



**Finanziato
dall'Unione europea**
NextGenerationEU



DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

RELAZIONE TECNICA

PIATTAFORMA BANDI "PA DIGITALE 2026"

Agosto 2022



INDICE

FINALITA' E CONTENUTI DEL DOCUMENTO	3
IL SISTEMA INFORMATICO PA DIGITALE 2026	5
2.1 Descrizione delle caratteristiche funzionali della Piattaforma	5
2.2 Descrizione delle caratteristiche tecniche della Piattaforma	10
2.2.1 Modalità automatizzate di verifica della qualità e affidabilità dei dati	11
2.2.2 Cadenza degli aggiornamenti del Sistema informativo	12
2.2.3 Procedure per l'aggregazione dei dati	12
2.2.4 Implementazione di eventuali sistemi di interoperabilità con ReGiS	13
2.2.5 Procedure per garantire la sicurezza e la gestione del sistema informativo, l'integrità e la riservatezza dei dati, la conservazione dei dati e dei documenti	14
CONCLUSIONI	17

<i>Versione</i>	<i>Descrizione della revisione</i>	<i>Data Emissione</i>
1	Relazione tecnica PA digitale 2026	12 agosto 2022

1. FINALITA' E CONTENUTI DEL DOCUMENTO

Il documento *“Relazione tecnica illustrativa piattaforma Bandi Pa digitale 2026”* (di seguito **Relazione tecnica**) si pone l'obiettivo di offrire una panoramica compiuta del Sistema informativo **“Pa digitale 2026”**, attraverso il quale vengono garantite la gestione, il monitoraggio, la rendicontazione e il controllo degli **interventi a “Lump Sum”** previsti nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) di competenza del **Dipartimento per la trasformazione digitale** (DTD) della Presidenza del Consiglio dei ministri.

La redazione di questo documento risponde, in primo luogo, all'esigenza di dimostrare come la Piattaforma sia effettivamente in grado di garantire:

- l'efficace esecuzione di **controlli sulla qualità e affidabilità dei dati**;
- le **verifiche sul rispetto di alcuni principi cardine** della normativa nazionale ed euro-unionale (divieto di conflitto d'interesse, divieto di doppio finanziamento, il principio di politica ambientale “Do Not Significant Harm”, ecc.);
- **l'interoperabilità tra Sistemi**;
- la **sicurezza, l'integrità, la riservatezza e la corretta conservazione dei dati e dei documenti trattati**, contribuendo così al raggiungimento di milestone e target e quindi al riconoscimento delle risorse finanziarie da parte della Commissione Europea.

La Relazione tecnica vuole altresì essere una risposta alle osservazioni, pareri e indicazioni emerse a seguito della procedura di audit di sistema svoltasi *on desk* e *in loco* e che ha avuto ad oggetto – inter alia – il sistema informativo, con particolare riferimento alle possibilità offerte dalla Piattaforma per la raccolta e l'accesso ai dati di cui all'art. 22.2 lettera d) del Regolamento (UE) 2021/241.

La Relazione tecnica si apre con una descrizione sintetica delle macroaree funzionali di cui si compone la Piattaforma Bandi e prosegue con l'illustrazione delle logiche di funzionamento dell'applicativo in merito a:

- modalità automatizzate di verifica della qualità e affidabilità dei dati;
- frequenza degli aggiornamenti rilasciati dal vendor e dai system integrator;

- aggregazione dei dati trattati;
- integrazione e interoperabilità con sistemi e database esterni;
- sicurezza, integrità, riservatezza nella conservazione e nell'utilizzo dei dati e dei documenti di progetto.

Il sistema informatico è in via di realizzazione secondo un piano di rilasci incrementale che consente al DTD di rispondere alle esigenze di gestione digitalizzata delle misure oggetto di monitoraggio nella Piattaforma, in linea con la *timeline* di pubblicazione degli Avvisi e con le necessità di attuazione e consuntivazione della spesa da parte delle PA target.

In particolare, allo stato attuale, sono state già pienamente rilasciate ed operative le funzionalità per la pubblicazione degli Avvisi, la gestione delle candidature, l'ammissione e decretazione dei finanziamenti e, in ultimo in ordine di data, la comunicazione dell'avanzamento degli step intermedi di attuazione e monitoraggio degli interventi (fascicolo elettronico di progetto e gestione del cronoprogramma).

La Relazione tecnica è corredata da una serie di tool aggiuntivi quali diagrammi di flusso, immagini e tabelle in grado di offrire una visione d'insieme delle caratteristiche funzionali e tecniche dell'applicativo.

Il documento è da considerarsi, allo stato attuale, in una versione preliminare, nelle more della piena disponibilità del Sistema Regis e dei relativi standard e policy per l'interoperabilità.



2. IL SISTEMA INFORMATICO PA DIGITALE 2026

2.1 Descrizione delle caratteristiche funzionali della Piattaforma



Il sistema informatico si compone delle seguenti macroaree funzionali:

- L'area **Gestione Utenti e Registrazione a Sistema** è finalizzata ad assicurare la registrazione e l'accesso alla Piattaforma da parte degli utenti di Back-Office e Front-end, sia da area pubblica che privata. Il sistema informatico consente infatti di definire ruoli e responsabilità da associare ad ogni utente abilitato all'uso dello stesso, configurando il profilo degli operatori sulla base dei permessi legati alle funzionalità disponibili e nel rispetto dei requisiti di sicurezza ed accessibilità. In particolare, il Sistema prevede la possibilità di assegnare utenze specifiche a:
 - o **Soggetti attuatori** per l'inserimento dei dati di attuazione/avanzamento fisico, procedurale e finanziario dei progetti;
 - o **Operatori di Back-office**, per gli aspetti autorizzativi e ai fini dei controlli gestionali ed a campione sull'evoluzione delle candidature e dei progetti finanziati;
 - o **Soggetti esterni incaricati dei controlli e del supporto specialistico** su base territoriale (es. Transformation Office).

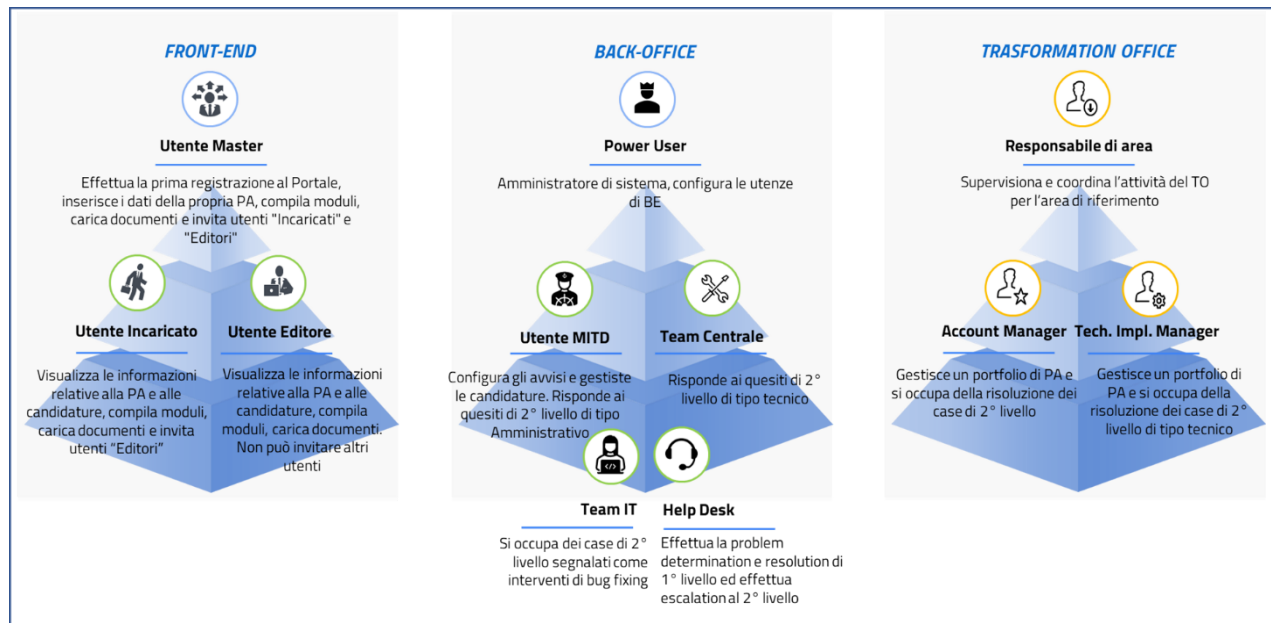


Figura 2 - Utenti e con di visibilità

Questa macroarea funzionale si compone dei seguenti moduli:

Accesso al Sistema per gli Utenti Master o collaboratori registrati, attivi o non attivi, inclusivo dell'autenticazione tramite SPID o CIE;

Registrazione Utente Master, comprensivo della gestione delle richieste di supporto e dei case di subentro;

Gestione Utenti collaboratori, che include l'invito, la modifica e la revoca dei collaboratori dell'utenza Master (Incaricato ed Editore);

Creazione/Accesso utenza MITD, che include la creazione, l'attivazione e l'accesso a Sistema degli operatori del MITD;

Supporto agli utenti esterni di Front Office, nella forma di ricezione e presa in carico dei ticket.

- L'area **Set-up degli Avvisi Pubblici** è finalizzata alla configurazione delle Misure e degli Avvisi pubblici, alla modalità di ricerca di specifici Avvisi all'interno del Portale ed a tutti agli aspetti legati alla loro visualizzazione. Si compone dei seguenti moduli:

Creazione e gestione Avvisi e associazione del budget, inclusivo della creazione delle Misure e dei nuovi Avvisi e della loro configurazione sulla base delle logiche di clusterizzazione (tipologia e dimensione dell'Ente), della gestione delle finestre temporali del singolo Avviso e del budget associato, della pubblicazione degli Avvisi e della gestione degli allegati;

Visualizzazione Avvisi pubblicati, che permette la visualizzazione degli avvisi in area pubblica (pagina "Avvisi" del portale) e in area privata (Scrivania), la ricerca di Avvisi di interesse all'interno del Portale e l'accesso al dettaglio del singolo Avviso;

- L'area **Candidatura** è finalizzata alla gestione *end-to-end* del processo di candidatura dell'Ente/Soggetto attuatore potenziale beneficiario di finanziamento. Si compone dei seguenti moduli:

Generazione della Candidatura, che consente all'utente di Front end di inserire i propri dati anagrafici, di autodichiarare la conformità alla normativa pertinente, di selezionare i servizi per i quali si intende ottenere il finanziamento, di visualizzare una scheda di riepilogo delle informazioni inserite e di procedere alla validazione della candidatura a valle dei controlli previsti sulla firma digitale.

Ammissione e non ammissione della candidatura, sulla base del budget disponibile e relative comunicazioni;

- L'area **Accettazione del finanziamento** è finalizzata alla verifica di ammissibilità al finanziamento delle candidature ricevute nella finestra temporale di riferimento da parte del MITD e alla gestione del processo di accettazione del finanziamento da parte dei Soggetti attuatori. Si compone dei seguenti moduli:

Registrazione del Codice Unico di Progetto, attraverso la procedura concordata con il DIPE e basata sul Codice template di progetto.

Accettazione o non accettazione del finanziamento, per inserimento o mancato inserimento del CUP e relativo aggiornamento del counter dei fondi disponibili;

Decreto di finanziamento, inclusivo della generazione del decreto di finanziamento e dei controlli sulla presenza e validità della firma digitale del Capo del Dipartimento per la Trasformazione digitale;

- L'area **Attuazione degli interventi finanziati** è finalizzata alla gestione *end-to-end* dei progetti, dalla selezione dei soggetti realizzatori e fino all'invio della richiesta di finanziamento. Tutte le informazioni relative ai progetti sono messe a disposizione dei diversi soggetti, per quanto riguarda le attività di competenza (monitoraggio, controllo, valutazione), secondo le forme più opportune (sola visualizzazione, estrazione di report analitici, dati aggregati). L'area funzionale si compone dei seguenti moduli:

Fascicolo elettronico di progetto, contenente l'anagrafica dell'operazione, le informazioni *in progress* sull'avanzamento delle attività e relative notifiche/alert personalizzate sulla base del calendario degli adempimenti del beneficiario.

Aggiunta soggetto realizzatore e subappaltatore, per l'assegnazione di ciascun servizio scelto in fase di candidatura ad uno o più fornitori e inclusivo delle autodichiarazioni di conformità al DNSH (verifiche ex-ante);

Contrattualizzazione dei fornitori, per il caricamento dei contratti di fornitura;

Completamento delle attività, per modificare lo stato di avanzamento del progetto inteso come completamento dell'integrazione dei servizi scelti in fase di candidatura;

Richiesta di erogazione del finanziamento, che include l'indicazione del responsabile e del luogo di conservazione della documentazione progettuale, l'inserimento dei dati contabili, le autodichiarazioni di conformità al DNSH (verifiche ex-post), le autodichiarazioni di conformità al divieto di conflitto d'interesse e doppio finanziamento, la generazione della richiesta di erogazione del finanziamento, il caricamento di allegati.

- L'area **Controlli** è finalizzata a garantire la correttezza delle procedure gestionali ed amministrative; a limitare al massimo il rischio di frodi, di conflitto d'interesse e doppio

finanziamento, assicurando al contempo la compliance normativa e regolamentare; a storicizzare gli esiti delle verifiche; a gestire le eventuali fasi di integrazione documentale o controdeduzione. Si compone dei seguenti moduli:

I controlli automatizzati sull'ammissibilità delle candidature e sull'accettazione del finanziamento, che includono i controlli su Firma digitale, Codice fiscale del rappresentante legale, Fondi disponibili e Codice Unico di progetto;

I controlli gestionali sul 100% dei progetti, che comprendono la valutazione della conformità tecnica del progetto da parte di soggetti terzi indipendenti, la compilazione di checklist di conformità e il caricamento (eventuale) di documentazione a Sistema.

Le verifiche a campione dei Progetti, basate di metodologie di campionamento stabilite extra-sistema e che possono condurre a richieste di integrazioni da parte del DTD e ad eventuali controdeduzioni a cura delle PA target.

- L'area **Monitoraggio e Reportistica** è finalizzata alla registrazione, aggregazione e rielaborazione dei dati necessari per l'estrazione degli indicatori di output, dei dati finanziari e per ogni altra esigenza di monitoraggio dell'avanzamento fisico e finanziario e del progressivo avvicinamento alle milestone ed ai valori target (tracking checkpoints) nazionali ed europei. In tal senso il prodotto Salesforce mette a disposizione strumenti per l'estrazione di report ad hoc personalizzati, strumenti per l'estrazione automatica, anche in forma aggregata, delle informazioni relative all'attuazione dei progetti, cruscotti di monitoraggio ed estrazioni in file editabili per la consultazione di apposite tavole numeriche. Più precisamente, l'area funzionale garantisce, a titolo esemplificativo, i seguenti moduli minimi:

Dashboard di adozione, i cui componenti sono: numero enti registrati all time (metric chart), % enti registrati su totale platea (gauge chart), numero enti con almeno una richiesta (metric chart), % enti con almeno una richiesta su totale platea (gauge chart), enti registrati ed enti con almeno una richiesta per regione

(vertical bar chart), numero candidatura per giorno e cumulate per giorno (line chart);

Dashboard case management, i cui component sono: numero Case non chiusi su coda helpdesk (metric chart), numero Case non chiusi spaccati su code secondo livello (donut chart), numero Case aperti alla data (line chart), Ageing Case non chiusi (vertical bar chart), Top 10 tipologia Case creati all time (horizontal bar chart), Tempo medio chiusura in ore per coda lavorazione (vertical bar chart);

Export andamento misure, i cui campi di interesse sono: Misura, Tipologia Ente, Area geografica Ente, Nome Ente, Candidatura, Importo richiesto, Stato candidatura, Data Creazione, Settimana Creazione, Anno Creazione.

2.2 Descrizione delle caratteristiche tecniche della Piattaforma

Il Sistema Pa digitale 2026 si basa su un'**architettura modulare**, coerentemente con i processi amministrativi di programmazione, attuazione, gestione contabile, rendicontazione e controllo del PNRR e consente, a ciascun profilo abilitato, di eseguire, all'interno dei diversi moduli, le specifiche attività di competenza.

Il Sistema Informatico assicura la rilevazione costante dello stato di attuazione degli interventi in termini di avanzamento finanziario, fisico e procedurale ed è stato sviluppato sulla base di un'**architettura tecnologico-funzionale ibrida**, fondata sull'utilizzo delle feature disponibili della soluzione *product* (Salesforce), fornita su licenza al MITD, e sullo sviluppo *custom* di una soluzione di front-end applicativa integrata con le componenti di back-end. Le funzionalità del Sistema a supporto della fase di candidatura e selezione (Fase 2) sono state rilasciate in data 4 aprile 2022 mentre quelle che consentono alle PA target di gestire la fase di attuazione degli interventi (fase 3) sono attualmente in corso di rilascio, secondo un ordine di priorità che riflette le esigenze pratiche di rendicontazione, controllo e monitoraggio degli Avvisi pubblicati dal Ministero. Si propone di seguito una rappresentazione grafica delle principali caratteristiche tecnologiche che caratterizzano il Sistema Pa digitale 2026.

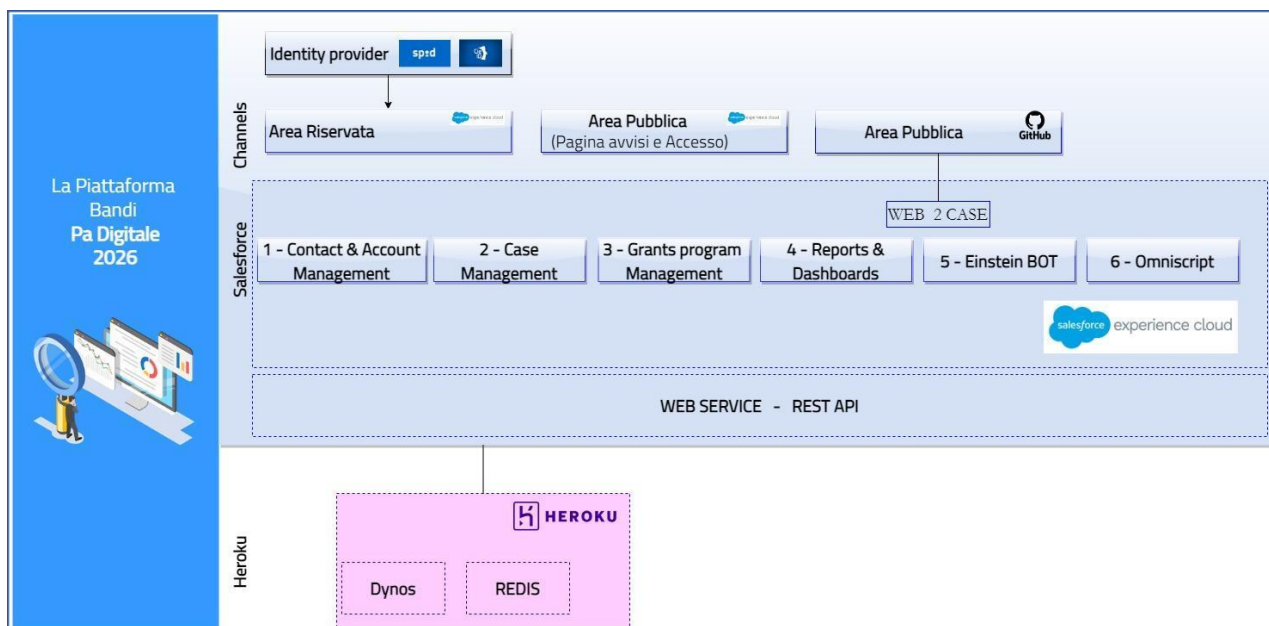


Figura 3 - Rappresentazione grafica delle principali caratteristiche funzionali che caratterizzano il Sistema "Pa digitale 2026"

2.2.1 Modalità automatizzate di verifica della qualità e affidabilità dei dati

Il Sistema Pa digitale 2026 è uno strumento funzionale alle richieste di partecipazione agli Avvisi pubblici emanati dal MITD. La compilazione delle domande di partecipazione e, in seguito, l'avanzamento progettuale prevedono l'inserimento di una molteplicità di dati da parte dell'utente rappresentativo della PA target. La piattaforma prevede pertanto controlli automatizzati sulla qualità e l'affidabilità dei dati inseriti o recuperati da fonti esterne.

Tra le modalità automatizzate di verifica della qualità ed affidabilità del dato si evidenziano:

- o **I controlli sulla firma digitale** (presenza della firma, validità della firma, identità della firma) apposta sulla documentazione in fase di candidatura.
- o **I controlli**, attualmente in corso di realizzazione, **relativi alla veridicità delle dichiarazioni** delle PA nelle aree di esecuzione di determinate attività e/o integrazioni tecniche:
 - Database pago Pa, app IO, CIE e SPID.
 - Esistenza e accessibilità sito internet.

I dati relativi alle PA vengono invece acquisiti dalla fonte IPA e non sono imputate manualmente da ciascun Ente. Gli aggiornamenti e le modifiche che possono interessare il DB IPA vengono importate e recepite sul Sistema attraverso un batch notturno.

2.2.2 Cadenza degli aggiornamenti del Sistema informativo

Con riferimento alla policy adottata da *Salesforce* in tema di aggiornamenti e alla periodicità degli stessi, la casa madre rilascia aggiornamenti alla propria Piattaforma software SaaS attraverso **tre roll-out su base annuale**. Da un punto di vista funzionale gli aggiornamenti consistono principalmente nell'introduzione di estensioni e, talvolta, nella creazione di nuove feature. Una volta rilasciati, gli aggiornamenti diventano automaticamente validi.

Per quanto concerne gli aggiornamenti rilasciati dai system integrator, **le evoluzioni funzionali sono stabilite in coerenza con quanto richiesto dalle esigenze del DTD ed in linea con il piano di progetto condiviso**. La frequenza dei rilasci non è dunque prestabilita ma dipende dallo sviluppo della progettualità. Allo stato dell'arte, vengono effettuati rilasci migliorativi/evolutivi ogni 15 giorni ma si prevede che, a partire dal mese di agosto 2022, la cadenza dei rilasci verrà diluita lasciando prevalentemente spazio ad attività di fine-tuning.

2.2.3 Procedure per l'aggregazione dei dati

Il software memorizza tutti i dati a livello di dettaglio e la totalizzazione a fini di rendicontazione e comunicazione deve essere ottenuta da questi.

Per la conduzione di due specifici processi, ossia la **generazione del decreto di finanziamento** e per **l'esposizione dei fondi residui** nella pagina web di dettaglio dell'avviso, vengono utilizzati campi totalizzati dai valori di dettaglio.

Esistono invece **strumenti di reportistica e visualizzazione di dati aggregati**. Il pieno controllo di queste procedure, di certificazione del dato aggregato è nella disponibilità del DTD.

Il Sistema supporta il DTD, attraverso report e dashboard, nel censire, aggregare e visualizzare il dato, anche nell'ottica del monitoraggio e della verifica del raggiungimento di milestone e target (c.d. tracking checkpoints).

2.2.4 Implementazione di eventuali sistemi di interoperabilità con ReGiS

Nel suo rapporto provvisorio di audit di Sistema, l'autorità indipendente ha sollecitato l'Amministrazione Centrale del PNRR a predisporre, per quanto di propria competenza, tutto il necessario per garantire l'interoperabilità tra Regis e la Piattaforma Bandi Pa digitale 2026. A tal proposito, come già anticipato all'interno del Sistema di Gestione e Controllo (Si.Ge.Co), si segnala che Pa digitale 2026, in ottemperanza a quanto stabilito dal DPCM Monitoraggio del 15 settembre 2021, basa la propria architettura dei dati, la sintassi degli stessi, lo state model e i relativi livelli di obbligatorietà su quanto previsto dalle policy, dai manuali utenti e dai protocolli applicativi del Sistema ReGIS – Sistema informatico di cui all'articolo 1, comma 1043 della legge di bilancio n. 178/2020 (legge bilancio 2021) – sviluppato per supportare le attività di gestione, monitoraggio, rendicontazione e controllo del PNRR e atto a garantire lo scambio elettronico dei dati tra i diversi soggetti coinvolti nella governance del PNRR.

In riferimento alle capability dell'infrastruttura in termini di interoperabilità, le caratteristiche native della Piattaforma garantiscono, secondo logiche di interoperabilità aperte e sicure, il dialogo e la collaborazione tra pubbliche amministrazioni e soggetti terzi, per mezzo di standard tecnologici che assicurano l'interazione e lo scambio delle informazioni registrate e classificate all'interno della banca dati. Più nel dettaglio, Salesforce si interconnette a Regis utilizzando il **protocollo di comunicazione remoto SOAP il cui stack si basa su un protocollo http**. Il corpo dei messaggi (contenuto) è formattato in **XML**.

L'integrazione con sistemi esterni potrebbe potenzialmente avvenire anche attraverso **REST API, conformemente alle linee guida AGiD sull'interoperabilità dei sistemi**. Essendo basata su Salesforce, la Piattaforma ha infatti la potenzialità per esporre API, rispettandone tutte le best practices con riferimento, in particolare, a:

- tracciabilità delle diverse versioni delle API, allo scopo di consentire evoluzioni non distruttive (versioning);
- documentazione coordinata con la versione delle API (documentation);
- limitazioni di utilizzo collegate alle caratteristiche delle API stesse e della classe di utilizzatori (throttling);
- tracciabilità delle richieste ricevute e del loro esito (logging e accounting);
- un adeguato livello di servizio in base alla tipologia del servizio fornito (SLA);
- configurazione scalabile delle risorse.

Nel caso di utilizzo di REST API, il contenuto dei messaggi sarebbe formattato in **Json**, determinando vantaggi in termini di maggiore flessibilità, velocità superiore e larghezza di banda ridotta. Ulteriori vantaggi di quest'ultimo metodo consistono nella compatibilità con la maggior parte delle applicazioni più note e nella semplicità d'integrazione.

2.2.5 Procedure per garantire la sicurezza e la gestione del sistema informativo, l'integrità e la riservatezza dei dati, la conservazione dei dati e dei documenti

La Piattaforma dispone nativamente di procedure per la gestione del ciclo di vita del software che garantiscono la sicurezza e la gestione del sistema informativo, l'integrità e la riservatezza dei dati, la conservazione dei dati e dei documenti.

Ambiti	Descrizione
SSO (Single Sign On):	In termini di modalità di autenticazione, l'SSO Shibboleth è basato sullo standard SAML. eventualmente l'SSO può anche basarsi su protocollo OpenID Connect.
Esposizione del servizio:	Internet
Sistema di Autenticazione:	IDPC, MFA (MultiFactor Authentication)
Modalità di Esposizione:	https con cifratura TLS
Applicativo Cloud-Ready	

Figura 4 - Caratteristiche architetture della piattaforma

In primo luogo, l'accesso alla Piattaforma, oltre ad essere consentito ai soli utenti autorizzati, è protetto grazie all'adozione delle seguenti misure di sicurezza:

- **Protocollo HTTPS:** il trasferimento dei dati nel Sistema avviene esclusivamente attraverso tale protocollo che utilizza un **sistema di crittografia TLS >= 1.2**. Esso consente la creazione di un canale di comunicazione per prevenire l'intercettazione, la manomissione e la falsificazione dei dati scambiati.
- **Policy per le password:** a livello di back-office, la sicurezza del Sistema è garantita dall'implementazione delle policy di Salesforce relative alla generazione, alla modifica ed al recupero delle password, consultabili al sito:
https://help.salesforce.com/s/articleView?id=sf.admin_password.htm&type=5.

A livello di front-end, la sicurezza del Sistema è garantita dall'implementazione delle policy definite da AGiD relative alla generazione, modifica e recupero delle password necessarie per l'accesso attraverso SPID e CIE (si veda, ad esempio, il Regolamento recante le modalità attuative per la realizzazione dello SPID - articolo 4, comma 2, DPCM 24 ottobre 2014: https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regolamento_modalita_attuative_v1.pdf).

- **Procedure di backup:** all'interno della piattaforma informativa sono presenti e costantemente verificate le best practices di Salesforce in tema di backup automatico, recupero rapido dei dati e disaster recovery.

Come anticipato, il cuore dell'architettura della piattaforma è costituito dal software Salesforce Commerce Cloud. All'interno di questa struttura organizzata e complessa viene garantita la storicizzazione delle informazioni e la tracciabilità delle modifiche, ove richiesto, effettuate dagli attori a diverso titolo coinvolti nella gestione degli interventi.

Ad ulteriore garanzia del fatto che il prodotto Salesforce si pone in linea con gli standard di sicurezza internazionali per un'adeguata raccolta, registrazione e conservazione informatizzata dei dati si rimanda alla consultazione delle certificazioni possedute (<https://compliance.salesforce.com/en>).

In particolare, nel contesto della legislazione europea, Salesforce dispone delle seguenti certificazioni:

Certificazioni	Descrizione
C5 (ISAE 3000)	ISAE 3000 (Revised) Report on Management's Description of salesforce.com, inc.'s Salesforce Services system on German Federal Office for Information Security BSI Cloud Computing Compliance Controls Catalogue (C5).
Disaster Recovery & BCP	Salesforce mantiene un piano di Disaster Recovery che supporta una solida strategia di continuità aziendale per i servizi e le piattaforme di produzione. Questo piano è stato sviluppato da metodologie accettate dal settore e comprende principi di ingegneria ad alta disponibilità. Il piano di Disaster Recovery è costantemente misurato rispetto a severi requisiti normativi e di governance ed è una parte cruciale del piano di accettazione quando si apportano modifiche o integrazioni all'ambiente di produzione.
ISO 27001	ISO/IEC 27001:2013 (ISO 27001) è lo standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano)
ISO 27017	Lo standard ISO/IEC 27017, rientrante tra gli standard della serie ISO/IEC 27001, definisce controlli avanzati sia per fornitori di servizi cloud sia per i clienti degli stessi servizi.
ISO 27018	ISO/IEC 27018:2019 è il codice di condotta incentrato sulla protezione dei dati personali nel cloud.
PCI DSS	Il PCI DSS è lo standard internazionale per la protezione dei dati e coinvolge tutte quelle entità che si occupano di memorizzare, elaborare o trasmettere i dati dei titolari di carta e/o i dati sensibili di autenticazione.
SOC 1	I report SOC (Service Organization Controls), noti anche come SOC 1, SOC 2 o SOC 3, sono framework stabiliti dall'American Institute of Certified Public Accountants (AICPA) per fornire resoconti sui controlli interni di un'organizzazione.
SOC 2	Questi report sono essenziali per controllare e monitorare le protezioni integrate nella base di controllo dei dati al fine di verificarne il corretto funzionamento.
SOC 3	

Figura 5 - Certificazioni Salesforce

La componente core del Sistema Informatico si occupa pertanto di gestire tutte le informazioni storicizzate in Piattaforma. In particolare, la conformità alla normativa **ISO:27001** assicura il rispetto dei requisiti per impostare, gestire e migliorare un Sistema di Gestione della Sicurezza delle Informazioni ed include una serie di controlli relativi alla sicurezza logica, fisica ed organizzativa, che assicurano la protezione delle informazioni.

I controlli sono raggruppati nelle seguenti aree:

- Politiche per la sicurezza delle informazioni;
- Organizzazione della sicurezza delle informazioni;
- Sicurezza del personale;
- Gestione degli Asset;
- Controllo degli accessi "logici" ai sistemi, ai servizi e alle informazioni;
- Crittografia (es. encrypting in transit tramite HTTPS);
- Sicurezza fisica e ambientale;
- Sicurezza dei processi IT (es. Backup, Log, ecc.);

- Sicurezza delle reti e dei sistemi di comunicazione;
- Acquisizione, sviluppo e gestione del software applicativo;
- Gestione dei Fornitori;
- Gestione dei incidenti;
- Aspetti di sicurezza per gestione della Business Continuity;
- Conformità normativa.

Per ciò che concerne le policy garantite a tutela della privacy dei dati, si segnala che il prodotto Salesforces commerce cloud è conforme ai i principi previsti dalla **normativa europea GDPR**.

I principali punti cardine del sistema a supporto di tale normativa sono i seguenti:

- Riservatezza, confidenzialità e integrità dei dati;
- Notifica di violazione;
- Valutazione del rischio;
- Privacy by design e by default;
- Conservazione dei registri.

3. CONCLUSIONI

Facendo leva sulle esperienze maturate nella gestione e rendicontazione dei fondi strutturali europei, sulle competenze acquisite nel presidio dei domini tecnologici rilevanti e sul ricorso a metodologie Agile di Project Management, è stata realizzata e messa a regime una Piattaforma che risponde a requisiti di accessibilità ed usabilità, sicurezza, affidabilità e qualità nel trattamento e nella conservazione dei dati.

I requisiti di accessibilità ed usabilità, in particolare, sono stati rispettati attraverso il ricorso alle linee guida Sogei in materia di Customer Experience e Designer Italia in materia di UX/UI. I requisiti di sicurezza, affidabilità e qualità dei dati sono stati invece raggiunti verificando costantemente che la soluzione applicativa scelta nonché i suoi successivi sviluppi *custom* fossero pienamente conformi alla normativa pertinente.

Tale strumento applicativo è progettato e realizzato in maniera personalizzata per rispondere alle peculiarità delle misure Lump-Sum di competenza del DTD, in affiancamento al Sistema Regis, in modo da supportare i processi di attuazione, monitoraggio, rendicontazione e controllo degli interventi finanziati dal PNRR. Ciò consente alla scrivente Amministrazione di dare attuazione all'articolo 1, comma 1044, della legge 30 dicembre 2020, n. 178, in materia di modalità di rilevazione dei dati di attuazione finanziaria, fisica e procedurale relativi a ciascun progetto nell'ambito delle componenti del Next Generation EU. Il suddetto sistema informatico garantirà il continuo e tempestivo presidio dell'avanzamento finanziario, procedurale e fisico degli interventi del PNRR, con particolare riferimento al monitoraggio dei progressi nell'attuazione, consentendo la puntuale e costante verifica dei milestone e target (UE e nazionali) del Piano.