CAPITOLATO TECNICO E D'ONERI

SECURITY CONSULTANT & COMPLIANCE

GDPR - REGOLAMENTO UE 679/2016

SERVIZIO 2021 -2023

Sommario

1. PREMESSA

La direttiva del 1 agosto 2015 del Presidente del Consiglio dei Ministri, impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici ed individua nell' Agenzia per l'Italia Digitale (AGID) l'organismo che dovrà rendere gli indicatori degli standard di riferimento in linea con quelli già esistenti a livello europeo ed internazionale.

La circolare n. 2 del 18 aprile 2017 dell'AGID indica, infatti, le misure minime per la sicurezza che devono essere adottate per contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi, attraverso regole, standard e guide tecniche in materia di sicurezza informatica.

Le pubbliche amministrazioni devono adeguarsi entro il 31.12.2017, con la predisposizione del Piano per la sicurezza informatica che attuerà gli adempimenti richiesti.

Il Regolamento Generale sulla Protezione dei dati personali (Regolamento UE 679/2016 – General Data Protection Regulation - "GDPR") è un atto con il quale la Commissione europea ha inteso rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all'interno che all'esterno dei confini dell'Unione Europea. Il testo è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, è applicato in via diretta in tutti i Paesi UE. Tale Regolamento si inserisce all'interno di quello che, insieme alla Direttiva 2016/680, è stato definito il "Pacchetto europeo protezione dati".

Le disposizioni contenute nel Regolamento europeo per la protezione dei dati personali impongono alle Pubbliche Amministrazioni di assicurare l'applicazione della normativa europea sul trattamento dei dati, la cui responsabilità ultima cade sul titolare del trattamento, Il D.Lgs. n. 101/2018 adegua l'ordinamento italiano alle disposizioni di cui al predetto regolamento, che ha modificato e integrato le disposizioni di cui al vigente D. Lgs. 30/06/2003 n. 196 – Codice Privacy; l'adozione delle disposizioni di cui al GDPR e l'applicazione del citato Decreto hanno inciso e incidono notevolmente sull'organizzazione interna e richiedono la costante ricognizione, la valutazione e l'adeguamento delle misure di sicurezza normative, organizzative e tecnologiche, già adottate dall'Agenzia a tutela della privacy.

Dal momento che l'adeguamento alle nuove norme deve essere inteso non come mero "adempimento" ma come occasione di riflessione sull'organizzazione dell'Ente e sul livello di sicurezza del trattamento dei dati attualmente in essere, al fine di apportare i correttivi ed i miglioramenti necessari, l'attività da svolgere presuppone l'incrocio di competenze informatiche e giuridiche difficilmente riscontrabili in una sola professionalità.

Merita sicuramente particolare attenzione la figura professionale che va ad affiancarsi a quelle del "titolare", del "responsabile" e dell' "incaricato" del trattamento dei dati. Tale figura è quella del Data Protection Officer ("DPO"), il "responsabile della protezione dei dati", professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati. Il DPO, nominato obbligatoriamente, avrà tra i suoi compiti l'individuazione dei rischi e le misure di tutela che dovranno essere adottate all'interno di tutte le aziende pubbliche, in materia di tutela, trattamento e conservazione dei dati personali cui l'Agenzia dovesse avere disponibilità nelll'ambito delle sue attività d'Istituto. Il DPO rappresenta quindi una figura indipendente di garanzia ed a supporto del "titolare del trattamento dei dati personali" nominato dall'Agenzia.

La figura del DPO riveste un ruolo importante all'interno dell'azienda, in quanto deve avere una elevata professionalità e deve essere in grado di rapportarsi con le figure di vertice dell'Agenzia con un elevato grado di autonomia e indipendenza.

Ecco i suoi principali compiti:

1. informare e consigliare il titolare o il responsabile del trattamento dei dati, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento;
2. verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors;
3. fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
4. fungere da punto di contatto per gli interessati, in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti alla tutela;
5. fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

1.1 Scopo del Capitolato

Il presente Capitolato descrive gli aspetti tecnici relativi alla fornitura di Security & Compliance Consulting Services allo scopo di:

A. consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della Pubblica Amministrazione, con riferimento a quanto previsto dalla Direttiva del Presidente del Consiglio dei Ministri del 1 agosto 2015 in materia di Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni;
B. adeguarsi ai termini ed alle scadenze imposte dal Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, alla libera circolazione di tali dati, in abrogazione alla Direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
C. nominare il Data Protection Officer (DPO).
D. L'Agenzia Regionale per la Protezione dell'Ambiente ha inteso organizzare la presente iniziativa di acquisizione di un servizio al fine di rispondere in modo efficiente e flessibile alle esigenze sopra riportate, considerando sia gli aspetti tecnologici che di implementazione.

Tutte le prescrizioni contenute nel presente Capitolato tecnico rappresentano requisiti minimi della Fornitura.

1.2 Definizioni e abbreviazioni

Salva diversa esplicita indicazione, ai termini seguenti viene attribuito, ai fini del presente documento, il significato di seguito indicato:

- **Capitolato tecnico**: indica il presente documento;
- **Committente/Amministrazione**: Agenzia Regionale per la Protezione dell'Ambiente del Friuli Venezia Giulia – ARPA FVG
- **Data di Attivazione**: primo giorno lavorativo utile, successivo alla data di approvazione del Piano di Lavoro, da parte della Amministrazione;
- **Servizio**: indica, nel suo complesso, l'erogazione dei servizi oggetto del presente Capitolato tecnico;
- **Fornitore/Impresa/Società**: indica l'aggiudicatario del Servizio;
- **Piano Operativo**: indica il documento di pianificazione dei Servizi Continuativi;
- **Proposta Tecnico Operativa (PTO)**: indica il documento di pianificazione dei Servizi iniziali;
- **Resoconto Attività**: indica il documento di consuntivazione delle attività oggetto del Servizio.

1.3 Acronimi

- **GP**: Giorno/i Persona;
- **SAL**: definizione dello stato avanzamento del Servizio
- **DPCM**: Direttiva del Presidente del Consiglio 1° agosto 2015;
- **GDPR**: Regolamento UE 2016 679.

2. DEFINIZIONE DEI SERVIZI OGGETTO DEL PRESENTE CAPITOLATO

2.1 Oggetto del Servizio

L'oggetto del Servizio è rappresentato dal complesso dei servizi comunemente definiti di *Security & Compliance Consulting* descritti nel Capitolo 3 del presente Capitolato tecnico e dalle attività ad essi associate volte a garantire la sicurezza minima delle infrastrutture e dei dati di ARPA FVG, a rispondere in maniera efficace in caso di attacchi informatici, a mantenere la perfetta efficienza delle infrastrutture di sicurezza ICT, nonché a fornire, alla Amministrazione, il supporto necessario per assicurare il costante allineamento con l'evoluzione normativa e tecnologica del mercato ICT security e a definirne la crescita, in coerenza con gli obiettivi strategici, secondo la seguente articolazione:

Security & Compliance Consulting Services	
Servizi Iniziali	Servizi Continuativi
Gap Analysis	Compliance Maintenance
Remediation Consulting	Security & Compliance Audit
	Security System Support

Per l'erogazione dei servizi oggetto del presente Capitolato tecnico, l'Impresa dovrà definire le seguenti figure professionali che potranno essere ricoperte anche dalla stessa persona:

- **Responsabile del contratto**, il quale ha la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del contratto (es. fatturazione, verifica del rispetto dei livelli di servizio, definizione e aggiornamento del team di cui al paragrafo 3.5); nonché la richiesta di attivazione di nuovi Servizi, tra quelli definiti;
- **Responsabile tecnico** per l'erogazione dei servizi, avente la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente Capitolato tecnico e di essere il punto di riferimento tecnico per la gestione dei Servizi, tra quelli definiti. Il Responsabile tecnico dovrà inoltre coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL di progetto;
- **Data Protection Officer**: per verificare l'attuazione, l'applicazione e la progettazione di nuovi sistemi/servizi IT in conformità alla normativa europea.

I SAL, che potranno essere sviluppati di concerto con il Direttore dell'esecuzione del contratto, definito come da art. 111 del d.lgs 50/2016 e s.m.i., sotto forma di relazioni, report o riunioni operative, da tenere con le prime due figure a cadenza mensile e/o su esplicita richiesta dell'Amministrazione, dovranno riguardare almeno i seguenti argomenti:

- dettaglio delle attività svolte e di quelle ancora da svolgere;
- eventuali problematiche insorte e soluzioni attuate/proposte;
- questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione dell'Amministrazione;
- avanzamento economico dell'appalto.

A fronte di eventuali problematiche che dovessero presentarsi, il SAL dovrà comprendere anche le relative proposte di risoluzione e la relativa ripianificazione delle attività impattate.

Il Responsabile tecnico del servizio, durante i SAL mensili, dovrà presentare alla Amministrazione il "Resoconto Attività", contenente lo stato delle fasi in lavorazione. Tali informazioni e dati saranno successivamente vagliati dal Direttore dell'esecuzione del contratto in sede di verifica di conformità.

L'Impresa, al momento della stipula, dovrà comunicare all'Amministrazione il numero di recapito telefonico e l'indirizzo e-mail attraverso i quali contattare le suddette figure professionali.

Per le attività svolte dalle figure di Responsabile del contratto, di Responsabile tecnico e di Data Protection Officer, non sarà riconosciuto alcun corrispettivo economico aggiuntivo, ritenendosi gli stessi ricompresi nell'offerta economica presentata.

2.2 Sedi di erogazione delle prestazioni

Le prestazioni oggetto del presente Capitolato dovranno essere erogate, a seconda delle esigenze specifiche di progetto, presso:

- le sedi dell'Amministrazione di Udine, Trieste, Gorizia, Pordenone, e la sede centrale di Palmanova;
- altre sedi che verranno eventualmente indicate in fase di esecuzione;
- la sede dell'Impresa.

2.3 Durata del contratto

La durata massima del contratto è fissata in 36 mesi decorrenti dalla Data di Attivazione di cui al par. 4.3 del presente Capitolato.

3. DESCRIZIONE DEL SERVIZIO

3.1 Security & Compliance Consulting

Di seguito è fornita una descrizione di massima del contesto tecnologico e delle caratteristiche tecniche dei servizi richiesti, relativi al Security & Compliance Consulting, che saranno organizzati in due aree principali:

- Servizi Iniziali: ossia tutti i servizi di supporto ad alto valore aggiunto che saranno attivati nelle tempistiche di esecuzione concordate per dare avvio, compiutezza ed efficacia al Servizio in appalto;
- Servizi Continuativi: ossia tutti i servizi che richiedono una continuità operativa presso le sedi della Amministrazione, al fine di offrire un servizio di presidio e supporto dedicato a specifici ambiti della sicurezza, del rispetto delle norme di buona tecnica e per garantire la conformità alle norme di settore tempo per tempo applicabili.

Il Fornitore prende atto che, nel corso dell'erogazione dei servizi, a fronte delle evoluzioni in ambito ICT, l'introduzione di nuove tecnologie potrà comportare significative variazioni del contesto tecnologico di inizio Fornitura e si impegna ad erogare i servizi richiesti adeguando le conoscenze del personale impiegato nell'erogazione degli stessi o inserendo nei gruppi di lavoro risorse con adeguate conoscenze e competenze, senza alcun onere aggiuntivo per l'Amministrazione.

Tutti gli eventuali strumenti utilizzati a supporto dell'erogazione dei servizi descritti nel presente Capitolato saranno a totale onere dell'Impresa.

3.2 Servizi Iniziali

Nell'ambito dell'insieme di attività che definiscono il servizio di Security & Compliance Consulting, relativamente alle aree di intervento che saranno di seguito illustrate.

3.3 Analisi stato attuale (AS IS)

Attività mirata a supportare l'Amministrazione nella valutazione e verifica dell'attuale stato di implementazione dei propri sistemi ed applicazioni con le normative esistenti in ambito di interesse e cogenza, il loro grado di efficacia e rispondenza rispetto agli obiettivi istituzionali, e la predisposizione di un piano di applicazione orientato al miglioramento continuo e alla copertura di eventuali problematiche o ambiti non ancora indirizzati.

In particolare il servizio sarà orientato a supportare l'Amministrazione sui seguenti ambiti:

- Descrizione del livello di conformità rispetto a quanto previsto dalla DPCM 1 agosto 2015 in tema di Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni;
- Descrizione del livello di conformità rispetto a quanto previsto dal Regolamento UE 2016 679 (GDPR).

Il servizio sarà erogato secondo le indicazioni riportate nel paragrafo 4.2.

3.4 Azioni correttive (TO BE)

Attività relativa al supporto specialistico per la definizione di possibili azioni da svolgere e strategie da mettere in atto al fine di consentire una efficace e adeguata copertura degli elementi di criticità e disallineamento emersi e riconosciuti nel corso del processo di Analisi AS IS.

Il servizio specifico si articola nelle seguenti sotto-attività:

1. adeguamento dei punti di criticità emersi, mediante identificazione e definizione di soluzioni e *best practice* per l'innalzamento della sicurezza applicativa, in aderenza a quanto richiesto e previsto dalle normative d'interesse cogente applicabili (DPCM 1 ago 2015 e GDPR);
2. individuazione e definizione del livello di esposizione in termini di sicurezza derivante dall'adozione di nuovi servizi, nuove tecnologie o modifiche infrastrutturali ed applicative (architetture, codice sorgente, applicativi commerciali, open source o in riuso) in funzione dei vincoli presenti, delle *best practice* di gestione della sicurezza e dei rischi intrinsechi derivanti dall'adozione stessa;
3. definizione di piani operativi per l'implementazione delle azioni identificate e stabilite come attuabili, sulla base di criteri di priorità e complessità stabiliti in accordo con l'Amministrazione;
4. redazione di nuove politiche e linee guida di sicurezza, laddove l'Amministrazione ne riscontri la mancanza, o di adeguamento delle politiche e procedure esistenti, rispetto ai cambiamenti infrastrutturali e organizzativi intrapresi;
5. individuazione e definizione del livello di esposizione, e delle relative misure di mitigazione, derivante dalle architetture dei propri software sviluppati ed in fase di sviluppo in funzione dei vincoli presenti, delle *best practice* di sviluppo (privacy by design) e dei rischi intrinsechi derivanti dall'adozione degli stessi.

Il servizio sarà erogato secondo le indicazioni riportate nel paragrafo 4.2.

3.5 Servizi Continuativi

I servizi continuativi sono costituiti da interventi specifici che, per loro natura, hanno la caratteristica di essere appunto continuativi nel tempo e mirati alla gestione di specifici percorsi e compiti direttamente presso le sedi dall'Amministrazione.

I suddetti servizi saranno attivati secondo le modalità indicate nel successivo par. 4.3.

3.5.1 Compliance Maintenance Support

Il servizio prevede un'attività di supporto per la gestione del mantenimento dello stato di conformità raggiunto dai sistemi dell'Amministrazione, al fine di supervisionare la garanzia nel tempo dello stato di adeguatezza di quanto implementato, rispetto alla dimensione normativo-cogente richiesta.

Il servizio di mantenimento riguarda in particolare le seguenti attività:

1. partecipazione ai gruppi di lavoro interni all'Amministrazione a intervalli prefissati e con cadenza programmata, in relazione alle necessarie attività da supervisionare, verificare e validare;
2. gestione delle iniziative sui processi di sicurezza in funzione delle precedenti analisi e implementazione;
3. servizio di supporto al settore ICT per la definizione e mantenimento dell'elenco dei software applicativi adottati e/o utilizzati sui sistemi in dotazione all'Agenzia;

Il servizio sarà erogato secondo le indicazioni riportate nel paragrafo 4.3.

3.5.2 Security & Compliance Audit Security & Compliance Audit

Nell'ambito del presente servizio è prevista la gestione delle campagne di audit di sicurezza e conformità rispetto alle normative vigenti o agli standard interni definiti per lo specifico ambito sotto analisi. Nell'ambito del presente servizio è previsto, inoltre, anche lo svolgimento dei compiti del Data Protection Officer come previsto dal regolamento in oggetto alla presente iniziativa.

Le attività da svolgere sono le seguenti:

1. analisi delle attività degli Amministratori di Sistema, in conformità al Provvedimento del Garante per la Privacy/GDPR;
2. valutazione dell'effettiva attuazione delle policy, delle linee guida e degli standard di sicurezza definiti dalle normative di settore vigenti e applicabili ;
3. verifica della conformità delle configurazioni dei sistemi, postazioni di lavoro, ecc. in esercizio alle normative, alle best practice e agli standard di riferimento;
4. validazione della rispondenza dei contratti in essere rispetto ai vincoli delle normative vigenti applicabili (Direttiva del Presidente del Consiglio 1° agosto 2015, GDPR).
5. valutazione del grado di consapevolezza del personale interno rispetto a specifiche problematiche di sicurezza o al recepimento di determinate normative interne;
6. rilevazione dello stato attuale della Gestione della Sicurezza delle informazioni rispetto agli standard ISO/IEC 27001 e alle linee guida ISO inerenti la gestione del rischio e i controlli di sicurezza.

Il servizio sarà erogato secondo le indicazioni riportate nel paragrafo 4.3

3.5.3 Security System Support

Nell'ambito del presente servizio è previsto il supporto tecnico alla divisione tecnica dell'amministrazione atta al mantenimento degli adeguati livelli di sicurezza dell'infrastruttura di rete e di sistema (Server e Storage) prevista rispetto alle normative vigenti o agli standard interni definiti per lo specifico ambito sotto analisi. Inoltre è previsto un supporto atto a mettere in essere tecniche e tecnologie per incrementare ed adeguare il livello di sicurezza dell'infrastruttura IT alle nuove minacce di sicurezza date dall'evoluzione tecnologica

Le attività da svolgere sono le seguenti:

1. Rilevazione dello stato attuale del livello di esposizione al rischio dell'infrastruttura IT mediante attività di Vulnerability Assessment sul perimetro esterno della rete e sulla rete interna secondo standard di settore e linee guida (NIS, AgID)
2. Stesura di un Report operativo a seguito del punto 1
3. Pianificatone e supporto sistemistico da parte di tecnici senior in ambienti eterogenei (Windows e Linux) in particolare per il supporto all'attuazione e messa in opera delle misure previste dalle norme di riferimento (Provvedimento del Garante per la Privacy/GDPR, Misure minime AgID) e del report di del punto 2.
4. verifica della conformità delle configurazioni dei sistemi, postazioni di lavoro, ecc. alle normative, alle best practice e agli standard di riferimento;
5. Predisposizione di un piano di adeguamento, ove ritenuto necessario, che individui gli investimenti e le risorse necessarie per dare attuazione alle misure riportate nel Report operativo di cui al precedente punto 2.

Il servizio sarà erogato secondo le indicazioni riportate nel paragrafo 4.3

3.6 Orario di servizio

L'orario dei servizi di Security & Compliance Consulting è riportato nel seguito:

A. i Servizi Iniziali sono svolti nei giorni feriali dal lunedì al venerdì, indicativamente tra le 09.00 e le 18.00, fatte salve eventuali eccezioni concordate in anticipo con il Fornitore per permettere lo svolgimento degli stessi anche in fasce orarie/giorni differenti;
B. i Servizi Continuativi, sono svolti nei giorni feriali dal lunedì al venerdì indicativamente dalle 09.00 alle 18.00.

3.7 Gruppo di lavoro e Profili professionali richiesti

L'Impresa, per formare il team che si occuperà delle attività previste per il Security Consulting Services, dovrà avvalersi di personale specializzato nelle varie aree d'intervento descritte nei paragrafi precedenti e in possesso di competenze specifiche nonché di certificazioni funzionali al ruolo di riferimento.

Le risorse che verranno proposte dal fornitore dovranno avere diversi profili ciascuno con una propria certificazione a seconda del ruolo assunto nel progetto:

- certificazione ITIL Foundation e qualifica di Lead Auditor ISO 27001 (profilo: tecnico per la gestione della sicurezza)
- certificazione CISA (Certified Information System Auditor)
- certificazione Eucip CORE (profilo: programmatore)

Le qualifiche richieste nella documentazione di gara devono essere state rilasciate da un ente certificatore o da un'impresa di formazione accreditata.

Le risorse in possesso delle certificazioni specificate dovranno essere rese disponibili per l'intera efficacia del contratto e dovranno essere impiegate nei team di lavoro che garantiscono l'erogazione dei servizi oggetto della fornitura anche senza espressa richiesta dell'Amministrazione.

Il Fornitore sarà tenuto a garantire la disponibilità effettiva degli specialisti componenti il team di lavoro, rispettando la richiesta delle certificazioni sopra descritte, fatta salva la possibilità per l'Amministrazione di richiederne la sostituzione delle risorse se ritenute non idonee e compatibili con l'ambiente di lavoro.

4. MODALITÀ DI ESECUZIONE DEL SERVIZIO

4.1 Modalità di esecuzione dei servizi e delle attività

Al fine di descrivere l'esecuzione della Fornitura, nell'ambito del Security & Compliance Consulting, si richiama la descrizione del servizio nel cap.3.1.

Si sottolinea che, a prescindere dall'organizzazione adottata dal Fornitore per l'erogazione dei diversi servizi, è richiesto un alto grado di sinergia delle risorse messe a disposizione dal Fornitore operanti presso le sedi di ARPA FVG, al fine di garantire un adeguato grado di omogeneità nelle varie soluzioni adottate e uniformità di comportamento nei confronti degli utenti.

L'erogazione dei servizi deve comunque prevedere un alto grado di responsabilizzazione delle risorse del Fornitore, attitudine a lavorare per obiettivi, capacità di operare in team e rispetto delle scadenze pianificate.

4.2 Modalità di esecuzione dei servizi Iniziali

I servizi di Security & Compliance Consulting, di cui al paragrafo 3.2 e 3.3, dovranno essere definiti, concordati e attivati a fronte di una pianificazione specifica da parte del Direttore dell'esecuzione del contratto nominato dall'Amministrazione e concordata con il titolare del trattamento dei dati personali che verrà trasmessa al Responsabile del Contratto del Fornitore, attraverso un incontro programmatorio in cui verranno definite le seguenti informazioni di riferimento:

- data prevista di inizio attività;
- data prevista di fine attività;
- eventuali date vincolo (ad esempio legate a date di esercizio);
- tipologia di servizio richiesto;
- obiettivi e ambito di intervento;
- eventuali riferimenti a documentazione esistente;
- risultati attesi;
- modalità operativa di intervento (on-site, soggetti interni ed esterni da coinvolgere e modalità di interazione con gli stessi, frequenza di aggiornamento dei SAL, ecc.);

In esito all'incontro programmatorio il Responsabile Tecnico del Fornitore predispone una Proposta Tecnica Operativa (PTO) entro un termine congruo stabilito nel corso dell'incontro stesso;

La Proposta Tecnica Operativa (PTO) riporterà almeno i seguenti elementi:

- data prevista di inizio attività;
- data prevista di fine attività;
- il dettaglio delle attività che verranno erogate;
- possibili metodologie applicabili al contesto e la modalità di esecuzione delle attività;
- eventuali bozze e schemi rappresentativi delle attività che possono essere messi a disposizione dell'Amministrazione prima della accettazione formale della PTO;
- la lista completa delle esigenze ed obiettivi dell'Amministrazione intesi anche in termini di documentazione rilasciata, report o verbali di consegna, o altri elementi che certifichino l'andamento delle attività ed il raggiungimento degli obiettivi;
- le risorse coinvolte: in particolare è prevista la presentazione di un team di lavoro che il Fornitore dovrà impiegare nelle varie aree di servizio richieste;
- il piano di lavoro dell'intero periodo di attività sotto forma di diagramma di GANTT delle attività, evidenziando i vari ambiti e obiettivi di progetto suddivisi per contesti operativi (work packages).

A fronte di una PTO l'Amministrazione potrà chiedere eventuali delucidazioni sulla modalità operativa di svolgimento e sui deliverable proposti al Responsabile del Contratto e/o al Responsabile Tecnico, richiedendo eventualmente la rivisitazione dell'intervento o l'attivazione solo di specifici work package o servizi all'interno dello stesso. A fronte dell'eventuale richiesta di rivisitazione/modifica, il Fornitore dovrà riproporre la PTO aggiornata entro 3 giorni lavorativi, dalla data di richiesta dell'Amministrazione.

Nell'ambito della presentazione della PTO, il Fornitore dovrà descrivere anche il modello organizzativo che sarà adottato per garantire in maniera efficace ed efficiente sia il processo di attivazione delle richieste di intervento, sia l'esecuzione degli interventi stessi ponendo attenzione alla modalità di costituzione del/i gruppo/i di lavoro, le modalità di coordinamento degli stessi e il modello di pianificazione, controllo e comunicazione verso l'Amministrazione, sullo stato di avanzamento dei vari interventi.

L'Amministrazione potrà chiedere anche più interventi su ambiti diversi all'interno della stessa richiesta, in tal caso la PTO dovrà includere tutti gli interventi differenziati per aree di intervento/tipologia, riportando per ciascuno di essi le informazioni precedentemente illustrate.

Ai fini della verifica della congruità del corrispettivo proposto dall'operatore economico in sede di offerta il dimensionamento di ciascun intervento è effettuato in giorni persona per ciascuna figura professionale prevista e costituisce un riferimento fisso.

Tutte le attività preliminari e/o precedenti alla accettazione della PTO restano interamente a carico del Fornitore.

Una volta accettata formalmente la PTO di riferimento da parte dell'Amministrazione, l'Impresa dovrà attivare il servizio entro la data prevista nella PTO e garantire la pianificazione proposta, incluso il rilascio dei deliverable concordati e la rispondenza degli stessi agli obiettivi dell'intervento. Su questi ultimi parametri saranno misurati i livelli di produttività del Servizio e applicate le penali di riferimento in caso di mancato rispetto delle pianificazioni o non coerenza e non completezza dei deliverable rispetto agli obiettivi iniziali.

4.3 Modalità di esecuzione dei servizi continuativi

I servizi di carattere continuativo, di cui al paragrafo 3.5, dovranno essere definiti, concordati e attivati a partire dalla Data stipula del contratto di servizio. L'attività verrà concordata tra il Direttore dell'esecuzione del contratto nominato dall'Amministrazione e il Responsabile del Contratto del Fornitore, attraverso un incontro programmatorio in cui verranno definite le modalità operative e di controllo delle attività definite al paragrafo 3.5. L'appaltatore entro un termine congruo stabilito nel corso dell'incontro programmatorio presenterà un programma operativo dove descriverà in maniera sintetica gli approcci metodologici e di dettaglio volti al raggiungimento degli obiettivi di cui al par. 3.5. Il documento, per ogni obiettivo, dovrà riportare una scheda dettagliata con le indicazioni dei riferimenti degli incaricati delle singole attività, il calendario degli interventi previsti e i tempi di risposta alle eventuali richieste del Direttore dell'esecuzione del contratto in relazione agli obblighi imposti dalle normative di riferimento. Nel medesimo documento dovranno essere riportate le generalità e referenze professionali del DPO incaricato ai fini della formalizzazione della nomina da parte dell'Agenzia.

Le attività oggetto di servizio continuativo da ricomprendere nel Piano Operativo sono:

- Compliance Maintenance Support - gestione del mantenimento dello stato di adeguatezza dei sistemi dell'Amministrazione
- Security & Compliance Audit Security & Compliance Audit – attività relativa e connessa al titolare DPO
- Security System Support – Supporto a ICT nel contesto della vulnerabilità e sicurezza dei sistemi

4.4 Trasferimento del know-how

Negli ultimi due mesi solari di validità del contratto, o nel caso di cessazione anticipata del rapporto contrattuale, il Fornitore, dovrà fornire al personale dell'Amministrazione il trasferimento del know- how sulle attività condotte, al fine di rendere l'eventuale prosecuzione delle attività quanto più efficace possibile.

Pertanto, il Fornitore si impegna:

- a trasferire il know how necessario, nonché l'eventuale supporto operativo;
- alla restituzione nella disponibilità dell'Amministrazione degli eventuali strumenti e/o attrezzature resi disponibili dall'Amministrazione per lo svolgimento dei Servizi;
- a facilitare la presa in carico da parte del Fornitore subentrante anche attraverso la disponibilità ad eseguire attività operative di affiancamento al pari del personale dell'Amministrazione.

Al termine delle attività contrattuali, la documentazione prodotta/modificata nell'ambito dell'appalto sarà consegnata alla Committente secondo le modalità che saranno concordate. Tale periodo di affiancamento è organizzato secondo le modalità concordate con l'Amministrazione.

Le attività di trasferimento del know how si intendono ricomprese nel corrispettivo dei servizi.

5. INDICATORI DI QUALITÀ

Di seguito viene descritto un insieme minimo di requisiti di qualità della Fornitura e delle relative modalità di verifica e controllo. Il Fornitore è tenuto, per l'intera durata dei servizi, a rendicontare gli indicatori di qualità (IQ).

Si precisa che:

1. per periodo di riferimento si intende l'arco di tempo entro il quale sono rilevate le grandezze necessarie per la determinazione dei requisiti di qualità. È specificato per ogni indicatore di qualità (IQx);
2. per ore e giorni si intendono ore lavorative e giorni lavorativi;
3. per mese, trimestre, semestre, si indica il mese, il trimestre, il semestre di calendario nell'ambito della durata contrattuale.

Si precisa che agli Indicatori di Qualità sono, di volta in volta, associate azioni contrattuali quali l'applicazione di penali.

5.1 IQ1: sostituzione del responsabile tecnico della fornitura

Aspetto da valutare	Sostituzione del Responsabile tecnico della Fornitura operata su iniziativa dell'Impresa e non a fronte di richiesta dell'ARPA FVG.
Unità di misura	Responsabili sostituiti
Fonte dati	Lettera di sostituzione del Responsabile tecnico della Fornitura da parte del Fornitore
Periodo di osservazione	Semestre precedente la rilevazione
Frequenza di misurazione	Semestrale
Dati da rilevare	Sostituzione permanente del Responsabile tecnico della Fornitura non richiesta da ARPA FVG(Nsostituzioni)
Regole di campionamento	Vanno considerate le sostituzioni non richieste dall'ARPA FVG che riguardano il Responsabile tecnico della Fornitura.
Formula	IQ1= NSostituzioni
Regole di arrotondamento	Nessuna

Valore di soglia	IQ1 = 0
Azioni contrattuali	Applicazione delle penali come indicato al paragrafo 6

5.2 IQ2: personale della fornitura inadeguato

Aspetto da valutare	Personale della Fornitura inadeguato
Unità di misura	Richiesta di sostituzione
Fonte dati	E-mail, lettere, verbali
Periodo di riferimento	Semestre precedente la rilevazione
Frequenza di misurazione	Semestre
Dati elementari da rilevare	Numero di sostituzioni, richieste formalmente da ARPA FVG, del personale della Fornitura (N_Sostit_rich).
Regole di campionamento	Vanno considerate le sostituzioni richieste da ARPA FVG che riguardano il personale della Fornitura nel periodo di riferimento.
Formula	IQ2 = N_Sostit_rich
Regole di arrotondamento	Nessuna
Valore di soglia	IQ2 <= 2
Azioni contrattuali	Applicazione delle penali come indicato al paragrafo 6

5.3 IQ3: turn over del personale

Aspetto da valutare	Turn over del personale: numero di risorse sostituite su iniziativa del Fornitore nel periodo di riferimento.
Unità di misura	Risorsa sostituita
Fonte dati	E-mail, lettere, verbali
Periodo di riferimento	Semestre precedente la rilevazione
Frequenza di misurazione	Semestrale
Dati elementari da rilevare	Numero di sostituzioni effettuate su iniziativa del Fornitore nel periodo di riferimento (N_Sostit).
Regole di campionamento	Nessuna
Formula	IQ3 = N_Sostit
Regole di arrotondamento	Nessuna
Valore di soglia	IQ3 <= 3
Azioni contrattuali	Applicazione delle penali come indicato al paragrafo 6

5.4 IQ4: slittamento di una scadenza contrattuale

Aspetto da valutare	Il rispetto di ciascuna scadenza (inserimento/sostituzione risorse, di un deliverable, attivazione di un servizio/ fine attività di un servizio, ecc.) stabilita dal contratto e/o dal Piano di Lavoro e/o dalla PTO e/o di carattere trasversale ai servizi.
Unità di misura	Giorno lavorativo
Fonte dati	E-mail, fax, verbali
Periodo di riferimento	Evento
Frequenza di misurazione	Giornalmente
Dati elementari da rilevare	Data prevista (data_prev); Data effettiva (data_eff).
Regole di campionamento	Nessuna
Formula	IQ4 = data_eff- data_prev

Regole di arrotondamento	Nessuna
Valore di soglia	IQ4 = 0
Azioni contrattuali	Applicazione delle penali come indicato al paragrafo 6

6. PENALI

Lo scopo delle penali è quello di riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dall'Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate a regola d'arte.

Le penali da adottare sono individuate contrattualmente e sono organizzate in modo progressivo in relazione alla gravità o al ripetersi della mancata soddisfazione degli adempimenti richiesti.

Le penali applicate saranno le seguenti:

- IQ1: € 500 ogni sostituzione oltre il valore soglia per ciascuna figura sostituita.
- IQ2: € 250 ogni sostituzione richiesta da ARPA oltre il valore soglia. Alla quinta richiesta di sostituzione la penale sarà elevata a € 500.
- IQ3: € 250 ogni sostituzione disposta dal fornitore oltre il valore soglia. Alla quinta richiesta di sostituzione la penale sarà elevata a € 500.
- IQ4: € 100 ogni giornata di slittamento della scadenza concordata a decorrere dal giorno successivo alla scadenza. Dopo i primi 5 giorni lavorativi la penale viene elevata a € 300 al giorno per tutte le giornate di inadempienza (a decorrere dal giorno successivo alla scadenza).

In accordo con le previsioni di cui all'art. 113bis Del d.lgs 50/2016 il superamento dell'importo per penali superiore al 10% del valore del contratto d'appalto costituisce grave inadempimento e può comportare la risoluzione del contratto in danno dell'appaltatore-

7. CORRISPETTIVO DELL'APPALTO E TERMINI DI PAGAMENTO

L'appalto della durata complessiva di 3 anni (tre anni) è quantificato a corpo a fronte di un corrispettivo quantificato in relazione alla complessità e all'articolazione del Servizio nonché alla richiesta di specifiche professionalità in complessivi € 125.000,00 (centoventicinquemila euro) a base di gara comprensivi di ogni altro onere e spese per rendere il servizio a regola d'arte, escluso IVA.

Il corrispettivo dell'appalto, come desunto dall'offerta presentata in sede di gara, costituisce importo fisso e non negoziabile se non nei termini previsti dall'art. 106 del d.lgs 50/2016.

corrispettivo dell'appalto a base di gara	A	€ 125.000,00
incentivo per le funzioni tecniche 2% di A	B	€ 2.500,00
IVA 22% di A	C	€ 27.500,00
totale stanziamento A+B+C	D	€ 155.000,00

totale stanziamento 2021	€ 68.850,00
totale stanziamento 2022	€ 49.450,00
totale stanziamento 2023	€ 36.700,00

Il pagamento avverrà entro 30 giorni dalla presentazione della fattura a cadenza trimestrale a maturazione del corrispettivo una volta riscontrata la regolarità del servizio reso da parte del DEC.