ALLEGATO 5

(ART. 7)

Descrizione modello di funzionamento

Il trattamento dei dati personali è effettuato nell'ambito del nuovo sistema di gestione del foglio di servizio elettronico, che disciplina le modalità di tenuta e compilazione dello stesso ai fini dello svolgimento del servizio di noleggio con conducente effettuato esclusivamente mediante autovettura o motocarrozzetta e ne individua le specifiche tecniche.

L'utilizzo del Foglio di Servizio è previsto per i seguenti soggetti:

- Gli Utenti Vettore NCC, come definiti nell'articolo 2 dello schema di Decreto;
- Gli Utenti Conducenti, ossia i collaboratori, ovvero dipendenti del medesimo, in qualità di dipendenti subordinati, parasubordinati o nell'ambito del contratto di gestione o collaboratore familiare di un vettore NCC, come definiti nell'articolo 2 dello schema di Decreto.

Per questi utenti l'utilizzo dell'applicativo è possibile solo in seguito alla corretta iscrizione (ed al mantenimento della stessa) al Registro Elettronico NCC Taxi (di seguito, *«RENT»*) da parte dell'Impresa del Vettore NCC cui fanno capo.

Con riferimento alle modalità di accesso, ciascun vettore NCC e conducente, in quanto censito tramite CF dall'Impresa del Vettore NCC stesso, come definito nell'Allegato Tecnico dello schema di Decreto del RENT (paragrafo 1), è abilitato ad accedere tramite il proprio SPID di livello 2, per l'esecuzione delle attività associate al profilo, come di seguito riportato. Si specifica che le credenziali di accesso possono essere attivate esclusivamente su un unico dispositivo.

Il vettore NCC può eseguire le seguenti operazioni:

- abilitazione e disabilitazione dei propri conducenti per operare sull'applicativo in esame;
- registrazione dei contratti di durata attraverso l'inserimento dei relativi dati che li qualificano;
- compilazione di un Foglio di Servizio dell'apposito modello A o B, come definito nello schema di Decreto, per i contratti per singolo servizio;
- inserimento e gestione di una prenotazione;
- inserimento e gestione di un Foglio di Servizio, ossia:
    - generazione di un Foglio di Servizio, collegato ad una prenotazione;
    - variazione eventuale dei dati presenti in un Foglio di Servizio;
    - eventuale annullamento di un Foglio di Servizio;
    - validazione del Foglio di Servizio al termine del medesimo.

Il conducente NCC può eseguire le seguenti operazioni:

- inserimento e gestione di una prenotazione;
- inserimento e gestione di un Foglio di Servizio, ossia:
    - generazione di un Foglio di Servizio, collegato ad una prenotazione;
    - variazione eventuale dei dati presenti in un Foglio di Servizio;
    - eventuale annullamento di un Foglio di Servizio;
    - validazione del Foglio di Servizio al termine del medesimo.

Nel caso in cui ricorressero le condizioni previste dall'articolo 6, comma 3, è necessario compilare un Foglio di Servizio cartaceo. Al venir meno di tali condizioni l'applicazione consente la generazione di un Foglio di Servizio digitale che, per il trasferimento a sistema delle informazioni riportate nel Foglio di Servizio cartaceo.

L'applicazione consente inoltre:

- agli organi di cui all'articolo 12 del decreto legislativo 30 aprile 1992, n. 285, di effettuare la consultazione delle informazioni relative a tutti i Fogli di Servizio;
- ai Comuni, tramite personale appositamente autorizzato, di consultare i dati relativi ai servizi svolti dai vettori titolari di autorizzazioni rilasciate dai medesimi;
- al CED della Direzione Generale per la Motorizzazione la gestione della manutenzione ed evoluzione del sistema.

L'applicazione assicura l'interoperabilità tra i dati riportati nei Fogli di Servizio e quelli presenti nel RENT (come riportato nella figura dell'architettura applicativa). Pertanto, i Comuni e gli organi, di cui all'articolo 12 del decreto legislativo 30 aprile 1992, n. 285, potranno consultare i dati presenti nel Foglio di Servizio, secondo le modalità precedentemente indicate, tramite un'apposita interfaccia grafica (app mobile) o attraverso un sistema che garantisce la cooperazione applicativa tra i sistemi.

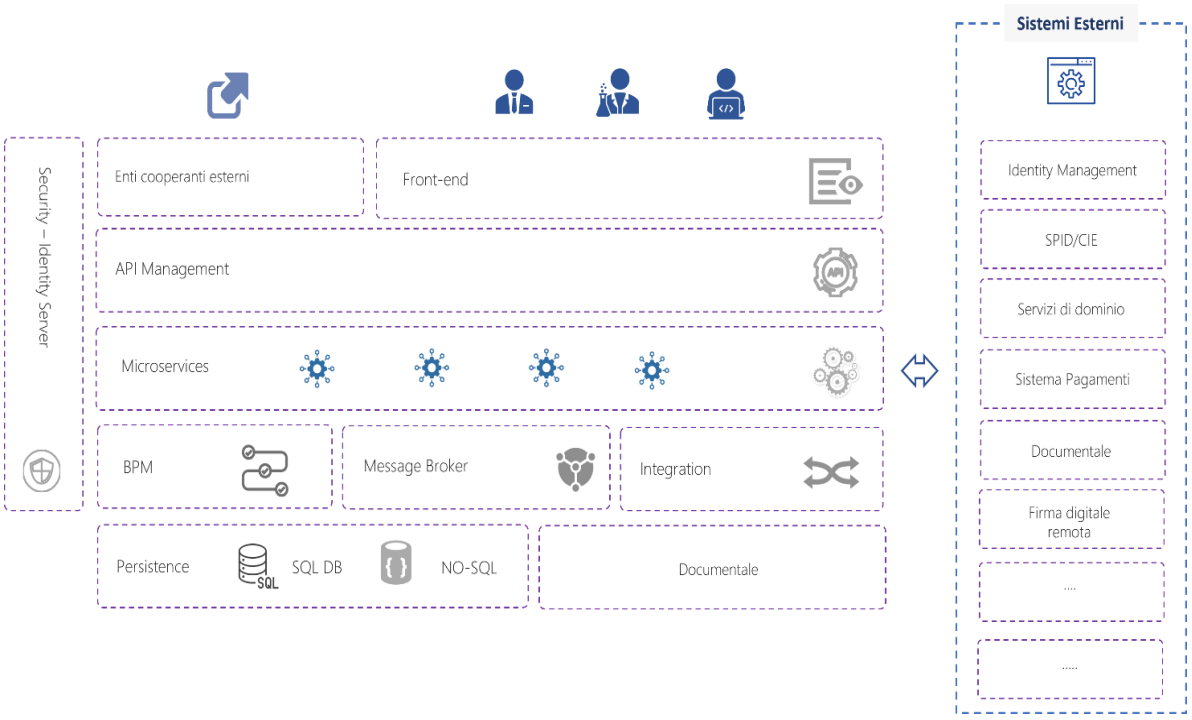
Le operazioni eseguibili dagli utenti all'interno del Foglio di Servizio, ciascuno nell'ambito della propria area di operatività, sono tracciate e monitorate al fine di garantire l'integrità e la correttezza del trattamento dei dati, in conformità alla disciplina di cui al GDPR.

Tanto fin qui riportato, si precisa che il Ministero delle Infrastrutture e dei Trasporti, in veste di Titolare del trattamento, sottopone agli Interessati l'informativa ai sensi degli articoli 13 e 14 del GDPR, contenente le informazioni in merito al trattamento dei dati eseguito nell'ambito del Foglio di Servizio.

Specifiche tecniche dell'applicazione informatica

La gestione dei fogli di servizio sarà resa fruibile agli utenti sia tramite applicazione web, che *App mobile.* Grazie allo sviluppo dell'applicazione con tecnologia *cloud enabled,* le funzionalità potranno essere erogate dal *private cloud* del MIT come da un *Cloud Service Provider. In* quest'ultimo caso, la scelta del CSP avverrà necessariamente tra quelli certificati dall'Agenzia per la Cybersicurezza Nazionale, orientando la scelta di una *Region* in Italia per l'hosting dell'infrastruttura e dei dati, in conformità con il GDPR ed adottando una strategia di *deployment* che privilegia l'implementazione di servizi PaaS (*Platform as a Service*).

Di seguito è mostrata l'Architettura Logica con le macro-componenti ed i *layer* che la caratterizzano.



In coerenza con l'architettura logica appena descritta, si riporta di seguito sia la soluzione in *Private Cloud* che una possibile soluzione *hybrid-cloud*, che vede l'utilizzo sia del *Private Cloud*, che di un *Public Cloud* certificato ACN.

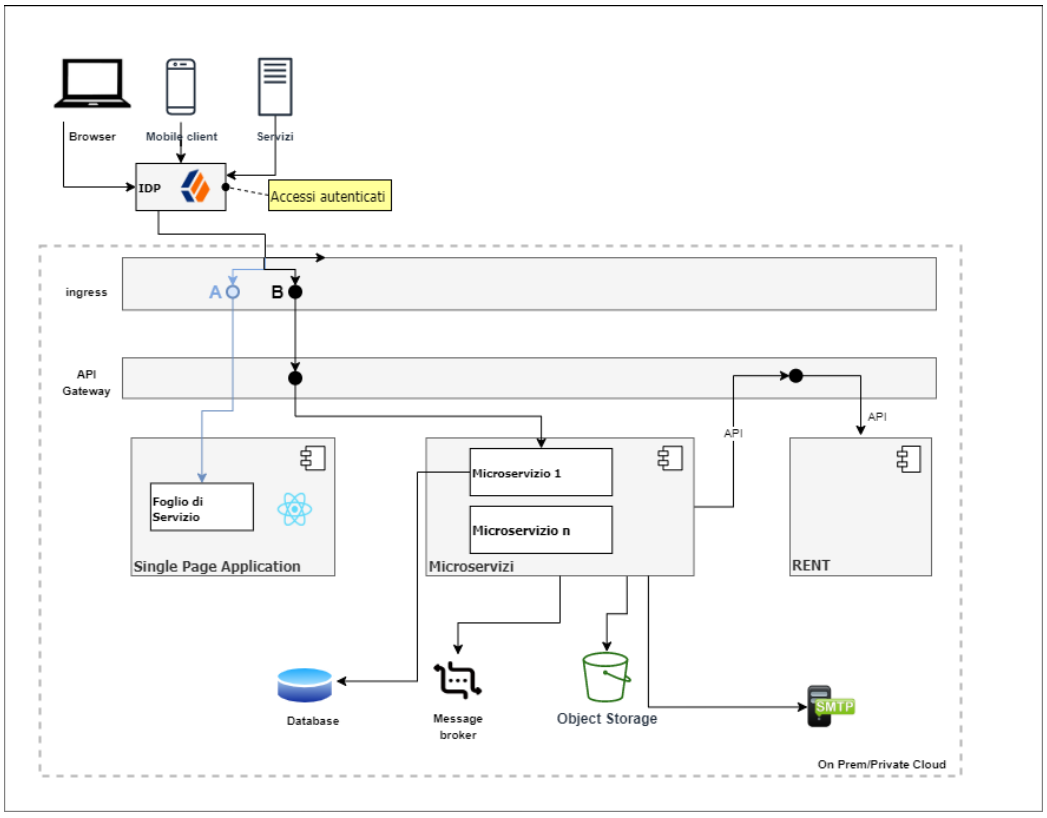


Figura 1 Soluzione architetturale in Private Cloud

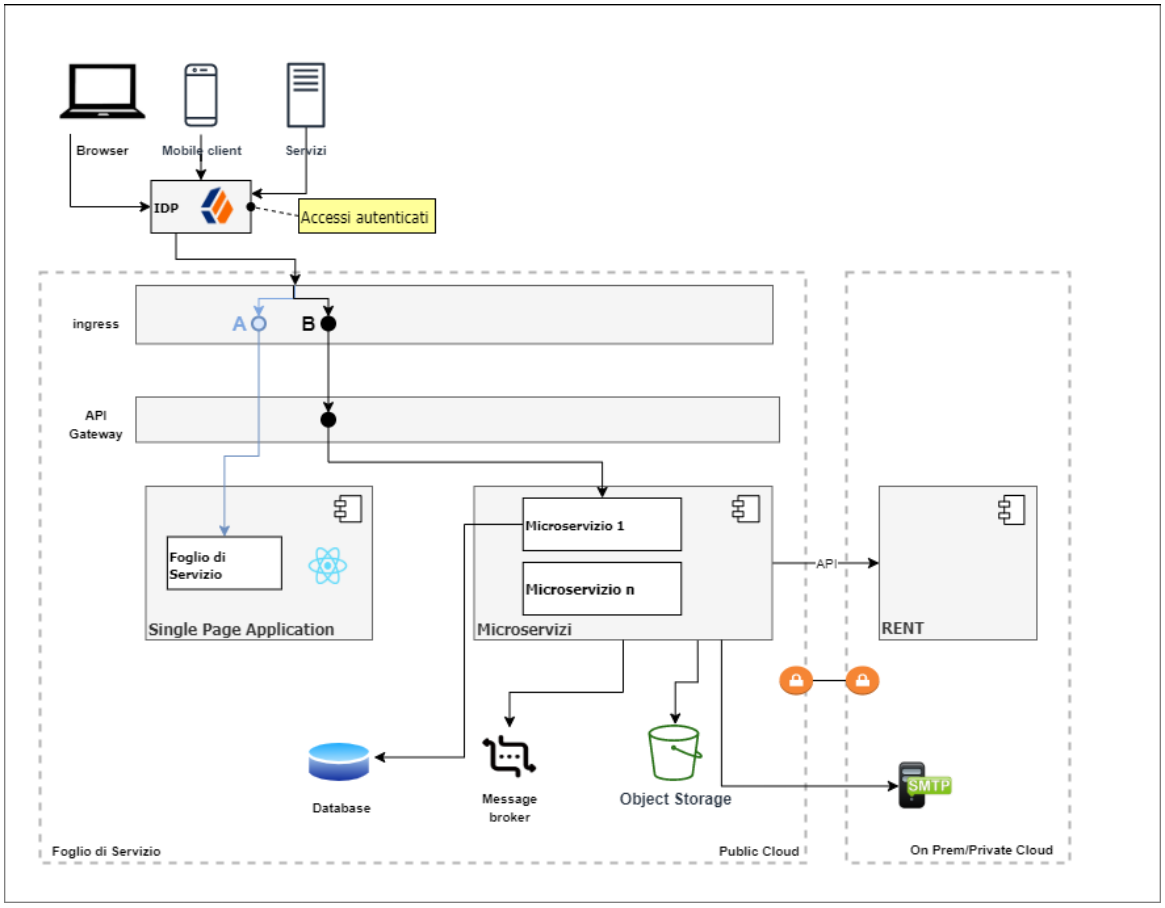


Figura 2 Soluzione architetturale in Hybrid Cloud

Seguendo l'architettura logica, l'applicazione Foglio di Servizio si può suddividere in:

- Livello di presentazione
  L'interfaccia utente è accessibile attraverso diverse modalità, comprese *Single Page Application* (SPA), *App mobile* e servizi *RESTful*. Questo livello fornisce una varietà di opzioni per l'interazione dell'utente con il sistema, garantendo flessibilità e fruibilità.
- Livello di *identity management*
  Questo strato è progettato per offrire un'esperienza di accesso sicura e unificata agli utenti, attraverso l'implementazione di funzionalità di *Single Sign-On* (SSO) e l'integrazione di moderni protocolli di federazione come lo SPID (Sistema Pubblico di Identità Digitale) e la CIE (Carta d'Identità Elettronica). Qui, l'autenticazione e l'autorizzazione degli utenti sono gestite tramite un *Identity Provider* (IdP) centralizzato. Il *gateway* verifica il *token* tramite IAM (*Identity Access Management*) e reindirizza le richieste ai microservizi *stateless*, garantendo che solo gli utenti autorizzati possano accedere alle risorse, in base al cono di visibilità configurato.
- Livello di *business logic*
  I microservizi *stateless*, costituiscono il nucleo della logica di *business* dell'applicazione. Questi servizi eseguono operazioni specifiche in risposta alle richieste degli utenti, implementando anche *Role-Based Access Control* (RBAC) per limitare l'accesso alle risorse in base al profilo dell'utente.

Il Foglio di Servizio interagisce con il sistema Foglio di Servizio, tramite API interne e protette da credenziali di sistema, per inviare e ricevere dati in modo sicuro e affidabile, garantendo che solo le entità autorizzate possano accedere e modificare le informazioni.

- Livello di persistenza dei dati
  I dati dell'applicazione sono gestiti da un database, utilizzando i pattern adeguati alle architetture a microservizi. L'*object storage* viene utilizzato per l'archiviazione documentale, sfruttando le feature di cifratura per garantire la sicurezza dei dati.
- Livello di comunicazione
  I servizi interni verranno invocati considerando sempre protocolli sicuri (HTTPS, TLS) e protetti da credenziali di accesso controllate dal layer di Identity Management.
  L'applicazione Foglio di Servizio in *Private cloud*, sfrutterà i componenti architetturali già in essere, in coerenza con quanto rappresentato nello schema architetturale riportato in alto.
  Nel caso di applicazione Foglio di Servizio erogata in *Hybrid cloud* e, quindi, con l'utilizzo di un CSP certificato, la comunicazione tra *Private* e *Public Cloud* avverrà in modo sicuro tramite una *Virtual Private Network* (VPN), che stabilirà un *tunnel* crittografato tra le due infrastrutture.
- Livello di orchestrazione e gestione
  I moduli dell'applicazione sono distribuiti per garantire un ambiente di orchestrazione scalabile e gestibile in modo efficiente. Le credenziali di accesso ai diversi servizi, inclusi *database*, *message broker* e *object storage*, sono gestite come *secrets*, garantendo un livello aggiuntivo di sicurezza.

Analisi dei rischi

Si è proceduto alla previa analisi dei rischi connessi all'utilizzo del Foglio di Servizio, i cui esiti si riportano in sintesi nella tabella che segue, contenente la descrizione dei rischi potenziali e l'individuazione del livello di rischio, calcolato sulla base della gravità e della probabilità che i rischi si verifichino:

Tipologia di rischio	Descrizione	Livello di rischio	Misure preventive
Malware, *virus*, *bug* introdotti via internet nel sistema e nelle postazioni di lavoro.	Tale rischio può verificarsi e può comportare la perdita di dati, la violazione della sicurezza, il rallentamento del sistema, il furto di informazioni personali e il danneggiamento dei sistemi.	Medio	• sistemi di *intrusion detection* e *prevention* • gestione sicura delle postazioni di lavoro • sicurezza dell'ambiente operativo
Intrusioni che possano comportare l'accesso illegittimo ai dati personali.	Il *Data Breach* è una violazione della sicurezza, che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati.	Medio	• controllo degli accessi logici ed autenticazione) • minimizzazione della quantità di dati personali • sicurezza del ciclo di vita delle applicazioni e nei progetti • sicurezza dell'ambiente operativo • sicurezza della rete e delle comunicazioni • tracciatura e monitoraggio • controllo degli accessi fisici • gestione degli incidenti di sicurezza e delle violazioni dei dati personali
Rischio di perdita accidentale di dati.	Tale rischio è riconducibile a problemi di funzionamento dei sistemi informatici o a condotte umane non corrette, che possono comportare la perdita o la distruzione accidentale di dati.	Basso	• manutenzione delle apparecchiature • sicurezza dell'ambiente operativo • sicurezza della rete e delle comunicazioni • controllo gestione sicura dell'*hardware*, delle risorse e dei dispositivi • *backup* • procedure previste dal Sistema di Gestione della sicurezza delle informazioni • protezione delle fonti di rischio ambientali

Attacco informatico che renda indisponibile il servizio.	Attacchi DoS o DdoS che vanno a saturare la banda disponibile o le risorse elaborative rendendo indisponibile il servizio.	Medio	• sistemi di *intrusion detection* e *prevention*: • sicurezza della rete e delle comunicazioni • sicurezza del ciclo di vita delle applicazioni e nei progetti
Sabotaggi di apparecchiature, *server*, apparati di reti.	Tali rischi possono verificarsi a seguito di accessi non autorizzati ai sistemi o qualunque azione dannosa che potrebbe portare al furto di dati sensibili o al blocco dei sistemi.	Basso	• controllo degli accessi fisici • gestione degli incidenti di sicurezza e delle violazioni dei dati personali • controllo gestione sicura dell'*hardware*, delle risorse e dei dispositivi • protezione delle fonti di rischio ambientali
Guasti tecnici, quali malfunzionamenti apparecchiature, interruzione alimentazione elettrica, e malfunzionamenti software.	Tali rischi possono verificarsi in mancanza di affidabilità delle apparecchiature e un cattivo comportamento del software può dipendere, da errori presenti nel codice, dall'ambiente esecutivo.	Basso	• controllo gestione sicura dell'*hardware*, delle risorse e dei dispositivi • protezione delle fonti di rischio ambientali

Regole tecniche, requisiti, garanzie e misure di sicurezza adottate

Il Ministero delle Infrastrutture e dei trasporti identifica il Responsabile del trattamento dei dati personali, ai sensi dell'articolo 28 del GDPR, tramite appositi atti di nomina, ai fini dell'affidamento dei servizi infrastrutturali, di gestione e sviluppo applicativo del sistema informativo del Ministero medesimo.
In adempimento all'articolo 32 del GDPR, il Ministero delle Infrastrutture e dei trasporti adotta sulle infrastrutture tecnologiche, anche per mezzo del Responsabile del trattamento dei dati personali, le seguenti misure di sicurezza infrastrutturali, oltre a quelle risultanti dalle valutazioni di impatto:

- con riferimento ai sistemi di *intrusion*, *detection* e *prevention*, i servizi esposti dal Sistema sono protetti da sistemi IDS/IPS che monitorano e bloccano gli attacchi di varia tipologia (es. DoS, DdoS, sfruttamento vulnerabilità, *syn flood*, ecc.);
- con riferimento al controllo degli accessi logici ed autenticazione, in particolare la parte di autenticazione è gestita con un *Identity Portal* IDP federato con SPID mentre la parte di accesso è gestita direttamente dall'infrastruttura dei Portali. Il sistema identifica l'utente

tramite il suddetto processo di autenticazione, associando a quest'ultimo uno dei profili previsti cui sono legate le regole di visibilità ed eventuale data masking dei dati;

- con riferimento alla gestione sicura delle postazioni di lavoro, le PDL del Ministero delle Infrastrutture e dei Trasporti sono sotto dominio e sotto antivirus e patch di sicurezza, controllate centralmente. Le PDL del Responsabile del trattamento dei dati personali, su cui quest'ultimo opera per la manutenzione dei sistemi, sono sotto dominio e si collegano alla rete del Ministero delle Infrastrutture e dei Trasporti attraverso un client VPN autenticato, tramite MFA;
- con riferimento alla manutenzione delle apparecchiature, su tutti gli apparati sono attivati contratti di manutenzione da parte del Ministero delle Infrastrutture e dei Trasporti;
- con riferimento alla minimizzazione della quantità di dati personali, le autorizzazioni e i permessi sono configurati secondo il principio del minimo privilegio, assicurando che gli utenti abbiano accesso solo alle sezioni e alle operazioni strettamente necessarie per le loro funzioni;
- durante l'erogazione del servizio, i dati identificativi degli utenti forniti al momento della prenotazione sono accessibili limitatamente al ciclo di vita del foglio di servizio generato ed esclusivamente da parte dei soggetti di cui all'articolo 12 del codice della strada. Al momento della chiusura del foglio di servizio i dati relativi all'utente sono pseudonimizzati senza ritardo;
- con riferimento alle modalità di conservazione, al termine del singolo servizio i dati relativi agli utenti sono pseudonimizzati al pari degli ulteriori dati. Resta ferma la possibilità di accesso ai predetti dati, in chiaro, solo ed esclusivamente per finalità di natura giurisdizionale; in tal caso ai fini dell'accesso è presentata istanza debitamente motivata da parte del soggetto legittimato a richiedere l'accesso in funzione delle predette esigenze di natura giurisdizionale e la direzione generale competente provvede autorizzando l'estrazione del dato esclusivamente per le finalità indicate;
- con riferimento alla sicurezza del ciclo di vita delle applicazioni e nei progetti, il *Change Management* effettuato tramite processi in linea con i principi di *Security & Privacy by Design*. Viene effettuato il *patching* periodico della sicurezza dei Sistemi e vengono effettuati dei VA infrastrutturali e dei *Penetration Test* lato applicativo in modalità *Blackbox* con cadenza semestrale;
- con riferimento alla sicurezza dell'ambiente operativo, sono previste le seguenti misure: (i) manutenzione HW e SW di base; (ii) installazione tempestiva degli aggiornamenti di sicurezza distribuiti dal produttore ("*patching*"); (iii) rimozione di servizi, applicazioni e protocolli che non sono utilizzati; (iv) configurazione di Utenti autorizzati con i relativi permessi; (v) configurazione di sistemi di controllo delle risorse per il monitoraggio degli accessi e delle violazioni; (vi) *Change Management* con riferimento sicurezza della rete e delle comunicazioni, la rete è perimetrata e il servizio di accreditamento del Sistema è separato a livello III nella parte di *frontend* e di *backend*;
- con riferimento alla tracciatura e al monitoraggio, le applicazioni sono configurate per produrre i *log* necessari a tracciare gli eventi significativi, e una piattaforma di *Log*

Management è configurata per raccogliere, interpretare, indicizzare e conservare gli stessi per un anno;

- con riferimento al controllo degli accessi fisici alla sede di Via G. Caraci a Roma, lo stesso è consentito al personale autorizzato, nonché ai visitatori, mediante l'assegnazione (definitiva per il personale fisso e temporanea per gli ospiti) di un *badge* che permette l'accesso al perimetro e, ove configurato, al Palazzo dove è situato il CED;
- con riferimento alla gestione degli incidenti di sicurezza e delle violazioni dei dati personali, il Dipartimento, nell'ambito del suo sistema di gestione della sicurezza delle informazioni, ha definito un processo di gestione degli incidenti e una procedura specifica di *Data Breach* che è adottata qualora l'evento riguardi i dati anche di questo specifico trattamento in esame;
- con riferimento alla gestione sicura dell'hardware, delle risorse e dei dispositivi, i server sono posizionati in un CED e sono dotati di armadi *rack* con serratura, controllo della temperatura con impianto di refrigerazione, sistemi di antincendio oppia linea di alimentazione con UPS (batteria tampone) e gruppo di continuità per garantire la continuità elettrica;
- con riferimento alla protezione delle fonti di rischio ambientali, il CED è dotato di un sistema antiincendio a gas inerti, un sistema di allagamento. Tutti i *server* sono attestati su una doppia linea di alimentazione che in cascata è dotata di un UPS dedicato e un gruppo elettrogeno;
- con riferimento alle procedure previste dal Sistema di Gestione della sicurezza delle informazioni, le stesse sono definite nel Piano di Sicurezza;
- con riferimento al *Backup*, sono utilizzati specifici *tool* e *appliance* per la conservazione (su disco e su nastro) degli stessi;
- con riferimento alla cancellazione sicura, la stessa viene effettuata attraverso *software* specifici;
- con riferimento alle *policy* e alle procedure per la protezione dei dati personali, come definito nel piano della sicurezza, il Ministero delle Infrastrutture e dei trasporti adotta integralmente quanto stabilito dal Codice *privacy* e dal GDPR**.**