Capitolato Tecnico per la fornitura di Storage e accesso a un ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche e servizi di integrazione con il Sistema AGE di Autostrade per l'Italia

	Struttura aziendale	Riferimento
Redatto da:	DIDT / BDE	Giuseppe Capuano
Quality Gate:	DIDT / BDE	Francesco Spadafora
Approvato da:	DIDT / BDE	Marco Federico
	DIDT / CISO	Massimiliano Masi
	DIDT / CDO	Riccardo Marchiani

Sommario

1. Introduzione

1.1. Scopo del documento

Il presente Capitolato Tecnico ha l'obiettivo di descrivere e classificare le varie attività in ambito di:

- Fornitura di Storage e accesso ad un ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche.
- Servizi di integrazione con il Sistema AGE di Autostrade per l'Italia (di seguito, anche, "ASPI" o "Committente") e interventi di nuovi sviluppi e di manutenzione evolutiva.

Il Capitolato Tecnico disciplina le categorie di servizi richiesti, le relative modalità d'erogazione, le figure professionali necessarie a costituire il Gruppo di Lavoro, i livelli di servizio attesi e le relative penali in caso di mancato rispetto dei livelli stessi.

1.2. Definizioni, Acronimi e Abbreviazioni

AGE: Sistema Informativo di Autostrade per l'Italia per la gestione e rappresentazione dei propri asset su piattaforma cartografica GIS basata su tecnologia Google Maps Platform per Sistemi Desktop

KML/KMZ: Formato cartografico proprietario di Google

IRIS: Veicolo a terra ad alto rendimento di proprietà di Autostrade per l'Italia per il rilievo di foto sferiche e dati laser

SHP (Shapefile): Formato cartografico proprietario di ESRI

ASPI: Autostrade per l'Italia.

DIDT: Direzione IT e Digital Transformation

BDE/EAC: "Business Domain Engineering, Construction & Planning Team / Engineering & Construction", struttura di ASPI facente parte di DIDT, responsabile di garantire lo sviluppo e la manutenzione dei sistemi GIS e richiedente i servizi oggetto della presente gara d'appalto.

RIA: Responsabile Informatico di un'Applicazione. Figura definita nell'organizzazione interna di ASPI, con il ruolo di supervisionare lo sviluppo, la manutenzione e l'evoluzione di una o più applicazioni informatiche. Anche Responsabile Applicativo.

RUP: Responsabile Unico del Progetto. Figura nominata dalla stazione appaltante, prevista dal Codice degli appalti, che vigila sullo svolgimento delle fasi di progettazione, affidamento ed esecuzione dell'intervento e provvede a creare le condizioni affinché il processo realizzativo risulti condotto in modo unitario in relazione ai tempi e ai costi preventivati, alla qualità richiesta, alla manutenzione programmata, alla sicurezza e alla salute dei lavoratori e in conformità alle disposizioni di legge in materia.

DEC: Direttore dell'Esecuzione del Contratto. Figura nominata dalla stazione appaltante, prevista dal Codice degli appalti, che coadiuva il RUP nel coordinamento, direzione e controllo tecnico-contabile dell'esecuzione del contratto stipulato dalla stazione appaltante, in modo da assicurarne la regolare esecuzione.

RT: Referente Tecnico del contratto: figura nominata dall'Appaltatore e deputata al coordinamento organizzativo dell'attività lavorativa del personale impiegato nella esecuzione delle attività oggetto del contratto, nonché interfaccia nei confronti della Committente per qualsiasi esigenza ad esso connessa.

2. Ruolo struttura coinvolta di Autostrade per l'Italia

La struttura denominata **"Engineering & Construction"** (EAC) ha la responsabilità, in particolare, delle attività di progettazione, sviluppo e gestione dei Sistemi Informativi Territoriali (GIS) utilizzando informazioni delle varie aree tematiche e di business, integrandole con dati geografici e basi cartografiche georeferenziate con riferimento al grafo stradale di ASPI.
Tali servizi sono erogati verso Autostrade e, in maniera più o meno estesa, verso le altre società del Gruppo.

L'organizzazione interna della struttura EAC prevede che ciascuna Applicazione, tra cui AGE, sia presidiata da un referente applicativo denominato **RIA – Responsabile Informatico dell'Applicazione,** che ha il compito di assicurarne la manutenzione correttiva ed evolutiva, il supporto e tutti gli altri servizi inerenti ad essa.

EAC, nell'ambito delle attività previste nel presente Capitolato Tecnico, rivestirà il ruolo di project management e parteciperà con propri specialisti a tutte le fasi, coordinandone le attività.

3. Oggetto dell'appalto

Costituiscono oggetto dell'appalto le prestazioni di messa a disposizione di uno storage e di accesso ad un ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche nonchè i servizi di integrazione con l'ambiente AGE di Autostrade per l'Italia; la gestione dei sistemi di erogazione Cloud deve essere in linea con le norme ISO 27018 e 27017.

Le attività previste dall'appalto sono riconducibili alle seguenti categorie di prestazioni:

- **Fornitura dello storage in ambiente cloud:** spazio disco in cloud, messo a disposizione dall'Appaltatore, in cui ASPI potrà effettuare l'upload di immagini sferiche in formato .jpg e file lidar in formato. las dei rilievi effettuati con il veicolo IRIS;
- **Ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche:** applicazione raggiungibile in internet messa a disposizione dall'Appaltatore con cui ASPI potrà visualizzare, navigare, misurare ed effettuare il download dei dati laser e delle immagini sferiche precedentemente caricate nello storage cloud;
- **Integrazione con l'ambiente AGE:** fornitura di API o altro strumento informatico per la sincronizzazione della navigazione nell'ambiente web con il Sistema AGE.

L'Appaltatore dovrà altresì, su richiesta della Committente, eseguire interventi di nuovi sviluppi e/o di manutenzione evolutiva delle funzionalità, necessari al corretto funzionamento dei prodotti. A titolo esemplificativo, potranno esser richiesti all'Appaltatore interventi di potenziamento dell'integrazione con AGE, finalizzati allo scambio di ulteriori informazioni oltre la mera posizione geografica, oppure il caricamento nell'ambiente web in cloud di shapefile proprietari (ad esempio, grafo autostradale, opere d'arte, barriere di sicurezza, segnaletica verticale, ecc…) ai fini di una miglior contestualizzazione della navigazione nella nuova di punti e nelle immagini sferiche. Altresì potranno esser richiesti interventi per il riconoscimento automatico di oggetti all'interno della nuvola di punti o delle immagini sferiche.

Nel capitolo 5 saranno descritti in maniera dettagliata la natura di ogni categoria di servizio e le attività che si richiede doversi svolgere nell'ambito della fornitura.

I servizi sopra elencati saranno erogati secondo un modello di gestione descritto nel capitolo 7 di questo Capitolato Tecnico.

4. Ambito dei servizi

In questo capitolo vengono descritti gli ambienti tecnologico e applicativo, vengono fornite informazioni su numerosità e dimensioni dei componenti dei Sistemi:

- **AGE-Google Maps in Autostrade**: È il Sistema Informativo di Autostrade per l'Italia per la gestione e rappresentazione dei propri asset su piattaforma cartografica GIS basata su tecnologia Google Maps Platform per Sistemi Desktop.

Dovranno essere garantiti i requisiti di sicurezza previsti nell'appendice "Misure di Sicurezza" parte integrante del seguente capitolato.

4.1. Ambiente tecnologico

Viene di seguito fornito il dettaglio dell'ambiente tecnologico e funzionale di riferimento per il Sistema AGE.

4.1.1. Storage in ambiente cloud

Relativamente allo storage in ambiente cloud che sarà messo a disposizione del fornitore, è necessario il rispetto del seguente punto:

1. Ne sia garantita la raggiungibilità in maniera sicura e controllata da parte di ASPI che attiverà una sincronizzazione verso il proprio cloud al fine di condividere i file .las e le immagini sferiche 360 .jpg ad altre strutture Aziendali che dovranno accedere direttamente ai dati. I dati sono di proprietà di ASPI, non potranno essere condivisi od usati da altri; i dati dovranno rimanere disponibili per un minimo di 12 mesi dopo il termine di scadenza del contratto per permettere le eventuali operazioni di passaggio ad altro fornitore. L'aggiudicatario si impegna con la stipula del contratto a fornire supporto ed assistenza al fornitore subentrante, compresa la messa a disposizione di un canale per lo spostamento diretto dei dati.

4.1.2. Ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche

Relativamente all'ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche, è necessario il rispetto del seguente punto:

1. Per quanto la via preferenziale di fruizione dello strumento sarà quella di accesso mediante integrazione con AGE (Rif. 4.1.3) dovrà essere garantito l'accesso diretto via WEB alla piattaforma del fornitore, mediante federazione con i sistemi di autenticazione di ASPI, a tutti gli utenti AGE: il numero di utenti ad oggi è circa 2.500, con una media di circa 500 accessi distinti al giorno.

4.1.3. AGE - Ambiente Google Maps Platform

Viene di seguito fornito il dettaglio degli ambienti tecnologici su cui si basa il sistema "AGE – Google Maps Platform":

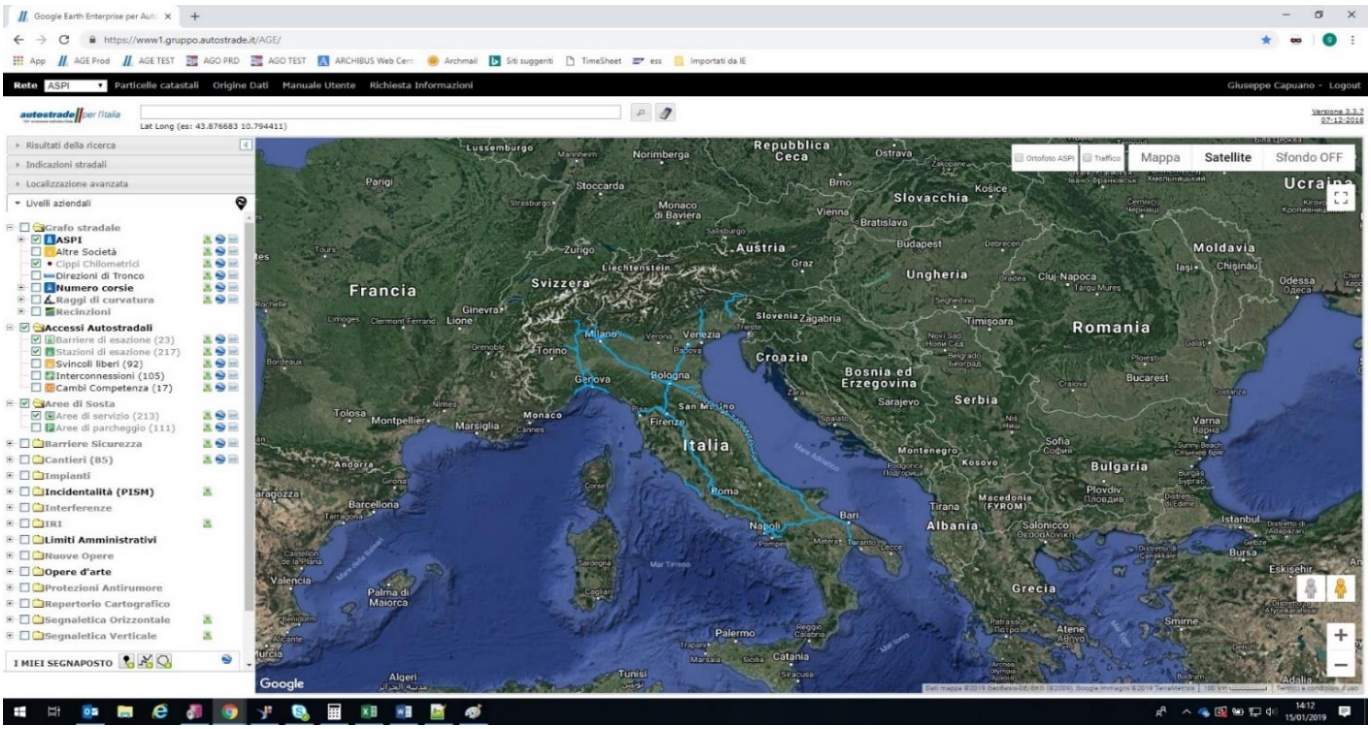
- API Google Maps Platform
- Linguaggi e tool di sviluppo quali PHP, .NET, C#, Visual Basic, Java, SQL, Oracle, JQuery, HTML, XML, IIS/MTS e di altri web application server. Protocolli applicativi come https, http e funzionalità di ssl.
- DBMS Oracle 19c con estensioni spaziali, IBM DB2, Microsoft SQL SERVER.
- BM Security Access Manager (ISAM) come server di autorizzazione OAuth
- RESTFul Web Services
- Linguaggi script korn shell, bash shell, windows batch.
- Javascript, jQuery.
- Application server: Apache 2, Apache Tomcat, IIS
- Sistemi di versionamento: SVN e GIT

- Script Unix/PLSQL e JAVA, per schedulare processi batch tramite lo scheduler Control-M in uso presso ASPI.

4.2. Ambiente applicativo e funzionalità del Sistema AGE

Di seguito viene fornita una descrizione del sistema AGE attualmente in uso presso ASPI.

AGE è un'applicazione WebGIS che utilizza l'infrastruttura Google Maps Platform, con servizi in cloud, per visualizzare su sfondo Google Maps la geometria e i dati di dettaglio del grafo stradale di AST, dei cippi km, delle stazioni, delle aree di servizio, delle aree di parcheggio, gallerie, ponti/viadotti, sottopassi, opere di attraversamento idraulico, impianti radio/elettrici, interferenze, particelle catastali, immagini di veicoli proprietari per la pavimentazione. L'accesso ai singoli layer è gestito tramite un servizio di profilatura utente, con alcuni layer aperti a tutti gli utenti, ed altri disponibili solo agli utenti con idoneo profilo abilitativo.



Home Page del Sistema AGE

Il Sistema di riferimento cartografico utilizzato per le tabelle spaziali di AGE è l'EPSG 4326 (coordinate latitudine e longitudine GPS sull'ellissoide di riferimento WGS84).

5. Categorie di servizi - dettaglio

Il presente capitolo descrive in maniera dettagliata e per ogni servizio le attività che si richiede svolgere nell'ambito della fornitura. I servizi in questione sono:

- Fornitura dello storage in ambiente cloud;

- Ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche;

- Integrazione con l'ambiente AGE.

Come indicazioni generali dei servizi, gli utenti di Autostrade per l'Italia che saranno nominati amministratori del Sistema devono accedere alla piattaforma tramite le credenziali aziendali. Ciò implica che la piattaforma dovrà

integrarsi con i meccanismi di Autorizzazione e Autenticazione utilizzati in ASPI. Anche eventuali integrazioni Machine 2 Machine (M2M) dovranno seguire gli standard di sicurezza internazionali ed adeguarsi ai meccanismi adottati in ASPI. Tutte le connessioni dovranno avvenire su canali cifrati con il protocollo TLS alla versione 1.2 o maggiore.

Per l'autenticazione utenti:

- Federazione SAML oppure OIDC2.0, con Identity Provider di ASPI. (Soluzione Raccomandata)
- Autenticazione tramite Azure AD con Active Directory ASPI (Soluzione possibile, ma non preferita)

Per l'autorizzazione utenti:

- OAuth2.0 con grant type "Authorization Code Grant" (RFC 6749, sez. 4.1)

Per l'autenticazione delle comunicazioni M2M:

- Utilizzo del protocollo mTLS (mutual TLS, autenticazione client tramite certificato) alla versione 1.2 o maggiori.

Per l'autorizzazione nelle comunicazioni M2M:

- OAuth2.0 con grant type "Client Credentials Grant" (RFC 6749, sez. 4.4)

Dovranno essere pertanto garantiti i requisiti di sicurezza previsti dall'appendice "Misure di Sicurezza", parte integrante del presente capitolato.

Viene, di seguito, fornito il dettaglio delle attività che sono contemplate nei servizi sopra descritti, raggruppandole per Tipologia.

5.1. Fornitura dello storage in ambiente cloud

Autostrade per l'Italia stima la produzione di circa 50 Tb l'anno di rilievi composti da immagini 360° e file .las grazie al veicolo IRIS, con l'obiettivo di mantenere a regime gli ultimi due anni di rilievo, per un totale di 100 Tb di spazio storage. L'Appaltatore dovrà mettere a disposizione uno storage in ambiente cloud che possa contenere i rilievi del veicolo IRIS. I rilievi arriveranno gradualmente, con le missioni del veicolo IRIS che copriranno circa 50 – 100 km di strada alla volta. L'obiettivo è coprire i 6.000 km di carreggiate e l'intera rete degli svincoli di stazione, delle aree di servizio, delle aree di parcheggio, per circa 7.000km di rilievo stradale. I dati del rilievo saranno poi messi a disposizione dell'ambiente web di visualizzazione, descritto nel paragrafo successivo.

ASPI dovrà poter sostituire a piacimento parti di rilievo già effettuate nel corso dell'anno, qualora si renda necessaria rilevare una tratta della rete stradale già caricata in precedenza.

Inoltre, le immagini 360 e i file .las saranno a disposizione di ASPI che attiverà una sincronizzazione verso il proprio cloud al fine di condividerli ad altre strutture Aziendali che dovranno accedere direttamente ai dati.

5.2. Ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche

Autostrade per l'Italia fornirà i rilievi eseguiti dal mezzo aziendale IRIS per essere fruibili in ambiente web in cloud: questi dati sono composti da immagini 360° e file .las dei rilievi eseguiti sulla rete autostradale di competenza ASPI, circa 7.000km svincoli compresi, eseguiti due volte l'anno, per un totale circa di 14000 km/anno. L'ambiente dovrà permettere all'utente che accede da web, sia direttamente (mediante federazione delle utenze), che tramite la piattaforma AGE, di poter navigare in modo intuitivo in un ambiente 3D virtuale definito dalla nuvola di punti e dalle

immagini 360° in modo sincrono tra immagini e nuvole di punti, di effettuare calcolo distanze, aree e volumi, mediante una suite di comandi predisposta (es. Misurazioni intradosso sovrappassi rispetto al piano autostradale, larghezza del piano bitumato), di esportare sezioni trasversali/longitudinali e porzioni di nuvola di punti e dati per integrazione con sistemi GIS/CAD.

La piattaforma dovrà pertanto offrire apposita funzionalità di export delle feature selezionate nei vari formati standard: LAS, SHP, CSV, DXF.

5.3. Integrazione con l'ambiente AGE

L'Appaltatore dovrà mettere a disposizione di ASPI delle API (Application Programming Interface) o Web Services che possano essere richiamati da AGE. Si vuole accedere infatti all'ambiente cloud in maniera mirata sull'area geografica in cui l'utente sta navigando in AGE; inoltre, man mano che l'utente si sposta variando la posizione geografica nell'ambiente cloud, l'aggiornamento della posizione deve essere riportata anche su AGE. In questo modo ci sarà un sincronismo tra la navigazione nell'ambiente cloud e la posizione dell'utente nella mappa AGE. Si precisa che l'integrazione delle API o dei Web Services nel Sistema AGE non sono oggetto di fornitura ma le stesse saranno utilizzate dall'attuale fornitore del Sistema AGE. L'aggiudicatario dovrà fornire tutte le informazioni tecniche e materiali a supporto per realizzare tale integrazione.

Come indicato al precedente par. 3, potranno altresì esser richiesti all'Appaltatore interventi di sviluppo nuove funzionalità e/o manutenzione evolutiva quali, a titolo esemplificativo:

- Interventi di potenziamento dell'integrazione con AGE, finalizzati allo scambio di ulteriori informazioni oltre la mera posizione geografica;
- Interventi per il caricamento nell'ambiente web in cloud di shapefile proprietari (ad esempio, grafo autostradale, opere d'arte, barriere di sicurezza, segnaletica verticale, ecc…) ai fini di una miglior contestualizzazione della navigazione nella nuova di punti e nelle immagini sferiche;
- Interventi per il riconoscimento automatico di oggetti all'interno della nuvola di punti o delle immagini sferiche.

6. Gruppo di lavoro - Figure professionali

L'Appaltatore dovrà mettere a disposizione, per l'espletamento dei servizi delle fasi di Erogazione dei Servizi, un gruppo di lavoro formato da risorse dedicate, costituito dalle seguenti figure professionali:

- Specialista di Prodotto Senior: n. 2 risorse

e che nel suo insieme garantisca la piena padronanza di tutto l'ambiente tecnologico descritto al paragrafo 4.1.

In considerazione della tipologia dei servizi e della necessità di interagire con diverse strutture aziendali, anche alla luce di esperienze pregresse, è richiesto come requisito necessario che tutte le risorse siano di madrelingua Italiana oppure, se non lo sono, possiedano un'ottima conoscenza della lingua Italiana nella comprensione, nello scritto e nel parlato, dimostrando di aver conseguito un livello di certificazione C2 (Livello di padronanza della lingua in situazioni complesse) secondo il *Quadro comune europeo di riferimento* per la conoscenza delle lingue.

Tutte le risorse devono essere pertanto in grado di:

- comprendere con facilità praticamente tutto ciò che sentono e leggono;
- riassumere informazioni provenienti da diverse fonti sia parlate che scritte, ristrutturando gli argomenti in una presentazione coerente;

- esprimersi spontaneamente, in modo molto scorrevole e preciso, individuando le più sottili sfumature di significato in situazioni complesse.

L'Appaltatore garantisce che le persone che saranno impiegate per lo svolgimento delle attività oggetto del presente Capitolato Tecnico posseggono i requisiti minimi di cui al successivo par. 6.1.3 (o i requisiti migliorativi eventualmente dichiarati dall'Appaltatore in offerta tecnica).

6.1. Specialista di Prodotto Senior

6.1.1. Finalità del ruolo

È la figura professionale che raccoglie e analizza requisiti utente identificando la soluzione funzionale più idonea, analizza e definisce i processi di business e i relativi flussi, redige l'analisi funzionale, le schede di collaudo e la documentazione di pertinenza.

È autonomo nello svolgimento delle attività di sviluppo, manutenzione, testing e documentazione. In base alle specifiche funzionali, è in grado di procedere con l'analisi di dettaglio e la realizzazione delle relative componenti dell'ambiente web richiesto al paragrafo 5.2

È in grado di scrivere e manutenere API/web services per il passaggio informazioni tra l'ambiente web di fruizione dati lidar ed immagini 360 con il Sistema AGE.

6.1.2. Attività tipiche del ruolo

Configurare l'ambiente web richiesto al paragrafo 5.2, consentendo il caricamento dei dati del veicolo IRIS da parte di ASPI.

Scrivere e manutenere API/web services per il passaggio informazioni tra l'ambiente web e il Sistema AGE, come richiesto al paragrafo 5.3.

6.1.3. Requisiti minimi

Sono di seguito elencati i requisiti minimi che le risorse che ricopriranno i ruoli di Specialista di Prodotto Senior (GIS) dovranno necessariamente possedere, pena la non accettazione:

1. Diploma di scuola media superiore, tecnico o scientifico;
2. Ottima conoscenza della lingua italiana nella comprensione, nello scritto e nel parlato da comprovare con appartenenza a madrelingua italiana o certificazione minima C2;
3. Comprovata esperienza di almeno 5 anni in progetti relativi al trattamento di dati lidar e immagini sferiche 360 (almeno 1 progetto);
4. Comprovata esperienza di almeno 5 anni in progetti relativi alla programmazione di API o web services utili al passaggio di dati tra due applicazioni.

6.2. Formazione del Gruppo di Lavoro

Nelle fase di avvio del contratto, ASPI e l'Appaltatore procederanno alla formalizzazione del Gruppo di Lavoro mediante la sottoscrizione di un apposito Verbale di formalizzazione del Gruppo di Lavoro che evidenzi i nominativi delle risorse e la corrispondenza con le figure professionali richieste, nonché la data di inizio della fase di erogazione dei servizi.

6.3. Sostituzione di una risorsa

L'Appaltatore deve prevedere, per tutta la durata contrattuale, la disponibilità delle risorse componenti il Gruppo di Lavoro i cui CV sono stati presentati in fase di gara.

Eventuali richieste di sostituzioni dovranno esser debitamente motivate e potranno comunque esser effettuate solo previo benestare della Committente, salvo ragioni di congiunturale urgenza. La richiesta di sostituzione dovrà esser trasmessa alla Committente con un preavviso di almeno 20 giorni lavorativi rispetto alla data di uscita della risorsa, pena l'applicazione delle penali previste nel contratto, e dovranno avvenire con risorse di analoga professionalità ed esperienza, documentata e certificata e le risorse proposte in sostituzione dovranno essere sottoposte a successiva ed insindacabile accettazione da parte della Committente.

In caso di accettazione da parte di Autostrade per l'Italia, il sostituto dovrà essere disponibile per l'inserimento nel Gruppo di Lavoro entro la data di uscita del sostituendo e le parti provvederanno a sottoscrivere un nuovo Verbale di formalizzazione del Gruppo di Lavoro.

Il sostituto dovrà essere formato tramite affiancamento, a spese dell'Appaltatore, per almeno 10 giorni lavorativi senza alcun onere aggiuntivo per Autostrade per l'Italia.

Al fine di garantire la massima qualità del servizio, la Committente si riserva di valutare, anche in corso di esecuzione, l'idoneità delle figure professionali effettivamente impiegate per l'esecuzione dell'appalto.
Ove la Committente ritenga che la/e figura/e professionale proposta/e o utilizzata/e non sia/siano idonea/e allo svolgimento delle attività previste, ne darà comunicazione all'Appaltatore che si impegna a reperire una nuova risorsa idonea entro il termine di 15 giorni lavorativi dalla predetta comunicazione e, se richiesto, a sospendere l'impiego - anche con effetto immediato - della risorsa ritenuta non adeguata.
L'eventuale sostituzione delle risorse nel Gruppo di Lavoro non deve pregiudicare il corretto svolgimento delle attività.

7. Erogazione dei servizi

7.1. Sede di lavoro e strumenti

La struttura EAC di ASPI svolge le proprie mansioni presso la sede della Direzione Generale di Firenze di Autostrade per l'Italia, Limite di Campi Bisenzio (FI).

I Servizi oggetto del presente Capitolato verranno erogati, per tutta la durata del contratto, presso la sede dell'Appaltatore.

Qualora attività di analisi o di approfondimento richiedano la presenza di personale dell'Appaltatore presso una delle altre sedi di Autostrade, le stesse verranno concordate tra il Direttore dell'Esecuzione di ASPI ed il Referente tecnico dell'Appaltatore. Il numero delle **giornate di trasferta presso altra sede di Autostrade per L'Italia** sarà in misura **non superiore al 5%** del totale delle giornate richieste.

L'Appaltatore dovrà provvedere in proprio alla postazione di lavoro necessaria allo svolgimento delle attività previste, rispettanti le *policy* di sicurezza di ASPI.

7.2. Orario di servizio

L'Appaltatore erogherà i Servizi secondo il seguente orario:

Orario base del Servizio	Note
Lunedì-Venerdì **(*)** - 07:30-20:30	Comprensivo dell'intervallo mensa

(*) *Sono escluse, salvo richieste specifiche, le festività nazionali di legge (es: 1° gennaio, 6 gennaio, Pasqua, 25 aprile, 1° maggio, 2 giugno, 15 agosto, 8 dicembre, 25-26 dicembre).*

7.3. Tabella dei servizi

Viene di seguito esposta la matrice relativa alle modalità di Attivazione e di Rendicontazione per le diverse tipologie di attività previste nel presente Capitolato:

Servizi	Modalità di Attivazione	Modalità di Rendicontazione
Storage in ambiente cloud	All'avvio del servizio	Triennale anticipata
Funzioni di navigazione in cloud	All'avvio del servizio	Triennale anticipata
Integrazione con AGE	Continuativa a ticket (Service Request/ Technical Request)	Mensilmente, in base all'effort sulle figure

I successivi paragrafi illustrano in dettaglio il processo di erogazione relativo a ciascun servizio.
Dovranno essere pertanto garantiti i requisiti di sicurezza previsti dall'appendice "Misure di Sicurezza".

7.4. Storage in ambiente cloud

Il fornitore metterà a disposizione di ASPI lo storage per complessivi 100Tb e fornirà il supporto e le istruzioni che consentiranno ad ASPI di caricare i dati lidar e le immagini sferiche nell'ambiente cloud con metodi e protocolli sicuri (es. FTPS, via browser o similari) che permettano la gestione di grosse moli di dati su canali asincroni.

Inoltre, ASPI potrà dover modificare o cancellare il contenuto di quanto già caricato per sostituire con dati più freschi tratte autostradali già rilevate e caricate in precedenza.

7.5. Funzioni di navigazione in cloud

L'ambiente web in cloud dovrà consentire la visualizzazione, la misurazione e il download di dati lidar, nei formati LAS, SHP, CSV, DXF, in sovrapposizione con le immagini sferiche 360.

L'accesso dovrà essere garantito a potenzialmente tutti gli utenti del Sistema AGE che desiderano collegarsi (mediante accesso con le credenziali federate). Alla data di settembre 2023 gli utenti registratati del Sistema AGE sono circa 2.500.

7.6. Integrazione con Sistema AGE

L'accesso all'ambiente web in cloud dovrà avvenire direttamente dal Sistema AGE sulla base delle coordinate GPS che caratterizzano la posizione a quel momento dell'utente in AGE. Sarà necessario che l'ambiente web metta a disposizione delle API o dei servizi web con cui AGE potrà passare le proprie coordinate GPS consentendo l'accesso all'utente nella stessa posizione della mappa AGE.

8. Modello di governance

Il modello di Governance è la struttura organizzativa, finalizzata alla gestione delle relazioni tra ASPI e il Fornitore.

Come previsto dal Codice degli Appalti, ASPI nominerà una figura che sarà indicata come **Direttore dell'Esecuzione del Contratto (DEC)** che coadiuverà il RUP nel coordinamento, direzione e controllo tecnico-contabile dell'esecuzione del contratto, in modo da assicurarne la regolare esecuzione. In particolare, il DEC ha la funzione di coordinare il team dei **Responsabili Informatici delle Applicazioni** (**RIA**) interni.

Il Fornitore, a sua volta, metterà a disposizione una figura di **Referente Tecnico (RT)**, unico per l'intera fornitura, a coordinamento di tutte le attività erogate, del team di specialisti esterni e chiamato a svolgere tutti gli adempimenti amministrativi.

DEC e RT si interfacceranno in maniera periodica e ogniqualvolta se ne presenti la necessità per supervisionare lo stato di avanzamento delle varie attività, per effettuare i consuntivi mensili, per risolvere problematiche emerse nell'erogazione dei servizi, ecc. come è descritto in dettaglio nel paragrafo relativo all'erogazione del coordinamento della fornitura.

9. Livelli di Servizio

I livelli di servizio (Service Level Agreement - SLA) sono misure concordate tra le Parti (relative ai processi di erogazione dei Servizi che saranno adottati e alla gestione del gruppo di lavoro) che consentono di quantificare e qualificare i Servizi erogati ad Autostrade per l'Italia.

Per i servizi oggetto della presente fornitura sono stati individuati SLA afferenti alle seguenti categorie:

- **Disponibilità dello storage in cloud (cifato)**. Per questa si adottano delle misure mensili dei tempi di disponibilità dello storage previsto (100 Tb complessivi), con percentuale di disponibilità maggiore del 98%
- **Raggiungibilità dell'ambiente web in cloud**. Per questa si adottano delle misure settimanali dei tempi di raggiungibilità dell'ambiente web in cloud, con percentuale di disponibilità maggiore del 98%, corrispondente a un'indisponibilità inferiore alle 2 ore all'interno di una settimana lavorativa.
    - A tal fine Autostrade utilizzerà il software di monitoraggio Zabbix
- **Corretto funzionamento dei servizi di integrazione con AGE:** Per questa sono state definite delle misure in relazione alla tempestività di risoluzione delle anomalie e del grado di correttezza della risoluzione.
- **Tutti i dati dovranno essere trattati, processati ed archiviati in ottemperanza alle normative vigenti, in particolare GDPR, con server in Europa;** dovranno inoltre essere adottate tutte le politiche necessarie a garantire il rispetto dei seguenti tempi di RPO (Recovery Point Objective) e RTO (Recovery Time Objective):

9.1. SLA per Disponibilità dello storage in cloud.

Percentuale di disponibilità rispetto ai 100 Tb previsti di spazio cloud	Penale applicata per ogni giorno di indisponibilità riscontrata a seguito di upload fallito nel cloud per mancanza di spazio
90% - 98%	200 € per ogni giorno di indisponibilità
80% – 90%	350 € per ogni giorno di indisponibilità
< 80%	500 € per ogni giorno di indisponibilità

9.2. SLA per disponibilità ambiente web in cloud per la visualizzazione, misurazione, download di dati lidar e immagini sferiche

Percentuale di disponibilità settimanale nell'orario indicato al paragrafo 7.2	Penale applicata per l'indisponibilità del sistema calcolata all'interno di una settimana lavorativa come indicato nel paragrafo 7.2
88% - 98%	1.000 € per ogni settimana di indisponibilità
< 88%	3.000 € per ogni settimana di indisponibilità

9.3. SLA per Corretto funzionamento dei servizi di integrazione con AGE

Severità degli errori

ASPI classifica le anomalie secondo una scala di severità che va da 1 a 3:

- **Severità 1:** Alta
- **Severità 2:** Media
- **Severità 3:** Bassa

sulla base di una serie di elementi quali: l'area applicativa interessata, la sua rilevanza aziendale, l'impatto che provocano, l'urgenza dichiarata dall'utente che ha aperto l'incident, il personale coinvolto, i tempi di risoluzione necessari, ecc.

Ai fini della determinazione dei livelli di servizio per la Manutenzione Correttiva dei sistemi nell'ambito della presente fornitura, la scala di severità verrà ridotta a tre sole fasce:

- **Severità 1:** errore/malfunzionamento grave che impedisce l'utilizzo di almeno una "funzionalità critica" per l'azienda, o per le aziende che usufruiscono dei servizi erogati da Autostrade per l'Italia, con impatto grave o paralizzante su tutte le operazioni utente; non è possibile giungere al risultato finale utilizzando funzionalità alternative.
- **Severità 2:** errore/malfunzionamento che limita l'utilizzo di almeno una "funzionalità critica" per l'azienda, ma consente comunque di proseguire le operazioni, seppure con serie limitazioni;
- **Severità 3:** errore/malfunzionamento e/o problemi di usabilità che causano un degrado di prestazione su una funzionalità con un degrado di prestazione tollerabile per periodi limitati. Non necessitano di intervento urgente.

L'Appaltatore fornirà ad Autostrade per l'Italia con frequenza mensile un consuntivo degli interventi di Manutenzione Correttiva per la relativa misurazione dei Livelli di Servizio.

In caso di mancato raggiungimento degli obiettivi, verrà indetta immediatamente una revisione straordinaria tra l'Appaltatore ed ASPI per esaminare le cause del mancato rispetto dei tempi ed attuare un piano di recupero.

In caso di mancato raggiungimento degli obiettivi, Autostrade potrà applicare le penali previste.

L'Appaltatore sarà sollevato dall'obbligo di soddisfare qualsiasi Livello di Servizio qualora si rilevi che il malfunzionamento sia causato da azioni o mancate azioni da parte di ASPI o inadempienze da parte di Terze Parti sotto diretto controllo di Autostrade per l'Italia, o circostanze di situazioni di emergenze, o eventi di forza maggiore.
Nell'ambito delle attività di Manutenzione Correttiva, i Livelli di Servizio minimi richiesti al Fornitore (SLA) sono descritti di seguito.

9.3.1. SLA_01_MC – Tempestività nella risoluzione delle anomalie

L'Appaltatore dovrà garantire un servizio tempestivo, definito tale se inferiore o uguale al tempo massimo previsto per la risoluzione dei malfunzionamenti in base alla priorità. Sono di seguito indicati i dettagli relativi allo SLA minimo:

Ambito		Manutenzione Correttiva	
KPI		SLA_01_MC	
Descrizione KPI		% risoluzione degli incident segnalati nei tempi richiesti	
Obiettivo KPI		Misurare la performance del fornitore per quanto riguarda le tempestività di risoluzione delle anomalie.	
Perimetro di applicazione		AGE	
Algoritmo		$SLA\_01\_MC = \frac{\text{N. Incident risolti nei tempi richiesti (mensile)}}{\text{N. Incident mensili}} \times 100$	
Sorgente informativa		Sistema di monitoraggio Autostrade	
Periodo di rilevazione		Misurazione e rilevazione mensile. Si fa riferimento a tutti e soli i malfunzionamenti chiusi dal Fornitore nel periodo di osservazione e all'intero ambito per il quale si svolge il servizio.	
Livello di Servizio minimo Richiesto	*Sev. 1*	8 ore lavorative	SLA_01_MC_1 ≥ 95%
	Sev. 2	20 ore lavorative	SLA_01_MC_2 ≥ 94%
	Sev. 3	32 ore lavorative	SLA_01_MC_3 ≥ 90%

Il Tempo di Risoluzione è il tempo, espresso in ore lavorative, che intercorre tra il momento della segnalazione dell'anomalia da parte di Autostrade e quello in cui l'Appaltatore individua e segnala la soluzione del problema.

Tutti i tempi sopra indicati sono da intendersi validi all'interno della finestra di orario standard giornaliero del servizio (vedi paragrafo 7.2), al netto della disponibilità di accesso al sistema, ove necessario e applicabile a malfunzionamenti delle applicazioni riproducibili nell'ambiente di sviluppo/test da parte del Fornitore.

Le sospensioni delle attività dovute a fattori esterni al team del Fornitore verranno annotate e detratte dal computo del tempo utilizzato per la risoluzione.

Per le anomalie di Severità 1, il Fornitore dovrà garantire, ove possibile, l'immediata soluzione del problema, ovvero, in accordo con Autostrade per l'Italia, la predisposizione di soluzioni provvisorie che permettano almeno il ripristino delle funzionalità degradate.

ID	Descrizione	SLA	Penale
SLA_01_MC_1	Rispetto dei tempi di risoluzione degli incident/incidenti gestiti nel mese	95,00%	0,1% (zero virgola uno per cento) del valore del contratto per ogni punto decimale percentuale di differenza rispetto al valore target.
SLA_01_MC_2	Rispetto dei tempi di risoluzione degli incident/incidenti gestiti nel mese	94,00%	0,1% (zero virgola uno per cento) del valore del contratto per ogni punto decimale percentuale di differenza rispetto al valore target.

SLA_01_MC_3	Rispetto dei tempi di risoluzione degli incident/incidenti gestiti nel mese	90,00%	**0,1% (zero virgola uno per cento)** del valore del contratto per ogni punto decimale percentuale di differenza rispetto al valore target.

Le suddette penali verranno applicate come di seguito indicato:
Ad esempio, laddove, a seguito di rilevazione mensile, risulti che relativamente allo SLA_01_MC_1, il livello raggiunto sia 94,50% rispetto al 95,00% target, la penale da applicare sarà:
95,00% - 94,50% = 0,50% => 5 punti decimali di differenza
Penale = 5 x [0,1% del valore complessivo del contratto] = 0,5% del valore complessivo del contratto.
Laddove, in offerta tecnica, l'Appaltatore abbia indicato degli SLA migliorativi rispetto agli SLA_01_MC_1, SLA_01_MC_2 e SLA_01_MC_3, le penali troveranno applicazione, con le medesime modalità, con riferimento agli SLA migliorativi indicati dall'Appaltatore.

10. Garanzia

Gli interventi a seguito di attività di nuovi sviluppi e di manutenzione evolutiva, sulla base degli ordinativi di lavoro, saranno considerati operativi alla data di accettazione dei relativi prodotti, o in alternativa il loro uso produttivo, ed è previsto un periodo di 12 (dodici) mesi di garanzia a partire da tale data.

In detto periodo l'Appaltatore correggerà, tempestivamente ed a sua cura e spese, tutte quelle parti per le quali si dovessero riscontrare vizi e/o errori delle attività compiute, fatti salvi i casi in cui gli stessi derivino da cause a lui non imputabili.

La garanzia decade:

- qualora si rilevi che il malfunzionamento sia causato da azioni o mancate azioni da parte di ASPI o inadempienze da parte di Terze Parti sotto il controllo di Autostrade per l'Italia, o circostanze di situazioni di emergenze, o eventi di forza maggiore.
- sui programmi o parte degli stessi modificati da ASPI e da Terze Parti sotto il controllo di Autostrade per l'Italia, senza coinvolgimento ed accordo con il Fornitore.
- sui programmi o parte degli stessi eseguiti su piattaforme hardware/software diverse da quelle prescelte per la realizzazione dei programmi.

Appendice "Misure di Sicurezza"

Ambito	Categoria	ID	Clausole di sicurezza
Misure tecniche	Protezione da malware	1	I sistemi del Contraente devono essere protetti contro i malware mediante l'utilizzo di idonei strumenti di protezione come, ad esempio, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), antivirus e anti-malware mantenuti costantemente aggiornati. In particolare, sono adottate adeguate misure di sicurezza per prevenire, rilevare ed eliminare virus informatici o altri programmi dannosi. Il Contraente mantiene costantemente aggiornati i sistemi operativi, gli antivirus, i firewall ed altri programmi per la sicurezza delle informazioni e dei dati personali.
Misure tecniche	Credenziali di autenticazione	2	Il Contraente che accede ai sistemi del Committente si impegna a comunicare tempestivamente al Committente i casi di trasferimento e cessazione dell'operatività del personale coinvolto nell'erogazione del servizio, al fine di consentire al Committente una corretta gestione delle utenze e dei relativi privilegi di accesso.
Misure tecniche	Credenziali di autenticazione	3	I sistemi del Contraente devono essere configurati con modalità atte a consentire l'accesso unicamente a soggetti dotati di credenziali di autenticazione univoche (username e password), non riassegnabili agli utenti neppure in tempi diversi al fine di evitare che accessi indebiti ai sistemi del Contraente diano accesso ai dati del Committente.
Misure tecniche	Credenziali di autenticazione (Cloud)	4	Nell'ambito dell'erogazione dei servizi cloud, il Contraente deve garantire la registrazione/de-registrazione degli utenti interni al Committente ai vari servizi in cloud.
Misure tecniche	Password	5	Le password utilizzate dal Contraente sui propri sistemi devono presentare, al minimo, le seguenti caratteristiche di sicurezza di base: - obbligo di modifica al primo accesso; - lunghezza minima; - regole di complessità - scadenza - history - valutazione contestuale della robustezza e archiviazione dell'hash. Deve essere imposto un formato della password per evitare l'utilizzo di password banali o che contengano riferimenti agevolmente riconducibili all'utente al fine di garantire che le password siano adeguatamente robuste. Inoltre, il Contraente assicura che le password non siano salvate né trasmesse in chiaro. Il Contraente si assicura che tutti gli utenti siano sensibilizzati circa le modalità di conservazione sicura delle password, come ad esempio: evitare di comunicare a terzi la propria parola chiave, modificare la password in caso di compromissione, etc..

Misure tecniche	Password	6	Il Contraente deve assicurare che le password utilizzate per accedere ai sistemi del Committente non siano salvate né trasmesse in chiaro. Il Contraente, inoltre, assicura che tutti gli utenti siano sensibilizzati circa le modalità di conservazione sicura delle password.
Misure tecniche	Log Management	8	I sistemi del Contraente sono configurati con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze, incluse quelle degli Amministratori di Sistema, e protetti da adeguate misure di sicurezza che ne garantiscono l'integrità, la riservatezza e la disponibilità. Il Contraente implementa un set di log standard che consentono di monitorare una serie di eventi e rilevare eventuali attacchi. I log sono analizzati con adeguata frequenza e con strumenti automatici (es. sistema centralizzato di Security Information and Event Management) al fine di verificare che non ci siano state anomalie.
Misure tecniche	Log Management (Cloud)	10	Il Contraente che eroga servizi Cloud garantisce che i sistemi e/o applicazioni sono configurati con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze, incluse quelle degli Amministratori di Sistema, e protetti da adeguate misure di sicurezza che ne garantiscono l'integrità, la riservatezza e la disponibilità. Il Contraente implementa un set di log standard che consentono di monitorare una serie di eventi e rilevare eventuali attacchi. Il Committente ritiene sufficiente il seguente set di log: - Autenticazione - Autorizzazione - Gestione della configurazione - Attività degli amministratori - Gestione degli accessi - Attività svolte sui dati con particolare attenzione ai dati personali - Utilizzo di funzionalità a più alto rischio - Connessioni di rete Inoltre, il Committente può verificare se tale set di log è sufficiente e in linea con le proprie politiche; diversamente, deve definire con il Contraente i requisiti per la registrazione degli eventi e verificare che il servizio soddisfi tali requisiti. Il Contraente che eroga servizi Cloud garantisce l'adozione di un sistema centralizzato di event logging e dà la possibilità al Committente di esportare i log sui propri sistemi, secondo quanto richiesto dalle soluzioni tecnologiche adottate dal committente.
Misure tecniche	Continuità Operativa	11	Il Contraente adotta idonee misure per garantire il ripristino dell'accesso ai dati del Committente in tempi certi in caso di danneggiamento degli stessi (es. procedure di backup, prove di ripristino dei dati, etc.). Sono predisposti dal Contraente un piano di continuità operativa e di disaster recovery che comprendono le attività per rispondere, recuperare, riprendere e ripristinare a un livello predefinito i servizi a seguito di un'interruzione degli stessi anche nel caso di eventi avversi di portata

			rilevante, applicando le buone pratiche presenti nello standard ISO/IEC 22313.
Misure tecniche	Continuità Operativa	12	Il contraente garantisce una continuità operativa in linea con il capitolo 9 livelli di servizio
Misure tecniche	VA/PT	14	Il Contraente adotta sui propri sistemi e applicazioni misure utili a identificare immediatamente le vulnerabilità non appena diventano note e procede con gli opportuni aggiornamenti per risolvere le vulnerabilità. Il Contraente effettua periodicamente attività di analisi delle vulnerabilità tecniche, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco. I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e attuare le migliorie necessarie a garantire il livello di sicurezza atteso. Il Contraente si impegna ad installare le patch di sicurezza disponibili per i componenti del sistema e i programmi software in uso; devono essere eseguiti appropriati test prima della loro distribuzione.
Misure tecniche	Amministratori di Sistema	18	Il Contraente implementa policy e procedure interne per garantire, mediante validi documenti identificativi, la corretta identificazione e profilazione degli utenti inclusi quelli privilegiati (es. amministratori di sistema, utenti di emergenza, utenze tecniche), distinguendo fra utenti interni ed esterni, laddove applicabile, che accedono alle componenti di sistema che gestiscono i dati del Committente.
Misure tecniche	Amministratori di Sistema	19	Il Contraente, al quale sono stati assegnate una o più utenze con privilegi amministrativi per accede ai sistemi del Committente, si impegna a mantenere e aggiornare la lista delle utenze attive e a richiedere al Committente le sole abilitazioni necessarie a svolgere le mansioni che gli sono assegnate in coerenza con i principi del need to know e least privilege.

Misure tecniche	Gestione degli incidenti	20	Il Contraente definisce le regole che le proprie strutture aziendali devono seguire per assicurare una risposta rapida ed efficace a fronte del verificarsi di un incidente relativo alla sicurezza delle informazioni; Tali regole devono prevedere l'implementazione di sistemi e l'esecuzione di attività in linea con quanto definito all'interno delle Condizioni Generali di Acquisto e coerenti con quanto raccomandato dagli standard di sicurezza internazionali (p.e. ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 27035), e garantire la notifica degli stessi al Committente nel rispetto di quanto previsto nell'atto di nomina ex art. 28 GDPR e all'art. 33 GDPR laddove siano coinvolti dati personali del Committente. Il Contraente assicura la massima trasparenza nella gestione degli eventi di sicurezza, garantendo al Committente appropriata visibilità dei processi di issue tracking e assistenza tecnica. Il Contraente deve definire le tempistiche per la presa in carico e gestione degli eventi di sicurezza in funzione di diverse priorità, dichiarando i livelli di servizio garantiti.
Misure tecniche	Gestione dei supporti rimovibili	21	Il Contraente definisce le modalità di gestione sicura dei supporti rimovibili (dispositivi portatili, dischetti, CD, DVD ecc.), per proteggere i supporti e formattarli. I supporti rimovibili se non utilizzati sono distrutti o resi inutilizzabili, altrimenti possono essere riutilizzati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Misure tecniche	Sicurezza Fisica	22	L'accesso fisico ai locali e ai Data Center del Contraente deve essere regolato da procedure interne e limitato ai soli soggetti autorizzati. Il Contraente che assegna servizi di Data Center a sub-fornitori nominati sub-responsabili, deve garantire che questi ultimi implementino appropriate e idonee misure di sicurezza per assicurare nel tempo la riservatezza, la disponibilità e l'integrità dei dati personali ivi conservati e trattati, ai sensi dell'art. 32 GDPR. Anche in tale caso l'accesso ai data center dovrà essere regolato da procedure interne e limitato ai soli soggetti autorizzati.
Misure tecniche	Sicurezza Fisica	23	Il Contraente che eroga servizi ICT nell'ambito dei quali tratta dati riservati del Committente, rende nota la localizzazione dei propri data center e degli end-point all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup).
Misure tecniche	Sicurezza Fisica	24	Il Contraente che eroga servizi Cloud rende nota la localizzazione dei data center propri e/o dell'infrastruttura Cloud utilizzata per erogare anche parzialmente il servizio e/o all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup).

Misure tecniche	Sicurezza delle comunicazioni	26	Il Contraente adotta protocolli di comunicazione sicuri sui propri sistemi e in linea con quanto la tecnologia rende disponibile. Il Contraente, inoltre, prevede l'utilizzo di canali di comunicazione cifrati e sicuri per lo scambio di informazioni verso l'esterno e l'interno, adeguati alla criticità delle informazioni trattate. Inoltre, i flussi di dati da e verso i sistemi in cloud esposti su internet sono protetti utilizzando un canale sicuro TLS in modo da assicurare: - autenticazione del server con algoritmo di cifratura asimmetrica, considerata ragionevolmente sicura alla data (e.g. chiave da almeno 2048 bit); - cifratura della sessione con algoritmo di cifratura simmetrico, considerato ragionevolmente sicuro alla data, con una chiave di sessione di almeno 128 bit.
Misure tecniche	Crittografia	27	Il Contraente implementa misure tecniche di crittografia sui propri sistemi adottando meccanismi di cifratura con un livello di robustezza adeguato rispetto alla criticità delle informazioni trattate. Il Contraente deve garantire la sicurezza dei dati del Committente in transito attraverso adeguati meccanismi di cifratura. Inoltre, il Contraente deve trasmettere i dati del Committente su canali cifrati, attraverso l'utilizzo di protocolli di comunicazione sicuri (es. SFTP, HTTPS, SSH, VPN).
Misure tecniche	Crittografia (Cloud)	29	Il Contraente che eroga servizi Cloud tramite servizi SaaS e PaaS dichiara quale tipo di crittografia utilizza per proteggere la riservatezza dei dati scambiati.
Misure tecniche	Network	31	Il Contraente deve adottare misure di sicurezza adeguate a prevenire e mitigare qualsiasi evento di sicurezza che potrebbe compromettere le funzionalità delle proprie componenti di rete tra cui, firewall, sonde IPS (i.e. Intrusion Prevention System), strumenti di analisi del traffico, limitazioni del traffico in entrata e in uscita da-verso reti non attendibili etc. Il Contraente deve implementare misure tecniche di difesa in profondità (ad es. deep packet analysis, strozzatura del traffico e black-holing) e appropriate misure di sicurezza per rilevare e rispondere tempestivamente agli attacchi di rete (es. MAC spoofing, ARP poisoning) per garantire la continuità del servizio fornito in caso di attacchi DoS (Denial of Service) in grado di avere un impatto sulla disponibilità del servizio erogato al Committente. I sistemi di rilevamento intrusione sono mantenuti aggiornati in relazione alle migliori tecnologie disponibili. Il Contraente assicura la segregazione delle reti da quelle utilizzate dal Committente.
Misure tecniche	Network	32	Il Contraente che eroga servizi Cloud assicura l'osservanza di una Policy di sicurezza delle informazioni per la configurazione delle reti virtuali VLAN.
Misure tecniche	Change Management	33	Il Contraente implementa un processo di Change Management per la gestione tempestiva ed efficiente di ogni cambiamento nell'ambito della propria infrastruttura, al fine di garantire che modificando il sistema del contraente non vengano impattati i dati e i sistemi del Committente.

Misure tecniche	Change Management	**34**	Il Contraente implementa un processo di Change Management, al fine di garantire che vengano utilizzate procedure e metodi standard per la gestione tempestiva ed efficiente di ogni cambiamento nell'ambito dell'erogazione del servizio effettuato sull'infrastruttura del Committente. Inoltre, il Contraente garantisce la disponibilità tempestiva di informazioni al Committente circa i cambiamenti e le migliorie introdotte in seguito ad aggiornamenti apportati alle modalità di funzionamento e fruizione dei servizi erogati. È definito un periodo temporale prima del quale il Contraente deve dare comunicazione al Committente degli interventi di manutenzione attraverso un canale di comunicazione diretto.
Misure tecniche	Change Management	**35**	Il Contraente che eroga servizi Cloud garantisce l'applicazione di misure di sicurezza per separare logicamente l'ambiente virtuale del Committente da quello di altri Clienti e impedire di accedere o esporre il contenuto a persone non autorizzate.
Misure tecniche	Hardening	**36**	Il Contraente pone in essere apposite attività di hardening sui propri dispositivi finalizzate a prevenire il verificarsi di eventi avversi minimizzando le debolezze architetturali dei sistemi operativi, delle applicazioni e degli apparati di rete. Qualora non fossero presenti le procedure, è necessaria la predisposizione del software di base in modalità sicura attraverso, a titolo esemplificativo e non esaustivo, l'eliminazione dei servizi non necessari, l'eliminazione delle utenze non necessarie, la modifica delle password di default, etc.
Misure tecniche	Sincronizzazione degli orologi	**37**	Tutti i sistemi cloud del Contraente utilizzano il protocollo sicuro per la sincronizzazione degli orologi. Il fuso orario utilizzato è CEST.
Misure organizzative	Ruoli e responsabilità	**43**	Il Contraente identifica e comunica al Committente un referente per la sicurezza delle informazioni responsabile del coordinamento e del monitoraggio delle norme e procedure sulla sicurezza e che svolgerà il ruolo di interfaccia con il team di security del Committente.
Misure organizzative	Gestione e utilizzo dotazioni informatiche	**44**	Relativamente ai servizi IT il Contraente applica regolamenti che tutti gli utenti con accesso ai sistemi informativi devono rispettare per il corretto utilizzo delle dotazioni informatiche aziendali, al fine di ridurre il rischio di un loro utilizzo non corretto, intenzionale o involontario, e di assicurare che il sistema informativo ed informatico del Contraente sia salvaguardato e gestito correttamente.
Misure organizzative	Focal point incidenti di sicurezza	**45**	Il Contraente deve individuare un Focal Point con cui il Committente possa dialogare in caso di incidente sui sistemi del Contraente. In particolare, il Contraente deve rendere disponibile il contatto di tale Focal Point al Committente.
Misure organizzative	Autorizzazione accessi	**46**	Il Contraente deve autorizzare gli accessi agli ambienti contenenti dati del Committente al proprio personale secondo i principi del "need to know" e del "least privilege", assegnando in modo univoco i diritti di accesso ad ogni user account. Il Contraente deve, dunque, definire criteri e politiche di assegnazione dei privilegi d'accesso che garantiscano l'adozione del criterio della separazione dei compiti. Per gli accessi logici il Contraente definisce una procedura interna per la

			gestione del ciclo di vita delle utenze che comprende, tra le altre, le fasi di creazione, disabilitazione temporanea, disabilitazione definitiva, modifica del profilo di autorizzazione dell'utenza e revisione periodica. I profili di autorizzazione sono definiti in funzione delle mansioni assegnate in modo da consentire l'accesso ai soli dati necessari per espletare le mansioni oggetto del contratto. Tali profili sono oggetto di controlli periodici. Quando l'accordo è risolto per qualsiasi ragione o è scaduto, tutti gli accessi ai dati del Committente devono essere immediatamente revocati. Tutte le informazioni e i dati del Committente in possesso del Contraente devono essere restituiti al Committente, se richiesto, e poi, salvo eventuali obblighi di legge, essere rimossi e cancellati in modo sicuro (p.e. wiping) dai dispositivi del Contraente.
Misure organizzative	IAM	47	Il Contraente, nel caso di erogazione di servizi applicativi che prevedono l'utilizzo di credenziali di accesso ai sistemi del Committente, deve garantire l'integrazione con il sistema di Identity e Access Management del Committente in modo tale da permettere al Committente di gestire l'autenticazione e i profili di accesso degli utenti.
Misure organizzative	Provisioning e Deprovisioning utenze	48	Per gli accessi logici il Contraente definisce una procedura per la gestione del ciclo di vita delle utenze che comprende, tra le altre, le fasi di creazione, disabilitazione temporanea, disabilitazione definitiva, modifica del profilo di autorizzazione dell'utenza e revisione periodica. I profili di autorizzazione sono definiti in funzione delle mansioni assegnate in modo da consentire l'accesso ai soli dati necessari per effettuare le operazioni relative ai trattamenti di competenza. Tali profili sono oggetto di controlli periodici.
Misure organizzative	Gestione interventi di assistenza IT	49	Gli interventi di assistenza garantiscono l'esecuzione delle sole attività previste contrattualmente per impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Committente. Il Contraente fornisce la documentazione tecnica, le guide d'uso e/o altro materiale di supporto, ivi compresa la documentazione dettagliata delle API e delle interfacce CLI, GUI e SOAP/REST, se previste dal servizio. Il supporto deve essere accessibile mediante opportuni canali di comunicazione e adeguati sistemi di gestione (issue tracking), al fine di consentire al Committente di effettuare in completa autonomia le segnalazioni di malfunzionamenti e potenziali pericoli per la sicurezza e la fruibilità del servizio.

Misure organizzative	Change Management	**51**	Il Contraente deve applicare una specifica procedura di gestione dei cambiamenti in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa. Il Contraente integra i processi di Project Development e Change Management con i principi di privacy by design/by default. In particolare, sin dalla fase di progettazione di una nuova iniziativa e per l'intero ciclo di vita dei dati personali coinvolti: - definisce chiari obiettivi di protezione quali la riservatezza, l'integrità e la disponibilità dei dati personali; - prevede (implementa e testa) misure tecnico-organizzative di sicurezza volte ad attuare in modo efficace i principi di protezione dei dati personali e la tutela dei diritti degli interessati e garantisce che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità di trattamento (principio di minimizzazione).
Misure organizzative	Sviluppo sicuro e test per servizi IT	**54**	L'ambiente di sviluppo software del Contraente è accessibile esclusivamente al personale a ciò preposto. Il processo di sviluppo del Contraente segue rigide linee guida di sviluppo sicuro finalizzate a garantire il rispetto dei principi di Security by Design, pertanto, deve integrare i processi e gli strumenti per il Secure Software Development Lifecycle (SDLC) con controlli / requisiti di sicurezza appropriati (es. Source Code Security Analysis). Il test del codice segue un processo predefinito finalizzato a valutare sia la funzionalità del codice sia la presenza di vulnerabilità gravi. L'iter approvativo per il passaggio in produzione viene opportunamente tracciato. Tutti i test effettuati, i risultati ed eventuali piani di rimedio devono essere tracciati su un apposito registro custodito in sicurezza. Gli ambienti di sviluppo, test e produzione sono fisicamente e logicamente separati.
Misure organizzative	Formazione	**55**	Il Contraente eroga periodicamente ai propri dipendenti coinvolti nelle attività di gestione dei servizi corsi sulla sicurezza delle informazioni e sulla corretta gestione dei dati personali nonché sulle proprie politiche e procedure pertinenti il servizio erogato.
Misure organizzative	Audit Interni	**56**	Il Contraente assegna a personale esterno qualificato l'esecuzione di audit interni sulla sicurezza delle informazioni e sulla privacy; la periodicità di tali attività è specificata nel programma almeno annuale degli audit.