ADVANCED ANALYTICS AND IOT SOLUTIONS

Whitepaper MangrovialoT SaaS

Soluzioni avanzate per Asset Management e Operational Intelligence

WHP-SAAS-001-1.0

SORINT.tek s.r.l.
Via Zanica, 17 | 24050 Grassobbio (BG) | Italy | Tel +39 0356975211 | Fax +39 0356975290
COD. FISC., N. REG. IMPR. BG 04153090164 | PART. IVA 04153090164 – REA BG 439855 | CAPITALE SOCIALE € 10.000,00i.v.
Società Soggetta a Direzione e Coordinamento di SORINT.lab S.p.A. con sede in Via Zanica, 17 - 24050 Grassobbio (BG) | Italy con COD. FISC., N. REG. IMPR. BG 95164770166.

DOCUMENT INFORMATION

COPYRIGHT

CONTACTS

COMPANY	NAME	EMAIL ADDRESS
Sorint.tek	Roldano Malvesititi	mangroviaiot@sorint.com

DOCUMENT REVIEW

VERSION	DATE	AUTHOR	APPROVED BY	ISSUED BY
1.0	24/11/2025	Roldano Malvesititi	Emilio Tresoldi	Marco Pozzi

CHANGE HISTORY RECORD

VERSION	DATE	LAST MODIFIED
1.0	24/11/2025	Prima Emissione

REFERRAL DOCUMENTS

VERSION	DATE	DOCUMENT
NA	NA	NA

SUMMARY

Introduzione

Il presente documento è un Whitepaper sul servizio MangroviaIoT in modalità Software as a Service (SaaS), focalizzato sugli aspetti architetturali, di sicurezza e di compliance gestiti da SORINT.tek S.R.L.

1. Legenda

1. **LATEK:** SORINT.tek S.R.L. Via Zanica, 17 – 24050 Grassobbio (BG) – Italy
2. **CSC**: il cliente
3. **SaaS – Software as a Service**: è un modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera e gestisce un'applicazione che mette a disposizione dei propri clienti via Internet.
4. **Software/Moduli Applicativi**: la piattaforma MangroviaIoT.
5. **Credenziali di Accesso:** il codice di identificazione e le chiavi di accesso forniti da LATEK necessari per l'utilizzo dei moduli applicativi e del software associati al Cliente e necessari allo stesso per la creazione delle utenze dedicate degli utenti autorizzati.
6. **Codice Licenza:** il codice di identificazione e le chiavi di accesso forniti da LATEK al Cliente necessari per l'installazione dei moduli applicativi e del software da parte del cliente su proprio hardware.
7. **Devices (Dispositivi):** i dispositivi e gli strumenti (es. sensori, centraline, ecc.) definiti nel contratto e di cui il cliente deve autonomamente dotarsi, procedere alla loro installazione sui supporti fisici e materiali - dei quali i devices devono rilevare il dato informativo da trasmettere ai moduli applicativi e al software - e provvedere alla loro configurazione e connessione ai moduli applicativi e al software.
8. **Connettività:** la connessione dei devices ai moduli applicativi e al software mediante collegamento a una rete di telecomunicazioni o a internet di cui il cliente deve autonomamente dotarsi e procedere al costante monitoraggio e adeguamento.
9. **CSP**: Cloud Service Provider
10. **GCP**: Google Cloud Platform
11. **SSRM**: Modello di Responsabilità Condivisa (Shared Responsibility Model)

2. Modulo applicativo

MangroviaIoT è una piattaforma tecnologica **modulare e multilivello** sviluppata e di proprietà esclusiva di SORINT.tek S.R.L. (LATEK) finalizzata all'asset management e all'operational intelligence in quanto permette l'acquisizione, l'elaborazione e l'analisi dei dati IoT finalizzati a supportare analisi predittive e prescrittive. In particolare, i principali obiettivi dell'applicazione sono:

1. Gestire e monitorare lo stato di una infrastruttura di device, tramite la gestione anagrafica e operativa di asset distribuiti sul territorio, con controllo dello stato di comunicazione dei sensori, rappresentazione e segnalazione di eventuali anomalie.
2. Acquisire, collezionare, monitorare e visualizzare i dati dei sensori tramite il governo completo del ciclo di vita dei dati generati dai sensori, dall'acquisizione alla rappresentazione, con un sistema di verifica metrologica e notifica di superamento di soglie configurabili.

3. Advanced Analytics tramite gli strumenti statistici e gli algoritmi di machine learning finalizzati alle analitiche predittive e prescrittive incluse nella soluzione.

3 Modello di erogazione SaaS

La modalità di erogazione in modalità Software as a Service (SaaS) consiste nella messa a disposizione del software e dei relativi moduli applicativi (nello specifico MangroviaIoT) agli utenti autorizzati attraverso la fruizione di un'unica copia ospitata nello spazio cloud di LATEK.

4 Architettura Cloud e responsabilità (SSRM)

L'architettura MangroviaIoT è concepita per essere **cloud-agnostic** dal punto di vista applicativo, basandosi su un'architettura a micro-servizi su Kubernetes.

4.1 Infrastruttura e segregazione

L'ambiente SaaS è ospitato presso il Cloud Service Provider (CSP) di Google Cloud Platform (GCP) che garantisce le seguenti caratteristiche:

- **Localizzazione dei dati**: i dati e i servizi cloud sono localizzati in Europa. L'ambiente cloud primario per MangroviaIoT SaaS è situato nella regione europe-west8 (Italy). L'ambiente secondario di Disaster Recovery (DR) è situato nella regione europe-west9 (France). LATEK documenta e monitora i requisiti relativi all'ubicazione geografica dei dati.
- **Segregazione logica**: la separazione tra i clienti è garantita dall'uso di namespace dedicati per i clienti B2B e namespace comune per i clienti B2C. LATEK implementa rigorose misure tecniche per garantire la segregazione logica.
- **Flessibilità di installazione**: a livello applicativo il prodotto è cloud-agnostic e può vivere in qualsiasi installazione di Kubernetes
- **Implementazione multi-tenant**: l'installazione avviene in modalità multi-tenant all'interno del servizio gestito da GKE (Google Kubernetes Engine).

LATEK si impegna a comunicare preventivamente e tempestivamente ai propri clienti l'eventuale ingresso di nuovi fornitori di infrastruttura.

4.2 Modello di Responsabilità Condivisa (SSRM)

L'erogazione del servizio in cloud segue il Modello di Responsabilità Condivisa (Shared Responsibility Model), dove LATEK e il Cliente (CSC) assumono ruoli definiti in base all'area di responsabilità.

Area di Responsabilità	Responsabilità LATEK (CSP)	Responsabilità Cliente (CSC)
Infrastruttura fisica e Data Center	Monitora periodicamente il Cloud Service Provider (GCP) per il rispetto degli impegni di sicurezza, gestione incidenti e disponibilità.	Nessuna Responsabilità
Rete, virtualizzazione e HW	Assicura hardening dei sistemi, monitoraggio della rete e segregazione ambienti virtuali e tenant	Nessuna Responsabilità
Piattaforma	Gestisce le configurazioni infrastrutturali di base (GKE, Load Balancer, storage), assicurando sicurezza, aggiornamenti regolari e alta disponibilità del servizio.	Nessuna Responsabilità
Applicazione SaaS Applicativo	Sviluppa e mantiene il software mediante adozione approccio di sviluppo sicuro. Concede in licenza d'uso del Software.	Gestione dell'uso del Software per le Finalità definite. È esclusivo responsabile della completezza, correttezza, aggiornamento e veridicità dei dati immessi nei Moduli Applicativi e, comunque, nel Software.
Crittografia e Gestione Chiavi	Garantisce la cifratura dei dati “at-rest” e “in-transit” e la corretta gestione delle chiavi crittografiche (gestite da GCP o fornite dal cliente), assicurando riservatezza, integrità e protezione dei dati	Ha facoltà di fornire le proprie chiavi di cifratura garantendo contestualmente la loro corrette gestione e protezione
Accesso e Utenti	Fornitura Credenziali di Accesso per amministratore del cliente (accesso applicativo). LATEK fornisce le credenziali iniziali tramite canale sicuro, prevedendo l’obbligo di modifica della password al primo accesso da parte dell’amministratore del Cliente. Implementazione di MFA/OTP per gli amministratori (per accesso ad infrastruttura)	Creazione e gestione delle Utenze Dedicate per gli Utenti Autorizzati. Custodia e protezione delle Credenziali, essendo l'unico responsabile per l'uso da parte di terzi. Revisione periodica degli account applicativi e delle relative autorizzazioni, assicurando privilegi assegnati rispettino il principio del “least privilege”
Proprietà Intellettuale	Mantiene piena ed esclusiva titolarità del Software e Moduli Applicativi.	Nessuna responsabilità

Risorse umane	Garantisce che il personale abbia adeguata formazione, competenza ed esperienza. Il personale è formato e sensibilizzato sulle tematiche di sicurezza, sul cybercrime in generale e sulle best practice da attuare in CLOUD.	Assicura che il personale che utilizza il servizio sia adeguatamente formato in termini di capacità e sicurezza informatica
Subappaltatori	LATEK è legittimata a delegare l'esecuzione di alcune prestazioni del Contratto a società ad essa collegate. LATEK rimarrà tuttavia solidalmente responsabile nei confronti del Cliente per le prestazioni eseguite dai soggetti poc'anzi elencati.	

5. Sviluppo, testing e sicurezza del codice

LATEK adotta rigorose pratiche di sviluppo sicuro del software, conformi ai principi di **Security by Design** e basate sulle linee guida **OWASP**.

5.1 Pratiche di Sviluppo Sicuro (SDLC)

La **Procedura di Sviluppo Sicuro del Codice** adottata da Sorint.TEK si concentra in particolare sulle applicazioni **web based** come nel caso di MangroviaIoT.

Le pratiche includono:

1. **Autenticazione:** applicazione di criteri di complessità e rotazione delle password. I tentativi di accesso non validi sono registrati, e le password sono memorizzate tramite meccanismi di *hashing*.
2. **Gestione Sessione:** I token di sessione sono gestiti dal server, e le sessioni autenticate scadono dopo inattività (Time Out).
3. **Controllo Accessi:** verifica che l'utente sia autorizzato ad agire sui dati di destinazione (Business Layer) e implementazione del principio del minimo privilegio.
4. **Validazione Input e Output Encoding:** la convalida dell'input deve avvenire il prima possibile per evitare l'ingresso di dati non corretti. Per prevenire attacchi come SQL Injection, è **espressamente vietato** utilizzare la concatenazione di stringhe per costruire istruzioni SQL con dati controllati dall'utente, ed è **obbligatorio** l'uso di query parametrizzate.
5. **Logging**: I registri non contengono informazioni riservate, inclusi dettagli di sistema, credenziali o password non necessari. Devono essere registrati tutti i tentativi di autenticazione, in particolare gli errori e tutti i fallimenti del controllo accessi.

5.2 Segregazione degli ambienti

È garantita la **separazione fisica e logica tra gli ambienti di produzione e sviluppo** per prevenire cancellazioni accidentali (in cluster GKE separati). La **modalità di debug** è supportata solo negli ambienti di sviluppo/testing.

5.3 Protezione dei dati di test

LATEK implementa misure per la protezione dei dati di test. I criteri di preferenza sono:

- Utilizzo di *data set* che **non contengono dati personali**.
- Se non è fattibile, i dati devono essere **anonimizzati o pseudonimizzati**.
- Nel caso sia necessario usare dati reali, l'attività sarà tracciata e giustificata. I dati saranno eliminati in modo sicuro al termine dell'utilizzo.

5.4 Gestione e controllo delle vulnerabilità

LATEK adotta un approccio sistematico e tracciabile alla gestione delle vulnerabilità tecniche, al fine di garantire un livello di sicurezza adeguato e costantemente aggiornato. Le attività previste includono:

1. **Verifiche mensili delle vulnerabilità**: con cadenza mensile viene effettuata un'analisi delle vulnerabilità relative al codice sorgente (SAST), alle librerie e ai componenti di terze parti. Tali verifiche sono eseguite tramite il tool Semgrep, integrato nella pipeline di rilascio di GitLab, assicurando un controllo continuo e automatizzato.
2. **Valutazioni annuali indipendenti (VA/PT):** con periodicità annuale viene commissionata a società esterne specializzate l'esecuzione di attività di Vulnerability Assessment e Penetration Test.

Queste verifiche indipendenti consentono di individuare eventuali criticità non rilevabili tramite gli strumenti di analisi automatica e di rafforzare il livello complessivo di sicurezza dell'ambiente.

6. Continuità operativa e Reversibilità

LATEK ha definito procedure specifiche di **High Availability** (HA) e **Disaster Recovery** (DR) per il prodotto MangroviaIoT SaaS.

6.1 Architettura per la continuità

Il Software MangroviaIoT, basato su Kubernetes, è strutturato per garantire l'alta disponibilità (HA) mediante:

- **Supporto Multi-AZ:** Le VM, i dischi e i *bucket* di *cloud storage* sono configurati per il supporto **Multi-AZ** (Zone) all'interno della regione primaria (**europe-west8, Italia**) o della regione secondaria (**europe-west9, France)**, garantendo la ridondanza su diverse Zone.
- Utilizzo di servizi managed Kubernetes (GKE) di **tipo regionale con supporto multi-az** e node pools configurati sulle diverse az.
- I dati applicativi vengono sottoposti a backup con frequenza giornaliera e retention settimanale. I backup sono archiviati all'interno di bucket di tipo dual-region.
- Le informazioni applicative (versioni dei micro-servizi, configurazioni e *secrets*) sono **versionate e mantenute persistentemente in progetti Gitlab esterni al cloud provider**, e non vengono mai modificate direttamente in cloud, ma tramite *pipeline* CI/CD in Gitlab. Questo è fondamentale per la ripristinabilità.

6.2 Backup e obiettivi di ripristino (DR)

La responsabilità per il **Backup delle Informazioni** è in capo a LATEK. I sistemi di backup sono configurati per mantenere copie multiple dei dati in luoghi fisicamente/logicamente diversi: i backup sono conservati su storage cloud multi-AZ con replica dual-region.

Per garantire la continuità operativa e la resilienza dell'infrastruttura, sono previste diverse strategie di Disaster Recovery (DR), calibrate sui diversi scenari di rischio e necessità operative, le modalità di DR supportate includono:

- **DR Intra-Region (Guasto di una AZ):** L'obiettivo è garantire **RPO (Recovery Point Objective): 0h** (nessuna perdita di dati) e **RTO (Recovery Time Objective): 4h**.
- **DR Multi-Region (Indisponibilità totale della regione primaria):** La strategia si basa su un approccio *Backup & Restore* in una regione di backup (eu-west4), con obiettivi definiti: **RPO: 1 giorno** (pari alla frequenza di backup dei dati) e **RTO: 3 giorni**.
- **Ripristino:** La procedura DR multi-region prevede la ricostruzione del *cluster* GKE nella regione secondaria e il *restore* dei DB Postrgres necessari, utilizzando i backup dei dati disponibili. La procedura di ripristino in caso di DR Multi-region viene verificata su base annuale.

Portabilità e Migrazione Tecnica: Poiché l'architettura è cloud-agnostic, LATEK ha una procedura formalizzata (**Procedura Migrazione Cloud Provider**) che copre il passaggio a un fornitore alternativo. Le configurazioni, i *secrets* e le versioni dei microservizi sono **mantenuti persistentemente in progetti Gitlab esterni al cloud provider**, permettendo la ricostruzione dell'istanza in un ambiente differente.

L'esecuzione completa del processo di migrazione richiede **5 giorni lavorativi**.

6.3 Reversibilità Contrattuale (Offboarding)

- Alla cessazione del Contratto, LATEK provvederà alla **cancellazione sicura e definitiva di tutti i dati e le Informazioni del cliente** (inclusi i dati personali - PII), decorsi 60 giorni dalla data di effettiva risoluzione, salvo eventuali obblighi legali di conservazione.
- Il **Cliente** ha la **facoltà e la responsabilità di estrarre e trasferire i propri dati** e le Informazioni in qualsiasi momento prima della cancellazione, utilizzando le funzionalità di export standard del Software. Ciò garantisce il diritto alla portabilità dei dati in coerenza con quanto previsto dall'Art. 20 del GDPR.
- In via eccezionale, il Cliente potrà richiedere al Fornitore, entro il termine di 60 giorni, un **servizio a pagamento di assistenza all'export dei dati**. Tale servizio sarà soggetto a preventivo e tariffe orarie da concordare e dovrà essere completato entro un termine massimo di 30 giorni, dopo il quale la cancellazione definitiva sarà comunque eseguita.

7. Gestione degli Accessi e Sicurezza Operativa

7.1 Accesso al Software e Credenziali

L'accesso applicativo al Software MangroviaIoT da parte del cliente e degli utenti autorizzati avviene tramite **Credenziali di Accesso** (User ID e Password) fornite inizialmente da LATEK.

È facoltà di LATEK adottare, in aggiunta o in alternativa ad User ID e Password, ulteriori o diverse modalità di accesso alla fruizione dei moduli applicativi e del Software quali, a titolo esemplificativo e non esaustivo, certificati digitali su smart card o MFA/OTP con l'obbligo di preventiva comunicazione al Cliente.

- **Responsabilità del cliente:** Il cliente è l'esclusivo responsabile della creazione e gestione delle **utenze dedicate** per gli utenti autorizzati. Le credenziali di accesso e i codici di autorizzazione sono **strettamente personali e non cedibili**. Il cliente ha l'obbligo di custodirli con la massima diligenza.
- È facoltà del cliente richiedere attivazione di modalità di accesso ad autenticazione forte già supportate nativamente dall'applicativo, quali autenticazione a due fattori (MFA/OTP).
- L'accesso all'infrastruttura e ai servizi cloud, sui quali risiede MangroviaIoT, è ad uso esclusivo del personale LATEK ed è soggetto a criteri di autenticazione forte e gestione degli accessi privilegiati.
- **Autenticazione Forte (MFA):** LATEK ha implementato una procedura di Strong Authentication a due fattori (MFA/OTP) per tutti gli accessi che utilizzano ID nominali all'infrastruttura SORINT.Tek e per gli amministratori negli ambienti Cloud, promuovendola come *best practice*.
- **Accesso Privilegiato:** L'uso di programmi di utilità privilegiati è definito e regolamentato.

7.2 Sicurezza delle Comunicazioni e Crittografia

LATEK applica controlli crittografici sia ai dati *at rest* che *in transit*.

- **Crittografia in Transito:** Per la trasmissione su reti pubbliche (necessaria per la **Connettività** del Cliente), è richiesto l'uso di protocolli crittografici **TLS 1.2 o superiore (preferibilmente TLS 1.3)** per garantire la sicurezza *in transit* e l'integrità dei dati personali o sensibili.
- **Crittografia a Riposo:** La **Procedura Hardening Sistemi** impone l'obbligo di crittografia (AES-256) *at rest* per la protezione dei dati.
- **Gestione delle Chiavi:** LATEK definisce e documenta le procedure di Key Management e, ove possibile, utilizza i servizi nativi dei cloud provider per la gestione e la rotazione automatica delle chiavi e dei certificati. È comunque lasciata al cliente la facoltà di fornire e gestire le proprie chiavi di crittografia qualora preferisca mantenere un controllo diretto.

7.3 Logging e Monitoraggio

La raccolta e l'analisi dei log degli eventi rappresentano un elemento fondamentale della sicurezza operativa. In particolare:

- I log degli Amministratori di Sistema sono oggetto di monitoraggio continuo, con particolare attenzione a eventi critici quali il blocco delle utenze in Keycloak. In caso di eventi rilevanti, viene attivato un sistema di notifica automatica via email agli amministratori.

- I log degli Amministratori di Sistema sono conservati per un periodo **non inferiore a 6 mesi** e sono protetti per garantire l'assenza di informazioni sensibili quali credenziali o password.
- I log applicativi sono mantenuti per un periodo di 1 mese.

LATEK monitora costantemente le risorse cloud per garantire la corretta erogazione del servizio e il rispetto degli SLA contrattualizzati.
La capacità e le performance vengono superivsionate attraverso:

- I sistemi di monitoraggio ed observability del Cloud Service Provider (CSP)
- Il monitoraggio continuo della disponibilità e dello stato dei pod GKE con sistemi di alert automatici e notifiche email in caso di indisponibilità, riavvii o degrado del servizio

Questo approccio consente di anticipare esigenze di scalabilità, prevenire colli di bottiglia e garantire la continuità operativa della piattaforma.

7.4 Gestione del Cambiamento

Le modifiche tecniche e ai processi sono gestite tramite un processo approvativo, mediante procedure di notifica ai clienti dove necessario, sono inclusi nelle procedure di notifica dettagli relativi a:

- Categoria e motivazione dei cambiamenti;
- Data e ora dell'intervento pianificato;
- Descrizione tecnica dei cambiamenti all'infrastruttura o agli applicativi ospitati;
- Notifica di inizio o fine dell'intervento.

Ogni modifica applicativa a MangroviaIoT viene gestita attraverso una pipeline CI/CD, garantendo che nessuna modifica venga applicata direttamente agli ambienti cloud di produzione. Questo approccio assicura controllo delle versioni, tracciabilità delle modifiche, automazione del deployment e riduzione del rischio operativo.

Inoltre, LATEK si impegna a notificare ai clienti qualsiasi cambiamento eseguito o programmato dai CSP che dovesse avere impatto sui servizi cloud attivi.

8. Protezione dei Dati Personali (PII) e Ciclo di Vita

LATEK (Sorint.Tek S.R.L.) si impegna a trattare i dati personali (PII) nel rispetto del **Regolamento Europeo 679/2016 (GDPR)** e delle linee guida **ISO/IEC 27018:2019**.

8.1 Ruoli e Obblighi

Il **cliente** è il **Titolare del Trattamento** dei dati personali. Le Parti si impegnano a sottoscrivere un apposito **Data Processing Addendum (DPA)** per disciplinare le responsabilità, essendo onere del Titolare fornire il DPA a LATEK.

- **Limitazione delle Finalità:** Le PII sono trattate da LATEK solo per le finalità strettamente necessarie all'erogazione del servizio, come indicato nella Cloud Policy, e non per scopi di marketing o pubblicità.

L'accesso alle PII nei servizi cloud è strettamente controllato e limitato al personale autorizzato che ne ha effettivamente bisogno per svolgere le proprie mansioni.

- **Diritti degli Interessati:** LATEK fornisce al Cliente i mezzi e la cooperazione per facilitare l'esercizio dei diritti degli interessati (accesso, rettifica, cancellazione).

8.2 Gestione dei Subappaltatori

LATEK è legittimata a delegare l'esecuzione di prestazioni a società collegate o subappaltatori. Tuttavia, LATEK rimane **solidalmente responsabile** nei confronti del Cliente per le prestazioni eseguite da tali soggetti. L'uso di subappaltatori per il trattamento di PII viene comunicato al Cliente prima dell'uso.

8.3 Gestione degli Incidenti e Data Breach

LATEK dispone di procedure formalizzate (Incident Response Plan, Data Breach Management Procedure) per la gestione degli incidenti di sicurezza.

- **Notifica:** In caso di Data Breach che coinvolga PII, LATEK informa tempestivamente il Cliente. L'SLA contrattuale deve definire i tempi massimi di notifica per violazioni di dati.
- **Contatti:** I clienti possono segnalare incidenti di sicurezza all'indirizzo `incident@sorint.com` o Data Breach al DPO (`dpo@sorint.com`). Le segnalazioni di assistenza sul prodotto Mangrovia vengono tracciate internamente tramite.

8.4 Cessazione del Servizio e Cancellazione Dati

Al termine del Contratto, le procedure di disattivazione del servizio garantiscono la gestione sicura dei dati:

- **Restituzione:** È espressamente inteso che **LATEK non avrà alcun onere di restituire o consegnare al Cliente i dati e le informazioni** presenti sul Software al momento della cessazione.
- **Cancellazione Sicura (Modalità SaaS):** Entro 60 giorni dalla cessazione del Contratto in Modalità SaaS, LATEK provvede alla **cancellazione e/o distruzione sicura** dei dati memorizzati sul Cloud, in conformità con le procedure interne (es. Information Deletion Procedure). LATEK implementa misure per la cancellazione sicura e irreversibile, raccomandando la sovrascrittura o la cancellazione crittografica per dati sensibili.

9. Supporto Tecnico e Performance

9.1 Supporto Clienti

Le richieste di assistenza sul prodotto Mangrovia possono essere aperte dai clienti tramite telefono o mail (support@mangroviaiot.com). Ogni richiesta è tracciata tramite il *tool* di ticketing aziendale.

Nei contratti è inclusa esclusivamente l'assistenza di supporto di secondo livello, erogata in orario d'ufficio dal lunedì al venerdì, dalle 9:00 alle 18:00.

9.2 Service Level Objectives (SLO) Interni

LATEK adotta un insieme strutturato di Service Level Objectives (SLO) interni, definiti per garantire un livello di servizio costante e misurabile.

Tali obiettivi vengono monitorati trimestralmente e rappresentano un impegno formale al miglioramento continuo delle performance e dell'affidabilità dei servizi erogati.

Per Incident o bug urgenti, questi gli SLO monitorati:

- **KPI Presa in carico: <** 2h (se segnalazione in orario ufficio) o < 11:00 (se segnalazione fuori orario o in giorni festivi).
- **KPI Risoluzione:** < 24h**.** Ove non possibile per necessità di sviluppi che eccedano 1 gg/uomo o quando necessario interfacciamento con altri fornitori/partner per risoluzione del problema, sarà da garantire un aggiornamento di follow-up al cliente ogni 4h (durante orari lavorativi) fino alla risoluzione del problema**.**

Per tutte le altre segnalazioni o richieste di supporto, questi gli SLO monitorati:

- **KPI Presa in carico:** giorno segnalazione (< 1d) (se segnalazione in orario ufficio) o < 13:00 (se segnalazione fuori orario o in giorni festivi).
- **KPI Risoluzione:** non previsti

È facoltà del cliente richiedere un report riepilogativo dettagliato relativo agli indicatori di servizio di proprio interesse. LATEK si impegna a fornire tale documentazione entro 15 giorni dalla richiesta, garantendo trasparenza e tracciabilità delle performance monitorate.

9.3 SLA disponibilità del servizio

LATEK assicura livelli di disponibilità del servizio allineati agli SLA garantiti dal Cloud Service Provider (CSP), GCP (Google Cloud Platform), su cui l'infrastruttura è ospitata.
I relativi valori di disponibilità, così come le condizioni applicabili, sono consultabili nella documentazione ufficiale del CSP (vedi: **Google Cloud Service Level Agreements**).

LATEK ha implementato un processo periodico sul fornitore critico GCP per verificare il rispetto degli impegni assunto in merito alla gestione della sicurezza interna e relative certificazioni, della gestione eventi di sicurezza ed effettiva disponibilità dei servizi.

9.4 Riferimento Contrattuale e Limitazione

Il presente Whitepaper descrive l'architettura tecnica, le misure di sicurezza adottate e gli obiettivi interni (SLO) del servizio MangroviaIoT in modalità SaaS.
Si specifica che tutti gli impegni di servizio vincolanti, i termini di licenza d'uso, le condizioni economiche, la disciplina della Proprietà Intellettuale, la gestione della responsabilità e le disposizioni sulla Reversibilità dei dati (Offboarding) sono interamente regolati dal Contratto sottoscritto tra il Cliente e LATEK (Sorint.tek s.r.l.), e dalle sue Condizioni Generali MangroviaIoT.
In caso di qualsiasi conflitto o divergenza tra il contenuto di questo Whitepaper e i termini contrattuali, prevarranno sempre e comunque le clausole contenute nel Contratto e nelle Condizioni Generali MangroviaIoT.

9.5 Nota sui Controlli ISO 27017 e 27018

SORINT.tek garantisce che le proprie pratiche operative e i requisiti contrattuali verso i CSP e i Clienti siano allineati ai controlli specifici per i servizi cloud (ISO 27017) e per la gestione delle PII (ISO 27018). Questo include la verifica

periodica delle certificazioni dei CSP e l'applicazione di policy rigorose per la gestione degli accessi privilegiati e la segregazione dei tenant.