



Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico

Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane

Capitolato tecnico



Sommario

1. Glossario	3
2. Obiettivo e ambito di applicazione	4
2.1 Ambito di applicazione.....	5
3. Oggetto	6
4. Requisiti della Piattaforma a supporto del processo di Smart Recruiting	12
4.1 Classificazione dei Requisiti.....	12
4.2. Requisiti funzionali della Piattaforma	13
4.3 Requisiti tecnici della Piattaforma	17
4.3.1 Requisiti tecnici applicativi.....	17
4.3.2 Requisiti tecnici architetturali della Piattaforma SaaS.....	24
4.3.3 Requisiti organizzativi.....	50
4.4 Requisiti relativi alla qualità della fornitura	61
4.5 Requisiti relativi Sostenibilità e Codice Etico	63
5. Attività	65
5.1. Attività e requisiti per il Set-up della Piattaforma	65
5.2. Attività e requisiti per la messa a regime e funzionamento della Piattaforma	68
5.3 Attività di dismissione della Piattaforma.....	70
6. Monitoraggio del servizio e livelli di servizio attesi	71
6.1 KPI e Livelli di servizio attesi.....	71
7. Penali	80
8. Data Protection	83
8.1 Obiettivi	83
8.2 Requisiti relativi ad aspetti organizzativi.....	86
8.3 Modello di interazione	87
8.4 Riservatezza e identificazione delle persone autorizzate al trattamento.....	87
8.5 Requisiti relativi ad aspetti tecnici.....	89
8.6 Progettazione del trattamento e protezione dei dati personali	89
8.7 Esercizio dei Diritti da parte degli interessati	90
8.8 Pronta notifica	91
8.9 Audit di Data Protection.....	93
8.10 Processo di rilevazione e segnalazione del Data Breach.....	93



1. Glossario

Cloud: Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio.

Private cloud: il private cloud consiste nell'accesso tramite rete ad un insieme di risorse informatiche offerte da un gestore e dedicate ad una specifica organizzazione cliente. Questa soluzione consente l'ottenimento dei benefici derivanti dal cloud computing, quali l'elasticità ed il self-service, pur preservando un alto livello di controllo sulla Piattaforma fornita, in termini di sicurezza, prestazioni e gestione dati.

SaaS (Software as a Service): con il termine SaaS si fa riferimento al modello di distribuzione di un'applicazione o servizio. Il modello di servizio "Software as a Service" prevede che il servizio sia un'applicazione software utilizzabile su richiesta. Il fornitore del servizio gestisce l'infrastruttura (computer server, dati, firewall e load balancer) e la Piattaforma (il middleware costituito da framework e strumenti di sviluppo), installa l'applicazione e ne consente l'accesso ai clienti mediante interfaccia web.

Sistema di Talent Acquisition (TA): software per la gestione dei processi di ricerca e selezione dei candidati sia da mercato esterno che da job posting interno. La soluzione consente di gestire il Data Base con i CV dei candidati sia esterni sia interni, e l'intero iter di selezione, dall'identificazione dei bisogni alla selezione ed inserimento dei nuovi dipendenti, tracciando ogni fase del processo fino all'assunzione o, nei casi di Job Posting interno, fino all'assegnazione del dipendente a nuova struttura organizzativa.



2. Obiettivo e ambito di applicazione

Ferservizi SpA (di seguito, per brevità, “Ferservizi”), Società con socio unico soggetta alla direzione e coordinamento di Ferrovie dello Stato Italiane SpA, in nome e per conto di FSTechnology S.p.A., intende procedere all’affidamento per la fornitura di una Piattaforma, e relativi servizi, per la somministrazione, attraverso strumenti digitali, di test e video colloqui per la pre-selezione di candidati aventi profili in linea con le ricerche di personale attivate dalle Società del Gruppo Ferrovie dello Stato Italiane tramite procedura aperta svolta in modalità telematica.

Le prestazioni oggetto della procedura saranno affidate alle condizioni previste nel presente Capitolato Tecnico, nel Disciplinare di gara, e relativi allegati e nello Schema di Accordo Quadro e relativi allegati nonché nei Regolamenti disponibili al seguente indirizzo: [Supplier Station Gruppo FS](#).

L’invio dell’offerta comporta l’assunzione da parte del mittente della qualifica di “Concorrente”, ai fini di quanto di seguito descritto.



2.1 Ambito di applicazione

La Piattaforma dovrà garantire la gestione delle attività sintetizzate in Figura 1.

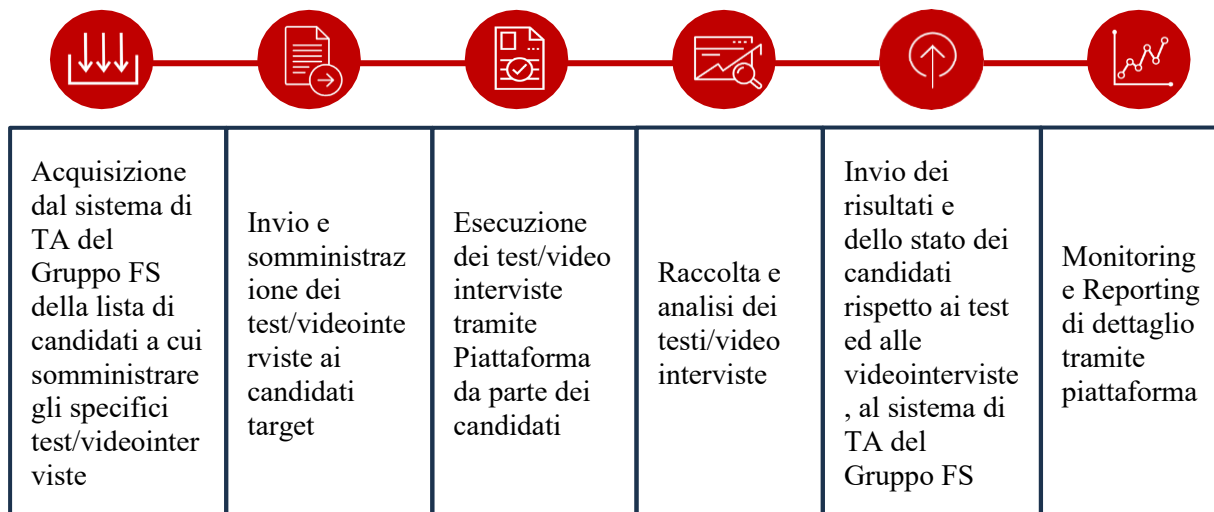


Figura 1 – Fasi di processo

FASE 1 – Acquisizione dal sistema di Talent Acquisition (TA) del Gruppo FS della lista di candidati a cui somministrare gli specifici test e video interviste: la Piattaforma deve consentire l'integrazione con il sistema di TA per l'acquisizione dell'elenco dei candidati a cui somministrare gli specifici test e/o video interviste.

FASE 2 – Invio e somministrazione dei test/video interviste ai candidati target: la Piattaforma deve consentire l'invio e la somministrazione dei test e delle video interviste ai candidati secondo le specifiche definite (data inizio/data fine della disponibilità dei test e video intervista, punteggio previsto, eventuale giudizio qualitativo, ecc...).

FASE 3 – Esecuzione dei test/ video interviste tramite Piattaforma da parte dei candidati: i candidati devono poter effettuare i test e le video interviste tramite la Piattaforma.

FASE 4 – Raccolta e analisi dei risultati dei test/video interviste: la Piattaforma deve consentire di raccogliere e analizzare i risultati dei test/ videointerviste dei candidati.

FASE 5 – Invio dei risultati e dello stato dei candidati rispetto ai test e alle video interviste al sistema di Talent Acquisition del Gruppo: la Piattaforma deve mettere a disposizione del sistema di Talent Acquisition i risultati conseguiti e lo stato dei candidati.

FASE 6 – Monitoring e reporting di dettaglio tramite Piattaforma: la Piattaforma deve consentire il monitoraggio e l'analisi dei dati raccolti, relativi all'intero processo di Smart Recruiting.



3. Oggetto

La fornitura concerne l'affidamento per la fornitura di una Piattaforma, e relativi servizi, per la somministrazione, attraverso strumenti digitali, di test e video colloqui da considerarsi "prove" a cui sottoporre i candidati per la preselezione di quelli aventi profili in linea con i ruoli professionali di interesse per le Società del Gruppo Ferrovie dello Stato Italiane.

L'attività di digital testing e somministrazione di video interviste viene stimata in **50.000 test per anno**. Rispetto ai volumi di testing, è richiesto un approccio "flat" per candidato, con la possibilità di somministrare tutte le tipologie di test necessarie, nonché di video interviste senza vincoli economici.

A tal fine, la Piattaforma deve fornire un catalogo di test certificati e funzionalità di video intervista. La componente di test dovrà assicurare la disponibilità di una ampia libreria certificata sia per la scientificità che per l'attendibilità.

Relativamente alla Piattaforma, la fornitura dovrà essere erogata in modalità Software as a Service (SaaS) e la soluzione dovrà essere integrabile con il sistema di Talent Acquisition in uso nel Gruppo FS.

Attraverso il proprio sistema master di Talent Acquisition, il Gruppo FS gestisce in modo centralizzato l'intero processo della selezione di personale da mercato sia interno che esterno. Il sistema, partendo dalla formalizzazione dell'esigenza (Job description; nr di risorse ricercate; Divisione/Direzione richiedente; data necessità; ecc), copre le ulteriori fasi di:

1. definizione e pubblicazione dell'annuncio di ricerca
2. screening dei candidati con CV in linea con la ricerca
3. gestione dell'iter di selezione dei candidati
4. gestione dell'iter di preassunzione (nel caso di candidati esterni).

Le fasi indicate ai punti 2 e 3 dovranno essere supportate dall'erogazione di prove (rappresentate da test digitali e/o video interviste) somministrate mediante la Piattaforma a supporto del processo di Smart Recruiting.

In particolare, attraverso il sistema master di Talent Acquisition verrà identificato, in funzione del Job Profile ricercato e della Società interessata alla ricerca: il set di test e/o video interviste da somministrare, i candidati coinvolti, la data di attivazione e l'eventuale data di scadenza dei test/video interviste.

Tale insieme di dati sarà inviato alla piattaforma di digital test e video interviste, la quale invierà notifica al candidato per l'accesso profilato alle prove.

Completate le prove un flusso di ritorno garantirà l'acquisizione dei risultati sul sistema Talent Acquisition.



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

Il fornitore della Piattaforma di test digital e video interviste dovrà inoltre garantire: il servizio di setup ovvero della personalizzazione della piattaforma secondo i requisiti indicati nel presente capitolato tecnico e dalle esigenze espresse dal committente durante la fase di predisposizione del *Piano di Lavoro, Progettazione, Configurazione e Attivazione*, i servizi inerenti l'esercizio della piattaforma secondo i requisiti espressi dal committente, l'assistenza ed il supporto ai candidati esterni ed ai recruiter utilizzatori del Back End della soluzione, il servizio di manutenzione evolutiva, ed i servizi progettuali opzionali che si renderanno necessari durante le fasi di esercizio e dismissione della piattaforma.

Pertanto, la fornitura oggetto della presente gara, in sintesi, si riassume come segue:

- Fornitura della **Piattaforma a supporto del processo di Smart Recruiting**, da erogarsi secondo le modalità SaaS (Software as a Service) per la durata di **36 mesi ed opzionalmente per un massimo di ulteriori 36 mesi**.

Si precisa che la soluzione SaaS offerta, non dovrà comportare alcun investimento in infrastrutture, hardware e licenze software per il Gruppo FS in quanto la gestione dell'intera architettura tecnica ed applicativa sarà a carico del Service Provider assegnatario. La Piattaforma dovrà rispondere ai requisiti espressi nel presente capitolato;

- **Servizi professionali** per le seguenti attività:
 - Setup iniziale, da quotare a forfait;
 - Servizi per l'esercizio della piattaforma inclusi nel canone di utilizzo della piattaforma espresso nella tariffa flat per candidato;
 - Servizi di supporto agli utenti interni ed esterni (candidati) inclusi nel canone di utilizzo della piattaforma espresso nella tariffa flat per candidato;
 - Servizi progettuali opzionali per lo sviluppo della piattaforma, da quotare utilizzando le tre figure professionali indicate nel capitolato;
 - Servizi progettuali opzionali per la dismissione della stessa da quotare utilizzando le tre figure professionali indicate nel capitolato;
 - progettazione d e messa in esercizio nonché l'addestramento degli utenti preposti;

Tutti i servizi professionali dovranno essere erogati attraverso tre tipologie di figure professionali:

- Project Manager;
- Senior Specialist;
- Junior Specialist;



La soluzione SaaS dovrà prevedere il tipico ciclo di vita contraddistinto dalle seguenti fasi:

Predisposizione (o provisioning): la predisposizione delle risorse Cloud infrastrutturali necessarie all'installazione ed erogazione della soluzione SaaS. Tipicamente si tratta di risorse virtuali di tipo computazionale, di storage e di rete.

Dispiegamento (o deployment): fase in cui avviene da parte del fornitore SaaS l'installazione e la configurazione dei moduli e componenti applicativi che costituiscono la soluzione SaaS.

Esercizio: fase in cui la soluzione SaaS è fruibile da parte dell'acquirente che è in grado di utilizzarla secondo quanto previsto contrattualmente.

Manutenzione: fase costituita da brevi periodi temporali in cui la soluzione SaaS esce dalla fase di esercizio risultando non fruibile da parte dell'acquirente in occasione di attività di aggiornamento, manutenzione o risoluzione di malfunzionamenti da parte del fornitore SaaS; al termine di tali brevi periodi si avrà nuovamente una regolare fase di esercizio.

Disattivazione: fase di terminazione della fornitura in seguito alla quale la soluzione SaaS non sarà più utilizzabile dall'acquirente.



In conformità con tale ciclo di vita, il Service Provider dovrà svolgere le seguenti attività:

- **Attività di set up** (attività necessarie per la messa in opera della Piattaforma di Smart Recruiting) consistente in:
 - a) *Fornitura di un Piano di Lavoro, Progettazione, Configurazione e Attivazione*: il Service Provider dovrà presentare ai referenti di Ferrovie dello Stato Italiane un **Piano di Lavoro (PDL)**, così come indicato al paragrafo 5.1 punto P.1 del Capitolato Tecnico. Successivamente all'approvazione del Piano di Lavoro (PDL), il Service Provider dovrà produrre un **documento di progettazione della soluzione**, con documentazione tecnica a supporto, così come indicato al paragrafo 5.1 punto P.2 del Capitolato Tecnico. Il Service Provider, una volta ricevuta l'approvazione del documento di progettazione della soluzione, dovrà procedere con le **attività di configurazione e attivazione** della stessa. Tali attività termineranno con la **fase di collaudo**, così come indicato al paragrafo punto P.3 del presente documento. Nelle more della realizzazione dell'integrazione tra il sistema master di Talent Acquisition e la Piattaforma, dovrà essere garantita la erogazione dei test e delle video interviste ai candidati e il ritorno dei risultati sul sistema master, mediante file con tracciati di tipo CSV;
 - b) *Formazione per gli utenti interni del Gruppo FS* che interagiranno con la Piattaforma, inclusa la fornitura del **manuale utente** e materiale multimediale come tutorial a supporto delle attività utente esercitate a sistema, sviluppati a valle degli interventi di personalizzazione effettuati.

L'attività di set up, comprensiva della formazione, avrà una **durata massima di 3 mesi**, dovrà essere valutata economicamente a forfait, quindi onnicomprensiva di tutti i servizi professionali, e si considererà conclusa con il superamento positivo del Collaudo.



- **Attività di esercizio della Piattaforma** (attività necessarie che sono richieste a partire dal positivo collaudo della Piattaforma):
 - a) *Supporto agli utenti finali*: nel corso del periodo di sottoscrizione del servizio, il service Provider dovrà garantire la necessaria assistenza operativa agli utenti finali, come definito al paragrafo 5.2.1 del presente documento;
 - b) *Operazioni di gestione della Piattaforma*: il Service Provider dovrà garantire l'esecuzione di tutte le attività necessarie all'ottimale funzionamento della Piattaforma, ivi inclusa la manutenzione da realizzarsi attraverso l'installazione tempestiva di eventuali aggiornamenti, la sistemazione di bug, l'installazione di patch di sicurezza, la produzione di documentazione tecnica a supporto, l'allocazione di nuove risorse hardware ecc., al fine di garantirne la disponibilità secondo gli SLA definiti al paragrafo 5.2.1.

L'attività di esercizio sarà erogata per tutta la durata contrattuale, e verrà remunerata all'interno del canone d'uso della Piattaforma, ovvero nella tariffa flat a candidato espressa dal Service Provider.

Pertanto, a titolo non esaustivo, data la particolare natura del servizio in modalità SaaS, le attività di esercizio della Piattaforma dovranno prevedere i seguenti servizi:

- Helpdesk
- Gestione Infrastruttura ed elaborazione dati
- Sicurezza logica
- Disaster recovery/ business continuity
- Conduzione applicativa
- Gestione Interventi progettuali
- Incident Management
- Problem Management
- Change & release Management
- Configuration Management
- Inventory Management
- Capacity & performance Management

L'insieme dei servizi illustrati deve essere compreso nella remunerazione del canone periodico relativa all'erogazione del servizio SaaS.



Il Service Provider dovrà garantire, con un preavviso massimo di 48 ore, il necessario aumento delle risorse messe a disposizione per gestire eventuali incrementi degli accessi alla Piattaforma rispetto quanto indicato e congruito con il committente nel *Piano di Lavoro, Progettazione, Configurazione e Attivazione*.

Qualora tali incrementi dovessero comportare oneri economici, gli stessi saranno oggetto di una specifica proposta di intervento progettuale che FSTechnology valuterà in maniera opportuna.

- **Interventi progettuali opzionali sulla Piattaforma** (richiesti a seguito di eventuali variazioni alla procedura di Smart Recruiting):
 - a) *Valutazione degli impatti*: nel corso del periodo di sottoscrizione del servizio, il Service provider a seguito dell'avanzamento di una richiesta di cambiamento, dovrà fornire preventivamente all'attuazione, la soluzione tecnica, i tempi e i costi utilizzando le tariffe professionali delle tre figure specifiche offerte. Sulla base del carico di sviluppo applicativo/infrastrutturale derivante dall'intervento, il Service provider dovrà identificare le aree di rischio impattate con le relative azioni di contromisura per la loro mitigazione;
 - b) *Aggiornamento della documentazione*: il fornitore è obbligato ad aggiornare la documentazione sia tecnica, sia utente, a corredo della Piattaforma, generata durante le precedenti fasi di start up e messa a regime.

- **Attività di dismissione del servizio** (richiesta a seguito di recessione anticipata dal contratto):
 - a) *Raccolta dati*: consegna di tutti i dati derivati e di backup di proprietà dell'acquirente presenti sulla Piattaforma, generati durante l'erogazione del servizio;
 - b) *Eliminazione permanente dei dati*: il fornitore, a valle della consegna dei dati presenti sulla Piattaforma all'acquirente, è obbligato a procedere con la loro cancellazione sicura da ogni supporto di memorizzazione impiegato per lo svolgimento delle attività e lo stoccaggio delle informazioni storicizzate, secondo i requisiti indicati nel paragrafo 4.3.



4. Requisiti della Piattaforma a supporto del processo di Smart Recruiting

Nel presente documento sono descritti i requisiti funzionali, tecnici, di qualità e quelli relativi ai servizi, inerenti alla fornitura della Piattaforma e dei relativi servizi, per la gestione del processo di Smart Recruiting. Tali requisiti rappresentano i criteri attraverso i quali verrà operata la selezione delle soluzioni che verranno proposte dal mercato in risposta alla presente gara.

4.1 Classificazione dei Requisiti

I requisiti illustrati nel presente documento sono suddivisi nelle seguenti categorie:

- ***Requisiti Funzionali della Piattaforma (rif. paragrafo 4.2)***
- ***Requisiti Tecnici della Piattaforma (rif. paragrafo 4.3) contraddistinti ulteriormente in:***
 - a) *Requisiti tecnici applicativi;*
 - b) *Requisiti tecnici architetturali della Piattaforma SaaS;*
 - c) *Requisiti organizzativi;*
- ***Requisiti relativi alla Qualità della fornitura (rif. paragrafo 4.4.)***
- ***Requisiti relativi alla Sostenibilità e Codice Etico (rif. paragrafo 4.5.)***
- ***Requisiti relativi alle Attività di setup, messa a regime della piattaforma e servizi di dismissione (rif. paragrafo 5.1/5.2/5.3.)***

I suddetti requisiti sono diversificati in due diverse tipologie:

Requisiti Vincolanti: sono quegli elementi e quelle caratteristiche, indicate nel documento, che le attività e/o la Piattaforma devono necessariamente possedere, diversamente la proposta verrà ritenuta inadeguata e quindi esclusa dalla gara.

Requisiti Migliorativi: sono quegli elementi e quelle caratteristiche, indicate nel documento, che, se presenti nella proposta in esame, permetteranno l'attribuzione di un punteggio nell'ambito del massimale previsto per il requisito in esame.



4.2. Requisiti funzionali della Piattaforma

Sono riportati nella Tabella 1 i requisiti funzionali suddivisi per argomento. Accanto alla descrizione del singolo requisito è indicato se questo è vincolante (V) o migliorativo (M).

ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
RFx Requisiti funzionali			
RF1	Front end multilingua	Interfaccia e contenuti dei test e delle video interviste multilingue per gli utenti di Front End (Candidati): Italiano, Inglese, Francese, Tedesco, Spagnolo	V
RF2	Front end multilingua - lingue aggiuntive	Interfaccia e contenuti dei test e delle video interviste multilingue per gli utenti di Front End (Candidati): anche in altre lingue aggiuntive rispetto al requisito RF 1. Specificare quante	M
RF3	Back end multilingua	Interfaccia e contenuti per gli utenti di Back End (Recruiter) almeno in lingua italiana e inglese	V
RF4	Personalizzazione interfaccia	Possibilità di personalizzare l'interfaccia con la digital identity di ciascuna Società del Gruppo FS	M
RF5	Tipologie di digital test	<ul style="list-style-type: none">• Disponibilità di almeno un test per le valutazioni delle competenze linguistiche;• Disponibilità di almeno un test psico attitudinali per le seguenti tipologie:<ul style="list-style-type: none">○ Ragionamento logico-matematico;○ Ragionamento deduttivo, induttivo, numerico, astratto, meccanico, spaziale, verbale;○ Attenzione/vigilanza/concentrazione;• Disponibilità di almeno questionario di personalità;• Disponibilità di almeno un questionario motivazionale;• Disponibilità di test o questionari per la valutazione delle soft skills (adattabile al modello di leadership del Gruppo FS)	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

RF5A	Aggiornamento test disponibili	Possibilità di aggiornare periodicamente i test a disposizione nella piattaforma	M
RF5B	Tipologie di digital test	Disponibilità di gaming e/o business case per valutare le competenze del modello di leadership FS (in allegato) e le seguenti capacità: 1. Digital skills 2. Learning Agility 3. Intercultural skills e diversity skills	M
RF5B1	Costruzione nuovi Test	Capacità da parte del fornitore di costruire test ad hoc e di finalizzarne la relativa validazione psicometrica. I test così realizzati potranno essere finalizzati a misurare attitudini e comportamenti e gli item rimarranno di proprietà esclusiva del Gruppo FS. A tal fine il fornitore potrà anche avvalersi di partnership con istituti accademici e universitari	M
RF6	Numerosità test	Disponibilità di test aggiuntivi rispetto al requisito RF5. Specificare quanti	M
RF6A	Varietà delle tipologie	Disponibilità di tipologie di test aggiuntive rispetto al requisito RF5. Specificare quante.	M
RF6B	Differenziazione per target	Possibilità di associare le suite di test rispetto alle diverse tipologie di processo di recruiting	M
RF6C	Differenziazione per job profile	Possibilità di associare le suite di test rispetto ai diversi job profile.	V
RF7	Certificazioni UE per i digital test (almeno una certificazione)	Rispetto a ciascun test è richiesto il possesso di almeno una delle certificazioni rilasciata da uno dei seguenti enti (specificare quale): - International Test Commission – ITC - European Test Publisher Group – ETPG - European Association of Psychological Assessment – EAPA - International Association of Applied Psychology – IAAP.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

RF7A	Certificazioni UE per i digital test (più di una certificazione)	<p>Possesso, in aggiunta a quanto indicato nel requisito RF 7, di una ulteriore certificazione rilasciata da uno dei seguenti enti:</p> <ul style="list-style-type: none"> - International Test Commission – ITC - European Test Publisher Group – ETPG - European Association of Psychological Assessment – EAPA - International Association of Applied Psychology – IAAP. <p>Tali certificazioni aggiuntive dovranno essere possedute per almeno una delle tipologie di test offerte.</p>	M
RF8	Modularità dei test per tipologia di figura professionale	Possibilità di raggruppare i test da somministrare ai candidati a seconda del job profile, permettendo la creazione in autonomia di template, scegliendo i test da un catalogo pre-approvato.	M
RF9	Customizzazione Suite da catalogo	Consentire a Ferrovie dello Stato di accedere al catalogo dei test da cui poter attingere in autonomia per la creazione di nuove suite.	M
RF10	Definizione soglie e punteggi	Possibilità di convertire i punteggi delle singole competenze valutate o raggruppamenti di competenze in scale e valori soglia modificabili	V
RF11	Esiti e Ranking	Esiti espressi sia con output numerici/quantitativi, (anche attraverso un ranking, attribuzione di pesi specifici e variabili ai risultati del singolo test) sia output qualitativi (report sulle competenze)	V
RF12	Strumenti di monitoraggio e reporting	Disponibilità di funzionalità di monitoraggio e di reporting sia a disposizione dei candidati esterni (grafico qualitativo delle competenze) che degli utenti interni, con possibilità per gli utenti interni di generare reportistica custom on demand e reportistica sugli esiti dei test. La reportistica riservata agli utenti interni dovrà essere disponibile sia in italiano che in inglese indipendentemente dalla lingua di somministrazione del test.	V
RF12A	Strumenti di monitoraggio e reporting	Possibilità di rendere disponibile al termine del test un messaggio customizzabile da restituire al candidato	V
RF12B	Strumenti di Monitoraggio e Reporting	Possibilità di avere reportistica indicativa degli esiti dei test divisi per tipologia di ruolo	M



Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico

RF13	Test di tipo randomico	Rotazione randomica degli items: si richiede che in tutti i test psicoattitudinali la presentazione degli item venga selezionata in maniera randomica garantendo la variazione delle domande e della sequenza di esse mantenendo lo stesso livello di complessità generale del test.	V
RF14	Video interviste customizzabili	Disponibilità di somministrare video interviste con domande a scelta	V
RF15	Fruizione mobile	Fruibilità dei test e delle video interviste anche tramite mobile.	V
RF16	Supporto in lingua italiana e inglese	Supporto in lingua sia italiana sia inglese in termini di assistenza tecnico/operativa nelle diverse fasi del processo (verso il recruiter, l'IT e i candidati esterni).	V
RF17	Adverse impact	Disponibilità di un servizio di adverse impact da modulare tramite la somministrazione di specifici test/video interviste ad un campione significativo di candidati.	M
RF18	Accessibilità	Strumenti progettati secondo logiche di design for all per garantire l'accessibilità e la corretta fruizione di tutti i test previsti verso candidati con disabilità e/o esigenze speciali, comprese le neurodivergenze. Laddove le suite di test non siano tutte progettate secondo logiche di design for all il fornitore si impegna sviluppare e rendere disponibili strumenti ad hoc per la committenza.	V
RF19	Divisione Ricerca e Sviluppo	Disponibilità di un dipartimento di Ricerca e Sviluppo e/o di professionisti con documentata esperienza in ambito psicometrico e di testing anche per la creazione e validazione di nuovi test.	V
RF20	Tempi di retention	La Piattaforma deve assicurare la cancellazione sia fisica che logica (o, alternativamente, l'anonimizzazione certificata che garantisca l'impossibilità dell'identificazione dell'interessato anche a fronte di incrocio di record di dati o per una clusterizzazione di eccessivo dettaglio) dei dati personali allo scadere di un tempo di retention definito.	V
RF21	Supporto alla gestione delle casistiche data protection	Disponibilità di esperti su tematiche data protection per la gestione di specifiche osservazioni/ricieste/accessi agli atti da parte di candidati del Gruppo	V



Tabella 1 - Requisiti funzionali della Piattaforma

4.3 Requisiti tecnici della Piattaforma

Il sistema di Talent Acquisition del Gruppo FS Italiane è l'applicativo attraverso il quale vengono gestite le fasi di creazione di job search, candidatura, screening e gestione iter di selezione del Gruppo. La modalità di integrazione della Piattaforma di test digitali e videointerviste con il sistema di Talent Acquisition del Gruppo FS dovrà avvenire tramite servizi web tipo Rest API che consentano di avere interfacce parametrizzabili mediante recordset JSON.

Dovranno essere previsti inoltre servizi di autenticazione di tipo SSO con protocolli SAML2.0 e Oauth2.0 integrabili con l'identity provider del Gruppo FS.

In questo paragrafo sono elencati i requisiti tecnici, richiesti per la Piattaforma di digital test e videointerviste, distinti per tipologia (*applicativi, architetturali e di sicurezza per la mobilità aziendale*) e definiti con l'indicazione dei Vincolanti e dei Migliorativi.

4.3.1 Requisiti tecnici applicativi

ID	Item	Descrizione	Requisiti vincolante (V) o requisito migliorativo (M)
RTA1.x Responsività			
RTA1.1	Mobile friendly	La Piattaforma deve essere responsive, in modo che si possa visualizzare e usufruire da ogni dispositivo. In particolare, da Mobile per Android da versione 9.0 in poi - IOS da versione IOS 12 in poi.	V
RTA2.x Accesso alla Piattaforma			
RTA2.1	Accesso alla Piattaforma	La Piattaforma deve essere accessibile sia agli utenti interni al Gruppo FS, sia ad utenti esterni.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

RTA2.2	Personalizzazione interfaccia	Il sistema gode di flessibilità sufficiente per l'adattamento dei form di compilazione alle specifiche funzionali e di layout previste in fase di progettazione.	V
RTA2.3	Gestione dei contenuti	Il sistema, in conformità con la segregazione dei ruoli, permette la personalizzazione dei contenuti che compongono l'interfaccia grafica con cui l'utente interagisce.	M
RTA2.4	Telelavoro	La Piattaforma è accessibile dagli utenti preposti alla gestione e al trattamento dati delle iniziative, da connessioni esterne all'organizzazione, di concerto con i meccanismi di sicurezza riportati nelle specifiche tecniche infrastrutturali.	M
RTA2.5	Disponibilità della Piattaforma	La Piattaforma deve essere disponibile 7 giorni su 7 festivi inclusi e H24	V
RTA3.x Requisiti Tecnici Applicativi			
RTA3.1	Modalità Integrazione	Capacità di integrazione dati attraverso meccanismi di interoperabilità con flussi/eventi di dati e API, incluso il provisioning di dati in-stream per consentirne il successivo utilizzo o analisi.	V
RTA3.2	Flessibilità della soluzione	Disponibilità dei dati elaborati dalla soluzione per un periodo di tempo almeno pari alla durata del contratto.	V
RTA3.3	Modularità della soluzione	La piattaforma deve essere modulare e garantire l'interoperabilità dei moduli della stessa grazie ad un'integrazione nativa.	M
RTA3.4	Supporto della soluzione con servizi professionali	Soluzione deve essere supportata dal mercato con l'erogazione di servizi professionali	M
RTA3.5	Cloud native	Soluzione cloud native, non vincolata ad un cloud services provider specifico	M
RTA3.6	Multi-tenant	La piattaforma deve garantire di poter essere configurata in modalità multitenant.	M



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

RTA4.x Gestione privilegi			
RTA4.1	I dati di produzione devono essere esclusi dagli ambienti di sviluppo e certificazione	Negli ambienti di sviluppo e certificazione devono essere utilizzati dati fittizi o se necessario un sottoinsieme dei dati di produzione che abbiano preventivamente subito un processo di anonimizzazione/mascheramento	V
RTA4.2	Restrizioni sui dati consultabili dal personale tecnico in ambiente di produzione	Il personale tecnico, nel corso delle sue attività di manutenzione in ambiente di produzione, non ha la possibilità di consultare il contenuto sensibile presente sulla Piattaforma.	M
RTA4.3	Meccanismi di autorizzazione	La Piattaforma deve prevedere l'implementazione di controlli che consentano la definizione delle operazioni che un determinato utente può compiere, in modo tale che: - siano concesse alle utenze esclusivamente i privilegi strettamente necessari a svolgere le attività per le quali sono autorizzate secondo il principio di Segregation of duties; - ogni utenza sia autorizzata a trattare solo i dati essenziali allo svolgimento della loro mansione secondo i principi need to know\use.	V
RTA4.4	Gestione utenze privilegiate	Il fornitore deve prevedere dei meccanismi di controllo specifici per le utenze che godono di privilegi ampi.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

RTA5.x Gestione upgrade/update della Piattaforma			
RTA5.1	Compatibilità a fronte di nuove release della Piattaforma	Il fornitore deve assicurare, a fronte di rilasci di nuove versioni principali o secondarie della Piattaforma (major/minor release), la compatibilità con tutte le configurazioni/personalizzazioni effettuate per rispondere all'esigenze dell'organizzazione. Inoltre, il service provider deve descrivere, mediante documentazione opportuna, il processo e le modalità di aggiornamento dell'applicazione SaaS, indicando in maniera trasparente e chiara l'impatto di ogni operazione sulle funzionalità del servizio.	V
RTA5.2	Aggiornamento del software sulla base del contesto tecnologico	Il Fornitore SaaS si assume l'onere di eseguire un monitoraggio del contesto tecnologico e operativo riferibile all'erogazione del servizio, atto a individuare e implementare migliorie e aggiornamenti dello stesso.	V
RTA5.3	Comunicazione e documentazione a seguito di aggiornamenti	Il Fornitore SaaS, in seguito ad aggiornamento del software, deve garantire: - una comunicazione puntuale all'utenza dei cambiamenti e delle migliorie introdotti; - la produzione di documentazione e manualistica aggiornata.	V



RTA6.x Gestione supporto			
RTA6.1	Sistema di trouble ticketing	<p>Il fornitore deve allestire un sistema di trouble ticketing di tipo web-based, per la raccolta e la piena condivisione al Gruppo FS delle difformità e dei disservizi riscontrati durante l'esercizio. In particolare, il sistema deve consentire:</p> <ul style="list-style-type: none">- il monitoraggio in maniera autonoma dei ticket aperti e del loro stato di elaborazione;- la generazione di reportistica relativa all'insieme di ticket aperti in un determinato periodo di riferimento.	V



RTA7.x Portabilità del servizio e dei dati			
RTA7.1	Estrazione completa dei dati	Deve essere sempre possibile da parte del Gruppo FS, su richiesta oppure in modalità self-service, l'estrazione di una copia completa dei dati memorizzati e gestiti dal servizio (in formato standard, non proprietario e riutilizzabile), ivi compresi i dati derivati quali log e statistiche di utilizzo, nonché le configurazioni del servizio. Tali prerogative devono essere garantite per un periodo di almeno due mesi (phase out) a partire dalla cessazione della fornitura (anche nel caso in cui la cessazione sia stata determinata dalla revoca della qualifica).	V
RTA7.2	Migrazione verso altro fornitore	Deve essere sempre possibile la migrazione dei dati del servizio verso un altro Fornitore SaaS con conseguente eliminazione permanente dei dati di proprietà del Gruppo FS al termine della procedura di migrazione (inclusi i dati derivati e i dati di backup).	V
RTA7.3	Recupero dati nel caso di fallimento	La proprietà dei dati deve essere mantenuta dal Gruppo FS anche in seguito ad operazioni di acquisizione o fallimento del fornitore SaaS. In caso di fallimento, chiusura dell'attività o dismissione del servizio, il fornitore SaaS deve garantire al Gruppo FS di poter recuperare i dati (in formato standard, non proprietario e riutilizzabile) e di poter migrare il servizio. Il periodo di tempo a disposizione del Gruppo FS dovrà consentirgli di completare il recupero dei dati e la migrazione del servizio e non potrà comunque essere inferiore a due mesi.	V
RTA7.4	Definizione piano di migrazione	Il fornitore SaaS deve predisporre un dettagliato piano di reversibilità, contenente le procedure e le modalità per migrare il servizio SaaS e tutti i dati pertinenti (anche derivati).	V



RTA8.x Integrazioni			
RTA8.1	Integrazione con il sistema di Talent Acquisition	<p>Integrazione con il sistema di Talent Acquisition del Gruppo FS (attivazione e somministrazione di test/videointerviste in fase di application del candidato alla ricerca di personale attivata da una delle Società del Gruppo e restituzione al sistema di Talent Acquisition dei risultati ottenuti dai candidati, sia in termini di output quantitativi che qualitativi).</p> <p>Al fine di garantire l'integrazione come descritto anche nel capitolo "Obiettivo e ambito di applicazione" del presente Capitolato Tecnico, il fornitore dovrà realizzare una soluzione per l'integrazione con il sistema di Talent Acquisition servizi web tipo Rest API per garantire lo scambio di informazioni continuo tra i due sistemi. A titolo esemplificativo e non esaustivo devono essere disponibili servizi per ottenere il catalogo dei test/videointerviste, effettuare la registrazione di una nuova prova del candidato e ottenere i risultati delle prove in termini di % Completamento, Esito della prova, Punteggio in centesimi, Data inizio prova, Data ultimo accesso alla prova. Deve essere prevista la possibilità di aggiungere ulteriori informazioni alla comunicazione tra i due sistemi mediante recordset JSON.</p>	V
RTA8.2	Integrazione con Identity Provider del Gruppo FS	La modalità di integrazione dovrà prevedere servizi di autenticazione di tipo Single Sign On (SSO) con protocolli SAML2.0 e Oauth 2.0.	V

Tabella 2 - Requisiti tecnici applicativi



4.3.2 Requisiti tecnici architetturali della Piattaforma SaaS

ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
SaaS_RT1.x Change e release management/ Configuration management			
SaaS_RT1.1	Change Management	Il servizio deve prevedere l'adozione di procedure/strumenti di change management per tenere traccia delle modifiche eseguite sulle configurazioni del sistema. In aggiunta, il fornitore deve prevedere la definizione di un processo formale che documenti la fase di autorizzazione e implementazione delle modifiche e dell'installazione delle patch all'interno di processi, sistemi o strutture aziendali.	V
SaaS_RT1.2	Separazione ambienti in sviluppo, certificazione e produzione	Il servizio deve consentire la separazione degli ambienti in sviluppo, certificazione e produzione, con il rispetto dei passaggi previsti per favorire l'esecuzione delle attività di sviluppo e testing in modo controllato e sicuro.	V
SaaS_RT1.3	Utenze di test	Il fornitore SaaS deve rendere disponibile un account di test per ogni ruolo ed un URL utilizzabili dall'acquirente per effettuare ogni tipo di verifica che si renderà necessaria per il rilascio ed il mantenimento della qualificazione	V
SaaS_RT1.4	Test nuovi rilasci	Il fornitore deve garantire che i nuovi rilasci effettuati in certificazione, siano testati rigorosamente, in accordo con piani di test predefiniti e documentati, e che i risultati siano approvati e firmati dal cliente interno, prima dell'installazione in ambiente di esercizio.	V



SaaS_RT1.5	Integrità dei file	Devono essere utilizzati opportuni strumenti di verifica dell'integrità dei file per assicurare che i file critici di sistema (compresi eseguibili, librerie e file di configurazione) non siano stati alterati. Nel caso in cui la verifica venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert. Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica. I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	V
SaaS_RT2.x Disaster Recovery/Business continuity			
SaaS_RT2.1	Backup & Restore - BC e DR	Il Fornitore SaaS deve disporre di un piano di continuità operativa (business continuity) in cui sono previste azioni orientate al ripristino dell'operatività del servizio (disaster recovery) al verificarsi di eventi catastrofici/imprevisti. Il piano di ripristino raccoglie tutte le procedure necessarie al ripristino del servizio e dei dati ad esso relativi.	V



SaaS_RT2.2	Valutazione della resilienza della soluzione	<p>Il Fornitore SaaS deve descrivere il comportamento della soluzione SaaS nell'eventualità di un evento catastrofico, fornendo una valutazione del rischio a seguito della manifestazione dei seguenti eventi:</p> <ul style="list-style-type: none"> ○ perdita o inconsistenze di dati; ○ alterazioni o non accessibilità ai dati; ○ perdita delle transazioni; ○ perdita delle chiavi crittografiche per decifrare i dati; ○ impossibilità di ripristinare il servizio da un backup precedente; ○ impossibilità di operare con il servizio nella sua pienezza. 	V
SaaS_RT3.x Gestione infrastruttura ed elaborazione dati			
SaaS_RT3.1	Localizzazione Data Center	Il fornitore deve avere il/i Data Center all'interno dell'Unione Europea.	V
SaaS_RT3.2	Backup & Restore	Il servizio deve essere oggetto di Back up periodico. In particolare, deve essere prevista l'effettuazione pianificata di copie di riserva finalizzate a duplicare, con una periodicità prestabilita, i dati, le configurazioni e le immagini di sistema su appositi supporti di memorizzazione.	V
SaaS_RT3.3	Decommissioning e cancellazione sicura	Il servizio deve prevedere l'adozione di procedure e tecniche di dismissione dei sistemi che prevedono la cancellazione sicura dei dispositivi di memorizzazione/backup del sistema. Lo smaltimento o la riassegnazione dell'hardware devono essere eseguiti in modo sicuro quando non più necessario. In particolare, tutte le informazioni e i software memorizzati sull'hardware devono essere oggetto di un processo di cancellazione e/o sovrascrittura sicuri (e.g. sovrascritture, degausser, DBAN software).	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT3.4	Backup & Restore - High availability	Il fornitore deve prevedere l'implementazione di un modello che permetta, tramite l'adozione di strumenti tecnologici ridondati, di avere un sistema altamente disponibile ai propri utenti. La resilienza dei sistemi deve essere garantita utilizzando le seguenti misure di sicurezza: - duplicazione dei componenti hardware (ad esempio processori, hard disk driver, schede di rete e di memoria) per creare sistemi fault-tolerant, ovvero in grado di resistere a errori e/o malfunzionamenti. - Utilizzare metodi "Hot Standby" (conosciuti anche come "Hot Spare") dove un sistema (detto "hot standby") funziona contemporaneamente con un sistema primario identico; in caso di fallimento di quest'ultimo, l'"hot standby" prende il suo posto. In questo metodo, i dati sono sempre sincronizzati in tempo reale tra i due sistemi. - Utilizzare meccanismi di archiviazione resilienti (ad esempio mirroring del disco, dischi RAID).	V
SaaS_RT3.5	Backup ridondato geograficamente	Indicare se la Piattaforma presenta dei backup dislocati in più posizioni geografiche (all'interno dell'Unione Europea).	M
SaaS_RT3.6	Amministrazione e unica risorse infrastrutturali	Il Fornitore SaaS, durante tutto il ciclo di vita della soluzione SaaS opera in qualità di amministratore unico di tutte le risorse Cloud di tipo PaaS/IaaS utilizzate dal servizio che eroga.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT3.7	Piattaforma Single Tenant	Il fornitore deve erogare il servizio SaaS in modalità Single Tenant, rilasciando un ambiente caratterizzato da un'istanza software e un database dedicati, indipendente dalle soluzioni adottate per altri clienti.	V
SaaS_RT3.8	Test Backup periodici	Il fornitore deve implementare con periodicità annuale dei test di ripristino delle copie di backup.	V
SaaS_RT3.9	Protezione copie di backup	Le copie di backup devono essere protette mediante opportune misure di sicurezza fisica e logica.	V
SaaS_RT3.10	Cancellazione base	Il cloud provider prevede l'utilizzo di algoritmi e meccanismi generici per la cancellazione dei dati, quali ad esempio la sovrascrittura con una sequenza di zero o la formattazione.	V
SaaS_RT4.x Incident management			
SaaS_RT4.1	Gestione degli incidenti di sicurezza	Il servizio deve garantire la gestione degli incidenti di sicurezza attraverso l'attivazione delle procedure operative concordate con il Gruppo FS garantendo la loro registrazione, classificazione, risoluzione, comunicazione ed analisi a posteriori per identificare le cause e prevenirne future manifestazioni.	V
SaaS_RT4.2	Sistema di alerting per applicazione delle contromisure	Deve essere sempre attivo un sistema di monitoraggio e di alerting relativo a possibili incidenti di sicurezza e/o di violazioni delle policy. Questo sistema deve prevedere la pronta applicazione delle necessarie contromisure in maniera automatica e/o tramite l'intervento di un operatore. Le informazioni relative alle problematiche occorse devono essere registrate, insieme alle attività realizzate per rimediare, e devono essere messe a disposizione dell'acquirente.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT4.3	Valutazione dello stato di sicurezza del servizio a seguito della manifestazione di problematiche.	Qualora le risorse IaaS/PaaS, i dati e/o i software ospitati, oppure le loro configurazioni dovessero risultare alterati o utilizzati impropriamente, a seguito di un incidente di sicurezza, occorre mettere in atto le opportune attività di security assessment e audit, prima di porre il servizio nuovamente in esercizio. Questa misura preventiva va adottata al fine di valutare lo stato complessivo della sicurezza e la possibilità di procedere con l'utilizzo del servizio stesso in modo protetto e sicuro.	V
-------------------	--	---	---



SaaS_RT5.x Sicurezza logica			
SaaS_RT5.1.x Sicurezza logica – Network			
SaaS_RT5.1.1	Network Security - cifratura dei canali a livello di rete	La soluzione deve adottare tecniche e protocolli per la protezione del canale di comunicazione per connessioni provenienti da reti pubbliche/non controllate verso la rete ed i sistemi dell'organizzazione mediante l'uso di reti private virtuali (VPN) oppure tramite sistemi di mediation.	V
SaaS_RT5.1.2	Network Security - anti DDOS	Il fornitore deve garantire l'attivazione di un sistema di protezione Anti DDOS.	V
SaaS_RT5.1.3	Network Security – Firewall	<p>Il fornitore deve prevedere l'installazione di firewall sul perimetro di rete più esterno dell'organizzazione a protezione della soluzione. Questo dispositivo deve:</p> <ul style="list-style-type: none"> • filtrare specifiche tipologie di traffico (ad esempio indirizzi IP, porte TCP o informazioni sullo stato delle comunicazioni e degli utenti); • bloccare o limitare particolari tipi o sorgenti di traffico; • sviluppare regole (o tabelle) predefinite per filtrare il traffico, che rispettino il principio del "least access"; • proteggere i firewall da attacchi o guasti; • limitare la divulgazione di informazioni sulle reti; • monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione; • filtrare il contenuto del traffico web; • bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa. 	V
SaaS_RT5.1.4	Network Security – IDS	Il fornitore deve prevedere l'implementazione di Network-based Intrusion Detection Systems (IDS), con lo scopo di identificare tutte le sequenze di eventi aventi come obiettivo la	V



Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico

		<p>compromissione di un sistema, di un apparato o della rete. In particolare, questi sistemi devono rilevare:</p> <ul style="list-style-type: none">• interruzioni non pianificate dei processi o delle applicazioni;• attività tipicamente associate a malware;• caratteristiche di attacco note (ad esempio DoS e buffer overflow);• comportamenti insoliti del sistema (ad esempio identificazione di anomalie nei protocolli standard);• accessi non autorizzati (sia tentativi di accesso che accessi riusciti) a sistemi o informazioni. <p>Il fornitore deve garantire la gestione del servizio, contestualizzando le configurazioni rispetto alle tecnologie adottate, ottimizzando il servizio per ottenere il minor numero di falsi positivi e garantendo il massimo delle prestazioni rispetto all'assurance dei servizi.</p>	
SaaS_RT5.1.5	Network Security – IPS	Il fornitore deve prevedere l'implementazione di Network-based Intrusion Prevention Systems (IPS) per identificare, attraverso l'analisi del traffico, la presenza di accessi non autorizzati o codice malevolo nei sistemi.	V
SaaS_RT5.1.6	VPN e NAT Management	Il fornitore deve erogare il servizio di NAT Management per la gestione delle regole di traduzione degli indirizzi IP configurati all'interno dell'infrastruttura di rete ed il piano di indirizzamento complessivo, al fine di nascondere i dettagli dell'indirizzamento utilizzato all'interno di una rete quando ci si connette ad altre reti. Il fornitore deve erogare il servizio di VPN Management per la gestione degli accessi remoti ai server ed ai sistemi gestiti (sia di tipo client-VPN che Site-to-Site IPSEC).	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.1.7	Cifratura dei dati in transito a livello applicativo	La soluzione deve prevedere l'adozione di protocolli di tipo SSL o TLS 1.2 o superiore per crittografare i dati in transito. Le sessioni di applicazioni Web devono essere protette contro attacchi "session hijack", la clonazione o l'intercettazione: - garantendo che i SessionID non possano essere facilmente previsti ed identificati (ad esempio utilizzando SessionID generati casualmente); - configurando dei parametri di sicurezza nei "cookie" utilizzati per conservare le informazioni di sessione; - cifrando il traffico di rete tra il browser Web e il server web.	V
SaaS_RT5.1.8	Network Time Protocol (NTP)	Il sistema deve supportare il protocollo NTP al fine di sincronizzare il clock del sistema al fine di ridurre gli effetti derivanti dal clock skew.	V
SaaS_RT5.1.9	Web Application Firewall (WAF)	Utilizzo di Web Application Firewall per la protezione dei sistemi a livello di applicazione (secondo lo stack ISO/OSI).	V
SaaS_RT5.1.10	Hardening dei dispositivi di rete	I dispositivi di rete (inclusi router, switch e firewall) devono essere configurati opportunamente per: evidenziare condizioni di sovraccarico o eccezioni, quando si verificano; registrare gli eventi (logging) e salvarli su un sistema separato; integrarsi con meccanismi di controllo degli accessi (ad esempio per fornire autenticazione forte); assicurare che le password non vengano inviate in chiaro; disabilitare il "source routing", (tecnica di specificare all'interno dell'header IP il tragitto (route) che il pacchetto deve seguire per mantenere il controllo all'interno del dispositivo di inoltro dei pacchetti.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.1.11	Network Level Authenticatio n	L'infrastruttura del cloud provider deve supportare l'autenticazione a livello rete mediante 802.1X al fine di limitare e controllare quali dispositivi possono accedere alla rete. L'802.1X deve avere un link diretto all'asset inventory al fine di verificare i dispositivi autorizzati da quelli non autorizzati.	M
----------------------	--	--	---



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.1.12	Protezione server DNS	Il fornitore deve garantire la protezione dei server DNS per garantire la disponibilità della risoluzione dei nomi e quindi la possibilità di raggiungere l'applicazione.	M
SaaS_RT5.1.13	IP Tracking	Il fornitore deve prevedere l'implementazione di meccanismi che permettono di effettuare in qualsiasi momento l'associazione dei seguenti campi per l'identificazione dei dispositivi collegati alla rete dell'organizzazione: Indirizzo IP Host / Mac Address Hostname o ID univoco dell'utente.	V
SaaS_RT5.2.x Sicurezza logica - Sviluppo e Dati			
SaaS_RT5.2.1	Pseudonimizzazione dei dati	Il fornitore deve garantire tecniche di cifratura /mascheramento dei dati sia per i dati derivati, sia per i dati di backup ospitati nei database o nelle memorie di massa.	V
SaaS_RT5.2.2	Sviluppo sicuro	Il fornitore deve prevedere l'adozione di tecniche di sviluppo sicuro del codice sorgente.	V
SaaS_RT5.2.3	Crittografia	La soluzione deve essere in grado di impiegare un algoritmo di cifratura per: - proteggere la riservatezza delle informazioni sensibili o delle informazioni soggette a requisiti legali e normativi; - determinare se le informazioni critiche sono state alterate (ad esempio implementando funzioni hash o la firma digitale).	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.2.4	Sicurezza componenti software di terze parti (se presenti)	Il Fornitore SaaS può utilizzare componenti software realizzate da terze parti per implementare la propria applicazione (middleware, librerie, componenti da cui l'applicazione dipende), a patto che si renda garante anche della sicurezza di queste componenti.	V
SaaS_RT5.2.5	Verifica iniziale e periodica da eseguire sulle componenti sviluppate da terze parti (se presenti)	Il fornitore: assicura di aver utilizzato la fonte originale del software di terze parti e che non ci siano stati passaggi intermedi capaci di alterare il contenuto originale; è tenuto ad accertarsi che non siano presenti vulnerabilità note nel software utilizzato o che queste siano state opportunamente gestite e neutralizzate; deve garantire l'esecuzione periodica dei controlli e delle verifiche sulle componenti software di terze parti, apportare prontamente i fix necessari e/o rimuovere le dipendenze da quelle componenti con accertate vulnerabilità.	V
SaaS_RT5.2.6	Mascheramento dei dati	La Piattaforma deve prevedere l'esistenza di tecniche di data masking per minimizzare la visualizzazione e la lettura di dati personali, sulla base del principio del "need to know".	V



SaaS_RT5.2.7	Input validation	L'applicazione deve assicurare, attraverso opportuni meccanismi di convalida, che tutti i parametri in input, specificati dall'utente, siano congruenti a quanto atteso. In particolare, sui dati acquisiti in ingresso, l'applicazione deve prevedere l'implementazione di meccanismi di controllo che limitino il set di caratteri o valori, inseribili dall'utente, solo a quelli congruenti ai campi richiesti e/o alle forme di pertinenza, al fine di identificare ed annullare gli effetti di errori quali valori out-of-range o non pertinenti, caratteri invalidi negli stream, dati mancanti, etc. Per quanto riguarda i caratteri speciali, se presenti/richiesti in input, sono considerati pericolosi poichè la loro combinazione non può essere considerata semplice 'testo'.	V
SaaS_RT5.2.8	Code review	È necessario eseguire a valle di ogni intervento manutentivo dei controlli sul codice applicativo per identificare e indirizzare le vulnerabilità di sicurezza (ad esempio mediante analisi statica e dinamica del codice sorgente e test di unità).	V



SaaS_RT5.2.9	Protezione avanzata database	<p>L'integrità delle informazioni e dei dati contenuti nei database deve essere protetta utilizzando "metodi di concorrenza" dei dati, per garantire che le informazioni non siano danneggiate quando vengono modificate da più di un utente. I database devono essere protetti:</p> <p>memorizzandoli su un server centrale (e.g. per ridurre il rischio di modifiche accidentali o intenzionali e per garantire che i database vengano sottoposti a backup centralmente);</p> <p>limitando l'accesso alle sole persone autorizzate (e.g. utilizzando la protezione tramite password e creando opportune Access Control List);</p> <p>assegnando dei privilegi per limitare le funzionalità che le persone autorizzate possono eseguire sul database (e.g. definizione di profili utente e privilegi dell'utente per il personale che ha bisogno di aprire, leggere e modificare il contenuto dei database);</p> <p>utilizzando solo versioni approvate del database (e.g. utilizzando la versione del database corrente o un database approvato). L'accesso alle funzionalità del database deve essere limitato utilizzando la protezione tramite password per impedire la creazione non autorizzata di dichiarazioni, istruzioni e procedure che eseguono operazioni all'interno di un database. Le informazioni contenute nei database devono essere protette limitando l'accesso o rimuovendo i menu standard (e.g. nascondendoli o sostituendoli con un menu personalizzato per impedire l'accesso alle funzioni da sviluppatore).</p>	V
SaaS_RT5.2.10	Gestione dei consensi	La Piattaforma deve prevedere la gestione del versioning dell'informativa sulla privacy e dello storico dei consensi, affinché l'interessato, nel corso delle attività svolte a sistema, possa modificare le impostazioni fornite sulla raccolta dei consensi, in base alle proprie preferenze.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.2.11	Implementazione di soluzioni di gestione dei diritti digitali (DRM)	Il servizio deve prevedere l'implementazione di un sistema di gestione dei diritti digitali (DRM) per proteggere le informazioni e i software più critici che vengono utilizzati al di fuori del controllo dell'organizzazione.	V
SaaS_RT5.2.12	Implementazione di soluzioni di Data Loss Prevention (DLP)	Il servizio deve prevedere l'implementazione di soluzioni di Data Loss Prevention (DLP) per monitorare i flussi di dati all'interno della rete dell'organizzazione ed evidenziare eventuali anomalie.	V
SaaS_RT5.3.x Sicurezza logica - Policy, procedure e certificazioni			
SaaS_RT5.3.1	Conservazione dei dati	In conformità con l'Accordo di Data Protection, il fornitore deve garantire il rispetto delle modalità di conservazione dei dati effettuando le dovute operazioni di archiviazione e cancellazione ove previste.	V
SaaS_RT5.3.2	Certificazioni e qualifiche del Fornitore	Il fornitore deve disporre di certificazione aziendali ISO27001, CSA STAR Livello 1 (Autovalutazione), CSA STAR Livello 2 (Audit di Terza Parte), qualifica ACN (EX-AGID)	V
SaaS_RT5.3.3	Certificazioni e qualifiche del Fornitore ulteriori	Il fornitore può disporre di ulteriori certificazioni quali ISO/IEC 27002, 27017, 27018, 27701, 27031, ISO 22301, SOC 2, SOC 3	M
SaaS_RT5.3.4	Patch Management / Workaround Management	Il servizio deve garantire la costante distribuzione di release SW ed aggiornamenti di sicurezza sui sistemi/piattaforme o l'applicazione di workaround che mitigano la vulnerabilità, anche a seguito delle vulnerabilità riscontrate dagli assessment di sicurezza e dal servizio di security advisory. Il fornitore deve erogare il servizio garantendo la definizione di un piano di distribuzione degli aggiornamenti o workaround, la gestione del rilascio di configurazioni sicure preventivamente verificate e l'installazione	V



Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico

		<p>di patch di protezione raccomandate dai produttori o da terzi e volte ad eliminare o mitigare le vulnerabilità che possono essere sfruttate per un attacco ai sistemi.</p> <p>L'esecuzione del servizio deve comunque essere attuata in modo da garantire il corretto funzionamento di tutti i sistemi e servizi impattati senza deteriorare i connessi livelli di servizio.</p>	
SaaS_RT5.3.5	Controllo Accessi Logici	<p>Il servizio deve garantire l'utilizzo di utenze univoche e nominali: tutto il personale (interno ed esterno) è univocamente identificato e autenticato per accedere al sistema attraverso l'impiego di identificativi nominali (account).</p>	V
SaaS_RT5.3.6	Controllo Accessi Logici - password policy	<p>Il sistema deve essere sviluppato in modo da verificare che l'accesso ai servizi rispetti quanto segue:</p> <ul style="list-style-type: none">- Al primo accesso, l'utente deve cambiare la password (Tale requisito é da considerarsi applicabile per tutte le tipologie di utenze che accedono al sistema (utilizzatori, utenze M2M, amministratori ecc.)- È obbligatorio modificare le credenziali di default.- Il sistema deve essere costruito in modo da richiedere la sostituzione della password almeno ogni 3 mesi.- La lunghezza minima della password deve essere di almeno 14 caratteri.- La password deve includere almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale; non deve contenere nomi personali, parole di senso compiuto o parti di esse.- È necessario mantenere una history delle ultime 5 password utilizzate per evitare il riutilizzo delle stesse credenziali, oppure garantire che le stesse credenziali non possano essere riutilizzate per un periodo determinato (ad es. sei mesi).- La password deve essere diversa dall'ID utente associato, non deve essere facilmente indovinabile, né contenere riferimenti	V



Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico

		aziendali o parole di senso compiuto. - Le credenziali non utilizzate per almeno sei mesi devono essere disattivate, salvo quelle autorizzate per scopi tecnici. - Le credenziali devono essere disattivate anche in caso di perdita della qualità che consente l'accesso ai dati personali (es. dimissioni).	
SaaS_RT5.3.7	Controllo Accessi Logici - review utenze	Il servizio deve garantire la review periodica delle utenze; in particolare, deve essere definito un processo di revisione dei diritti di accesso assegnati agli utenti ed effettuata una review con cadenza semestrale.	V
SaaS_RT5.3.8	Controllo Accessi Logici - Strong authentication	Il servizio prevede meccanismi di Strong authentication; l'accesso alle risorse deve avvenire attraverso l'uso di sistemi di autenticazione a due fattori.	V
SaaS_RT5.3.9	Gestione degli accessi logici	Il servizio deve garantire la gestione dei sistemi di accesso logico alla rete, ai sistemi ed ai servizi (LDAP, Active Directory, ecc.). In particolare, l'attività prevede la gestione del ciclo di vita delle utenze sui sistemi (creazione, disabilitazione, eliminazione, ecc.) e la gestione delle modalità di autenticazione.	V
SaaS_RT5.3.10	End Point Protection (EPP)	Il Servizio di End Point Protection (EPP) deve essere in grado di garantire le seguenti funzionalità di base: antivirus (anche con funzionalità di antispyware, antitoolkit, ecc.); personal Firewall; application & device control, ovvero un sistema in grado di vietare/permittere all'utente finale l'utilizzo di programmi e/o risorse hardware solo se permesse dalle politiche di sicurezza aziendali;	V
SaaS_RT5.3.11	Security Assessment - VA	Il servizio deve essere oggetto di Vulnerability Assessment. Il fornitore è tenuto a svolgere queste sessioni almeno con una periodicità semestrale.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.3.12	Security Assessment – PT	Il servizio deve essere oggetto di Penetration Test. Il fornitore è tenuto a svolgere queste sessioni almeno con una periodicità semestrale.	V
SaaS_RT5.3.13	Rifiuti di apparecchiature elettriche ed elettroniche (RAEE)	Il servizio deve adottare opportuni accorgimenti/misure di sicurezza necessari per la dismissione dei supporti di memorizzazione, per prevenire accessi non autorizzati ai dati memorizzati nelle apparecchiature destinate ad essere reimpiegate, riciclate o smaltite.	V
SaaS_RT5.3.14	Contrasto agli attacchi DoS e DDoS	Il servizio deve garantire la gestione di sistemi di rilevamento e contrasto di attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS). Il fornitore deve garantire la gestione del servizio su internet, contestualizzando le configurazioni rispetto alle tecnologie e asset, ottimizzando il servizio per ottenere il minor numero di falsi positivi e garantendo il massimo delle prestazioni all'assurance dei servizi.	V
SaaS_RT5.3.15	Hardening dei sistemi	Il fornitore del servizio deve garantire l'implementazione di specifiche configurazioni su sistemi e componenti che incrementino la sicurezza complessiva dell'intera architettura di sistema. L'irrobustimento delle contromisure va effettuato sulle minacce che colpiscono: Sistemi operativi; Web servers; Application Server; DBMS. Per maggiori dettagli, si rimanda alle linee guida dell'AGID per l'adeguamento della sicurezza del software di base.	M
SaaS_RT5.3.16	Strumenti e Metodologie di Threat Intelligence	Deve essere definito e implementato un processo di Threat Intelligence, per raccogliere, analizzare ed elaborare le informazioni relative alle potenziali minacce che possono impattare l'organizzazione e appositi strumenti e data feed.	V
SaaS_RT5.3.17	Patch Management supportato	Il fornitore prevede l'adozione di tool automatici a supporto delle attività di patch management.	V



	dall'automazione		
SaaS_RT5.3.18	Simulazione red team vs blue team	<p>Il fornitore deve condurre simulazioni per testare il livello di efficacia dell'organizzazione nel contrastare attacchi alla propria infrastruttura di rete e condividere l'esito di queste campagne di valutazione con il gruppo FS. Il fornitore è tenuto ad indicare la periodicità con cui indice queste simulazioni, al fine di essere sottoposto ai criteri di valutazione previsti nella disciplinare di gara.</p> <p>La simulazione può essere condotta:</p> <ul style="list-style-type: none">almeno con cadenza biennale;con cadenza annuale;con cadenza semestrale.	M
SaaS_RT5.3.19	Requisiti di sicurezza software fornitori	<p>Il fornitore deve garantire che il proprio software soddisfi determinati requisiti di sicurezza (e.g. producendo report periodici di Vulnerability Assessment, Penetration Test, dimostrando l'aderenza agli standard e fornendo un metodo efficace per la gestione delle patch). Il fornitore è tenuto ad indicare le attività di mitigazione del rischio di potenziali vulnerabilità di sicurezza nel software, quali:</p> <ul style="list-style-type: none">• audit di terze parti (e.g. opinioni di un revisore esterno basati su criteri di sicurezza specifici, quali Common Criteria, FIPS);• identificazione e indirizzamento delle vulnerabilità di sicurezza (e.g. analisi dettagliata, test di malware, vulnerability scanning, partecipazione a forum/gruppi di discussione).	V
SaaS_RT5.3.20	Zero trust	L'infrastruttura adotta un modello di sicurezza "Zero Trust".	M



SaaS_RT5.4.x Sicurezza logica – Monitoraggio			
SaaS_RT5.4.1	Monitoraggi o correlazione degli eventi di sicurezza	Il servizio deve garantire la raccolta, correlazione, analisi, gestione e storicizzazione degli allarmi generati e delle informazioni raccolte nei file di log prodotti dagli apparati di sicurezza, garantendo la centralizzazione delle procedure di raccolta degli eventi di sicurezza, la gestione mirata delle notifiche e delle azioni di rimedio, l'identificazione di misure preventive, permettendo il monitoraggio del livello globale di sicurezza.	V
SaaS_RT5.4.2	Security Advisory / Early Warning	Il servizio deve garantire un monitoraggio continuo per la rilevazione di informazioni e notizie relative a nuove minacce e vulnerabilità che possono compromettere la sicurezza ICT del Cliente, con l'obiettivo di fornire una protezione preventiva a servizi ICT aziendali. Il servizio può essere attivato anche mediante notifiche provenienti dal Cliente stesso. Il fornitore deve garantire la registrazione delle informazioni raccolte e delle analisi condotte valutando l'impatto della minaccia sull'infrastruttura ICT da lui gestita per il Cliente e le relative vulnerabilità. Qualora la minaccia/vulnerabilità rappresenti un impatto per gli asset o le infrastrutture gestite, il fornitore deve definire la priorità da dare all'azione di rimedio sulla base del sistema di rating "CVSS2" se disponibile, o calcolando la priorità secondo una scala Low-Medium-High, concordate con la Direzione Centrale Protezione Aziendale, attivando conseguentemente il servizio di patch management/workaround management ed informando il Cliente mediante una lista di distribuzione.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.4.3	Logging - Accesso utenti	Il servizio deve prevedere l'attivazione di funzionalità di logging sui sistemi per il tracciamento degli accessi utenti	V
SaaS_RT5.4.4	Logging - Accesso AdS	Il servizio deve prevedere l'attivazione di funzionalità di logging sui sistemi per il tracciamento degli accessi AdS (Amministratori di sistema)	V
SaaS_RT5.4.5	Logging - Protezione e retention dei log	<p>Il servizio deve prevedere la protezione dei log da un uso improprio, quale la manomissione in transito o l'accesso, la modifica o la cancellazione non autorizzati; Esempi di misure di sicurezza dei log memorizzati in locale ("at rest") sono:</p> <ul style="list-style-type: none">memorizzare o copiare i log su storage in sola lettura;autorizzare, registrare e monitorare tutti gli accessi ai log;implementare meccanismi di rilevamento delle manomissioni, in modo da sapere se un record del log è stato modificato o eliminato;rivedere periodicamente i privilegi per l'accesso ai log. <p>Esempi di misure di sicurezza dei log in transito sono:</p> <ul style="list-style-type: none">se i log sono inviati su reti non attendibili (ad esempio Internet), utilizzare un protocollo di trasmissione sicuro/ cifrato (as esempio TLS 1.2 o superiore);Effettuare controlli di due diligence (normativi e di sicurezza) prima di inviare i log a terze parti. <p>La Retention dei log deve essere superiore o uguale ai 6 mesi per l'insieme di log caratterizzanti l'attività degli amministratori di sistema.</p>	V
SaaS_RT5.4.6	Logging - Tracciatura incident	Il servizio deve prevedere la registrazione, l'archiviazione e la notifica degli incidenti di sistema che impattano sull'applicazione.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT5.4.7	Monitoring (analytics)	Il servizio deve garantire la disponibilità dei log applicativi per le piattaforme di analisi e correlazione eventi (es: SIEM, CASB). In particolare, il fornitore dovrà rendere disponibili i log applicativi anche tramite API e dovrà supportare il Gruppo FS nell'interpretazione dei record raccolti.	V
SaaS_RT5.4.8	Monitoring	Il servizio deve includere il monitoraggio da parte di un Security Operation Center (SOC) h24 che analizza gli eventi di sicurezza rilevati al fine di individuare e gestire gli incidenti di sicurezza	V
SaaS_RT5.4.9	Antimalwar e sui server	Il servizio Antimalware deve garantire la protezione dei sistemi server gestiti da qualsiasi tipologia di software malevolo eseguibile e non (es. virus, trojan, Worm, Key loggers, rootkit, ransomware etc.). Si dovranno aggiornare in tempo reale le "firme" di protezione e l'aggiornamento periodico del motore dell'anti-malware. Tutti gli eventi malware-related devono essere inviati ad una Piattaforma centralizzata di collezionamento.	V
SaaS_RT5.4.10	Host Intrusion Detection System (HIDS)	Il cloud provider deve prevedere l'adozione di un Host Intrusion Detection System (HIDS), in grado di rilevare: <ul style="list-style-type: none">- interruzioni non pianificate dei processi o delle applicazioni;- attività tipicamente associate a malware;- caratteristiche di attacco note (es. DoS e buffer overflow);- comportamenti insoliti del sistema (es. identificazione di anomalie nei protocolli standard);- accessi non autorizzati (sia tentativi di accesso che accessi riusciti)	V
SaaS_RT5.4.11	Host Intrusion Prevention System (HIPS)	Utilizzo di un HIPS per identificare, attraverso l'analisi del traffico, la presenza di accessi non autorizzati o codice malevolo in esecuzione sui sistemi.	V
SaaS_RT6.x Capacity & performance Management			



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT6.1	Scalabilità	Il fornitore deve avere la possibilità di adeguare l'infrastruttura sottostante la soluzione SaaS al carico d'utenza presente sulla Piattaforma, mediante opportuni meccanismi di attivazione e dismissione delle risorse infrastrutturali (IaaS/PaaS) utili ad erogare il servizio. Il fornitore è tenuto ad accertare quanto illustrato mediante dichiarazione sottoscritta dal Responsabile dell'Accordo Quadro per l'Appaltatore.	V
SaaS_RT6.2	Indicatori prestazionali estraibili dalla Piattaforma sottostante il servizio SaaS	Il fornitore deve prevedere la possibilità di estrarre dalla sottostante Piattaforma IaaS/PaaS i KPI critici indicati nella sezione 7.3.1 del capitolato.	V
SaaS_RT6.3	SLA - RTO e RPO	Il fornitore deve rispettare i tempi di RTO ed RPO garantiti da contratto e specificati nella sezione 7.3.1 del capitolato.	V
SaaS_RT6.4	SLA - Availability	Il fornitore deve rispettare gli SLA di Availability garantiti da contratto ed illustrati nella sezione 7.3.1 del capitolato.	V
SaaS_RT6.5	Tempi di attivazione di nuove risorse	Il fornitore deve essere in grado di completare l'attivazione e la disattivazione delle risorse sulla base degli andamenti del carico d'utenza entro il successivo giorno lavorativo (next business day). Per accertare quanto richiesto, il fornitore è tenuto a dichiarare quanto illustrato mediante dichiarazione sottoscritta dal Responsabile dell'Accordo Quadro per l'Appaltatore.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT6.6	Continuità del servizio a seguito del ridimensionamento dell'infrastruttura	La scalabilità del servizio deve attivarsi correttamente al verificarsi delle condizioni operative prestabilite e deve garantire che non si subiscano interruzioni apprezzabili nell'erogazione del servizio. In particolare, in fase di decrescita delle risorse allocate, le istanze SaaS/PaaS/IaaS non più necessarie devono risultare correttamente disattivate in modo da non comportare costi di utilizzo. Il fornitore è tenuto ad accertare quanto illustrato mediante dichiarazione sottoscritta dal Responsabile dell'Accordo Quadro per l'Appaltatore.	V
SaaS_RT7.x Gestione degli interventi progettuali			
SaaS_RT7.1	Monitoraggio costi	Il calcolo dei costi imputati all'acquirente deve essere trasparente e accurato, rispettare le condizioni contrattuali ed essere monitorabile dall'acquirente stesso in tempo reale. In particolare, il Fornitore SaaS dovrà rendere disponibile all'Acquirente un set minimo di funzioni (API) che permettano di acquisire le informazioni sulle metriche di "billing".	V



SaaS_RT8.x Sicurezza Fisica			
SaaS_RT8.1	Gestione della sicurezza perimetrale	<p>Il servizio deve essere finalizzato a proteggere gli asset informatici da attacchi esterni, accessi e modifiche non autorizzate, garantendo il funzionamento continuo ed ottimale dell'infrastruttura di sicurezza, nonché monitorare il comportamento dei sistemi ed apportare le modifiche necessarie alle configurazioni delle politiche di sicurezza perimetrale.</p> <p>L'accesso fisico agli edifici che ospitano l'infrastruttura IT dell'organizzazione deve essere limitato agli individui autorizzati mediante le seguenti misure di sicurezza: controllo accessi all'ingresso degli edifici (reception e/o servizio di guardiania); il personale deve essere dotato di badge personale o di altro mezzo di identificazione (e.g. PIN).</p>	V
SaaS_RT8.2	Antincendio, Antiallagament o (Data center Primario)	Il cloud provider deve aver adottato misure di sicurezza per prevenire o far fronte ad un possibile incendio/allagamento del Data Center primario che ospita le macchine dell'organizzazione	V
SaaS_RT8.3	Controllo temperatura data center (Data center Primario)	Il fornitore deve svolgere delle attività di monitoraggio della temperatura interna del Data Center primario per tutelare le macchine in esso presenti.	V
SaaS_RT8.4	Sicurezza fisica dispositivi di rete (Data center Primario)	I cavi di rete ed i punti di accesso alla rete nel data center primario devono essere protetti mediante controlli fisici.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_RT8.5	Sicurezza fisica degli edifici (Data center Primario)	Gli edifici che ospitano l'infrastruttura IT del data center primario dell'organizzazione devono essere fisicamente protetti contro incidenti o attacchi di sicurezza.	V
SaaS_RT8.6	Protezione da sbalzi/interruzioni di corrente (Data center Primario)	Le infrastrutture IT del data center primario devono essere protette contro sbalzi o interruzioni di corrente.	V
SaaS_RT8.7	Antincendio, Antiallagamento (Data center secondari)	Il cloud provider ha adottato misure di sicurezza per prevenire o far fronte ad un possibile incendio/allagamento dei Data Center secondari che ospitano le macchine dell'organizzazione	M
SaaS_RT8.8	Controllo temperatura data center (Data center secondari)	Il fornitore svolge regolare attività di monitoraggio della temperatura interna dei Data Center secondari per tutelare le macchine in esso presenti.	M
SaaS_RT8.9	Sicurezza fisica dispositivi di rete (Data center secondari)	I cavi di rete ed i punti di accesso alla rete nei data center secondari sono protetti mediante controlli fisici.	M
SaaS_RT8.10	Sicurezza fisica degli edifici (Data center secondari)	Gli edifici che ospitano l'infrastruttura IT dei data center secondari dell'organizzazione sono fisicamente protetti contro incidenti o attacchi di sicurezza.	M
SaaS_RT8.11	Protezione da sbalzi/interruzioni di corrente (Data center secondari)	Le infrastrutture IT dei data center secondari sono protette contro sbalzi o interruzioni di corrente.	M

Tabella 3 – Requisiti tecnici architetturali



4.3.3 Requisiti organizzativi

L’Affidatario dovrà garantire e operare nel pieno rispetto delle normative vigenti applicabili in materia di protezione dei dati personali, in particolare per quanto previsto nel Regolamento UE 679/2016. Con l’affidamento del servizio, l’affidatario, in qualità di Responsabile del Trattamento, dovrà stipulare un Accordo di Data Protection ai sensi dell’art. 28 del Regolamento generale sulla protezione dei dati che lo vincoli al Titolare del Trattamento e che disciplini la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti delle parti, anche in termini di adozione di misure di sicurezza tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Le misure di sicurezza a livello organizzativo richieste consistono in:

ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.1	Ruoli e Responsabilità definiti formalmente in ambito Data Protection	Identificazione dei ruoli e delle responsabilità associate alle persone coinvolte nel trattamento dei dati. Devono essere opportunamente formalizzate, attraverso lettere di nomina, tutte le assegnazioni di responsabilità in ambito privacy (e.g. Nomine a responsabile del trattamento, Incaricato, Responsabile della Protezione dei dati o DPO, ecc.).	V
C.O.2	Formazione periodica in ambito Data Protection	Esistenza di corsi in aula o E-learning, newsletter, pillole formative periodiche per accrescere la conoscenza delle tematiche relative alla Data Protection	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.3	Svolgimento audit di sicurezza periodici e verifica in materia Data Protection	<p>Esistenza di un processo periodico relativo all'esecuzione di audit di sicurezza, anche da parte del Gruppo FS, inclusa la verifica della conformità normativa in ambito Data Protection</p> <ul style="list-style-type: none">- Gli audit di sicurezza devono essere eseguiti regolarmente, mediamente una volta l'anno oppure ogniqualvolta viene effettuato un cambiamento rilevante.- Gli audit di sicurezza dovrebbero essere condotti da enti indipendenti specializzati negli audit di sicurezza.- Un audit di sicurezza è un'indagine o una ricerca di evidenze per consentire l'analisi dell'adeguatezza dei meccanismi messi in campo per mitigare il rischio legato alla sicurezza delle informazioni, e deve essere effettuato soprattutto sugli ambienti dell'organizzazione critici per il conseguimento degli obiettivi strategici e operativi (ad esempio applicazioni critiche, sistemi informatici e reti che supportano servizi critici, apparecchiature per ufficio, ecc..).- Gli audit dovrebbe essere sia di tipo "procedurale", "fisico" e "tecnologico".	V
C.O.4	Monitoraggio periodico delle non conformità normative in ambito Data Protection	<p>Esistenza di un processo periodico di monitoraggio delle non conformità normative rilevate nei precedenti audit</p> <p>Il Fornitore dovrebbe essere tenuto ad eseguire il monitoraggio per proprio conto al fine di garantire efficacia del processo di remediation delle non conformità rilevate o eventualmente segnalate dal Titolare.</p>	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.5	Policy di sicurezza	Esistenza di politiche di sicurezza delle informazioni dell'intera organizzazione Deve essere definita e documentata una politica di sicurezza delle informazioni, da applicare a tutta l'organizzazione e deve essere nominata una persona (o un gruppo di persone) responsabile per il mantenimento di tale politica. La politica di la sicurezza delle informazioni dovrebbe specificare: - obiettivi di sicurezza delle informazioni (ad esempio sensibilizzare e formare il personale sulla sicurezza delle informazioni, garantire la sicurezza delle informazioni personali dei dipendenti, nel rispetto della normativa vigente ed a tutela del dipendente, rispettare gli impegni contrattuali inerenti alla sicurezza delle informazioni, garantire la sicurezza dei servizi erogati e i livelli di continuità operativa previsti nei contratti, ecc.); - strategia per il conseguimento degli obiettivi di sicurezza (ad esempio adottare un Sistema di Gestione della Sicurezza delle Informazioni, SGSI); - requisiti generali per il conseguimento degli obiettivi di sicurezza (ad esempio definire politiche e procedure per la sicurezza delle informazioni, definire ruoli e responsabilità della sicurezza delle informazioni, gestione del rischio, relazione con le terze parti, gestione degli asset, gestione della continuità operativa, ecc..)	V
C.O.6	Modello di controlli IT	Definizione di un set di controlli IT da implementare basati sui principali standard	V
C.O.7	Certificazione del sistema di sicurezza	Verifica di un sistema per l'acquisizione di un certificato che attesti che quel dato sistema soddisfa i requisiti di sicurezza dettati dall'entità certificatrice	V
C.O.8	Risk Assessment periodici	Devono essere periodicamente (almeno annualmente) effettuate delle sessioni di analisi, valutazione e trattamento dei rischi.	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.9	Implementazione inventario HW/SW	<p>Implementare un inventario dei dispositivi hardware e del software di proprietà dell'organizzazione. È necessario stilare un elenco di hardware e software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi.</p> <p>Non consentire l'installazione di software non compresi nell'elenco. Per tutti i dispositivi l'inventario deve indicare almeno:</p> <ul style="list-style-type: none">- il nome del sistema, la funzione;- le informazioni di configurazione (es. tipo e la versione del sistema operativo, RAM, CPU) ed il vendor;- il titolare responsabile della risorsa e l'ufficio associato.- il livello di criticità. <p>Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.</p>	V
C.O.10	Policy per la gestione degli accessi ai sistemi informatici	<p>Esistenza di politiche per la gestione degli accessi ai sistemi informatici</p> <p>Una politica (o policy) per il controllo degli accessi ai sistemi informatici è un documento che descrive i ruoli e le responsabilità e i requisiti di alto livello nell'ambito della gestione degli accessi logici nel corso dell'intero ciclo di vita delle utenze. A titolo esemplificativo ma non esaustivo, i requisiti previsti dalla politica per il controllo degli accessi sono:</p> <ul style="list-style-type: none">- restrizione dei diritti di accesso privilegiati (amministratori, utenze anonime quali ad esempio "root");- principi cardine dei diritti di accesso (need to know, separation of duties, least privilege, ecc.);- gestione dell'identificazione, autenticazione e autorizzazione degli utenti;- gestione delle password;- meccanismi di accesso.	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.11	Policy per la gestione del ciclo di vita del software (Secure SDLC)	Esistenza di una politica che definisce un ciclo di sviluppo sicuro del software secondo gli attuali standard di settore (es. OWASP)	V
C.O.12	Formazione sullo sviluppo sicuro	Assicurare che il personale che sviluppa abbia ricevuto un'adeguata formazione sulla scrittura di codice sicuro nel loro specifico ambiente di sviluppo.	V
C.O.13	Istruzioni operative per l'utilizzo delle risorse informatiche e internet	Definizione e implementazione di istruzioni operative per l'utilizzo delle risorse informatiche e internet.	V
C.O.14	Istruzioni operative per la cancellazione sicura dei dispositivi	Esistenza di una procedura che preveda la possibilità di cancellare in modo sicuro i dati dai dispositivi che trattano dati personali.	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.15	Clausola contrattuale, SLA e processo di monitoraggio dell'operato delle Terze Parti o "persone correlate"	<p>Definizione degli indicatori di prestazione chiave tra il Responsabile e le "Persone correlate" ad esso, al fine di fornire il livello di servizio desiderato e di revisionare periodicamente l'operato delle persone correlate.</p> <p>Nota bene: il termine "Persone correlate" è definito nell'accordo di riservatezza (NDA) Protocollo FS-AD-DCSPSA0011P20140000147 del 27/10/2014 . Ciò implica un processo di gestione delle relazioni per:</p> <ul style="list-style-type: none">a) monitorare le prestazioni del servizio per verificare che siano conformi agli accordi presi sui livelli di servizio (Service Level Agreement, SLA);b) rivedere periodicamente i report di servizio prodotti dalle persone correlate;c) condurre opportuni audit sulle persone correlate, confrontando i risultati con audit effettuati da revisori indipendenti, se disponibili, e predisporre delle opportune azioni di remediation per indirizzare le issue identificate;d) scambiare informazioni sugli incidenti di sicurezza delle informazioni;e) esaminare gli eventi relativi alla sicurezza delle informazioni, ai guasti e alle interruzioni relative al servizio erogato;f) risolvere e gestire qualsiasi problema riscontrato;g) assicurare che il fornitore possa garantire la continuità del servizio in caso di guasti gravi o disastri.	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.16	Reputation e Data Breach	<p>È necessario definire ed implementare un processo per tutelare la presenza sul web dell'organizzazione. In particolar modo identificare siti illegittimi e monitorare il web per identificare potenziali data breach.</p> <p>Deve essere definito ed implementato processo per garantire che:</p> <ul style="list-style-type: none">- i siti Web illegittimi (e.g. quelli utilizzati per gli attacchi phishing) vengano chiusi il più rapidamente possibile;- le relazioni con i provider di servizi internet siano coperte da un accordo sui livelli di servizio (Service Level Agreement, SLA);- siano rinnovate le registrazioni dei nomi di dominio (e.g. ogni due anni);- i dettagli dei server Web esposti su internet siano registrati in un apposito registro (o equivalente), che includa dettagli su hosting, indirizzo (o indirizzi) IP, nomi di dominio e certificati digitali utilizzati;- i nomi di dominio, che potrebbero essere utilizzati da un potenziale attaccante per mascherarsi come l'organizzazione, siano registrati dall'organizzazione;- i siti Web, impostati utilizzando nomi di dominio simili a quelli utilizzati dall'organizzazione, siano regolarmente monitorati (e.g. utilizzando servizi di monitoraggio delle parti esterne). <p>- potenziali data breach.</p>	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.17	Misure prescrittive per amministratori di sistema	<p>Esistenza di specifiche misure di sicurezza che devono essere adottate dagli amministratori di sistema Devono essere previsti dei controlli aggiuntivi quando si utilizzano delle utenze amministrative, in particolare:</p> <ul style="list-style-type: none">- gli accessi degli amministratori di sistema agli archivi elettronici devono essere registrati;- mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. Gestire l'inventario preferibilmente attraverso uno strumento automatico che segnali ogni variazione che intervenga.- Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.- Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, devono essere utilizzate solo per le situazioni di emergenza. Se si utilizzano utenze amministrative anonime bisogna specificare lo scopo di utilizzo, richiederne l'approvazione individuale per l'utilizzo, registrarne e monitorarne regolarmente l'uso.- Per le operazioni che richiedono privilegi, gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.18	Public Key Infrastructure - Processo di gestione chiavi di cifratura	Deve essere definito e documentato un processo per la gestione del ciclo di vita delle chiavi di cifratura / mascheramento dati (creazione, archiviazione, recupero, distribuzione, ritiro e distruzione). Il processo di gestione del ciclo di vita delle chiavi di cifratura / mascheramento dati deve essere definito e documentato e deve coprire almeno le seguenti tematiche: - ruoli e responsabilità dei proprietari delle chiavi di cifratura; - meccanismi di protezione delle chiavi di cifratura; - metodi utilizzati per la distribuzione delle chiavi di cifratura.	V
C.O.19	Public Key Infrastructure - Nomina dei responsabili delle chiavi di cifratura	Devono essere nominati i responsabili delle chiavi di cifratura / mascheramento dati e sensibilizzati sulle proprie responsabilità nell'uso e protezione delle chiavi. I responsabili delle chiavi di cifratura / mascheramento dati devono anche sottoscrivere che hanno compreso chiaramente le loro responsabilità per l'utilizzo e protezione delle chiavi di cifratura.	V
C.O.20	Ruoli e responsabilità in ambiente cloud	Devono essere definiti, registrati e comunicati in modo chiaro i ruoli e le responsabilità (in condivisione o suddivisione) in carico all'organizzazione e al Cloud Provider. Le informazioni e i file presenti nell'ambiente fornito dal cloud provider, creati o modificati durante l'utilizzo del servizio, possono essere fondamentali per la sicurezza delle operazioni, le attività di recovery e la continuità del servizio. La proprietà di tutti i beni e l'assegnazione delle responsabilità per le operazioni legate a tali attività, come quelle di backup e ripristino, devono essere definite e documentate. In caso contrario, c'è il rischio che il fornitore di servizi cloud presupponga che l'organizzazione esegua queste operazioni vitali (o viceversa), e può verificarsi una perdita di dati.	V



ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
C.O.21	Notifica data breach da parte del Cloud Provider	Il Cloud Provider deve segnalare tempestivamente all'organizzazione eventuali accessi non autorizzati a dati soggetti a regolamento GDPR, che possano causare perdite, divulgazioni o alterazioni dei dati.	V
C.O.22	Accordi di non divulgazione (Non Disclosure Agreement, NDA)	Il personale del Cloud Provider avente accesso a dati riservati deve essere soggetto ad obblighi di riservatezza. Il personale del Cloud Provider (e dei suoi sub-fornitori) deve sottoscrivere un accordo di non divulgazione (conosciuto anche come Non-Disclosure-Agreement, NDA) nel quale si dichiara di non divulgare dati riservati senza l'autorizzazione dell'organizzazione. Tale accordo deve essere valido anche a seguito della terminazione del contratto tra il Cloud Provider e l'organizzazione.	V



C.O.23	Processo formale di Change & Patch management	<p>Definizione di un processo formale che documenti la fase di autorizzazione e implementazione delle modifiche e dell'installazione delle patch all'interno di processi, sistemi o strutture aziendali</p> <p>Un processo di Gestione dei Cambiamenti (Change Management) deve trattare:</p> <ul style="list-style-type: none">- aggiornamenti e modifiche al software applicativo;- modifica delle informazioni dell'organizzazione (ad esempio file e database);- modifiche alle procedure utente/operative;- fix di emergenza;- modifiche a computer e reti. <p>Tipicamente, le attività sono:</p> <ol style="list-style-type: none">1) Richiesta di un cambiamento (Request for Change, RFC).2) Approvazione della richiesta.3) Test del cambiamento.4) Implementazione del cambiamento. <p>Il processo di gestione delle patch deve includere:</p> <ul style="list-style-type: none">- determinazione dei metodi per l'ottenimento delle patch;- determinazione dei metodi di convalida delle patch (ad esempio assicurare che la patch provenga da una fonte autorizzata);- identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione;- valutazione dell'impatto sull'organizzazione in seguito all'implementazione delle patch (o in seguito alla non implementazione di una patch specifica);- garantire che le patch siano testate in opportuni ambienti di test prima di essere installate in ambiente di esercizio;- descrizione dei metodi di distribuzione delle patch (ad esempio utilizzando tool di distribuzione del software);- installazione delle patch entro 30 giorni dalla comunicazione della vulnerabilità;- reportistica sullo stato di distribuzione delle patch in tutta l'organizzazione;- gestione dei fallimenti nella fase di distribuzione delle patch (ad esempio tentare nuovamente la distribuzione della patch fallita).	V
---------------	---	---	---



Tabella 10 – Requisiti di natura organizzativa

4.4 Requisiti relativi alla qualità della fornitura

ID	Item	Descrizione	Requisito vincolante (V) o requisito migliorativo (M)
IQ_1.2	Presentazione e Piano delle attività	<p>Ciascun Concorrente dovrà presentare, un Progetto tecnico costituito da:</p> <ol style="list-style-type: none">1. Un elaborato che dovrà essere suddiviso in tre parti:<ul style="list-style-type: none">• Descrizione della soluzione: descrizione della soluzione tecnica proposta, conforme ai requisiti vincolanti e, ove applicabile, dei requisiti migliorativi.• Capacità di gestione di progetti realizzativi descrizione degli strumenti e delle modalità di gestione e produzione della soluzione; delle metodologie adottate per la mitigazione delle criticità qualitative (manutenibilità, usabilità, affidabilità, sicurezza); degli strumenti e delle metodologie di testing a garanzia della conformità ai requisiti richiesti.	V



		<ul style="list-style-type: none">• Modalità di fornitura dei Servizi (massimo 5 pagine): illustrazione dell'organizzazione e dei processi aziendali per l'erogazione dei servizi e per la gestione delle attività di post-installazione.• [opzionale] una presentazione e descrizione della Società Offerente (massimo 2 pagine). <ol style="list-style-type: none">2. Video di presentazione della piattaforma3. Almeno un esempio di modalità di somministrazione del test e della video intervista4. Report (almeno tre esempi) generati dalla piattaforma, relativi ai risultati dei test e delle video interviste somministrate ai candidati.5. Un Piano delle attività (privo di indicazione del prezzo offerto) con dettaglio delle fasi, delle attività e della stima dell'impegno delle risorse, suddivisa per fasi e attività; eventuale introduzione di professionalità aggiuntive su richiesta e adozione di politiche di reiezione degli errori nelle attività progettuali, corredato da un documento in formato PowerPoint	
--	--	---	--



		(ppt) di massimo 1 slide contenente un Gantt riepilogativo (copertina e indice esclusi dal conteggio). Il dettaglio dei contenuti di cui sopra è presente sul disciplinare e/o relativi allegati	
IQ_1.2A	Piano delle attività valutazione	La qualità del piano delle attività proposto (IQ_1.2) verrà valutata dalla commissione di gara e comporterà attribuzione di un punteggio.	M
IQ_1.3	Curricula del Project Manager/Capo Progetto	Presenza di almeno 2 esperienze professionali, negli ultimi 5 anni maturate nell'ambito dello Smart Recruiting.	V
IQ_1.3A	Curricula del Project Manager/Capo Progetto specifica	Il Capo Progetto ha maturato, negli ultimi 5 anni, un'esperienza professionale nell'ambito dello Smart Recruiting con un'impresa avente dimensioni simili per numero di dipendenti e fatturato al Gruppo FS.	M
IQ_1.4	Curricula del Senior Specialist/professionis ta Senior	Aver maturato un'esperienza professionale di almeno 3 anni nell'ambito dello Smart Recruiting	V
IQ_1.5	Curricula del Junior Specialist/professionis ta Junior	Aver maturato un'esperienza professionale di almeno 1 anno nell'ambito dello Smart Recruiting	V

Tabella 5 – Indicatori di qualità della fornitura

4.5 Requisiti relativi Sostenibilità e Codice Etico



Sostenibilità 1	Certificazione UNI EN ISO 9001	Certificazione UNI EN ISO 9001 Sistemi di gestione della Qualità o Certificazione dei Sistemi di Gestione ISO/IEC 20000-1	M
Sostenibilità 2	Codici Etici e/o di Condotta	Adozione di Codici Etici e/o di Condotta, specie in relazione al trattamento di dati sensibili e personali	M
Sostenibilità 3	Parità di genere	Certificazione della parità di genere di cui all'articolo 46-bis del decreto legislativo n.196/2006	M
Sostenibilità 4	Certificazione SA 8000	Certificazione SA 8000 - Social Accountability	M

Tabella 6 – Indicatori di Sostenibilità e Codice Etico



5. Attività

Nel seguito vengono descritte le attività che il Service Provider dovrà effettuare nel periodo di vigenza contrattuale.

5.1. Attività e requisiti per il Set-up della Piattaforma

Si elencano nella Tabella le attività ed i requisiti specifici per il Set-up della Piattaforma.

ID	Item	Descrizione	Requisito Vincolante (V) o Requisito Migliorativo (M)
P.1	Piano di Lavoro	Il Service Provider, entro massimo 15 giorni lavorativi dalla sottoscrizione del contratto, dovrà sottoporre al Gestore del Contratto un Piano di Lavoro (PDL) contenente il dettaglio dei tempi di esecuzione di tutte le attività previste dall'avvio al Go Live della Piattaforma.	V
P.2	Progettazione	Si richiede che il Service Provider produca, entro e non oltre 20 giorni lavorativi dall'approvazione del PDL, come deliverable, un documento di Progettazione della Piattaforma contenente l'analisi dei requisiti ed il disegno della soluzione funzionale e tecnica comprendente anche l'integrazione con il sistema di Talent Acquisition del Gruppo.	V
P.3	Configurazione e attivazione	Il Service Provider, una volta ricevuta l'approvazione del documento di Progettazione della soluzione, dovrà procedere con le attività di configurazione e attivazione della stessa. È richiesta la completa configurazione ed il testing della Piattaforma, dei flussi di integrazione e dei sistemi informativi a supporto, in coerenza con il documento di Progettazione. La fase terminerà con il Collaudo che sarà condotto congiuntamente dal Gestore del Contratto, dal Service Provider e dal Fornitore del sistema di Talent Acquisition per la parte relativa all'integrazione tra le due soluzioni (sistema di Talent Acquisition e Piattaforma di test digitali e video interviste). Prima dell'avvio del Collaudo, il Service Provider dovrà condividere con il Gestore del Contratto e con il	V



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

		<p>Fornitore del sistema di Talent Acquisition un Documento di User Test, contenente i casi di Test da eseguire e che sarà aggiornato con i relativi esiti. Al termine del collaudo il Gestore del Contratto provvederà alla redazione di un Verbale di accettazione. Nel caso di esito negativo del Collaudo, il Service Provider dovrà provvedere, entro 8 giorni lavorativi, a svolgere ogni attività necessaria affinché il Collaudo sia ripetuto e positivamente superato, se necessario anche con il coinvolgimento del Fornitore del sistema di Talent Acquisition. Si richiede che si superi efficacemente il Collaudo prima della messa online della Piattaforma.</p> <p>La fase terminerà con l'attivazione della soluzione informatica che ha superato positivamente il Collaudo. Nelle more della realizzazione dell'integrazione tra il sistema master di Talent Acquisition e la Piattaforma, dovrà essere garantita la erogazione dei test e delle video interviste ai candidati e il ritorno dei risultati sul sistema master, mediante file con tracciati di tipo CSV. Anche per tale eventuale fase propedeutica è richiesto un documento di Progettazione e il Collaudo svolto con esito positivo.</p>	
--	--	---	--



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

ID	Item	Descrizione	Requisito Vincolante (V) o Requisito Migliorativo (M)
P.4	Formazione	È richiesto al Service Provider di effettuare attività formative in presenza per il team del Gruppo FS che utilizzerà la Piattaforma. La formazione dovrà essere tenuta in lingua italiana. È richiesto che siano erogate almeno 6 giornate formative della durata di 8 ore. La formazione dovrà essere erogata presso la sede di Ferrovie dello Stato Italiane sita in Roma a Piazza della Croce Rossa 1, da personale del Service Provider esperto della Piattaforma.	V
P.5	Manuale utente	Al termine della formazione dovrà essere rilasciato un Manuale utente e materiale multimediale come tutorial a supporto delle attività utente esercitate a sistema, sviluppati a valle degli interventi di personalizzazione effettuati.	V
P.6	Durata	È richiesto al Service Provider di indicare la durata della fase di start up.	V

Tabella 6 – Attività di set up



5.2. Attività e requisiti per la messa a regime e funzionamento della Piattaforma

Si riportano nella Tabella 7, le attività ed i requisiti per la messa a regime ed il funzionamento della Piattaforma.

ID	Item	Descrizione	Requisito Vincolante (V) o Requisito Migliorativo (M)
SaaS_S.1	Presenza in Europa	Il Service Provider deve avere una sede in Europa per garantire un supporto compatibile con il Gruppo FS.	V
SaaS_S.2	Presenza in Italia	Si richiede al Service Provider di specificare se ha sedi in Italia in grado di erogare supporto.	M
SaaS_S.3	Supporto tecnico e supporto operativo agli Utenti gestori	È richiesto al Service Provider di erogare supporto tecnico e supporto operativo agli utenti (interni) gestori della Piattaforma per l'intera durata dell'Accordo Quadro più eventuali proroghe.	V
SaaS_S.4	Canali di supporto base	È richiesto al Service Provider di supportare sia gli utenti interni del Gruppo FS, sia i candidati esterni attraverso i seguenti canali: e-mail.	V
SaaS_S.5	Canali di supporto extra	Il Service Provider supporta gli utenti interni del Gruppo FS attraverso un canale telefonico.	M
SaaS_S.6	Canali di supporto extra	Il Service Provider supporta gli utenti interni del Gruppo FS attraverso un canale live di messaggistica istantanea, chiamate audio e videochiamate, riunioni online.	M



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

SaaS_S.7	Integrazion e canale di supporto ticketing	Il Service Provider supporta il Gruppo FS attraverso un canale ticketing integrabile con i sistemi di governance IT. Per garantire l'interoperabilità occorre disporre di un web service di tipo SOAP o REST	M
SaaS_S.8	Orari supporto	Il Service Provider deve garantire il supporto sia agli utenti interni sia ai candidati esterni: 5 giorni alla settimana lavorativi secondo il calendario italiano dalle 9:00 alle 18:00 ora italiana nei giorni lavorativi del calendario italiano.	V
SaaS_S.9	Lingua supporto (in Italiano e Inglese)	Il supporto del Service Provider è fornito sia in lingua italiana, sia in lingua inglese, sia verso gli utenti interni della Piattaforma, sia verso i candidati.	V
SaaS_S.10	Lingua supporto integrative rispetto all'italiano e all'inglese	Il supporto del Service Provider è fornito in ulteriori lingue, rispetto a quella Italiana ed Inglese, riportate nel requisito SaaS_S.9.	M
SaaS_S.11	Canali di supporto – continuità del rapporto	Il Service Provider supporta il Gruppo FS mediante un team dedicato con cui è possibile interfacciarsi.	M

Tabella 7 – Requisiti per attività di messa a regime e funzionamento



5.3 Attività di dismissione della Piattaforma

Il fornitore si impegna ad eseguire le attività di dismissione del servizio entro 30 giorni dalla richiesta di cessazione dell'erogazione del servizio da parte di Ferrovie dello Stato S.p.A.

Al fine di preservare il patrimonio informativo maturato durante l'esercizio del sistema, il fornitore si assumerà l'onere, al termine del contratto, di consegnare l'esportazione e la raccolta di tutti i dati e i metadati caratterizzanti il processo di Smart Recruiting nei file in formato csv, xlsx, xml, mp4, avi, flv, e, se consentito dalla Piattaforma ospitante le informazioni, un backup che preservi la natura strutturata dei dati.

A valle della consegna a Ferrovie dello Stato S.p.A., su supporto magnetico e/o mediante un canale di comunicazione da concordare, il fornitore è tenuto a cancellare in modo permanente dalla propria Piattaforma i dati derivati e di backup relativi al processo di Smart Recruiting del gruppo Ferrovie dello Stato. Le modalità di scambio e di cancellazione dei dati dovranno rispondere ai criteri di portabilità del servizio e dei dati, descritti nei requisiti tecnici applicativi, di cui al paragrafo 4.3.1.



6. Monitoraggio del servizio e livelli di servizio attesi

6.1 KPI e Livelli di servizio attesi

In questo paragrafo sono riportati gli indicatori prestazionali del servizio erogato dal fornitore, con la definizione dei livelli di servizio attesi, parametrizzati in base al livello di severità e di priorità di una segnalazione di carenza riscontrata nell'esercizio delle funzionalità previste dalla Piattaforma.

Per la gestione dei problemi di servizio andrà impiegato il sistema di trouble ticketing adottato dal fornitore, il quale sarà alimentato con gli eventi necessari al calcolo dei KPI.

Al gruppo FS è consentito il pieno accesso a questo sistema per consultare i dati che concorrono alla determinazione degli indicatori ed il mancato rispetto di quelli identificati come critici comporta l'applicazione di penali. La tassonomia delle priorità è riportata nella Tabella 7 Tassonomia delle priorità mentre l'insieme degli indicatori prestazionali e loro livelli di servizi attesi nella Tabella 8 – Indicatori prestazionali e livelli di servizio.

Parametro	Definizione
Priorità 1	Problema bloccante per l'attività dell'utente o problemi che impattano gli utenti a contatto con il pubblico. Richiede un supporto risolutivo immediato, per consentire il proseguimento di un lavoro non rinviabile, con scadenza prevista per il giorno stesso o per il giorno successivo.
Priorità 2	Problema parzialmente bloccante per l'attività dell'utente. Richiede un supporto risolutivo per consentire il proseguimento di un lavoro non rinviabile o con scadenza fissata a pochi giorni di distanza.
Priorità 3	Problema non bloccante.

Tabella 8 – Tassonomia delle priorità



ID	KPI	Descrizione	Livello di servizio atteso
KPI_1.1	Recovery Time Objective (RTO) (Critico)	Recovery Time Objective (RTO, inteso come il massimo tempo di indisponibilità del servizio) minore o uguale a 4 ore. a. Periodo di riferimento del calcolo: mensile b. Periodicità di generazione del report: fine mese	≤4 ore di orologio nel periodo di riferimento
KPI_1.2	Disponibilità del servizio (Critico)	Disponibilità del servizio della Piattaforma deve essere 7 gg su 7gg festivi inclusi e H23; pertanto, lo SLA su base mensile viene definito in almeno il 98% dei minuti totali del periodo di riferimento (nel calcolo della disponibilità del servizio non saranno considerate interruzioni dovute a eventi di forza maggiore, inteso come un evento al di fuori del controllo del Service Provider o dovute a interventi manutentivi). a. Formula per il calcolo: $D = T_{ind} / T_d$ T_d = tempo in minuti del servizio nel periodo di riferimento; T_{ind} = tempo di reale disponibilità nel periodo di riferimento; b. Periodo di riferimento per il calcolo: mensile. c. Periodicità di generazione del report: fine mese	La percentuale di Disponibilità dell'applicazione deve essere $\geq 98\%$
KPI_1.3	Tempo medio di risposta dell'applicazione (indicativo)	Tempo medio di risposta calcolato su enne transazioni campione. a. Formula per il calcolo: Tempo medio di risposta = (Tempo di Risposta 1 + Tempo di Risposta 2 + Tempo di Risposta N)/N. N: numero transazioni campione; b. Periodo di riferimento per il calcolo: Trimestrale c. Periodicità di generazione del report: Trimestrale	La definizione delle transazioni campione e le modalità di rilevazione delle stesse saranno oggetto di analisi in fase post-contrattuale.
KPI_1.4	Recovery Point Objective (RPO) (critico)	Recovery Point Objective (X) indica la perdita massima di dati ammissibile, espressa come intervallo di tempo che intercorre tra l'ultimo backup effettuato e l'evento di compromissione tecnica del sistema. Minore o uguale a 4 ore di orologio.	$X \leq 4$ ore di orologio



KPI_2.1	Tempo di attesa per la presa in carico (canale telefonico) (Indicativo)	Tempo di attesa per la presa in carico di una chiamata di supporto telefonica. Per l'80% delle chiamate pervenute il tempo di presa in carico deve avvenire entro 20 secondi. <i>a. Formula:</i> $X \geq 80\%$ del totale delle chiamate telefoniche entranti devono essere prese in carico entro 20 s <i>b. Periodo di riferimento del calcolo:</i> mensile <i>c. Periodicità di generazione del report:</i> fine mese	$X \geq 80\%$ delle chiamate entranti prese in carico entro 20 secondi
KPI_2.2	Percentuale di chiamate entranti perse (canale telefonico) (Indicativo)	Percentuale di chiamate telefoniche di supporto entranti perse (abbandono per attesa o altri motivi). Deve essere inferiore al 5% del totale delle chiamate pervenute <i>a. Formula:</i> $X < 5\%$ del totale delle chiamate telefoniche entranti <i>b. Periodo di riferimento del calcolo:</i> mensile <i>c. Periodicità di generazione del report:</i> fine mese	$X < 5\%$ delle chiamate entranti deve essere perso o abbandonato per eccessiva attesa di risposta
KPI_2.3	Tempo di attesa per la presa in carico di segnalazioni provenienti da altri canali (escluso telefonico) (Indicativo)	Tempo di attesa per la presa in carico di segnalazioni e richieste di supporto non telefoniche. Per il 90% delle chiamate pervenute il tempo di presa in carico deve avvenire entro 4 ore di orologio. <i>a. Formula:</i> $X \geq 80\%$ del totale delle segnalazioni non telefoniche (altri canali) entranti devono essere prese in carico entro 4 ore <i>b. Periodo di riferimento del calcolo:</i> mensile <i>c. Periodicità di generazione del report:</i> fine mese	$X > 90\%$ delle segnalazioni entranti ad esclusione di quelle telefoniche, deve essere preso in carico entro 4 ore di orologio.



KPI_2.4	Tempo di assegnazione al supporto specialistico (Critico)	<p>Tempo di assegnazione della richiesta al supporto specialistico. Si divide per le 3 tipologie di priorità.</p> <p>a. Formula: <i>XP1 ≥ 90% del totale delle segnalazioni pervenute di Priorità 1 deve essere assegnato al supporto specialistico entro 10 minuti;</i> <i>XP2 ≥ 90% del totale delle segnalazioni pervenute di Priorità 2 deve essere assegnato al supporto specialistico entro 15 minuti;</i> <i>XP3 ≥ 90% del totale delle segnalazioni pervenute di Priorità 3 deve essere assegnato al supporto specialistico entro 20 minuti;</i></p> <p>b. Periodo di riferimento del calcolo: mensile</p> <p>c. Periodicità di generazione del report: fine mese</p>	Priorità 1: X ≥ 90% entro 10 minuti Priorità 2: X ≥ 90% entro 15 minuti Priorità 3: X ≥ 90% entro 20 minuti
KPI_3.1	Tempo medio di risoluzione delle richieste a partire dalla presa in carico (Critico)	<p>Tempo medio di risoluzione delle richieste di supporto, calcolate dalla presa in carico, diviso per priorità.</p> <p>a. Formula: <i>XP1 ≥ il tempo medio di risoluzione di almeno il 90% delle richieste pervenute di Priorità 1 deve essere stato inferiore o uguale a 2 ore di orologio;</i> <i>XP2 ≥ il tempo medio di risoluzione di almeno il 90% delle richieste pervenute di Priorità 2 deve essere stato inferiore o uguale ad 1 giorno next business day;</i> <i>XP3 ≥ il tempo medio di risoluzione di almeno il 90% delle richieste pervenute di Priorità 3 deve essere stato inferiore o uguale a 2 giorni next business day;</i></p> <p>b. Periodo di riferimento del calcolo: mensile</p> <p>c. Periodicità di generazione del report: fine mese</p>	Priorità 1: X ≥ 90% entro 2 ore Priorità 2: X ≥ 90% entro 1 gg next business day Priorità 3: X ≥ 90% entro 2 gg next business day



KPI_3.2	Percentuale di pianificazioni nei tempi (contenuti, stime impegno, tempi) delle manutenzioni programmate (Indicativo)	<p>Percentuale delle manutenzioni programmate effettuate entro 10 gg lavorativi dalla notifica.</p> <p>a. <i>Formula</i> $X = Neff / Ntot$ <i>Neff = Numero pianificazioni effettuate entro 10gg lavorative dalla notifica</i> <i>Ntot = Numero pianificazioni notificate</i></p> <p>b. <i>Periodo di riferimento del calcolo: mensile</i></p> <p>c. <i>Periodicità di generazione del report: fine mese</i></p>	X ≥ 90% entro 10 gg nbd
KPI_3.3	Rispetto della pianificazione dell'intervento (Critico)	<p>Percentuale di rispetto della risoluzione delle richieste.</p> <p>a. <i>Formula</i> $X = S / N$ (per le quattro tipologie) <i>S = numero richieste risolte nel rispetto della pianificazione concordata;</i> <i>N = numero totale di richieste pianificate nel periodo.</i></p> <p>b. <i>Periodo di riferimento del calcolo: mensile</i></p> <p>c. <i>Periodicità di generazione del report: fine mese</i></p>	<p>Adeguate: X ≥ 90%</p> <p>Adattive: X ≥ 90%</p> <p>Migliorative: X ≥ 90%</p> <p>Programmate: X ≥ 90%</p> <p>Altri interventi: X ≥ 90%</p>
KPI_3.4	Tasso di recidività (Indicativo)	<p>Percentuale di recidività</p> <p>a. <i>Formula</i> $X = R / N$ <i>R = numero di errori recidivi rilevati nel periodo;</i> <i>N = numero totale di errori rilevati nel periodo.</i></p> <p>b. <i>Periodo di riferimento del calcolo: mensile</i></p> <p>c. <i>Periodicità di generazione del report: fine mese</i></p>	X ≤ 5%
KPI_3.5	Difettosità del software in esercizio (Indicativo)	<p>Difettosità del SW in esercizio.</p> <p>a. <i>Formula</i> $X = R / N$ (per le tre tipologie di criticità) <i>R = numero di interventi di manutenzione correttivi effettuati sul software in esercizio;</i> <i>N = numero totale di function point in esercizio.</i></p> <p>b. <i>Periodo di riferimento del calcolo: mensile</i></p> <p>c. <i>Periodicità di generazione del report: fine mese</i></p>	<p>Criticità: Alta, X ≤ 0,4%;</p> <p>Criticità: Media, X ≤ 2%</p> <p>Criticità: Bassa, X ≤ 5%</p>



KPI_4.1	Tempestività aggiornamento delle firme di antivirus, antispam, sistemi di intrusion detection, database dei siti bloccati (Critico)	<p>Tempestività dell'aggiornamento delle firme. entro 1gg lavorativo</p> <p><i>a. Formula</i> $X = \text{Numero giorni lavorativi eccedenti la soglia di 1 giorno lavorativo di ritardo nell'aggiornamento di ciascuna firme per ogni tipologia di aggiornamento necessaria nel periodo.}$</p> <p><i>b. Periodo di riferimento del calcolo: mensile</i></p> <p><i>c. Periodicità di generazione del report: fine mese</i></p>	Soglia = 1gg lavorativo X è pari ai giorni totali eccedenti la soglia consentita (oltre 1 giorno)
KPI_4.2	Aggiornamento del motore antivirus (Indicativo)	<p>Tempestività dell'aggiornamento del motore antivirus.</p> <p><i>a. Formula</i> $X = \text{Numero giorni lavorativi eccedenti la soglia di 6 mesi di calendario nell'effettuare l'aggiornamento del motore antivirus nel periodo.}$</p> <p><i>b. Periodo di riferimento del calcolo: annuale</i></p> <p><i>c. Periodicità di generazione del report: fine anno</i></p>	S = 6 mesi di calendario
KPI_4.3	Tempo di identificazione di un attacco informatico (Indicativo)	<p>Tempo di identificazione di attacchi.</p> <p><i>a. Formula</i> $X = A / P$</p> <p><i>b. Periodo di riferimento del calcolo: mensile</i></p> <p><i>c. Periodicità di generazione del report: fine mese</i></p>	X < 20 minuti dal manifestarsi di malfunzionamenti nel 98% dei casi; X < 1 ora nel 100% dei casi;
KPI_4.4	Tempo di applicazione delle procedure di risposta ad un attacco (critico)	<p>Tempo di applicazione delle procedure di risposta ad un attacco. Soglia 1 ora di orologio.</p> <p><i>a. Formula</i> $P = \text{Numero ore di ritardo relative a tutte le procedure attivate oltre la soglia prevista di un'ora di orologio}$</p> <p><i>b. Periodo di riferimento del calcolo: mensile</i></p> <p><i>c. Periodicità di generazione del report: fine mese</i></p>	Soglia = 1 ora di orologio



<p>KPI_4.5</p>	<p>Tempo di erogazione dell'incident report (indicativo)</p>	<p>Tempo di produzione dell'incident report. Entro 22 gg lav. <i>a. Formula</i> $X = R / N$ <i>R = numero incident report prodotti entro 2 gg lavorativi;</i> <i>N = numero totale incident report prodotti nel periodo di riferimento</i> <i>b. Periodo di riferimento del calcolo: mensile</i> <i>c. Periodicità di generazione del report: fine mese</i></p>	<p>X < 2 gg lavorativi nel 99% dei casi</p>
<p>KPI_4.6</p>	<p>Tempo di applicazione dei workaround di sicurezza dal momento della conoscenza, della ricezione o della pubblicazione della vulnerabilità (critico)</p>	<p>Tempo di applicazione del workaround di sicurezza <i>a. Formula</i> $W = \text{numero workaround applicati oltre 2 gg lavorativi}$ <i>b. Periodo di riferimento del calcolo: mensile</i> <i>c. Periodicità di generazione del report: fine mese</i></p>	<p>Soglia= 2 gg lavorativi</p>
<p>KPI_4.7</p>	<p>Tempo di applicazione delle patch dal momento della loro pubblicazione (critico)</p>	<p>Tempo di applicazione delle patch <i>a. Formula</i> $X = P / N$ <i>P = numero patch applicate entro soglia;</i> <i>N = numero totale patch applicate nel periodo di riferimento</i> <i>b. Periodo di riferimento del calcolo: mensile</i> <i>c. Periodicità di generazione del report: fine mese</i></p>	<p>X ≤ 5 gg lavorativi per le vulnerabilità classificate come score HIGH nel 98% dei casi; X ≤ 10 gg lavorativi per le vulnerabilità classificate come score MEDIUM nel 98% dei casi; X ≤ 15 gg lavorativi per le vulnerabilità classificate come score LOW nel 98% dei casi; X ≤ 30 gg solari nel 100% dei casi;</p>
<p>KPI_5.1</p>	<p>Effettuazione periodica del test di DR (critico)</p>	<p>Test di Disaster Recovery. Un test a semestre. <i>a. Formula</i> $W = \text{numero test effettuati oltre la soglia prevista pari ad 1 a semestre.}$ <i>b. Periodo di riferimento del calcolo: annuale.</i> <i>c. Periodicità di generazione del report: fine anno</i></p>	<p>Soglia di un test per semestre</p>



KPI_6.1	Completamento attività del piano di progetto operativo (PPO) (<i>critico</i>)	<p>Percentuale di completamento delle attività inserite nel PPO nei tempi massimi previsti</p> <p><i>a. Formula</i> $X = A / N$ <i>A = numero attività completate entro i tempi massimi previsti.</i> <i>N = numero totale di attività del PPO.</i></p> <p><i>b. Periodo di riferimento del calcolo: per singola iniziativa progettuale</i></p> <p><i>c. Periodicità di generazione del report: fine iniziativa progettuale</i></p>	$X \geq 80\%$
KPI_6.2	Rilascio documenti e deliverable (su milestone del PPO) (<i>indicativo</i>)	<p>Percentuale di documenti e deliverable previste come milestone nel PPO, rilasciati entro i tempi massimi previsti.</p> <p><i>a. Formula</i> $X = D / N$ <i>D = numero di deliverable rilasciati e accettati entro i tempi massimi previsti.</i> <i>N = numero totale di deliverable consegnati.</i></p> <p><i>b. Periodo di riferimento del calcolo: per singola iniziativa progettuale</i></p> <p><i>c. Periodicità di generazione del report: fine iniziativa progettuale</i></p>	$X \geq 90\%$
KPI 7.1	Tempo di segnalazione di un data breach su dati oggetto di privacy	<p>Tempo di segnalazione di un data breach su dati oggetto di privacy</p> <p>Fonte dei dati: Strumenti per l'erogazione dei servizi resi disponibili dal Fornitore o dal Gruppo FS o sulla base delle comunicazioni relative all'eventualità di data breach tra Fornitore e Cliente</p> <p>Unità di misura: ore solari</p> <p>Dati da rilevare:</p> <ul style="list-style-type: none"> - Data di identificazione del data breach (DI) - Data di notifica del data breach (DN) <p>entrambi i valori non devono superare la soglia di 12 ore solari</p> <p>DP_NDB = 12 Ore solari (soglia)</p> <p>Periodo di rilevazione: ad evento</p>	DP_NDB= 12 ore solari



KPI 7.2	<p>Tempo di risposta del Fornitore al Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato</p>	<p>Tempo di risposta del Fornitore al Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato Unità di misura: GG Lavorativi Fonte dei dati: Risposta del Fornitore al Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato Dati da rilevare: • Data di risposta del Fornitore al Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato (Drisp) • Data di richiesta al Fornitore dal Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato (Drich) Valore soglia: $DP_TGR \leq 3$ gg lavorativi Formula $DP_TGR = Drisp \text{ e } Drich < 3$ gg</p>	<p>$DP_TGR \leq 3$ gg lavorativi</p>
KPI 7.3	<p>Tempo di notifica al Gruppo FS della richiesta di esercizio di diritti da parte di un interessato ricevuta direttamente dal Fornitore</p>	<p>Tempo di notifica al Gruppo FS della richiesta di esercizio di diritti da parte di un interessato ricevuta direttamente dal Fornitore Unità di misura: GG Lavorativi Fonte dei dati: Richiesta di esercizio di diritti da parte di un interessato ricevuta direttamente dal Fornitore Dati da rilevare: • Data di risposta del Fornitore al Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato (Drisp) • Data di richiesta al Fornitore dal Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato (Drich) Valore soglia: $DP_TGG \leq 3$ gg lavorativi Formula $DP_TGG = Drisp \text{ e } Drich < 3$ gg</p>	<p>$DP_TGG \leq 3$ gg lavorativi</p>

Tabella 9 – Indicatori prestazionali e livelli di servizio



7. Penali

Di seguito vengono indicate le penali previste relativamente ai KPI descritti nel paragrafo precedente.

ID	KPI	Livello di servizio atteso	PENALE
KPI_1.1	Recovery Time Objective (RTO) <i>(Critico)</i>	≤4 ore di orologio nel periodo di riferimento	Per ogni ora eccedente alle 4 ore, la penale prevede il pagamento del 2,5% del corrispettivo mensile del servizio, fino ad un massimale del 10% del canone mensile
KPI_1.2	Disponibilità del servizio <i>(Critico)</i>	La percentuale di Disponibilità dell'applicazione deve essere ≥ 98%	La penale prevede Il pagamento del 2,5% del canone mensile per ogni 0,1% di scostamento rispetto al valore soglia consentito, fino ad un massimale del 10% del canone mensile.
KPI_1.3	Tempo medio di risposta dell'applicazione <i>(indicativo)</i>	La definizione delle transazioni campione e le modalità di rilevazione delle stesse saranno oggetto di analisi in fase post- contrattuale.	KPI Indicativo non dà luogo a penale
KPI_1.4	Recovery Point Objective (RPO) <i>(critico)</i>	$X \leq 4$ ore di orologio	Per ogni ora di ritardo nel ripristino dati, si applica una penale pari al 2,5 % del corrispettivo mensile del servizio, fino ad un massimale del 10% del canone mensile.
KPI_2.1	Tempo di attesa per la presa in carico (canale telefonico) <i>(Indicativo)</i>	$X \geq 80\%$ delle chiamate entranti prese in carico entro 20 secondi	KPI Indicativo non dà luogo a penale
KPI_2.2	Percentuale di chiamate entranti perse (canale telefonico) <i>(Indicativo)</i>	$X < 5\%$ delle chiamate entranti deve essere perso o abbandonato per eccessiva attesa di risposta	KPI Indicativo non dà luogo a penale
KPI_2.3	Tempo di attesa per la presa in carico di segnalazioni provenienti da altri canali (escluso telefonico) <i>(Indicativo)</i>	$X > 90\%$ delle segnalazioni entranti ad esclusione di quelle telefoniche, deve essere preso in carico entro 4 ore di orologio.	KPI Indicativo non dà luogo a penale



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

KPI_2.4	Tempo di assegnazione al supporto specialistico (<i>Critico</i>)	Priorità 1: $X \geq 90\%$ entro 10 minuti Priorità 2: $X \geq 90\%$ entro 15 minuti Priorità 3: $X \geq 90\%$ entro 20 minuti	La penale prevede Il pagamento del 1 % del corrispettivo mensile del servizio per ogni 5% di scostamento rispetto alle soglie previste. Fino ad un massimale del 10% del canone mensile
KPI_3.1	Tempo medio di risoluzione delle richieste a partire dalla presa in carico (<i>Critico</i>)	Priorità 1: $X \geq 90\%$ entro 2 ore Priorità 2: $X \geq 90\%$ entro 1 gg next business day Priorità 3: $X \geq 90\%$ entro 2 gg next business day	La penale prevede l pagamento dello 1% del corrispettivo mensile del servizio per ogni 5% di scostamento rispetto alle soglie previste. Fino a massimale del 10% del canone mensile
KPI_3.2	Percentuale di pianificazioni nei tempi (contenuti, stime impegno, tempi) delle manutenzioni programmate (<i>Indicativo</i>)	$X \geq 90\%$ entro 10 gg nbd	KPI Indicativo non dà luogo a penale
KPI_3.3	Rispetto della pianificazione dell'intervento (<i>Critico</i>)	Adeguate: $X \geq 90\%$ Adattive: $X \geq 90\%$ Migliorative: $X \geq 90\%$ Programmate: $X \geq 90\%$ Altri interventi: $X \geq 90\%$	La penale prevede Il pagamento dello 0,25% del corrispettivo mensile del servizio per ogni 0,5% di scostamento rispetto alla soglia prevista, fino ad un massimale del 10% del canone mensile.
KPI_3.4	Tasso di recidività (<i>Indicativo</i>)	$X \leq 5\%$	KPI Indicativo non dà luogo a penale
KPI_3.5	Difettosità del software in esercizio (<i>Indicativo</i>)	Criticità: Alta, $X \leq 0,4\%$; Criticità: Media, $X \leq 2\%$ Criticità: Bassa, $X \leq 5\%$	KPI Indicativo non dà luogo a penale
KPI_4.1	Tempestività aggiornamento delle firme di antivirus, antispam, sistemi di intrusion detection, database dei siti bloccati (<i>Critico</i>)	Soglia = 1gg lavorativo X è pari ai giorni totali eccedenti la soglia consentita (oltre 1 giorno)	Per ogni giorno lavorativo eccedente, si prevede il pagamento di una penale pari a 100 euro, fino ad un massimale pari al 10% del canone mensile.
KPI_4.2	Aggiornamento del motore antivirus (<i>Indicativo</i>)	$S = 6$ mesi di calendario	KPI Indicativo non dà luogo a penale



**Piattaforma a supporto del processo di Smart Recruiting del Gruppo Ferrovie dello Stato Italiane
Capitolato Tecnico**

KPI_4.3	Tempo di identificazione di un attacco informatico <i>(Indicativo)</i>	X < 20 minuti dal manifestarsi di malfunzionamenti nel 98% dei casi; X < 1 ora nel 100% dei casi;	KPI Indicativo non dà luogo a penale
KPI_4.4	Tempo di applicazione delle procedure di risposta ad un attacco <i>(critico)</i>	<i>Soglia = 1 ora di orologio</i>	Si prevede il pagamento di una penale pari a 100 euro per ogni ora di ritardo per ogni procedura attivata oltre la soglia, fino ad un massimale pari al 10% del canone mensile.
KPI_4.5	Tempo di erogazione dell'incident report <i>(indicativo)</i>	X < 2 gg lavorativi nel 99% dei casi	KPI Indicativo non dà luogo a penale
KPI_4.6	Tempo di applicazione dei workaround di sicurezza dal momento della conoscenza, della ricevuta comunicazione o della pubblicazione della vulnerabilità <i>(critico)</i>	<i>Soglia= 2 gg lavorativi</i>	Si prevede il pagamento di una penale pari a 100 euro per ogni workaround applicato oltre la soglia, fino ad un massimale pari al 10% del canone mensile.
KPI_4.7	Tempo di applicazione delle patch dal momento della loro pubblicazione <i>(critico)</i>	X ≤ 5 gg lavorativi per le vulnerabilità classificate come score HIGH nel 98% dei casi; X ≤ 10 gg lavorativi per le vulnerabilità classificate come score MEDIUM nel 98% dei casi; X ≤ 15 gg lavorativi per le vulnerabilità classificate come score LOW nel 98% dei casi; X ≤ 30 gg solari nel 100% dei casi;	La penale prevede il pagamento dello 0,05% del corrispettivo mensile del servizio per ogni scostamento dell'1% rispetto alla soglia prevista, fino ad un massimale del 10% del canone mensile.
KPI_5.1	Effettuazione periodica del test di DR <i>(critico)</i>	Soglia di un test per semestre	Si prevede il pagamento di una penale pari a 2500 euro per ogni test non effettuato nei tempi previsti, fino ad un massimale pari al 10% del canone annuo.



KPI_6.1	Completamento attività del piano di progetto operativo (PPO) (<i>critico</i>)	$X \geq 80\%$	La penale prevede il pagamento dello 0,5% del corrispettivo mensile del servizio, per ogni 1% di scostamento rispetto alla soglia prevista, fino ad un massimale del 10% del canone mensile.
KPI_6.2	Rilascio documenti e deliverable (su milestone del PPO) (<i>indicativo</i>)	$X \geq 90\%$	KPI Indicativo non dà luogo a penale
KPI 7.1	Tempo di segnalazione di un data breach su dati oggetto di privacy	DP_NDB= 12 ore solari	1 euro/soggetto interessato per " DI e DN >12 ore (per ogni ora eccedente il valore soglia) fino ad un massimo di 50 ore per evento e per soggetto.
KPI 7.2	Tempo di risposta del Fornitore al Gruppo FS in merito ad una richiesta di esercizio di diritti da parte di un interessato	DP_TGR \leq 3 gg lavorativi	Azioni contrattuali: • Fino a 2 gg di ritardo: € 50 a record • Da 2 -10 gg di ritardo: € 100 a record • Da 10 - 20 gg di ritardo: € 1.000 a record • Oltre 20 gg di ritardo: € 10.000 a record
KPI 7.3	Tempo di notifica al Gruppo FS della richiesta di esercizio di diritti da parte di un interessato ricevuta direttamente dal Fornitore	DP_TGG \leq 3 gg lavorativi	Azioni contrattuali: • Fino a 2 gg di ritardo: € 50 a record • Da 2 -10 gg di ritardo: € 100 a record • Da 10 - 20 gg di ritardo: € 1.000 a record Oltre 20 gg di ritardo: € 10.000 a record

8. Data Protection

8.1 Obiettivi

Il Regolamento UE 2016/679 (Regolamento Europeo in materia di protezione dei dati personali, di seguito "GDPR") nonché le disposizioni e i Provvedimenti emanati dall'Autorità Garante per



la Protezione dei Dati Personali, si prefiggono di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

A tal fine, il Gruppo Ferrovie dello Stato Italiane si è dotato di un Framework di Data Protection inteso come l'insieme di ruoli e responsabilità, regole interne e metodologie volti ad accogliere i principi che il Regolamento stabilisce con particolare riferimento a:

- La necessità di strutturare un modello organizzativo per la Data Protection attraverso l'identificazione di ruoli e relative responsabilità in materia di trattamento di dati personali (c.d. principio di "accountability");
- La necessità di adottare approcci e politiche che tengano conto del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati e che garantiscano la protezione dei dati personali fin dalla fase di ideazione e progettazione di un trattamento o di un sistema informativo a supporto del trattamento (c.d. principio di "Data Protection by Design e by Default");
- La necessità di adottare approcci e politiche finalizzate alla gestione delle richieste di esercizio dei diritti da parte degli interessati;
- La necessità di valutare, gestire e mitigare i rischi connessi al trattamento di dati personali, mediante l'adozione di un insieme di misure di sicurezza adeguate a garantire la riservatezza, l'integrità e la disponibilità degli stessi.

Al fine di consentire il pieno rispetto dei principi suddetti, il Gruppo FS ricorre unicamente a Fornitori che assicurino il pieno adeguamento alle disposizioni del Regolamento UE 2016/679 e che soddisfino e sostengano, nel rispetto delle autonomie societarie, l'integrazione con il Framework di Data Protection di cui il Cliente si è dotato. Framework di Data Protection del Gruppo Ferrovie dello Stato Italiane

Nel rispetto della normativa in materia di Data Protection vigente e relativi regolamenti attuativi, i principi guida nella definizione e nell'attuazione delle misure tecniche ed organizzative a protezione dei dati personali prendono a riferimento i principali standard e best practice internazionali di Data Protection e security tra i quali a titolo esemplificativo e non esaustivo:



- ISO/IEC 27001:2022;
- ISO 27035:2016;
- ISO/IEC 27018:2019;
- ISO/IEC 29134:2017;
- COBIT 5;
- NIST Cybersecurity Framework for Critical Infrastructure, SP 800-145, SP 800-144, SP 500-299;
- ENISA Handbook on Security of Personal Data Processing;
- Cloud Control Matrix (CCM versione 4.0)
- EU NIS Directive 2022/2555;
- GDPR General Data Protection Regulation – Regolamento UE 2016/679;

Il Regolamento UE 679/2016 e il Framework di Data Protection adottato dal Gruppo FS necessitano di una sinergia tra Cliente (anche “Titolare del Trattamento”) e il Fornitore (anche “Responsabile del Trattamento¹”), richiedendo in particolare:

- Che il trattamento dei dati personali da parte del Fornitore e dei sub-fornitori si ispiri al rispetto dei principi generali del Regolamento UE 679/2016 e quindi che avvenga in modo lecito e secondo correttezza, valutando la pertinenza, l’adeguatezza e la non eccedenza dei dati rispetto alle finalità per le quali i dati sono trattati;
- Che i trattamenti effettuati da parte del Fornitore per conto del Cliente siano disciplinati da un apposito Accordo di Data Protection che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Cliente;
- Che il Cliente ricorra unicamente a Fornitori che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate al rischio dei trattamenti effettuati da parte del Fornitore per conto dello stesso;

¹ Si specifica che per alcuni trattamenti il Fornitore potrebbe essere identificato quale “Contitolare” o “Autonomo Titolare”. Il rapporto è in ogni caso disciplinato da specifici accordi di Data Protection.



- Che il Fornitore non possa designare un sub-fornitore – in qualità di sub-responsabile del trattamento – che effettui il trattamento, senza la previa autorizzazione da parte del Cliente. Il Fornitore garantisce che il sub-fornitore fornisca garanzie sufficienti per attuare misure tecniche ed organizzative adeguate al rischio dei trattamenti effettuati da parte del sub-fornitore per conto dello stesso;
- Che il Fornitore tratti i dati personali limitatamente alle attività di trattamento oggetto degli Accordi di Data Protection e soltanto su istruzione documentata del Cliente, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Fornitore; in tal caso, il Fornitore informa il Cliente circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- Che il fornitore trasferisca i dati personali provenienti dal cliente al di fuori dello Spazio economico europeo (SEE) solo previa autorizzazione scritta del Cliente stesso e sulla base delle istruzioni dallo stesso fornite, al fine di garantire che il livello di protezione delle persone interessate previsto dalla normativa vigente in materia di protezione dei dati personali non sia compromesso. Tuttavia, il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali può aver luogo, previa autorizzazione del Cliente, ai fini anche degli obblighi di informativa nei confronti degli interessati, nel caso in cui la Commissione europea abbia deciso che il Paese Terzo di destinazione garantisce un livello adeguato di protezione.
- Che il Fornitore garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- Che il Fornitore adotti tutte le misure e i controlli di Data Protection e Security definiti dal Cliente, a valle della valutazione dell'adeguato livello di sicurezza, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

8.2 Requisiti relativi ad aspetti organizzativi

Il Cliente comunicherà al Fornitore le proprie linee di indirizzo e le istruzioni specifiche in materia di Data Protection, sulla base delle quali, conseguentemente, il Fornitore dovrà effettuare il



trattamento dei dati personali.

8.3 Modello di interazione

Nell'ambito del trattamento dei dati personali per conto del Cliente, il Fornitore:

- Ove abbia nominato un Data Protection Office, comunica al Cliente i dati identificativi e di contatto dello stesso;
- Ove non abbia nominato un Data Protection Office – deve nominare un Referente/Focal Point che si interfacci con le Strutture di Data Protection del Cliente, per ogni tematica inerente il trattamento di dati personali; il Fornitore deve comunicare al Cliente i dati identificativi e di contatto della persona identificata.

Il *Data Protection Office* o Referente *Data Protection* del Fornitore, deve altresì assicurare la sua disponibilità a:

- Partecipare – su richiesta del Cliente – a Comitati Data Protection;
- Cooperare con il Cliente – tenendo conto della natura del trattamento e delle informazioni a disposizione – nel garantire il rispetto degli obblighi relativi alla valutazione d'impatto (Data Protection Impact Assessment) dei trattamenti dei dati che possono comportare un rischio elevato per i diritti e le libertà degli interessati;
- Collaborare con il Cliente nel rispetto di eventuali ordini emessi dall'Autorità Garante per la Protezione dei Dati Personali o dalle autorità giudiziarie in relazione al trattamento dei dati o accessi ispettivi;
- Trattare tempestivamente e adeguatamente tutte le richieste del Cliente in relazione al trattamento dei dati e attenersi alle linee guida e disposizioni dell'Autorità Garante per la Protezione dei Dati Personali in merito all'elaborazione dei dati.

8.4 Riservatezza e identificazione delle persone autorizzate al trattamento

Il Fornitore deve garantire che le persone autorizzate all'esecuzione del trattamento dei dati personali si siano impegnate a rispettare la riservatezza o che siano soggette ad un obbligo legale di riservatezza, anche per un periodo ragionevole dopo la fine del rapporto di lavoro con il Fornitore.

Il Fornitore e i sub-fornitori, se presenti, devono garantire che solo il personale qualificato,



debitamente autorizzato e addestrato tratterà i dati personali ai sensi degli Accordi di Data Protection stipulati.

Il Fornitore deve garantire, pertanto, che chiunque agisca sotto la sua autorità, che ha accesso ai dati personali, li tratti secondo specifiche istruzioni fornite dallo stesso o dal Cliente. In particolare, il Fornitore deve identificare l'ambito delle operazioni di trattamento consentite e deve:

- Identificare le persone autorizzate al trattamento e fornire alle stesse istruzioni dettagliate e formazione al fine di conformarsi alla normativa Data Protection e agli Accordi di Data Protection, assicurandosi che tali persone abbiano accesso solo ai dati personali la cui conoscenza è necessaria per svolgere i compiti loro assegnati;
- Adempiere alle prescrizioni ai fini della corretta applicazione dei provvedimenti del Garante per la Protezione dei Dati Personali relativi alla gestione degli amministratori di sistema, nonché alla normativa in vigore. I soggetti preposti dal Fornitore a svolgere funzioni di amministratori di sistema che godono di profili di accesso superiori a quelli degli utenti ordinari per quanto attiene le banche dati o gli applicativi contenenti i dati degli interessati oggetto delle operazioni di trattamento, devono essere previamente selezionati in base alla valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. La nomina degli amministratori di sistema deve avvenire per iscritto e con designazione individuale delle persone autorizzate al trattamento e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema operanti sui sistemi che ospitano i dati personali, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di richieste da parte del Cliente o accertamenti da parte del Garante. L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica, in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalla normativa in materia di protezione di dati personali. Il Fornitore deve provvedere
- al tracciamento dei log di accesso degli amministratori di sistema², secondo modalità definite in comune accordo con il Cliente. Entro il primo trimestre di ogni anno, il Fornitore

² L'operato degli amministratori di sistema deve essere oggetto di registrazione e memorizzazione mediante log delle attività (ad esempio: login, logout, ecc.) e adeguatamente protetto in modo da non poter essere cancellato da personale non autorizzato.



comunicherà al Cliente con apposito rapporto scritto il soddisfacimento delle prescrizioni in materia di Amministratori di Sistema.

I nomi di tali persone devono essere forniti al Cliente se richiesto.

8.5 Requisiti relativi ad aspetti tecnici

Tenendo conto della criticità dei trattamenti dei dati personali, sulla base dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, sia al momento di determinare i mezzi per il trattamento sia all'atto del trattamento, il Fornitore deve assicurare di porre in essere misure tecniche ed organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla (i) distruzione e perdita, dalla (ii) modifica, dalla (iii) divulgazione o accesso non autorizzato – in modo accidentale o illegale – a dati trasmessi, conservati o comunque trattati.

8.6 Progettazione del trattamento e protezione dei dati personali

La progettazione del trattamento dei dati personali e dei sistemi informativi a supporto deve essere improntata su un approccio di Data Protection By Design e By Default che prevede l'adozione di adeguate misure di sicurezza a tutela di tutto il ciclo di vita del trattamento dei dati personali.

Tali misure, identificate dal Cliente attraverso le attività di identificazione dei trattamenti a rischio elevato e Data Protection Impact Assessment svolte in collaborazione (ove previsto) con il Fornitore, sono tarate sul livello di criticità del trattamento e costituiscono parte integrante degli Accordi di Data Protection. Il Fornitore dovrà, pertanto, impegnarsi al rispetto delle misure identificate come adeguate in ragione del livello di rischio dei trattamenti di dati personali svolti per conto del Cliente. Il Framework di Data Protection del Gruppo FS prevede tre livelli di rischio dei trattamenti in ragione di probabilità di accadimento e possibili impatti per gli interessati.

A tali livelli sono associate le misure tecniche ed organizzative da adottare in funzione degli strumenti a supporto del trattamento (informatica individuale, server su intranet, server su internet, device mobili, Cloud) e di un giusto compromesso tra efficienza e costo del trattamento e limitazione del livello di rischio.

Tali misure, applicate in diverse combinazioni, definiscono tre livelli di protezione che agiscono a mitigazione della probabilità e dell'impatto:

- Livello 1: il trattamento di dati personali richiede by default l'adozione di misure di sicurezza tecniche ed organizzative (baseline);
- Livello 2: il trattamento di dati personali con una valutazione che comporti maggiori probabilità e impatti del rischio, richiede l'utilizzo di un livello di sicurezza medio aggiuntivo rispetto alla baseline.



- Livello 3: il trattamento di dati personali con una valutazione che comporti elevate probabilità e impatti del rischio, richiede l'utilizzo del livello di sicurezza massimo disponibile rispetto alla baseline.

In ragione del trattamento svolto dal Fornitore per conto del Cliente, il Fornitore si impegna ad adottare le misure di sicurezza adeguate al livello di rischio.

Su richiesta del Cliente il Fornitore è tenuto a restituire i dati personali trattati nell'ambito della prestazione dei Servizi e le relative copie ovvero cancella/distrugge tali dati, effettuando la dismissione sicura dei dispositivi di archiviazione e nel contempo certifica al Cliente che ha provveduto in tal senso, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. Al riguardo il Responsabile garantisce che non procederà più al trattamento di tali dati e assicura l'adozione di misure di sicurezza per la protezione degli stessi.

Inoltre, nel rispetto del principio di c.d. "limitazione della conservazione", sulla base delle istruzioni fornite dal Cliente per ciascun trattamento, il Fornitore provvede alla cancellazione (anche su copie esistenti) dei dati personali:

- Una volta terminato il periodo di retention;
- Su richiesta dell'interessato (si veda paragrafo successivo).

8.7 Esercizio dei Diritti da parte degli interessati

Il Fornitore, in caso di richieste pervenute al Cliente che fanno riferimento a dati personali trattati dal Fornitore, dovrà garantire al Cliente di poter soddisfare i seguenti diritti degli interessati (artt. 15 e ss. del GDPR):

- Diritto di Accesso: il Fornitore dovrà collaborare con il Cliente per confermare all'interessato se siano o meno in corso trattamenti di dati personali che lo riguardano, unitamente ad ulteriori informazioni che potrebbero essere nell'esclusiva disponibilità del Fornitore;
- Diritto di Cancellazione: il Fornitore, previa precisa ed esplicita conferma del Cliente, dovrà cancellare tutti i dati degli interessati richiedenti;
- Diritto di Portabilità: il Fornitore dovrà consentire al Cliente di trasmettere i dati personali che riguardano l'interessato, direttamente all'interessato o ad un altro Cliente indicato dall'interessato, attraverso un canale sicuro e utilizzando un formato strutturato, di uso comune e leggibile da dispositivo automatico, come concordato con il Cliente;
- Diritto di Rettifica: il Fornitore dovrà garantire al Cliente la rettifica e/integrazione dei Dati Personali degli interessati richiedenti;
- Diritto di Limitazione: il Fornitore dovrà garantire al Cliente la possibilità di limitare il trattamento dei dati personali dell'interessato richiedente, ad esempio: mediante dispositivi



tecniche che indichino chiaramente che il trattamento dei dati personali è stato limitato, in modo tale che i dati personali non siano sottoposti ad ulteriori trattamenti e non possano essere modificati;

- Diritto di Opposizione: il Fornitore dovrà garantire al Cliente che, in caso di opposizione al trattamento da parte dell'interessato, si astenga dal porre in essere qualsiasi ulteriore attività di trattamento dei dati personali.

Il Fornitore e i sub-fornitori comunicheranno ogni informazione utile al fine di aiutare il Cliente a rispettare i diritti degli interessati, e si attiveranno secondo le istruzioni del Cliente, entro 3 giorni lavorativi dal ricevimento dell'istanza da parte del Cliente.

Nel caso in cui il Fornitore riceva direttamente, o tramite un Sub-Fornitore, richieste di esercizio dei diritti, il Fornitore provvede a dare tempestiva comunicazione scritta al Cliente e comunque al massimo entro 3 giorni lavorativi dal ricevimento dell'istanza da parte dell'interessato, allegando una copia della richiesta e fornendo tutte le informazioni utili.

Il Fornitore e il Sub-Fornitore non rispondono a richieste degli interessati a meno che non siano autorizzati per iscritto dal Cliente a farlo.

8.8 Pronta notifica

Il Fornitore informerà tempestivamente il Cliente nei seguenti casi:

- Violazione dei dati (Data Breach) – Qualsiasi violazione dei dati personali della quale verrà a conoscenza, entro le tempistiche riportate nell'Appendice “Livelli di Servizio Attesi” dal momento in cui ne avrà notizia, fornendo gli elementi utili a valutare l'entità della violazione, tra i quali:
 - La natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - Nome e i dati di contatto di eventuali punti di contatto presso cui ottenere più informazioni;
 - Probabili conseguenze della violazione dei dati personali;
 - Misure adottate o di cui si propone l'adozione da parte del Cliente per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi);
 - Copia della eventuale notifica al Garante per la Protezione dei Dati della violazione dei dati personali (Data Breach)
- Richieste da parte degli interessati – Qualsiasi richiesta ricevuta direttamente dagli interessati nell'ambito dell'esercizio dei propri diritti, della quale verrà a conoscenza, entro le tempistiche riportate nell'Appendice “Livelli di Servizio Attesi” dal momento in cui ne avrà notizia;



- Istruzioni in violazione – Qualsiasi istruzione scritta ricevuta dal Cliente che, secondo il parere del Fornitore, è in violazione della Normativa Data Protection e/o in violazione dei doveri contrattuali ai sensi degli Accordi di Data Protection stipulati.



8.9 Audit di Data Protection

Il Fornitore rende disponibili al Cliente tutte le informazioni necessarie a dimostrare la conformità agli obblighi e delle istruzioni stabiliti nell'Accordo di Data Protection e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dallo stesso Cliente ovvero da un altro soggetto da questi autorizzato. In particolare, il Fornitore, su richiesta del Cliente ed entro 20 giorni lavorativi dalla medesima, si impegna a presentare le proprie procedure per il trattamento dei dati personali, ivi compreso l'elenco delle persone autorizzate, e a produrre una relazione di conformità dell'operato alla normativa vigente in materia di protezione dei dati personali.

Il Fornitore, inoltre, consente al Cliente l'accesso ai luoghi in cui viene effettuato il trattamento dei dati personali, compresi le strutture fisiche e i sistemi utilizzati e collegati al trattamento.

8.10 Processo di rilevazione e segnalazione del Data Breach

