



<p>REGIONE DEL VENETO</p>  <p>ULSS7 PEDEMONTANA</p>	<p>Regione del Veneto</p> <p>AZIENDA SANITARIA U.L.S.S. N. 7 PEDEMONTANA</p> <p>Via dei Lotti, 40 - 36061 Bassano del Grappa (VI) - Tel. 0424 888111 Cod. Fisc./P.IVA 00913430245 - www.aulss7.veneto.it Pec: protocollo.aulss7@pecveneto.it</p>	 <p>Finanziato dall'Unione europea NextGenerationEU</p>
---	--	--

ALLEGATO 3

CAPITOLATO TECNICO

DI APPALTO SPECIFICO

AFFIDAMENTO DI “FORNITURA DI APPARATI E SERVIZI PER LA CYBERSECURITY” MEDIANTE APPALTO SPECIFICO NELL’AMBITO DELL’ACCORDO QUADRO STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

ID 2174 – Lotto Unico



Indice

1	APPALTO SPECIFICO “FORNITURA DI APPARATI E SERVIZI PER LA CYBERSECURITY”	3
1.1	Definizioni	3
2	CONTESTO DELL’APPALTO SPECIFICO E ELEMENTI TRASVERSALI AI VARI SERVIZI	4
2.1	Contesto organizzativo, tecnologico e normativo	4
3	OGGETTO, DURATA DELL’APPALTO SPECIFICO E LUOGO DI ESECUZIONE	5
3.1	Oggetto della fornitura	6
3.2	Durata del contratto	6
3.3	Luogo di esecuzione ed orario di erogazione dei servizi	6
4	DESCRIZIONE DELLA FORNITURA	7
4.1	Garanzia	7
4.2	Prodotti	7
4.2.1	SIEM	7
4.2.2	PAM	8
4.2.3	WAF	9
4.3	Servizi	9
4.3.1	SERVIZIO BASE - Manutenzione	9
4.3.2	SERVIZIO BASE - Supporto Specialistico	10
4.3.3	SERVIZI AGGIUNTIVI - Incident Response	10
5	ULTERIORI REQUISITI DI AS	11
6	LIVELLI DI SERVIZIO E PENALI	11
7	PIANO OPERATIVO DELL’AS	12



1 Appalto specifico “FORNITURA DI APPARATI E SERVIZI PER LA CYBERSECURITY”

Il presente Appalto Specifico rientra nell’ambito dell’Accordo Quadro STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

Per tutto quanto non espressamente indicato nel Capitolato Tecnico di Appalto Specifico, dovrà farsi riferimento alle previsioni del Capitolato Tecnico di Accordo Quadro (Generale e Speciale) per le parti di pertinenza, che devono intendersi quindi obbligatorie e vincolanti.

In particolare i requisiti minimi del presente documento sono aggiuntivi ai requisiti minimi espressi in Accordo Quadro così come l’offerta migliorativa di Appalto Specifico deve essere aggiuntiva dell’offerta migliorativa di Accordo Quadro.

1.1 Definizioni

Nel corpo del presente Capitolato Tecnico, con il termine:

- **AQ** si intende l’Accordo Quadro stipulato da Consip;
- **AS** si intende il presente Appalto Specifico;
- **Amministrazione/Amministrazione Contraente**, si intende nel complesso le strutture organizzative facenti capo a ULSS7 Pedemontana
- **Punto Ordinante o, brevemente, PO** l’Amministrazione richiedente l’AS sul sistema di E-Procurement di Consip;
- **CTAQ** si intende il Capitolato Tecnico Speciale dell’Accordo Quadro;
- **OEAQ** si intende l’offerta economica vincolante del Fornitore Aggiudicatario per l’AQ;
- **OTAQ** si intende l’offerta tecnica vincolante del Fornitore Aggiudicatario per l’AQ;
- **OTAS** si intende l’offerta tecnica vincolante del Fornitore aggiudicatario dell’AS, che integra e migliora l’OTAQ;
- **CTGAQ** si intende il Capitolato Tecnico Generale dell’Accordo Quadro
- **CdO** si intende il Capitolato d’oneri dell’Accordo Quadro
- **Concorrente o Offerente**: il RTI che partecipa alla presente gara;
- **Contratto Esecutivo**: il contratto stipulato dall’Amministrazione con il Fornitore, che si perfeziona dopo l’aggiudicazione dell’Appalto Specifico;
- **CV**: centri di valutazione del Ministero dell’interno e del Ministero della difesa;
- **CVCN**: Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l’Agenzia per la cybersicurezza nazionale;
- **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;
- **Meta-prodotto**: rappresenta l’offerta di riferimento per ogni prodotto richiesto in prima fase. Ogni meta-prodotto è caratterizzato dalla sua descrizione funzionale, da requisiti minimi, dai requisiti migliorativi offerti in prima fase e da un prezzo di riferimento che non potrà essere superato in AS, **ma non da una specifica tecnologia** (marca, modello, release firmware/software);



- **Prodotto:** rappresenta uno specifico prodotto (marca, modello, release firmware/software) offerto in seconda fase come istanza del meta-prodotto offerto in prima fase. Lo specifico prodotto offerto avrà quindi descrizione funzionale, requisiti minimi, requisiti migliorativi del corrispondente meta-prodotto offerto in prima fase ed eventuali ulteriori requisiti migliorativi offerti in base alle richieste dell'Amministrazione Contraente. Il prezzo del prodotto non potrà superare quello del corrispondente meta-prodotto a meno di quanto espressamente previsto nel Capitolato d'Oneri;
- **Portale della fornitura:** il Portale implementato dal Fornitore aggiudicatario secondo le specifiche tecniche descritte nel Capitolato Tecnico parte Generale al paragrafo 4.1
- **Servizi Base:** i servizi, a condizioni non tutte definite, che possono essere richiesti dalle Amministrazioni a completamento della fornitura richiesta in AS, ad eccezione dei servizi inclusi nella fornitura che dovranno essere obbligatoriamente erogati;
- **Servizi Aggiuntivi:** i servizi, a condizioni da definire da parte delle Amministrazioni, che possono essere richiesti a completamento della fornitura prevista in AS. L'Amministrazione potrà valorizzare i servizi accessori secondo le regole riportate nel Capitolato d'Oneri;
- **Sistema telematico (o semplicemente "Sistema"):** indica la piattaforma telematica attraverso cui saranno gestiti gli Appalti Specifici;
- **Responsabile dell'Amministrazione:** la persona indicata dall'Amministrazione nel contratto esecutivo e individuata come interlocutore tecnico con il Fornitore per tutte le attività contrattuali.
- **Responsabile del Fornitore:** la persona indicata dal Fornitore, nell'ambito di ciascun contratto esecutivo, come referente operativo per le attività di fornitura ed erogazione dei relativi servizi connessi, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.2 del Capitolato Tecnico Generale di AQ;
- **RUAC:** responsabile unico delle attività contrattuali, cioè il referente del Fornitore nei confronti di Consip S.p.A. per tutte le attività di gestione relative all'AQ, dotato di appositi poteri di firma tali da impegnare in maniera esecutiva il Fornitore nei confronti delle Amministrazioni, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.1 del Capitolato Tecnico Generale di AQ;
- **Vendor/produttore:** si intende il produttore dello specifico prodotto.

2 Contesto dell'appalto specifico e elementi trasversali ai vari servizi

2.1 Contesto organizzativo, tecnologico e normativo

L'Azienda ULSS 7 Pedemontana insiste su un territorio composto da 55 Comuni e una popolazione di 366.429 residenti e garantisce l'assistenza sanitaria e socio sanitaria impiegando un'infrastruttura ICT articolata e complessa in grado di erogare servizi applicativi, di comunicazione dati e interscambio fonia ai diversi utenti nelle varie sedi e dislocati sul territorio.

In particolare l'infrastruttura si compone di circa 500 Server, 4.000 PDL, connettività in banda larga, software applicativi per la gestione degli eventi sanitari. I progetti, in linea con la programmazione regionale (FESr, SIO, LIS ...), realizzati e in fase di realizzazione sono finalizzati a consolidare la sicurezza dell'infrastruttura tecnologica, estendere l'informatizzazione dei processi produttivi e tecnologici su più ambiti ed accrescere il miglioramento dei servizi al cittadino. L'evoluzione della comunicazione in rete migliorerà il modo di comunicare con i cittadini e con gli utenti aziendali, sviluppando alcuni servizi on-line a beneficio degli stessi riducendo tempi di spostamento e di fruibilità dei documenti.

Gli obiettivi strategici aziendali sono riconducibili ad agire in una logica di rete, specializzare i servizi, valorizzare le buone pratiche, predisporre e attivare nuovi servizi, ridefinire modelli organizzativi, agire con trasparenza, sviluppare la telemedicina.



La UOSD Sistemi Informativi, in linea con le scelte strategiche regionali e aziendali, ha finalizzato gli interventi sui seguenti elementi fondamentali:

- Sicurezza: Si deve proseguire nel processo di consolidamento e messa in sicurezza dei sistemi, dalla Business Continuity al Disaster Recovery (in sintonia con le linee guida dell'AGID per realizzare un unico polo tecnologico certificato) ai sistemi di accesso / protezione dei dati e di privacy.
- Sviluppo ed omogeneizzazione del Sistema Informatico Aziendale: l'informatica è uno strumento che consente di cambiare e migliorare l'organizzazione, per renderla più efficiente ed efficace, per favorire e facilitare il cittadino nei suoi percorsi di cura, per incrementare i livelli informativi sui processi produttivi e gestionali. In tal senso prosegue lo sviluppo Sistema Informatico Aziendale finalizzato all'unificazione applicativa sanitaria.
- Supporto alla riorganizzazione dei servizi: facilitare ed applicare la ridefinizione dei modelli organizzativi implementando soluzioni tecnologiche e aumentando, omogeneizzando metodi e protocolli, l'assistenza e la formazione nell'uso dell'informatica.

L'obiettivo che si vuole ottenere dall'attivazione di questo Appalto Specifico è garantire maggiore sicurezza dell'infrastruttura aziendale, ottenibile tramite strumenti avanzati di monitoraggio e di gestione dei privilegi amministrativi ed alla messa in protezione delle applicazioni web pubblicate su piattaforma Internet.

Le soluzioni tecniche attualmente utilizzate, che devono essere integrate con i prodotti richiesti, sono le seguenti:

- Firewall Fortigate e CheckPoint;
- Google Workspace per la posta elettronica e sistemi di condivisione;
- Struttura Active Directory su sistemi Windows (con il nuovo dominio aulss7.veneto.it e i vecchi domini, in fase di dismissione ma ancora attivi, aslbassano.it e altovicentino.asl);
- Antivirus Sophos Cloud;
- Applicativi Web su server Apache, NGNIX o IIS;
- Server Windows o Linux (principalmente RedHat/CentOS);
- PDL Windows 10/11 e alcune postazioni con versioni precedenti;
- Network distribuita su più site due dei quali saranno quelli che daranno la connettività esterna all'azienda
- Server AIX;
- Infrastruttura virtuale VMWare su Nutanix;
- Share di rete DFS e su NetAPP.
- DB Oracle,Sql, SqlExpress,Cachè

L'ambito di I livello che si intende mappare con questo Contratto Esecutivo è relativo alla "Sicurezza Informatica" e gli obiettivi del piano triennale sono:

- Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA;
- Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione.

La procedura di questo appalto specifico afferisce agli investimenti pubblici finanziati tramite PNRR come da parere favorevole della Commissione Crite relativa alla scheda del 7 giugno 2022 Azienda ULSS7 Pedemontana 539 - Protocollo 272927 del 16 giugno 2022 della Regione Veneto e prot. 66093 del 16.06.2022 dell'AULSS7 Pedemontana.

3 Oggetto, durata dell'appalto specifico e luogo di esecuzione



3.1 Oggetto della fornitura

Il presente AS ha ad oggetto i seguenti prodotti/servizi:

Prodotti:

1. Security Information and Event Management (SIEM)
2. Privileged Access Management (PAM)
3. Web Application Firewall (WAF)

Funzionalità aggiuntive sui prodotti:

- Funzionalità aggiuntiva - SIEM - Ricezione informazioni di security threat intelligence attraverso un feed
- Funzionalità aggiuntiva - SIEM - Funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR (ad. es. dashboard specifiche, etc)
- Funzionalità aggiuntiva - WAF - Configurazione in alta affidabilità

Servizi base connessi alla fornitura:

- installazione e configurazione (inclusi nella fornitura)
- manutenzione profilo HP (comprensiva di help desk)
- Contact Center (incluso nella fornitura)
- supporto specialistico

Servizi aggiuntivi connessi alla fornitura:

- servizio di incident response.

Le funzionalità aggiuntive e i servizi aggiuntivi sono ricompresi nel limite del 40% della base d'asta totale di AS.

Si rimanda al paragrafo "Descrizione della fornitura" per le caratteristiche specifiche dei prodotti e servizi richiesti.

3.2 Durata del contratto

Per il presente appalto specifico è prevista una durata di 24 mesi a partire dalla verifica di conformità positiva.

3.3 Luogo di esecuzione ed orario di erogazione dei servizi

Le infrastrutture oggetto di fornitura saranno installate presso le sedi dei Datacenter dell'Amministrazione, collocati in:

- Bassano del Grappa, via dei lotti 40 (VI)
- Thiene, via boldrini 1 (VI)

Gli orari di erogazione previsti sono 24/7/365



4 Descrizione della fornitura

4.1 Garanzia

Per la garanzia dei prodotti, il Fornitore faccia riferimento al par. 2.1.10 del CTAQ.

4.2 Prodotti

Di seguito sono riportati i prodotti richiesti nell'ambito della presente iniziativa:

- SIEM
- PAM
- WAF

In particolare per i prodotti si richiede al fornitore di indicare come saranno realizzate le funzionalità aggiuntive, in quanto oggetto di valutazione tecnica.

4.2.1 SIEM

Di seguito le caratteristiche richieste per il prodotto SIEM

SIEM	
Requisito	Fascia 5 - fino a 1000 device e massimo 6000 eps
Dimensionamento	1000 Device, 6000 eps
Quantità	1
Funzionalità aggiuntive	<ul style="list-style-type: none">• Ricezione informazioni di security threat intelligence attraverso un feed• Funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR (ad. es. dashboard specifiche, etc)
Requisiti migliorativi oggetto di valutazione tecnica	<ul style="list-style-type: none">• AS.1.1 Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzioni:<ul style="list-style-type: none">○ Firewall Fortigate e CheckPoint;○ Google Workspace per la posta elettronica e sistemi di condivisione;○ Antivirus Sophos Cloud;tramite API non comprese tra quelle minime e migliorative previste in AQ• AS.1.3 - Qualità del feed di threat intelligence. Sarà premiata:<ul style="list-style-type: none">○ la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence;○ la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.)○ l'innovatività e la capacità dei motori di machine learning di correlare le informazioni di sicurezza provenienti da varie fonti, al fine di rendere più



	<p>rapida l'analisi di tali informazioni e il processo decisionale da parte degli operatori di sicurezza.</p> <ul style="list-style-type: none">AS.1.7 - Efficacia delle funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR, in termini di:<ul style="list-style-type: none">semplicità e rapidità nella produzione di reportistica adeguata a comprovare lo stato di compliance su dati storici e in real time, provenienti da un'ampia varietà di sistemi IT dell'organizzazione;semplificazione dell'attività di monitoraggio della compliance in real time;capacità di individuare i dati associati al GDPR più a rischio.
Punteggio tecnico massimo assegnabile	AS.1.1 - Tmax =2 Punteggio massimo assegnabile = 2 AS 1.3 - Dmax =5 Punteggio massimo definito dall'azienda = 4 AS 1.7 - Dmad =5 Punteggio massimo definito dall'azienda = 3

4.2.2 PAM

Al fine di realizzare un'architettura facilmente manutenibile si chiede la fornitura di un appliance PAM. Tale caratteristica sarà valutata nell'ambito del criterio AS.7.9. Di seguito le caratteristiche richieste

PAM	
Requisito	Fascia 3 - fino a 250 utenze
Dimensionamento	500 utenze
Quantità	2
Funzionalità aggiuntive	<ul style="list-style-type: none">Configurazione in alta affidabilità
Requisiti migliorativi	<ul style="list-style-type: none">AS.7.9 - Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.
Punteggio tecnico massimo assegnabile	AS 7.9 - Dmax =2 Punteggio massimo definito dall'azienda = 1



4.2.3 WAF

Di seguito le caratteristiche previste per il prodotto WAF

WAF	
Requisito	fascia 2- fino a 5 Gbps di throughput HTTP
Dimensionamento	2 Gbps di traffico HTTP e HTTPS
Quantità	2
Funzionalità aggiuntive	<ul style="list-style-type: none">• Configurazione in alta affidabilità
Requisiti migliorativi	<ul style="list-style-type: none">• AS.8.2 - Integrazione con soluzioni di sicurezza SIEM richiesta nel presente AS• AS.8.3 - Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.• AS.8.6 - Modalità di implementazione, varietà e numerosità delle policy/eccezioni alle policy associabili ad applicazioni in essere presso la PA al fine di semplificare la gestione in sicurezza degli applicativi
Punteggio tecnico massimo assegnabile	AS.8.2 - Tmax =3 Punteggio massimo assegnabile = 3 AS 8.3 - Dmax =2 Punteggio massimo definito dall'azienda = 1 AS 8.6 - Dmax =3 Punteggio massimo definito dall'azienda = 3

4.3 Servizi

Nell'ambito della fornitura dei prodotti riportati, in aggiunta ai servizi base obbligatori, sono richiesti i seguenti servizi che trovano diversa applicazione nei diversi prodotti.

4.3.1 SERVIZIO BASE - Manutenzione

Tutti gli apparati forniti dovranno prevedere il servizio di manutenzione con profilo **High Profile (h24) per 24 mesi**. La manutenzione dovrà prevedere tutte le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site, nel rispetto degli SLA di seguito indicati. Tutte le attività previste (interventi del Fornitore presso l'Amministrazione, rimozione degli elementi, riparazione degli elementi guasti, successiva installazione) sono da intendersi incluse nel costo del servizio.

Nell'ambito dell'attività di manutenzione, si richiede al fornitore di descrivere i processi le modalità operative specifiche che intende adottare nell'ambito del contesto ULSS7 Pedemontana, per la realizzazione del servizio.



4.3.2 SERVIZIO BASE - Supporto Specialistico

Il servizio di supporto specialistico richiesto deve garantire le seguenti attività:

FASE INIZIALE

I servizi in modalità “spot”, da prevedere in fase iniziale:

- supporto alla progettazione di basso livello e realizzazione di specifiche integrazioni tra i prodotti acquistati e le tecnologie già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dell'architettura acquisita e garantire la sicurezza del sistema nel suo complesso.
- supporto all'analisi di dettaglio e alla configurazione dei prodotti, definendo le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Azienda ULSS7

MODALITA' CONTINUATA (presidio)

Il servizio deve garantire il supporto operativo al personale dell'Amministrazione o a chi da essa delegato, nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito in modo continuativo nel corso della durata contrattuale. Il supporto dovrà essere di tipo proattivo e a titolo di esempio, dovrà prevedere almeno le seguenti attività:

- Monitoraggio degli eventi che coinvolgono le infrastrutture IT e security dell'Azienda ULSS7, tramite SIEM, analisi eventi e allertamento ed attivazione azioni di remediation.
- Monitoraggio WAF e supporto su gestione oltre alla risoluzione delle eventuali problematiche
- Monitoraggio PAM e supporto su gestione oltre alla risoluzione delle eventuali problematiche

Profilo	Giorni
Servizio di supporto specialistico - Security Principal - fascia standard	30
Servizio di supporto specialistico - Senior Security Architect- fascia standard	30
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	30

4.3.3 SERVIZI AGGIUNTIVI - Incident Response

Il servizio di incident response ha l'obiettivo di garantire all'Azienda ULSS7 una risposta rapida ed efficace alle violazioni di sicurezza informatiche che possano compromettere l'integrità, la disponibilità o la riservatezza dei dati dei propri sistemi e di adottare misure volte a prevenire gli incident.

Il servizio di incident response deve prevedere le seguenti fasi:

- redazione di un piano di incident response, con definizione delle procedure operative da seguire, nonché adozione di misure volte a prevenire il verificarsi degli incidenti di sicurezza;
- identificazione dell'attacco di sicurezza e dello scopo dell'attacco
- contenimento, bonifica e remediation
- ripristino del corretto funzionamento dei sistemi
- verifica ex post della corretta mitigazione dell'incidente informatico e della corretta implementazione di tutte le contromisure adottate.

Il servizio di Incident Response supporterà l'Amministrazione in caso di incidente anche tramite l'incident Response Team dedicato.



Nel contesto operativo dell'AULSS7 di circa 500 Server, 4.000 PDL le soluzioni tecniche attualmente utilizzate, sono le seguenti:

- Firewall Fortigate e CheckPoint;
- Google Workspace per la posta elettronica e sistemi di condivisione;
- Struttura Active Directory su sistemi Windows (con il nuovo dominio aulss7.veneto.it e i vecchi domini, in fase di dismissione ma ancora attivi, aslbassano.it e altovicentino.asl);
- Antivirus Sophos Cloud;
- Applicativi Web su server Apache, NGINX o IIS;
- Server Windows o Linux (principalmente RedHat/CentOS);
- PDL Windows 10/11 e alcune postazioni con versioni precedenti;
- Network distribuita su più site due dei quali saranno quelli che daranno la connettività esterna all'azienda
- Server AIX;
- Infrastruttura virtuale VMWare su Nutanix;
- Share di rete DFS e su NetAPP.
- DB Oracle,Sql, SqlExpress,Cachè

Tramite questo accordo quadro si vanno ad acquisire il SIEM, WAF e PAM per il potenziamento della Cybersecurity aziendale.

Gli asset da proteggere sono:

- dati residenti su DB e File System Aziendali
- i sistemi, in particolare a partire dai Server, Firewall, Appliance

5 Ulteriori requisiti di AS

Ai sensi di quanto previsto dall'art. 47 del DL 77/2021 conv. con L. 108/2021, è requisito necessario dell'offerta per il Fornitore, assicurare una quota pari almeno al 30 per cento, delle assunzioni necessarie per l'esecuzione del contratto esecutivo o per la realizzazione di attività ad esso connesse o strumentali, all'occupazione giovanile e femminile.

Sono inoltre requisiti migliorativi dell'offerta di AS le misure premiali di cui al criterio AS.9.4 del par. 3.1 della Richiesta di Offerta.

L'Aggiudicatario si impegna inoltre a rispettare i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale, in ottemperanza al principio di non arrecare un danno significativo all'ambiente "Do No Significant Harm" (DNSH), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.

6 Livelli di servizio e penali

Trovano applicazione i livelli di servizio e penali già previsti nel CTAQ.

Il mancato adempimento di quanto disposto dall'art. 47, commi 3, 3-bis e 4, del D.L. 77/2021, convertito in L. 108/2021, in conformità al comma 6 di detto articolo, determinerà l'applicazione di penali commisurate alla gravità della violazione, all'entità delle conseguenze legate al ritardo e proporzionali rispetto all'importo del contratto o alle prestazioni dello stesso.

Le penali dovute, in deroga all'art. 113-bis del D.Lgs. n. 50/2016, ai sensi dell'art. 50 della citata L. 108/2021, sono calcolate nella misura giornaliera dell'1 per mille dell'ammontare netto contrattuale e non possono comunque superare, complessivamente, il 20 per cento di detto ammontare netto contrattuale.



7 Piano Operativo dell'AS

Il Fornitore dovrà presentare entro 15 giorni lavorativi dalla data di stipula del Contratto e pena l'applicazione delle penali di cui al CTAQ, un *"Piano Operativo"* che riporti almeno i contenuti di cui al par. 3.2.1 del CTAQ.