junior - Specialista AWS	50%	12,5
Sistemista Senior	10%	2,5
Specialista di tecnologia/prodotto senior - Specialista WSO2 / SPID	5%	1,25
Specialista di tecnologia/prodotto senior - Specialista Backup e Disaster Recovery	5%	1,25
Specialista di tecnologia/prodotto junior - Specialista di Sicurezza	15%	3,75
	Effort complessivo	25

3.2 Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database

Il servizio è articolato in più sotto servizi.

3.2.1 Sviluppo del Software e Manutenzione Evolutiva del Software

Il servizio richiesto al Fornitore comprende tutte le attività necessarie per la realizzazione, l'evoluzione e/o la reingegnerizzazione dell'applicazione.

L'Aggiudicatario dovrà svolgere l'attività coordinandosi in modo costante con l'IVASS al fine di consentire il monitoraggio dell'attività di sviluppo e l'integrazione con i sistemi gestionali delle Imprese Assicurative operanti con PREVENTIVASS.

A tal fine è richiesta l'adozione di metodologie di gestione del ciclo di vita AGILI, preferibilmente *Scrum*, che consentano la definizione di momenti di incontro periodici e ravvicinati fra loro, indicativamente ogni 2 settimane.

Per quanto attiene alla gestione del sistema di controllo di versione viene utilizzata la seguente metodologia denominata "*Versioning semantico*" che si basa sulle *best practice* utilizzate per la gestione di multipli *branch*.

Il software attualmente sviluppato è suddiviso in quattro moduli indipendenti.

- Preventivatore Web;
- *Backoffice Admin*;
- *Backoffice Imprese/Intermediari*;
- API;
- Generazione flussi DWH.

Ciascun modulo ha un percorso di vita del tutto autonomo ed è contraddistinto da un *versioning* di tipo semantico caratterizzato da una numerazione che rispetta lo standard di riferimento.

La numerazione adottata usa il seguente formato *MAJOR.MINOR.PATCH*, dove nello specifico:

- versione *MAJOR* (modifiche non retro-compatibili);
- versione *MINOR* (modifiche apportate al *software* o nuove funzionalità retro-compatibili);
- versione *PATCH* (correzioni di bug in modo retro-compatibile).

a) Sviluppo del *Software*

Le attività di Sviluppo Software sono da erogarsi in modalità continuativa e saranno remunerate a canone. Tali attività comprendono l'implementazione di funzionalità a supporto di:

- attività istituzionali di controllo e verifica di competenza dell'IVASS (Motore di regole sul processo di preventivazione, sezione di *Business Intelligence* focalizzata su specifiche aree tematiche, motore di controllo sull'attività di integrazione e preventivazione delle imprese assicurative, reportistica aggiuntiva, progettazione/integrazione di algoritmi di Machine Learning per la generazione di indici sintetici che misurino il livello di conformità degli adempimenti realizzati dalle imprese alle disposizioni regolamentari emanate dall'Istituto, sia sotto il profilo tecnico che di business, etc.);
- attività evolutive riguardanti la connettività/integrazione con DWH ospitato nei sistemi di Banca d'Italia;
- attività riguardanti la connettività/integrazione con le banche dati già incluse nell'attuale architettura di Preventivass (SITA, SIVI, ATRC, Infocar/Infobyke, Egon).

b) Manutenzione Evolutiva del *Software*

Rientrano nel presente servizio gli interventi di Manutenzione evolutiva (MEV) dell'applicazione, da stimarsi ed effettuarsi su richiesta dell'IVASS, comprensivi dello svolgimento di tutte le attività necessarie a coprire

l'intero ciclo di vita dello sviluppo, dalla formalizzazione dei requisiti fino al rilascio in esercizio. In questa fattispecie è ricompresa la manutenzione migliorativa, consistente in piccoli interventi di breve durata finalizzati ad aumentare la fruibilità dell'applicazione.

Tutti gli eventuali interventi di Manutenzione evolutiva verranno espletati con modalità di erogazione di tipo progettuale nel rispetto del budget massimo spendibile individuato dall'Amministrazione per l'importo di euro 250.000,00 (duecentocinquantamila,00) da utilizzarsi qualora si evidenziasse la necessità di procedere con l'esecuzione di variazioni e attività non previste.

Per i dettagli sulla rendicontazione delle attività di MEV si rinvia al par. 3.2.7.

3.2.2 Manutenzione App Mobile

È richiesto al Fornitore di possedere le competenze indispensabili per rispondere all'eventuale necessità dell'IVASS di implementare sistemi con funzionalità integrate per il cittadino o per gli utenti professionali usabili su dispositivi mobili (tablet, smartphone e altri) che possono richiedere la progettazione e realizzazione di interfacce grafiche di tipo touch screen garantendo la portabilità su diversi *browser* e/o l'integrazione con sistemi di georeferenziazione e/o l'integrazione con Google application, etc..

3.2.3 Manutenzione Adeguativa e Correttiva

È richiesto al Fornitore lo svolgimento dei servizi di manutenzione correttiva e adeguativa con l'obiettivo di garantire la corretta funzionalità e l'aderenza ai vincoli normativi e istituzionali dell'applicazione presa in carico ad inizio contratto, nell'ottica di assicurarne la piena operatività.

Per il servizio di Manutenzione Correttiva il Fornitore è tenuto a svolgere l'insieme delle attività direttamente finalizzate ad eliminare i malfunzionamenti del *software* e le cause che li hanno determinati, considerando in tale ambito:

- malfunzionamenti o anomalie, ivi compresa la documentazione a corredo;
- problemi, potenziali o manifesti, derivanti da obsolescenza o incompatibilità tecnologica con componenti hardware e software utilizzati a supporto.

Nell'ambito della Manutenzione Adeguativa rientrano, invece, tutte le attività volte ad assicurare la costante aderenza delle componenti del sito/applicazione web all'evoluzione dell'ambiente tecnologico del sistema informativo e al cambiamento dei requisiti (organizzativi, normativi, d'ambiente).

Tipiche tipologie di manutenzione Adeguativa riguardano:

- adeguamenti dovuti a cambiamenti di condizioni al contorno (ad esempio per variazioni del numero utenti, per migliorie di performance, per aumento delle dimensioni delle basi dati, etc.);
- adeguamenti necessari a seguito di innalzamento di versioni del *software* di base;
- migrazioni di piattaforma.

Il servizio di Manutenzione Correttiva e Adeguativa si considera inclusivo delle seguenti attività:

- Analisi del malfunzionamento, comprensiva della valutazione degli impatti e dei vincoli sistemistici necessari all'individuazione della soluzione *software* da implementare;
- Sviluppo delle fix e test, da intendersi comprensivo dei test di non regressione sulle funzionalità esistenti e dei test di regressione dei *bug*;

- Rilascio della soluzione modificata negli ambienti di collaudo ed esercizio secondo le politiche di sicurezza definite;
- Attività di garanzia sul *software* sviluppato, finalizzate alla correzione di eventuali *bug*, malfunzionamenti o difformità di funzionamento rispetto a quanto espresso nei requisiti, da intendersi comprensivo dei test di non regressione rispetto alle funzionalità preesistenti lo sviluppo specifico che ha generato il *bug*/malfunzionamento;
- manutenzione della Gestione dei Contenuti, ovvero l'insieme di attività, risorse e strumenti di supporto per la gestione dei contenuti testuali che l'applicazione deve garantire nel rispetto del servizio erogato;
- produzione di misure e materiale funzionale alla determinazione della variazione della baseline applicativa, laddove sia necessario produrre un aggiornamento della stessa.

3.2.4 Conduzione Operativa Applicativi e Database

Il servizio comprende attività, risorse e strumenti di supporto per la gestione in esercizio di quanto sviluppato, gestito e mantenuto di cui si riporta di seguito un elenco non esaustivo:

- a. Gestione delle funzionalità e delle operazioni in esercizio, comprensiva di attività di gestione della configurazione:
 - ripristino base dati;
 - modifiche di parametri di esecuzione o di tabelle di riferimento o decodifica;
 - gestione della configurazione;
 - gestione dei *batch*;
 - gestione flussi DWH verso i sistemi di Bdl (par. 2.3.6);
 - gestione A2A e flussi di preventivazione massiva (par. 2.3.8);
 - verifica ed aggiornamento di eventuale documentazione specifica della gestione applicativa (ad es. FAQ, modi d'uso, modalità di esecuzione di particolari attività del servizio di gestione, etc.) in collaborazione con i gruppi di sviluppo responsabili della manualistica utente e di gestione.
- b. Presa in carico di nuove funzionalità in esercizio:
 - schedulazione e pianificazione della presa in carico di nuove funzionalità e del loro rilascio in esercizio;
 - verifica e validazione dei prodotti per la gestione: procedure, parametri e tabelle, manuali utente, manuale di gestione, definizioni relative ai dati;
 - supporto alla predisposizione dell'ambiente di esercizio e quanto necessario a consentire l'inizio delle attività da parte degli utenti;
 - gestione di nuove configurazioni;
 - supporto alla predisposizione dell'ambiente di esercizio e quant'altro necessario a consentire l'esercizio delle attività da parte degli utenti.

Nel servizio sono inoltre incluse le attività di integrazione con le Banche Dati esterne interconnesse al sistema (BD ATRC, BD SITA, BD SIVI, BD Infocar/infobike, Egon).

Le attività di gestione delle funzionalità correnti e di configurazione delle applicazioni andranno gestite secondo la seguente logica di processo:

- la pianificazione funzionale del servizio andrà realizzata in fase di presa in carico sulla base dell'*assessment* iniziale e, in seguito, continuamente aggiornata sulla scorta delle richieste provenienti dall'ingresso in esercizio di nuove funzionalità o dalle modifiche di funzionalità esistenti, nonché sulla base delle esigenze di modifica, parametrizzazione ed intervento provenienti dagli utenti;
- l'aggiornamento continuo implica che il team di conduzione deve aggiornare continuamente una precisa schedulazione delle attività correnti da realizzare e, inoltre, deve essere in grado di allocare dinamicamente risorse – eventualmente aggiuntive ove necessario - per l'esecuzione di *task* aggiuntivi o imprevisti, quali ad esempio risoluzione di richieste utente, ripristino di basi dati o modifiche di tabelle di codifica;
- il processo di continual service improvement richiesto deve garantire che ciascun elemento inserito nelle attività correnti venga opportunamente documentato e correttamente gestito e, inoltre, che si verifichi la sua coerenza complessiva con i processi in essere. In particolare, ciò può comportare la formulazione di proposte di ottimizzazione e semplificazione delle attività correnti.

3.2.5 Strumenti di *Test management*

Il Fornitore dovrà rendere disponibile una soluzione di test management, senza oneri aggiuntivi per l'IVASS, con cui gestire la fase di test relativa alle applicazioni gestite nell'ambito della presente fornitura. Con tale soluzione quindi dovrà essere possibile progettare i test, monitorare il grado di copertura degli stessi, verificare la completezza e la rispondenza dei test ai requisiti, controllare l'esecuzione e memorizzare i risultati, fornire tutti i report per le necessarie verifiche e consentire il riutilizzo dei test in successivi contesti (esempio: test di non regressione).

Sempre nell'ambito del test proceduralizzato la soluzione dovrà consentire un approccio collaborativo alle attività di test, quali ad esempio:

- individuazione dei gruppi dedicati al test;
- assegnazione dei *task* di test;
- controllo delle attività.

Il Fornitore dovrà consentire, sulla base dei test progettati, o di test progettati *ad hoc*, di effettuare in automatico l'attività di test (test automatizzato) per garantire esecuzione e ri-esecuzione periodica dei test automatici e controllo dei risultati.

Inoltre il Fornitore dovrà sviluppare test automatici relativi alle funzionalità web, utilizzando strumenti automatici come la suite *open source Selenium* o equivalenti.

3.2.6 Accessibilità

Il software prodotto deve rispettare i requisiti di accessibilità così come definito nelle linee guida AgID, con particolare riferimento allo standard WCAG 2.1 (*Web Content Accessibility Guidelines*).

Il Fornitore si impegna a produrre un report sul grado di accessibilità del software dal quale possano essere estratte informazioni utili alla redazione, da parte di IVASS, della “dichiarazione di accessibilità” prevista dalla normativa vigente. Il report dovrà essere redatto attraverso la compilazione del “modello di autovalutazione di accessibilità” messo a disposizione da AgID.

Una prima versione di tale report dovrà essere prodotta durante il periodo di presa in carico delle attività da parte del Fornitore. Successive versioni dovranno essere prodotte in concomitanza con ciascuna *Major Release* oppure su specifica richiesta di IVASS.

Si rende inoltre necessario eseguire test di usabilità ad ogni rilascio di nuove funzionalità. I test potranno essere condotti attraverso i più comuni metodi e strumenti presenti sul mercato, nonché seguendo le indicazioni AgID riportate nei link presenti su <https://www.agid.gov.it/it/design-servizi/usabilita>.

3.2.7 Composizione del team dei Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database

Le risorse preposte dal Fornitore al servizio dovranno acquisire e mantenere un'ottima preparazione sia funzionale sia tecnica sulle applicazioni in ambito e dovranno lavorare in sinergia con il team dei servizi di sviluppo e con i restanti team sugli altri servizi, al fine di rispondere prontamente ed efficacemente alle diverse attività contenute nel servizio stesso.

Le attività richieste per i Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database (par. 3.2) sono da erogarsi in modalità continuativa e saranno remunerate a canone (ad esclusione delle attività di Manutenzione Evolutiva) secondo quanto indicato in offerta economica, sulla base del dimensionamento del Team mix definito nella seguente Tabella A.

Per quanto riguarda la composizione del team di lavoro, il Team mix di riferimento richiesto è:

Tabella A

Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database	Peso %sul servizio	gg/mese
Capo progetto	5%	1,25
Analista Funzionale	10%	2,5
Analista Programmatore	30%	7,5
Programmatore	42%	10,5
Specialista di tecnologia/prodotto junior - Specialista di Sicurezza	5%	1,25
Specialista di tematica - Accessibilità	2%	0,5
Grafico Web	2%	0,5
Web Designer	4%	1
	100%	25

Unicamente per gli interventi di Manutenzione Evolutiva (MEV), di cui al par. 3.2.1 lett. b) - Sviluppo del *Software* e Manutenzione Evolutiva del *software* -, la modalità di erogazione richiesta sarà invece di tipo progettuale e remunerata considerando le giornate/team impiegate per ogni singolo intervento evolutivo e il prezzo medio offerto in sede di Gara dal Fornitore.

Il prezzo medio per definire la base d'asta del Team MEV (individuato in euro 378,40 per giorno/team) è stato calcolato considerando la composizione del team mix definito alla seguente Tabella B, mutuata dalla definizione prevista da Consip¹. Analogamente le remunerazioni dei singoli profili professionali dello stesso team si basano su una rivalutazione delle previsioni Consip.

Tabella B

Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database	Percentuale di utilizzo (mix) indicata nel Capitolato tecnico
Capo progetto	3,00%
Specialista di tematica	5,00%
Analista Funzionale	15,00%
Web Designer	12,00%
Analista Programmatore	30,00%
Programmatore	20,00%
Grafico Web	10,00%
Specialista di tecnologia/prodotto senior	5,00%

3.3 Servizio di *Backoffice* e supporto alle Imprese Assicurative e Intermediari

3.3.1 Descrizione del Servizio

In relazione alle necessità progettuali dell'Istituto è richiesta l'attivazione di un servizio di *backoffice* e supporto alle Imprese Assicurative e agli Intermediari assicurativi.

Di seguito un elenco non esaustivo delle attività richieste al servizio:

- caricamento puntuale delle imprese assicurative nel portale;
- supporto alle imprese in riferimento ai processi di abilitazione e autenticazione al portale dei propri amministratori;
- aggiornamento delle configurazioni del sistema;
- gestione delle analisi statistiche e delle attività di monitoraggio sull'operato degli utenti professionali (imprese assicurative e intermediari) in relazione all'utilizzo di PREVENTIVASS, anche tramite interrogazioni alle viste aggregate sui dati;
- visualizzazione e validazione degli aggiornamenti dei dati inseriti dalle imprese nell'area riservata di propria competenza (es. dati identificativi forniti dalle imprese);
- monitoraggio e analisi degli errori nelle richieste di preventivo e indirizzamento della relativa risoluzione;
- supporto alle imprese e agli intermediari in relazione all'utilizzo del Preventivatore;
- redazione e revisione di documentazione di progetto per condivisioni interne ed esterne;
- redazione e condivisione del materiale divulgativo contenente le specifiche tecniche da adottarsi per operare in Preventivass (Manuali Utente, Allegati tecnici, specifiche per l'integrazione, etc.);

¹ Vedi "Parametri di stima del valore dell'appalto" al par. 1.2 del presente documento

- aggiornamento costante in termini di contenuti e di adeguamenti normativi della documentazione e dei contenuti presenti sui portali;
- condivisione di documentazione tecnica e log applicativi con le imprese assicurative;
- attività di supporto agli Intermediari per il corretto utilizzo dell'applicazione (circa 250.000 intermediari);
- attività di supporto all'installazione e alla manutenzione dei sistemi di integrazione in modalità *Application to Application* di tipo on line e di tipo massivo rivolti alle imprese e agli intermediari;
- attività di gestione dei flussi *Application to Application* tra Preventivass e i sistemi delle Imprese assicurative a supporto del processo di preventivazione massiva per i rinnovi delle polizze (batch con picchi di oltre 50.000 record giornalieri e gestione di scarti/errori e comunicazione verso i responsabili di Impresa);
- analisi delle problematiche relative al processo di preventivazione oggetto di segnalazione da parte degli utenti delle imprese assicurative o dell'ANIA;
- analisi delle problematiche relative al processo di preventivazione oggetto di segnalazione da parte di consumatori o di richiesta di accesso agli atti;
- attività di gestione del servizio di *Incident Management*;
- attività di *Project Management* e gestione dei sopra citati filoni progettuali.

Nel dettaglio il team fornirà supporto tecnico specialistico all'attività di monitoraggio e supervisione dei flussi di preventivazione erogati dalle imprese. In particolare, dovrà monitorare eventuali problematiche, con relativa attività di *problem determination* degli errori, indirizzando tempestivamente la risoluzione verso il corretto interlocutore, sia esso il team di sviluppo, l'impresa assicuratrice o uno dei fornitori di servizi esterni (Ania, Infocar, Infobike, Egon), tracciando puntualmente le attività intraprese dall'inizio della problematica sino alla sua risoluzione, aggiornando costantemente l'Istituto con report giornalieri/settimanali sulle problematiche.

Rientra nelle attività del servizio anche il monitoraggio dei flussi di alimentazione del sistema Preventivass verso il DWH di Bdl.

Sarà cura del servizio la revisione della documentazione tecnica a supporto delle imprese e di IVASS, con verifica puntuale del corretto allineamento informativo tra il portale, la documentazione a supporto e le attività di MEV, MAD e MAC.

Il servizio provvederà inoltre, in collaborazione con l'IVASS, all'aggiornamento e alla redazione del Manuale Tecnico dell'Amministratore d'Impresa, di cui all'Allegato 1 al regolamento IVASS n. 51/2022.

Questo servizio richiede in primo luogo adeguata preparazione in materia contrattuale assicurativa, in particolare nel ramo r.c. auto, con specifico riguardo alle attività di emissione di preventivi. È inoltre richiesto un elevato livello di esperienze informatiche in ambito di servizi Cloud AWS o similari.

Le attività sopra elencate, da erogarsi in modalità continuativa, saranno remunerate a canone secondo quanto indicato in offerta economica sulla base del dimensionamento determinato nel seguente paragrafo.

3.3.2 Composizione del team del Servizio di *Backoffice* e supporto alle Imprese Assicurative

Per quanto riguarda la composizione del *team* di lavoro, il *Team mix* di riferimento richiesto è:

Servizio di Backoffice e supporto alle Imprese Assicurative	Peso %sul servizio	gg/mese
Capo progetto	5%	2,2
Specialista di Tematica	95%	41,8
	100%	44

È richiesta la presenza *on site* del *team* di progetto presso la sede dell'Istituto.

3.4 Servizi di Supporto Specialistico / Presidio on-site

È richiesto un Servizio di Supporto Specialistico negli ambiti della Fornitura con riferimento alla molteplicità di tematiche tecnologiche e funzionali relative ad ogni aspetto del sistema.

3.4.1 Descrizione del Servizio

Il servizio deve garantire che la soluzione applicativa sia la migliore risposta ai cambiamenti di natura normativa e alle mutate esigenze del mercato assicurativo, fornendo un contributo tematico specialistico a supporto dell'Istituto.

Il servizio si articola principalmente nei seguenti macro-ambiti:

- Supporto specialistico di prodotto, tecnologia e piattaforma;
- Supporto tematico, funzionale e di processo per gli aspetti caratterizzanti il perimetro della fornitura;
- Studi di fattibilità e analisi ad hoc nell'ambito di tematiche applicative, funzionali, infrastrutturali, di processo e di *customer experience*, sul perimetro dei servizi oggetto della fornitura.

Di seguito un elenco non esaustivo delle attività/competenze richieste:

- elevata competenza tecnica e conoscenza approfondita del Contratto Base r.c. auto e degli aspetti normativi inerenti la preventivazione r.c. auto;
- capacità di supporto tecnico specialistico per la interlocuzione con i referenti di business delle imprese assicurative su temi di natura assicurativa;
- analisi e valutazione dei costi previsti e sostenuti per tutti gli elementi che caratterizzano l'architettura compresi fornitori esterni e/o banche dati esterne (Infocar/Infobike, Egon, BD ANIA, *Google Recaptcha*);
- capacità di supporto tecnico specialistico per la interlocuzione con responsabili AGID e/o Identity provider, per aspetti relativi allo SPID ad uso professionale;
- supporto per attività di studio di fattibilità per la possibile integrazione con la banca dati ANPR gestita dal Ministero degli interni;
- supporto per attività di studio di fattibilità per la possibile integrazione con il servizio delle Patenti della Motorizzazione;
- coordinamento delle attività di progetto per tutte le tematiche progettuali;
- supporto tecnico agli utenti IVASS in tema di funzionalità descritte al par. 2.3.3 al fine dello svolgimento delle attività di propria competenza;
- supporto agli utenti IVASS nella redazione ed esposizione sul front end dell'applicazione di contenuti informativi e/o di messaggistica;

- supporto per le fasi di produzione dei report previsti a cadenza periodica o richiesti dall'IVASS, con successivo supporto nell'interpretazione, analisi e presentazione dei risultati;
- supporto agli utenti IVASS, relativamente alle integrazioni tecniche e di contenuto effettuate dalle imprese assicurative sull'applicazione;
- supporto al monitoraggio e aggiornamento delle integrazioni con nuove Banche Dati esterne;
- supporto specialistico per la predisposizione di relazioni tecniche e studi di fattibilità;
- supporto specialistico a seguito di segnalazioni provenienti dagli utenti di anomalie/difformità del sistema rispetto a quanto previsto dalla normativa riguardante il Contratto Base;
- supporto specialistico per la corretta gestione applicativa di problematiche di natura tecnica e/o normativa risultanti dal processo di preventivazione (Bonus Famiglia, Dopo voltura, Attestato di rischio, etc.);
- supporto specialistico alla formazione delle risorse dell'IVASS in tema di funzionalità del preventivatore per eventuali esigenze di servizio.

Il team fornirà supporto tecnico specialistico su tutte le tematiche inerenti il progetto, siano esse di natura normativa/giuridica che tecnica; per questo motivo viene richiesto che le risorse componenti il team di progetto abbiano consolidate competenze in entrambi gli ambiti.

Il servizio dovrà, altresì, essere promotore di adeguamenti/miglioramenti applicativi individuati sulla base di informazioni e/o requisiti provenienti da altri servizi presenti in Istituto e/o da altri utilizzatori dell'applicazione, andando a identificare eventuali punti di miglioramento dell'applicativo.

Le aree di miglioramento/adeguamento potranno interessare aspetti funzionali, della UX, e di sicurezza.

Le attività sopra elencate, da erogarsi in modalità continuativa, saranno remunerate a canone secondo quanto indicato in offerta economica sulla base del dimensionamento determinato nel seguente paragrafo.

3.4.2 Composizione del team del Servizio di Supporto Specialistico / Presidio on-site

Per quanto riguarda la composizione del *team* di lavoro, il *Team mix* di riferimento richiesto è:

Servizi di Supporto Specialistico / Presidio onsite	Peso % sul servizio	gg/mese
Capo progetto	2%	0,84
Specialista di Business	49%	20,58
Architetto/Progettista IT	49%	20,58
	100%	42

Considerando la tipologia del servizio da erogare, è richiesta la presenza fisica del *team* di progetto presso la sede dell'Istituto.

3.5 Servizio di *cyber security*

Il servizio richiesto al Fornitore comprende tutte le attività necessarie per l'adozione delle indicazioni di seguito descritte. Il Fornitore in linea generale deve conformarsi alle policy di sicurezza in essere presso l'IVASS e/o Banca d'Italia che verranno rese disponibili nel periodo di affiancamento di inizio fornitura.

3.5.1 Security Assessment

È richiesta in via generale l'esecuzione di procedure periodiche di *Security Assessment* concordate con l'IVASS, finalizzate a valutare il grado di protezione di tutte le componenti del sistema e la conformità delle soluzioni adottate alle previsioni contenute nelle Linee Guida emanate in materia dall'IVASS e dalla Banca d'Italia.

3.5.2 Code Review

Nelle fasi di analisi e progettazione, preliminari alle attività di sviluppo applicativo, dovranno essere rispettati dal Fornitore i requisiti di sicurezza derivanti dall'analisi del rischio dell'Istituto, in conformità con le best practice di settore (linee guida Banca d'Italia) in materia di sviluppo di codice *software* sicuro, con particolare riferimento allo standard OWASP.

Nella fase di rilascio del *software* il Fornitore deve garantire all'interno del proprio *team* applicativo, le attività di analisi del codice sorgente finalizzate a rilevare eventuali vulnerabilità introdotte in fase di sviluppo, verificando, in particolar modo, i seguenti aspetti:

- la presenza e la validità dell'implementazione dei meccanismi destinati ad assolvere al processo di autenticazione e autorizzazione degli utenti;
- la presenza e la validità dell'implementazione dei meccanismi di validazione ed integrità del dato destinato ad essere processato sia server che client side;
- la presenza di segmenti critici di codice che pur non essendo direttamente un problema potrebbero creare errori.

Resta tuttavia necessaria l'esecuzione complessiva dei *Security Assessment* a cadenza periodica.

3.5.3 Controllo Accessi Logici

Il Fornitore dovrà garantire il controllo degli accessi al sistema, distinto in due categorie:

- accesso ai sistemi/risorse mediante console AWS e sistemi WSO2;
- accesso all'applicazione.

L'Istituto ha scelto di affidarsi alla soluzione basata sul servizio AWS *CloudTrail*, al fine di registrare, conservare e consultare le attività effettuate da qualsiasi entità sulle chiavi KMS attraverso la scrittura di file di log contenenti tutti i dettagli necessari (ad esempio utente, date e ora di utilizzo, azione effettuata).

Il servizio AWS *CloudTrail* è utilizzato anche per fini di audit e compliance, in quanto fornisce uno storico delle attività nell'account AWS, eseguite tramite la Console.

Il Fornitore deve garantire anche il controllo degli accessi al sistema gestiti attraverso WSO2, che ospita i relativi log all'interno delle macchine virtuali che erogano tali servizi.

Tutti i file generati dovranno essere criptati, utilizzando chiavi gestite dal servizio KMS di AWS e sottoposti al processo di "*integrity validation*" che assicura la non manipolazione dei file dopo la loro creazione.

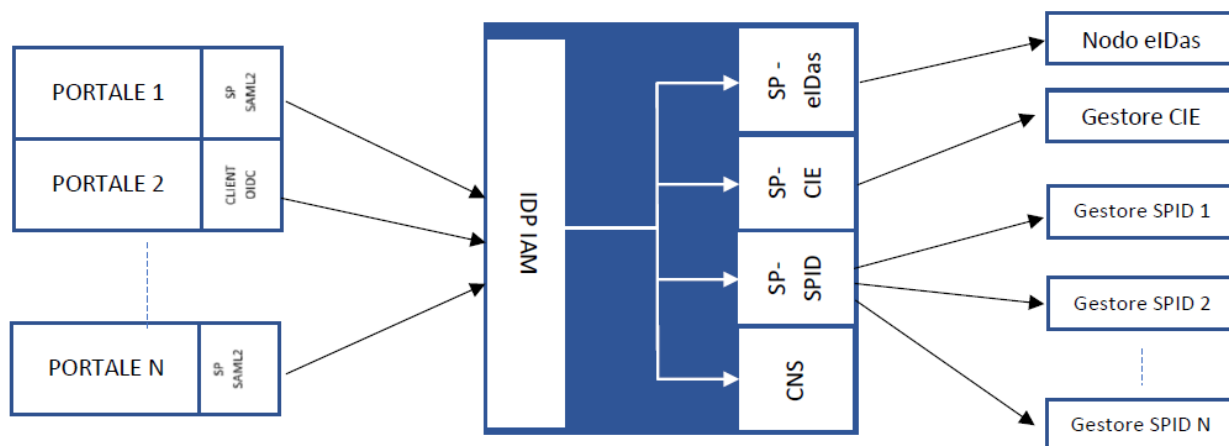
Il Fornitore, tenuto conto di quanto sopra esposto, dovrà comunque garantire per tutta la durata del contratto l'adozione delle *best-practice* di sicurezza.

Per gli accessi ai sistemi informativi del Committente, il Fornitore dovrà garantire la continuità dei processi di *onboarding* e *offboarding* delle identità aziendali e degli utenti IVASS, nonché dei diritti di accesso a loro collegati.

Tali processi prevedono:

- l'uso di user ID uniche così che gli utenti possano essere collegati alle proprie azioni ed essere resi in tal modo responsabili;
- il controllo dell'autorizzazione utente per l'accesso alla risorsa richiesta;
- il controllo di appropriatezza del livello di accesso concesso;
- la registrazione formale di tutti i soggetti che possono accedere alle varie risorse, la relativa storizzazione, eventuali riferimenti a contratti e servizi, motivazione all'accesso, data di concessione e revoca delle autorizzazioni, temporaneità dell'accesso;
- la rimozione immediata dei diritti d'accesso degli utenti per i quali non è più necessario o possibile mantenere accesso;
- il controllo periodico di *User ID* e account ridondanti, per la rimozione;
- la non riassegnazione delle *User ID* ridondanti o rimosse concesse precedentemente ad altri utenti.

Inoltre, sfruttando lo IAM in essere, e tramite la piattaforma WSO2 *Identity Server*, il Fornitore dovrà implementare tutte le modalità di accesso previste dal CAD (Codice dell'Amministrazione Digitale).



I portali applicativi si dovranno federare con lo IAM tramite protocolli standard (es. SAML 2, *Opened Connect*, etc). Ogni portale deve poter comunicare con la componente IDP (*Identity Provider*) dello IAM, che a sua volta dovrà presentarsi come Service Provider verso le tecnologie SPID, anche ad uso professionale, CNS, CIE ed eIDAS.

3.5.4 Strumenti di *Security Incident SIEM*

È richiesta al Fornitore aggiudicatario la disponibilità nel proprio Centro Servizi (par. 3.6.1) di strumenti per la gestione di *security incident SIEM*.

Il SIEM è il servizio che consente di raccogliere, archiviare, monitorare log e correlare eventi con l'obiettivo di identificare attacchi o violazioni di dati. Esso fornisce un utile strumento a supporto delle attività di indagine in risposta a incidenti di sicurezza.

Il SIEM consente di aggregare gli eventi che sono originati da una vasta gamma di elementi, tra cui apparati di sicurezza, apparati di rete, *endpoint* e applicazioni, tipicamente attraverso l'analisi dei *log* prodotti ma anche attraverso altre fonti, quali ad esempio il traffico di rete.

I dati raccolti possono essere arricchiti con ulteriori dati di contesto, quali ad esempio utenti, *asset*, minacce conosciute e vulnerabilità riscontrate.

Il SIEM effettua attività di normalizzazione delle informazioni raccolte dalle varie fonti, fornendo viste e report specifici che consentono di semplificare le attività di analisi della vasta mole di dati raccolta.

Per *Security Incident* si intendono gli incidenti in grado di causare una interruzione o un degrado dell'erogazione di un qualsiasi servizio che coinvolge principalmente gli aspetti relativi alla sicurezza e che possono ledere la disponibilità, l'integrità o la confidenzialità di qualsiasi fonte di dati gestita dal sistema IVASS.

A titolo esemplificativo si riportano di seguito alcune tipologie di evento rientranti nella suddetta definizione:

- accessi non autorizzati a file e/o dati;
- infezione di file da parte di virus;
- modifica delle *access control list*;
- introduzione di codice non autorizzato che consenta l'accesso non autorizzato o causi il danneggiamento di dati.

Nell'ambito di questo servizio è richiesto che il Fornitore realizzi e gestisca una piattaforma public o private cloud in modalità *Managed Security Service (MSS)*, comprensiva delle risorse necessarie per:

- tracciare gli eventi di sicurezza e inviarli al SIEM;
- la gestione dei *security incident*;
- ispezionare il traffico in entrata e in uscita;
- adottare funzionalità di "*Virtual Patching*" per proteggere da vulnerabilità note fino a quando non possono essere corrette;
- identificare e rimuovere immediatamente *malware* e bloccare i domini noti;
- la gestione centralizzata dei log di sicurezza generati da sistemi, applicazioni e apparati di sicurezza presenti sul perimetro di IVASS.

Per quanto riguarda le fonti di alimentazione del SIEM, queste sono costituite da:

- *Web application firewall*;
- *Agent* installati sugli *endpoint*;
- *Group Policy* di AWS.

Il Servizio dovrà prevedere una copertura H24 7x7.

Il Fornitore dovrà garantire un proprio *Security Operation Center (SOC)* deputato alla gestione di *security incident* mediante personale tecnico specializzato.

3.5.5 Strumenti di *Vulnerability Assessment*

Il Fornitore deve garantire l'esecuzione di procedure di *Vulnerability assessment* da effettuarsi almeno 2 volte all'anno; l'attività è finalizzata a rilevare eventuali vulnerabilità sulle applicazioni oggetto di affidamento.

Il Fornitore deve assicurare il rispetto almeno dei seguenti *standard e best practice*:

- ISECOM OSSTMM (*Open-Source Security Testing Methodology Manual*);
- OWASP (*Open-Source Mobile Application Security Project*).

A seguito dell'attività di *Assessment*, il Fornitore deve produrre un report in formato cifrato, con password fornita al responsabile di progetto, all'interno del quale siano riportate in elenco le vulnerabilità rilevate sul parco applicativo IVASS e le indicazioni per eliminarle.

L'assessment sarà realizzato da un *Security Assessment Team*, a supporto delle attività di sviluppo e soprattutto prima del rilascio in produzione, al fine di introdurre eventuali azioni correttive evidenziate dal rapporto prodotto dallo strumento di analisi.

3.5.6 Strumenti di *Penetration Test*

Il Fornitore deve garantire l'esecuzione di procedure di *Penetration Test*; l'attività è finalizzata a simulare attacchi informatici svolti da analisti altamente specializzati, detti "*Ethical Hacker*", in grado di rilevare vulnerabilità e di contestualizzarle sul sistema Ivass oggetto di affidamento.

Occorre garantire il rispetto degli standard e *best practice* a livello internazionale, quale OWASP WSTG (*Web Security Testing Guide*).

Tali attività vanno eseguite:

- Periodicamente: una volta l'anno;
- *Event Driven*, ovvero:
 - in caso di attacchi o minacce *cyber* di rilevante entità;
 - alla fine della fase di ripristino in seguito all'accadimento di un incidente di sicurezza;
 - in caso di modifiche rilevanti intervenute nel periodo su configurazioni/sistemi in perimetro.

A seguito dell'attività di *Penetration Test*, il Fornitore deve produrre un report in formato cifrato, con password fornita al responsabile di progetto, all'interno del quale siano riportate in elenco le vulnerabilità rilevate sul parco applicativo IVASS e le indicazioni per eliminarle.

3.5.7 Tool di *Log Management*

Il Fornitore deve garantire la gestione di un servizio di *Log Management* aggiuntivo avente come oggetto il trattamento degli accessi al sistema Preventivass da parte degli amministratori; tale servizio deve essere erogato in maniera conforme alle disposizioni della normativa italiana ed europea in materia.

Deve essere garantita anche la conformità alle disposizioni contenute nel regolamento UE 2016/679 (GDPR – *General Data Protection Regulation*) e alle relative eventuali specifiche indicazioni del Garante della Privacy sul tema indicato e sul contesto oggetto di affidamento.

Gli accessi devono essere registrati su un archivio (*log*) non cancellabile con funzioni di reset.

Su richiesta dell'amministrazione, il Fornitore deve consegnare i *log* di sistema generati, almeno in formato CSV o TXT. Tali *log* dovranno essere inviati ad IVASS entro tre giorni lavorativi successivi a quello in cui è avvenuta la richiesta.

Il Fornitore deve garantire, senza oneri aggiuntivi per l'Istituto, la raccolta e conservazione dei dati per un periodo che sarà comunicato nella fase di presa in carico.

Il Fornitore opererà garantendo la massima riservatezza sui dati gestiti.

3.5.8 Gestione del *Web Application Firewall* (WAF)

Nell'ambito del servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche è richiesta al Fornitore la gestione del WAF di AWS.

Il servizio AWS WAF è un firewall per applicazioni Web che protegge da attacchi malevoli. Attraverso l'adozione di determinate regole di sicurezza il WAF analizza tutte le chiamate ricevute dalla propria applicazione Web o API esposta e determina se permettere o meno di inoltrare la stessa alle risorse richiamate.

Il servizio di "*Web Application Firewall*" verrà fornito in modalità SaaS e dovrà permettere di filtrare, monitorare e bloccare il traffico HTTP da e verso un servizio Web, esaminando il traffico, utilizzando regole, analisi e firme per rilevare attacchi, proteggendo quindi il sistema dagli attacchi incorporati nei dati trasmessi dalle applicazioni web.

Il Fornitore, nell'ambito del servizio di *Web Application Firewall*, dovrà garantire almeno le seguenti funzionalità:

- protezione dagli attacchi più critici alle applicazioni web, quali ad esempio Iniezioni SQL, *Cross-site scripting* (XSS), inclusione di file e configurazioni di sistema impropri, dirottamento di sessioni, *buffer overflow*;
- capacità evoluta di filtraggio del traffico con possibilità di configurare l'utilizzo di *whitelist* e *blacklist*;
- funzionalità di apprendimento automatico che consentano di individuare un modello di comportamento dell'utente per distinguere il traffico benigno da quello dannoso delle applicazioni;
- rilevamento automatico della natura dei contenuti e rilevazione di attacchi che comportino la manomissione di cookie, sessioni o parametri;
- funzionalità di ispezione del traffico SSL criptato;
- capacità di identificare/bloccare gli allegati XML che nascondono contenuti dannosi e di convalidare gli schemi per i messaggi SOAP. Protezione di API e *web services* in tecnologia REST e SOAP;
- supporto per le regole di controllo degli accessi a livello di rete e componente basate sulla firma per rilevare le minacce note;
- trasmissione di eventi e log al SIEM;
- CDN (*Content Delivery Network*);
- *caching* dei contenuti statici;
- produzione di report periodici di sintesi.

Per quanto riguarda il dimensionamento, il WAF dovrà proteggere 1 dominio.

3.5.9 *Assessment* per la protezione dei dati personali

Il trattamento dei dati personali, da parte del Fornitore, dovrà ispirarsi al rispetto dei principi generali del Regolamento Europeo UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (c.d. "GDPR") e quindi avvenire in modo lecito e secondo correttezza, valutando la pertinenza, la completezza e la non eccedenza dei dati rispetto alle finalità dei trattamenti, in funzione delle attività assegnate.

In particolare, il Fornitore dovrà garantire l'adozione dei principi di "protezione dei dati fin dalla progettazione" e "protezione per impostazione predefinita", pertanto i sistemi e i servizi oggetto di gara dovranno essere disegnati fin dalla fase della progettazione tenendo conto della protezione dei dati

personali, come anche dei rischi per i diritti e le libertà delle persone fisiche coinvolte dal trattamento, al fine di attuare in modo efficace i principi di protezione dei dati e tutelare i diritti degli interessati.

3.5.10 *Hardening* dei sistemi

Il Fornitore è responsabile anche dell'*hardening* dei sistemi/configurazioni.

Le attività di *Hardening* dei sistemi includono tutte le operazioni di configurazione dei componenti specifici del sistema operativo che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità dello stesso, migliorandone pertanto la sicurezza complessiva.

I *server*, in particolare le macchine virtuali EC2, infatti devono operare nell'ambito di una configurazione di rete e di sistema che preveda l'abilitazione dei soli servizi necessari (*hardening* del sistema). Il rispetto di questa semplice regola deve essere in grado di produrre come risultato un sensibile miglioramento dei livelli di sicurezza attraverso alcuni accorgimenti tra i quali:

- la disabilitazione di tutti i servizi di rete non essenziali e, in particolar modo, di quelli affetti da vulnerabilità conosciute sotto il profilo della sicurezza;
- la rimozione dal sistema dei *files* corrispondenti ai servizi disabilitati;
- la disabilitazione delle porte (TCP ed UDP) in ascolto, non necessarie all'erogazione dei servizi;
- la rimozione o la disabilitazione di tutte le risorse non richieste in relazione al ruolo dell'*host* (compilatori, interpreti, *shell*, *scripts* ed altri strumenti analoghi);
- la corretta gestione degli utenti e dei loro privilegi;
- la predisposizione di regole adeguate all'accesso e l'uso delle risorse;
- l'accesso al sistema mediante utenze personali e ove necessario uso del comando *sudo* (*super user do*).

3.5.11 *Advanced Endpoint Protection* (AEP) e *Virtual Patching*

Il Fornitore deve fornire un servizio di Protezione *endpoint* che consenta di proteggere i sistemi server WSO2 definiti con risorse elaborative AWS dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli *endpoint* deve, inoltre, garantire che i dispositivi raggiungano un livello di sicurezza definito e siano conformi ai requisiti di conformità dell'Amministrazione.

Il Fornitore, nell'ambito del servizio di Protezione *endpoint*, dovrà garantire la disponibilità per l'IVASS almeno delle seguenti funzionalità:

- strumenti *antimalware*;
- protezione tramite meccanismi di *firewalling host-based*;
- servizi di IPS *host-based* con funzionalità di *Virtual Patching*;
- servizio di scansione delle vulnerabilità *host-based*;
- funzionalità di analisi dei log del sistema finalizzato all'identificazione di possibili problemi di sicurezza.

3.5.12 *Composizione del team* del Servizio di *cyber security*

Le attività sopra elencate, da erogarsi in modalità continuativa, saranno remunerate a canone secondo quanto indicato in offerta economica sulla base del dimensionamento determinato nella tabella seguente.

Servizi CyberSecurity	Peso % sul servizio	gg/mese
Capo progetto	2%	0,26
Specialista di tecnologia/prodotto senior - Specialista di Sicurezza	40%	5,2
Specialista di tecnologia/prodotto junior - Specialista di Sicurezza	58%	7,54
	100%	13

I servizi sopra citati dovranno essere garantiti dal Fornitore mediante il proprio Centro Servizi (par. 3.6.1).

3.6 Servizi trasversali

Il servizio richiesto al Fornitore comprende tutte le attività necessarie per l'adozione delle indicazioni di seguito descritte.

Tutti i Servizi dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio Italiano.

3.6.1 Centro Servizi

Il Fornitore deve disporre obbligatoriamente di un proprio Centro Servizi per l'erogazione di quanto previsto e richiesto dal presente documento. Il Fornitore dovrà descrivere dettagliatamente nell'offerta progettuale le soluzioni adottate per i Centri Servizi, che devono necessariamente rispondere a tutti i seguenti requisiti:

- i Centri Servizi in cui l'Aggiudicatario erogherà i servizi di cui al presente Capitolato dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio Italiano;
- è fatto obbligo inoltre al Fornitore di trattare, trasferire e conservare le eventuali repliche dei dati conservati dai suddetti Centri Servizi, ove autorizzate da Ivass, sempre all'interno del territorio comunitario; tali repliche dei dati dovranno essere conservate con livelli di sicurezza concordati con l'Amministrazione;
- l'infrastruttura tecnologica dei Centri Servizi dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza;
- è responsabilità del Fornitore assicurare che i propri Centri Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni siano protette mediante l'adozione di adeguati sistemi e metodologie, nel rispetto di quanto stabilito dallo standard ISO/IEC 27001.

3.6.2 Help Desk

Il Fornitore deve garantire e realizzare un servizio di *Help Desk*, dedicato all'assistenza in remoto, che abbia almeno le caratteristiche descritte di seguito nel capitolo e da considerarsi minime.

Il servizio di assistenza in remoto è rivolto ai Referenti identificati dall'Istituto e deve fornire un punto di accesso unificato per assistenza su aspetti funzionali e tecnici dei servizi oggetto della Fornitura; a tal fine, l'IVASS individuerà i propri Referenti funzionali che fungeranno da interlocutori con le strutture dell'*Help Desk*, gestendo al proprio interno il contatto con gli utenti finali dei servizi.

In particolare, deve essere reso disponibile almeno:

- un servizio di *help desk* telefonico, accessibile attraverso chiamata su un unico numero verde in tempo reale;
- un servizio di supporto via e-mail, integrato con il sistema di *Trouble Ticketing*;

- un'interfaccia *web* che consenta al referente dell'Amministrazione di inoltrare segnalazioni attraverso il sistema di *Trouble Ticketing*, sopra indicato.

L'*Help Desk* deve provvedere almeno a:

- assicurare una comunicazione tempestiva ed efficace con l'utenza;
- provvedere all'acquisizione e alla registrazione delle richieste di assistenza;
- censire le procedure di risoluzione, concordate con il committente, adottabili per far fronte alle segnalazioni dell'utenza;
- risolvere le segnalazioni per le quali è nota una procedura di risoluzione;
- smistare al secondo livello la risoluzione dei problemi non risolvibili al primo livello;
- controllare i processi di risoluzione attivati e verificarne gli esiti;
- comunicare all'utente la risoluzione della segnalazione o il suo inoltro al secondo livello;
- produrre statistiche sugli interventi ai fini di successive analisi.

In termini di dimensionamento il servizio richiesto dovrà far fronte a un numero di *ticket* su base annuale non superiore a 200.

3.6.3 Servizio di *Incident Management* e *Trouble Ticketing*

Il Fornitore deve realizzare e/o mettere a disposizione obbligatoriamente un "Sistema di *Trouble Ticketing*" accessibile tramite canale telefonico/mail/*web*.

Detto servizio deve provvedere a:

- la gestione dei *Trouble Ticket* (di seguito TT) aperti proattivamente dal Fornitore stesso;
- la gestione dei TT aperti da IVASS;
- l'assegnazione di TT al secondo livello;
- la riassegnazione di TT aperti in situazioni nelle quali l'ambito di competenza non sia individuato;
- il monitoraggio dello stato di avanzamento dei TT aperti.

La registrazione delle segnalazioni di malfunzionamento e/o delle richieste di servizio deve avvenire attraverso l'utilizzo del sistema di TT che dovrà tracciare almeno le informazioni minime seguenti:

- codice identificativo del TT;
- descrizione della segnalazione (malfunzionamento, richiesta di servizio, etc.);
- modalità di ricezione via telefono, internet, *web*, mail;
- data e orario di apertura;
- soggetto che ha richiesto l'intervento;
- elenco e numero di elementi complessivamente coinvolti dal malfunzionamento;
- classificazione della segnalazione (priorità, severità, etc);
- riferimenti operativi coinvolti nel caso specifico;
- smistamento al secondo livello qualora non fosse possibile fornire la soluzione;
- stato del TT;
- descrizione della soluzione;
- diagnosi del malfunzionamento, ove applicabile;
- data e orario di chiusura.

3.6.4 Strumenti di monitoraggio H24 dei sistemi

Il team messo a disposizione dal Fornitore si occuperà di garantire un servizio di monitoraggio a supporto dell'*Event/Incident management*.

L'attività di monitoraggio tecnico/applicativo dovrà essere eseguita 24 ore al giorno per 365 giorni all'anno, con soluzioni rese disponibili dal Fornitore stesso, per il monitoraggio di servizi AWS ritenuti critici e componenti applicative dettagliate nell'architettura oggetto di affidamento.

L'erogazione del monitoraggio dovrà avvenire "da remoto" attraverso il Centro Servizi messo a disposizione dal Fornitore, senza oneri aggiuntivi per l'Istituto.

Al verificarsi di eventi sulla piattaforma di monitoraggio il Fornitore dovrà attivare, nelle modalità che verranno stabilite con l'Istituto all'interno dei processi di *incident management*, i *team* responsabili dei servizi di competenza per i relativi interventi di ripristino.

Su base almeno semestrale il Fornitore avanzerà delle proposte di miglioramento del servizio e/o di introduzione di nuove modalità di monitoraggio.

La soluzione dovrà inoltre garantire la produzione ed il mantenimento dei dati del monitoraggio, sia per la produzione della reportistica contrattuale che per la storicizzazione delle informazioni.

Si evidenzia che è responsabilità del Fornitore provvedere all'adeguamento e manutenzione della Piattaforma di Monitoraggio per allineare i prodotti software alle versioni correnti.

3.6.5 Strumenti per la gestione degli sviluppi *DevOps*

Nell'ambito del servizio oggetto di fornitura, per quanto concerne le attività di predisposizione degli ambienti e di *deployment* del *software* negli ambienti operativi previsti (sviluppo, collaudo, produzione), si considera in via preferenziale l'adozione di modelli standard che dovranno essere sempre documentati e messi a disposizione dell'Istituto e delle Imprese Assicuratrici nel *repository* ufficiale.

Il progetto dovrà essere condotto secondo metodologia *DevOps* in declinazione Agile, attraverso strumenti e tecniche di *Continuous Integration/Continuous Delivery*.

L'Aggiudicatario dovrà adottare strumenti a supporto, quali ad esempio *Azure DevOps*, che rispondano ad esigenze di *governance*, tracciatura, automazione, anticipazione dei problemi e cooperazione tra sviluppo ed operation in ottica *DevOps*.

L'implementazione della piattaforma deve essere garantita e completata entro la fase di presa in carico del progetto.

L'utilizzo da parte dell'Aggiudicatario di tali strumenti, senza oneri aggiuntivi per l'Istituto, è richiesta al fine di assicurare la supervisione sulla *governance* del progetto, nelle fasi di progettazione, realizzazione, *delivery* ed esercizio.

3.6.6 Portale di governo e gestione della fornitura

Il Fornitore dovrà rendere disponibile un "Portale di Governo e Gestione della Fornitura" accessibile in modalità *web*, a ciascun utente abilitato (utente Ivass, Personale Banca d'Italia o altri Fornitori abilitati) mediante *login* e *password* assegnate.

Tale portale dovrà almeno:

- rendere disponibile un cruscotto sintetico di controllo e/o monitoraggio tecnico-operativo della fornitura, sulla base dei dati di propria competenza;
- rendere accessibili tutte le funzionalità e la reportistica relativa al monitoraggio tecnico-operativo della fornitura;
- rendere accessibili tutte le funzionalità e la reportistica forniti dal "Sistema di *Trouble Ticketing*";
- mettere a disposizione di ciascun utente abilitato i soli dati di propria competenza;
- rendere disponibili funzionalità di gestione e profilazione utenti.

Il Fornitore deve prevedere anche l'*hosting* della piattaforma.

3.6.7 Strumenti di *Change Management*

Il Fornitore deve garantire una soluzione di *Change Management* che dovrà fornire funzionalità per l'analisi, pianificazione, implementazione e monitoraggio del ciclo di vita dei cambiamenti minimizzando il rischio di interruzione del servizio nel rispetto della *policy* e dei processi adottati dall'Istituto.

Dovrà permettere di definire ed implementare processi di cambiamento standardizzati, che guidino l'Istituto attraverso l'intero ciclo di vita di una richiesta di modifica, dall'invio della stessa, alle fasi di pianificazione, attuazione e verifica.

In particolare, a titolo esemplificativo ma non esaustivo, si indicano le seguenti caratteristiche previste:

- assicurare che tutte le *change* siano registrate e oggetto di accurata valutazione affinché quelle autorizzate siano pianificate, testate, implementate, documentate e revisionate in base alla priorità e in modo controllato;
- verificare che i *configuration item* legati alle *change* siano registrati in un *Configuration Management Database* (CMDB).

Si evidenzia che l'adozione di una soluzione che integri i sistemi di *Trouble Ticketing* e di *Change Management* all'interno dello stesso prodotto sarà valutata positivamente in sede di analisi dell'offerta.

3.6.8 Strumenti di *Stress Test*

Il Fornitore deve assicurare la messa a disposizione di strumenti per lo svolgimento di test prestazionali (stress test) da erogarsi da remoto dal proprio Centro Servizi. La soluzione offerta, senza oneri aggiuntivi per l'Istituto, dovrà prevedere funzionalità di individuazione di percorsi critici e di esecuzione massiva di casi di test.

I dati statistici raccolti dalla soluzione di Test prestazionale verranno analizzati dai *team* di specialisti a supporto dei servizi oggetto del presente affidamento, al fine di gestire efficacemente l'architettura AWS in uso e prevenire degni prestazionali.

3.6.9 Reportistica

Il Fornitore deve assicurare la messa a disposizione della reportistica di seguito elencata:

- Reportistica a vantaggio di ogni singola impresa assicurativa integrata a Preventivass, disponibile all'interno dell'area riservata (backoffice) di competenza di ciascuna impresa, come indicato dalla disposizione n. 6 dell'Allegato 1 al regolamento IVASS n. 51/2022 (richieste di preventivo ricevute ed elaborate, livelli di servizio raggiunti, esiti dei controlli di validità e delle segnalazioni di errore di cui alle disposizioni nn. 5.1 e 5.2 del citato Allegato 1);

- Reportistica a disposizione degli utenti IVASS nel portale *Admin/Ivass* (*Admin Tool* Preventivatore) per il monitoraggio e il controllo delle attività di preventivazione delle imprese e l'espletamento delle attività istituzionali di vigilanza, studio e statistica. Detta reportistica dovrà essere fornita mediante apposita funzionalità dalla quale sia possibile visualizzare e scaricare diverse tipologie di resoconti di seguito elencati a titolo esemplificativo e non esaustivo:
 - "Preventivi totali": dettaglio dei risultati di tutte le richieste di preventivo ricevute, elaborate e trasmesse dall'applicazione e delle relative risposte di preventivo inviate dalle imprese assicurative, comprensivo degli esiti dei controlli di validità effettuati, delle segnalazioni di errore o incompletezza trasmesse dalle imprese stesse, delle tempistiche di risposta e delle mancate risposte;
 - "Provenienza richieste preventivo": dettaglio delle richieste di preventivo ricevute da ogni impresa assicurativa distinte per richieste inoltrate dall'applicazione *web* di Preventivass (con comparazione delle offerte formulate da tutte le imprese), richieste inviate in modalità di connessione A2A e richieste trasmesse per il tramite del singolo sito *web* di ogni impresa (senza comparazione delle offerte);
 - "Errori schema": dettaglio delle risposte di preventivo inviate dalle imprese assicurative non conformi allo schema di interscambio adottato, con specifica degli errori rilevati (errori *envelop*, errori *payload*);
 - "Classe di merito": dettaglio dei preventivi emessi dalle singole Compagnie distinti per preventivi privi di richiesta del c.d. Bonus Famiglia e preventivi nella cui richiesta sia stata selezionata l'opzione Bonus Famiglia, differenziando, per quest'ultima categoria, i preventivi per i quali le imprese hanno concesso il Bonus Famiglia dai preventivi per i quali il Bonus Famiglia non è stato accordato;
 - "Esito allineamento Infocar/Infobyke": dettaglio sull'esito del processo di allineamento "batch notturno" effettuato giornalmente;
 - "Esito interrogazioni Egon": dettaglio delle chiamate inoltrate al servizio di normalizzazione degli indirizzi, Egon, per ogni sessione di preventivazione, distinte per esito;
 - "Esito interrogazioni BD ANIA": dettaglio delle chiamate inoltrate alle BD ANIA per ogni processo di preventivazione avviato dagli utenti distinte per tipologia di banca dati interrogata (SIVI, SITA, ATRC), a loro volta differenziate per chiamate in errore e risposte corrette, diversificando, per quest'ultima categoria, le risposte corrette con esito positivo da quelle con esito negativo;
 - "Sessioni utente": dettaglio delle sessioni utente distinte per sessioni che hanno generato richieste di preventivo e sessioni di preventivazione non concluse, con specifica delle banche dati interrogate.
- Report relativi ai test case di cui al par. 3.2.5 (Strumenti di test management);
- Report sul grado di accessibilità dell'applicazione per la redazione, da parte di IVASS, della "dichiarazione di accessibilità" prevista dalla normativa vigente di cui al par. 3.2.6;
- Report giornalieri/settimanali sulle problematiche monitorate nell'ambito del Servizio di *Backoffice* e supporto alle imprese assicurative e Intermediari (par. 3.3.1) con relativa attività di *problem determination* degli errori e indirizzo della risoluzione verso il corretto interlocutore;
- Reportistica sulle attività previste all'interno del Servizio di *Cyber security* (par. 3.5) e dei Servizi Trasversali (par. 3.6).

3.6.10 Dimensionamento dei Servizi Trasversali

Le attività sopra elencate, saranno remunerate a canone secondo quanto indicato in offerta economica sulla base del dimensionamento stimato.

3.7 Fornitura Crediti AWS

Nella fornitura oggetto del presente Capitolato è richiesta l'acquisizione di crediti spendibili per l'approvvigionamento dei servizi disponibili sul catalogo *Amazon Web Services* (AWS) necessari al funzionamento dell'infrastruttura informatica.

L'acquisto dei predetti crediti dovrà garantire la disponibilità dei servizi AWS per tutta la durata della fornitura. A tal fine è richiesta l'attivazione di idoneo servizio di monitoraggio dei consumi e delle performance finalizzato ad ottimizzare l'infrastruttura AWS realizzata, migliorandone sicurezza e prestazioni e ridurre, così, i costi generali.

Per l'acquisto dei crediti il Fornitore applicherà lo sconto percentuale sul listino prezzi dei servizi AWS offerto in sede di Gara.

Per ciascun servizio acquistato sulla piattaforma AWS dovrà essere garantito un livello di qualità non inferiore a quello atteso di cui agli accordi tra Amazon ed i propri business partner.

4 Modalità di esecuzione della Fornitura

4.1 Luogo e orari di erogazione della Fornitura

I servizi dovranno essere erogati on site presso la sede di IVASS sita in Roma, Via del Quirinale 21 oppure "da remoto". L'IVASS mette a disposizione del Fornitore locali idonei presso la propria sede dotati della normale attrezzatura di ufficio e cablati per il collegamento degli elaboratori. Il Fornitore è tenuto ad attrezzare proprie stazioni di lavoro opportunamente equipaggiate con gli strumenti *software* necessari allo svolgimento dei servizi contrattualizzati e che dovranno rispettare le indicazioni sulla sicurezza e *policy* interne IVASS.

Il Fornitore dovrà comunque essere attrezzato anche per svolgere tutti i servizi da remoto. Resta a carico del Fornitore l'onere economico per le licenze dei prodotti *software* necessari alla gestione remota nonché la predisposizione e il dimensionamento del collegamento telematico.

Per la descrizione dei profili professionali minimi richiesti per lo svolgimento dei servizi previsti dal presente Capitolato si rinvia all'Appendice 2 allegata.

4.2 Tabella riepilogativa di luogo e orari di erogazione della fornitura

Servizio	Ubicazione servizio	Giorni	Orario
Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche	Da remoto	Lun - Ven	09:00 – 18:00
Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database	Da remoto	Lun - Ven	09:00 – 18:00
Servizio di <i>Backoffice</i> e supporto alle Imprese Assicuratrici e Intermediari	On-site	Lun - Ven	09:00 – 18:00
Servizi di Supporto Specialistico / Presidio <i>on-site</i>	On-site	Lun - Ven	09:00 – 18:00
Servizi <i>Cybersecurity</i>	Da remoto	Lun - Ven	09:00 – 18:00
Centro Servizi	Da remoto	Lun - Ven	09:00 – 18:00
<i>Help Desk</i>	Da remoto	Lun - Ven	09:00 – 18:00
<i>Incident Management</i>	Da remoto	365 per anno	H24
Monitoraggio sistemi	Da remoto	365 per anno	H24
Portale di governo della fornitura	Da remoto	365 per anno	H24

4.3 *Project Manager*

Per tutta la durata contrattuale l'aggiudicatario deve mettere a disposizione un *Project Manager* incaricato del coordinamento e del supporto alle diverse fasi progettuali e gestione del sistema nel suo complesso nonché referente nei confronti del Direttore Esecutivo del Contratto (DEC).

Il *Project Manager*, di elevata e comprovata professionalità, deve avere adeguata esperienza nella gestione e nel coordinamento di progetti nel settore di riferimento e nell'erogazione dei relativi servizi, nonché approfondita conoscenza delle diverse componenti del sistema, sia per l'aspetto *software* applicativo, sia per le componenti tecnologiche.

4.4 Reperibilità

Il Fornitore, senza oneri aggiuntivi per l'IVASS, deve sempre garantire la reperibilità del personale già impegnato nelle attività on-site diurne per rispondere tempestivamente ad eventuali situazioni critiche in orario notturno/festivo mediante dispositivi telefonici fissi e/o mobili o via posta elettronica, entro un'ora (1 ora) dalla segnalazione.

Per effettuare interventi in reperibilità il Responsabile del Fornitore, in base al tipo di intervento, deve far intervenire le risorse del medesimo Servizio ritenute idonee ai fini della risoluzione della problematica. La reperibilità telefonica non è remunerata ma è da considerarsi inclusa nel corrispettivo globale della fornitura.

4.5 Interventi fuori orario

Per le attività di conduzione operativa l'IVASS può richiedere interventi al di fuori dall'orario di lavoro base per esigenze contingenti di durata limitata nel tempo che richiedano la piena disponibilità del personale di conduzione oltre l'orario standard.

Gli interventi fuori orario non saranno remunerati ma sono da considerarsi inclusi nel corrispettivo globale della fornitura.

5 MODALITA' DI EROGAZIONE

Di seguito si riporta la tabella riassuntiva indicante i servizi oggetto della Fornitura, le modalità di erogazione, di consuntivazione e periodicità delle stesse nonché le quantità richieste.

ID Servizio	Descrizione Servizio	Modalità di Erogazione	Modalità di consuntivazione	Periodicità di consuntivazione	Quantità (unità)
1	Servizio di Conduzione Operativa e Manutenzione Infrastrutture Informatiche	Continuativa	A Canone	Mensile	24
2	Servizi di Sviluppo, Manutenzione e Conduzione Operativa Applicativi e Database (a esclusione della MEV)	Continuativa	A Canone	Mensile	24
3	Servizio di <i>Backoffice</i> e supporto alle Imprese Assicuratrici e Intermediari	Continuativa	A Canone	Mensile	24
4	Servizi di Supporto Specialistico / Presidio <i>on site</i>	Continuativa	A Canone	Mensile	24
5	Servizi di <i>cyber security</i>	Continuativa	A Canone	Mensile	24
6	Servizi Trasversali	Continuativa	A Canone	Mensile	24
7	<i>Phase-in</i> (inclusivi dei costi di setup, migrazione, configurazione agent etc..)	Progettuale	A corpo	Nessuna	1 n/a
	Manutenzione Evolutiva (MEV)	Progettuale	A consumo	(Task GG/PP) (Task GG/PP)	

La Modalità “continuativa” a canone prevede l'erogazione continuativa del servizio per tutta la durata della Fornitura, a decorrere dall'attivazione della stessa, con corrispettivo fisso a fronte della prestazione definita nel presente documento e nel rispetto dei livelli di servizio richiesti.

La Modalità “progettuale” a corpo prevede l'esecuzione delle specifiche attività indicate nel par. 1.3.1 con corrispettivo fisso consuntivabile solo all'esecuzione integrale della prestazione definita nel presente documento e nel rispetto dei livelli di servizio richiesti.

La Modalità “progettuale” a consumo si applica a *task* realizzativi di Manutenzione evolutiva soggetti a specifica valutazione di impegno professionale ed economico, da consuntivarsi a scalare dalla disponibilità budgetaria definita al par. 1.2.

6 QUALITÀ DELLA FORNITURA

6.1 PIANO DELLA QUALITÀ GENERALE

Al fine di assicurare che la Fornitura rispetti i requisiti di qualità il Fornitore dovrà obbligatoriamente predisporre entro 30 giorni lavorativi dalla stipula del Contratto un Piano della Qualità Generale.

Nel Piano della Qualità Generale il Fornitore descriverà il sistema di qualità adottato per garantire la corretta fornitura dei singoli servizi richiesti e l'erogazione degli stessi tramite il Centro Servizi (par. 3.6.1 del presente documento).

Il Piano della Qualità Generale dovrà essere redatto in conformità alle *best practice* in materia, descrivendo le metodologie previste per la gestione per la qualità del progetto e i modelli organizzativi e comunicativi adottati per la realizzazione di tutti i requisiti previsti nel contratto.

Nel Piano si richiede l'indicazione delle responsabilità di gestione per la qualità nell'ambito dell'organizzazione del gruppo di lavoro impegnato sugli adempimenti contrattuali, con specifica definizione, per ciascun ruolo professionale avente responsabilità specifiche per la qualità indicato nell'organigramma, dei compiti, delle responsabilità, dei poteri nell'ambito degli adempimenti descritti nel Piano e delle interazioni con gli altri responsabili.

È richiesto inoltre di specificare il sistema di controlli di qualità previsti per i processi di cui ai servizi oggetto della fornitura (progettazione, realizzazione, assistenza, etc.) e per tutte le risorse impiegate, precisando anche le modalità adottate per la gestione di eventuali irregolarità contrattuali e per la loro risoluzione.

L'IVASS si riserva la facoltà di verificare il Piano della Qualità Generale predisposto dal Fornitore e di richiederne, laddove ritenuto necessario, l'integrazione o modifica.

6.2 INDICATORI DI QUALITÀ E PENALITÀ Gli Indicatori di Qualità validi per l'intera fornitura e le azioni contrattuali previste nel caso di non rispetto dei valori di soglia sono di seguito riportati nella sottostante Tabella.

Alcuni di essi misurano esclusivamente gli aspetti di governo ed esecuzione della fornitura (es. gli Indicatori legati alle risorse impiegate) mentre altri misurano anche aspetti di carattere operativo.

Per la definizione di dettaglio si rinvia all'Appendice 1 allegata al Capitolato Tecnico.

Si precisa che qualora il Fornitore abbia, nella propria Offerta Tecnica, dichiarato il miglioramento dei valori di soglia rispetto a quanto indicato nell'Appendice 1 al Capitolato Tecnico, gli scostamenti al fine dell'applicazione delle penali saranno calcolati rispetto ai valori soglia dichiarati nell'Offerta Tecnica.

Ambito	Indicatore di qualità	Azione contrattuale	
		Rilievo	Penale
	IQ01 – Rispetto di una scadenza temporale		X

Governo della fornitura e servizi professionali	IQ02 – Qualità della documentazione	X	
	IQ03 – Rispetto tempistiche di inserimento/sostituzione di personale		X
	IQ04 – Inadeguatezza del personale proposto	X	
	IQ05 – Turn over del personale	X	
	IQ06 – Numerosità dei rilievi sulla fornitura		X
Centro servizi	IQ07 – Rispetto dell’RTO		X
	IQ08 – Rispetto dell’RPO		X
	IQ09 – Disponibilità dei dati a fine fornitura		X
help Desk	IQ10 – Percentuale di chiamate in ingresso gestite	X	
	IQ11 - Tempo di presa in carico		X
	IQ12 – Tempo di risoluzione		X
	IQ13 – Numerosità richieste riaperte	X	
Qualità di erogazione dei servizi	IQ14 – Tempo di attivazione degli interventi		X
	IQ15 – <i>Uptime</i> dei servizi oggetto di fornitura e degli strumenti a supporto	X	X
	IQ16 – Difettosità in esercizio		X
	IQ17 – Interventi di manutenzione correttiva recidivi		X
Collaudo dei Servizi	IQ18 – Casi di test negativi in collaudo	X	
	IQ19 –Difettosità in collaudo	X	
	IQ20 - Giorni di sospensione del collaudo		X