VERSIONE 6 - 18/05/2026

WHITEPAPER INFORMATIVA SUI SERVIZI CLOUD SAAS EROGATI DA GRUPPO INFORMATICA E SERVIZI GIES S.R.L.

Il presente documento, denominato "Whitepaper informativa servizi cloud", ha lo scopo di illustrare e definire aspetti e caratteristiche dei servizi cloud SaaS offerti da GIES.

SOMMARIO

DEFINIZIONI

Fornitore o GIES: la società Gruppo Informatica e Servizi GIES S.r.l., responsabile dell'erogazione, gestione e manutenzione dei Servizi SaaS oggetto del presente documento.

Cliente o Ente: il soggetto che si affida ai servizi SaaS proposti da GIES e che detiene la titolarità dei dati in essi inseriti.

Firmatario dell'affidamento: soggetto responsabile o il dirigente che ha firmato per l'affidamento dei servizi SaaS; in alternativa si intende il RUP nella fase di costituzione del progetto e, successivamente alla firma del contratto, il soggetto che lo sottoscrive, o quello indicato nel Capitolato, qualora presente.

Servizi: le piattaforme basate su cloud progettate ed erogate da GIES, nello specifico BabylonWeb e ROSS 1000.

Canale di Assistenza Tecnica: gli indirizzi email ufficiali indicati nella sezione "*13.1. CONTATTI ASSISTENZA*" del presente documento, ai quali il Cliente deve trasmettere le segnalazioni di malfunzionamenti, incidenti di sicurezza o richieste di gestione utenze ed export dati, al fine di garantire la corretta presa in carico e tracciabilità tramite ticket, come descritto nella sezione "*11. METODO DI EROGAZIONE DEL SERVIZIO DI ASSISTENZA*".

Regolamento Cloud ACN: regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

GLOSSARIO

1. **ACN** - Agenzia per la Cybersicurezza Nazionale.
2. **AGID** - Agenzia per l'Italia Digitale.
3. **API (Application Programming Interface)** - Interfacce che permettono l’interazione tra diverse applicazioni software.
4. **ARUBA** - Aruba S.p.A.
5. **CIA** - Confidentiality, Integrity, Availability, acronimo che indica i tre principi fondamentali della sicurezza delle informazioni.
6. **CSP** - Cloud Service Provider, fornitore di servizi Cloud.
7. **DPIA (Data Protection Impact Assessment)**: strumento per valutare gli impatti del trattamento dei dati personali.
8. **GIES** - Gruppo Informatica e Servizi GIES S.r.l.
9. **IaaS** - Infrastructure as a Service.
10. **KPI** - Key Performance Indicators: parametri oggettivi atti a monitorare il rispetto dello SLA.
11. **NDA** - Non Disclosure Agreements, accordo di riservatezza.
12. **NTP** - Network Time Protocol, protocollo per la sincronizzazione degli orologi dei server.
13. **PII** - Personally Identifiable Information, ovvero informazioni relativi alla persona fisica.
14. **RBAC (Role-Based Access Control)**: modello di sicurezza che assegna permessi agli utenti in base ai loro ruoli.
15. **RPD/DPO** - Responsabile della Protezione dei Dati/Data Protection Officer
16. **RUP** - Referente Unico del Progetto.
17. **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.
18. **SLA** - Service Level Agreement: accordo contrattuale che definisce i livelli di servizio attesi (come disponibilità e tempi di risposta) e le penali in caso di mancato rispetto degli stessi.
19. **PA** - Pubblica Amministrazione.
20. **TLS** - Transport Layer Security: protocollo crittografico principale progettato per garantire la sicurezza, la privacy (riservatezza) e l'integrità dei dati su reti informatiche.
21. **SSRM** - Shared Security Responsibility Model: framework per il cloud computing che ripartisce i compiti di protezione tra fornitore (sicurezza dell'infrastruttura) e cliente (sicurezza di dati e configurazioni).
22. **GDPR** - General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati): Regolamento UE 2016/679

1

AMBITO, CARATTERISTICHE E UBICAZIONE DELLA RELAZIONE COMMERCIALE E DEI SERVIZI OFFERTI

1.1. DESCRIZIONE GENERALE DEI SERVIZI SAAS DI GIES

I servizi SaaS forniti da GIES sono piattaforme basate su cloud progettate per l'erogazione e gestione dei servizi relativi a:

1. BabylonWeb: piattaforma utilizzata per la gestione tecnico-amministrativa dell'inventario, la gestione amministrativa di concessioni e locazioni, il monitoraggio utenze, la rendicontazione economica e l'assolvimento degli adempimenti verso gli organismi di controllo

2. ROSS 1000: piattaforma per la rilevazione dei flussi turistici territoriali, servizi tecnici e contabili, comprensivi di assistenza ed esternalizzazione delle attività tecniche, contabili e statistiche.

Le principali funzionalità sono elencate nelle rispettive schede pubblicate sul Catalogo delle Infrastrutture digitali e dei Servizi cloud.

È garantita agli utenti una soluzione scalabile, sicura e conforme agli standard internazionali, nonché conforme agli standard previsti all'interno delle certificazioni acquisite da GIES.

I costi dei servizi offerti non prevedono delle metriche a consumo e sono basati su un canone periodico.

1.2. INFRASTRUTTURA

L'infrastruttura Cloud è erogata da Aruba S.p.A., CSP in possesso delle qualificazioni per la PA previste dal "Regolamento Cloud ACN" (Decreto dell'Agenzia per la Cybersicurezza Nazionale n. 21007/2024), che garantisce adeguati livelli di integrità, disponibilità e riservatezza.
Condizioni, ruoli e responsabilità nella fornitura dell'infrastruttura Cloud e nel trattamento di informazioni in essa contenute, sono consultabili al seguente link **https://www.acn.gov.it/portale/w/ia-57**.

Il servizio SaaS utilizza, come sorgente di data e ora i server NTP forniti da Inrim **https://www.inrim.it/**.

1.3. PERIMETRO DELLE OPERAZIONI

Il perimetro operativo del servizio copre tutte le attività relative alla gestione della piattaforma SaaS, incluse: monitoraggio continuo, aggiornamenti software, backup periodici e risposta a eventi critici.
Le responsabilità del Cliente e del Fornitore sono definite in dettaglio nel *Modello di Responsabilità Condivisa (SSRM)* alla sezione 2.2.

REQUISITI DI SICUREZZA DELLE INFORMAZIONI

2

In ottemperanza alle norme ISO/IEC 27001:2022 e al GDPR, GIES osserva i principi di sicurezza delle informazioni adottando specifiche policy e procedure.

2.1. PRINCIPI DI SICUREZZA DELLE INFORMAZIONI

La sicurezza delle informazioni si basa sui principi fondamentali della triade “CIA”: confidenzialità, integrità e disponibilità. Per garantire questi principi, il servizio implementa controlli di accesso rigorosi, crittografia avanzata e monitoraggio continuo delle minacce.

Il servizio SaaS è erogato da GIES, azienda che detiene la piena proprietà del prodotto concesso in licenza d’uso. Al fine di garantire la sicurezza dei dati in ogni fase dell'utilizzo dell'applicazione, GIES ha messo in atto determinate misure tecniche e organizzative:

1. Le comunicazioni verso il servizio cloud avvengono all’interno di un canale sicuro TLS, con queste caratteristiche:
    - **Algoritmo della firma sha256;**
    - **Chiave pubblica RSA 2048 bit.**
2. GIES si rende disponibile a garantire la gestione delle chiavi crittografiche, qualora richiesta dall’ente. Per le specifiche si rimanda ai singoli contratti;
3. Il controllo degli accessi al sistema di gestione e configurazione della piattaforma avviene esclusivamente con le credenziali a doppio sistema di autenticazione a esclusivo utilizzo di operatori selezionati da GIES;
4. Viene utilizzata un’adeguata piattaforma di trasferimento di informazioni, tramite canale sicuro in area dedicata, oppure altro metodo alternativo con pari grado di sicurezza;
5. La pubblicazione del servizio, la protezione dei dati e la gestione dei backup vengono eseguite nell’osservanza delle Politiche aziendali, fornibili su richiesta;
6. Il prodotto software mette a disposizione adeguati strumenti per la protezione degli account utente per l’accesso al sistema (es. protezione da attacchi brute force) e di tutela delle PII in caso di sospetta compromissione delle credenziali di accesso (es. a seguito della loro presunta divulgazione involontaria);
7. Gli ambienti di sviluppo di GIES sono segregati e accessibili solo al personale autorizzato.
   Lo sviluppo del software segue le linee guida di sviluppo sicuro, atte ad assicurare che vengano rispettati i principi di Security by Design (integrati nei processi) e di Privacy by Design (applicati per impostazione predefinita), pubblicati da AGID;
8. Per le attività di sviluppo e di test è garantito un ambiente sicuro e separato da quello di produzione.

2.1.1. BACKUP

GIES ha stabilito politiche specifiche per la salvaguardia dei dati relativi ai servizi cloud. I backup sono preventivamente criptati con algoritmo AES-256 e successivamente trasferiti tramite canale sicuro su sistema fisicamente separato dall'ambiente di produzione, situato in Repubblica di San Marino o all'interno del territorio dell'Unione Europea.

Solo il personale autorizzato ha accesso alle location del backup. GIES effettua regolari verifiche sui backup eseguiti.

Il periodo di conservazione (retention) dei backup viene gestito come di seguito indicato:

- **Ogni backup viene conservato per minimo 1 anno dalla sua creazione;**
- **Ogni backup viene conservato per massimo 5 anni dalla sua creazione;**
- **Qualora il contratto cessi prima di questi tempi, ogni backup sarà eliminato 90gg dopo la data di cessazione del contratto.**

Il firmatario dell'affidamento può richiedere evidenza dell'avvenuta esecuzione delle verifiche sui backup inviando una richiesta tramite il canale di Assistenza Tecnica.

GIES si impegna a rispondere alla richiesta di verifica sui backup entro 15 giorni lavorativi, allegando dove possibile un report dettagliato del test effettuato.
Per maggiori informazioni si rimanda alla policy di politiche sulla sicurezza delle informazioni che su richiesta verrà inoltrata al Cliente.

2.1.2. SICUREZZA OPERATIVA

GIES riconosce che la gestione delle vulnerabilità tecniche dei sistemi informatici sia una delle attività fondamentali per garantire la sicurezza e la piena operatività dei propri servizi; a tal fine è stato predisposto un team con risorse dedicate, che si occupano di ricercare, gestire e risolvere le vulnerabilità tecniche individuate.

Qualora vengano riscontrate gravi vulnerabilità tecniche non risolvibili (0-day) sul sistema cloud, GIES invierà comunicazione al Cliente mezzo PEC o email.

2

2.1.3. FORMAZIONE DEL PERSONALE

Tutto il personale GIES è formato e sensibilizzato in materia di sicurezza delle informazioni e protezione dei dati personali, comprendendo le possibili conseguenze di comportamenti non conformi sia per l'organizzazione sia per gli interessati, con programmi di formazione periodica e documentata.

2.1.4. RESPONSABILITÀ DOPO CESSAZIONE O CAMBIO DI INCARICO

GIES applica procedure interne che garantiscono la revoca tempestiva degli accessi, la restituzione e la bonifica dei dispositivi aziendali e il mantenimento degli obblighi di riservatezza del personale anche dopo la cessazione o variazione del rapporto di lavoro.

Tali procedure sono formalizzate nelle policy di sicurezza aziendale e soggette a verifica periodica, a tutela della continuità e della protezione dei dati dei clienti.

2.1.5. SMALTIMENTO SICURO E RIUTILIZZO DELLE APPARECCHIATURE

GIES adotta procedure documentate volte a garantire la cancellazione sicura dei dati e la sanitizzazione dei supporti di memorizzazione prima del loro smaltimento o riutilizzo.

Tutte le apparecchiature, fisiche o virtuali, potenzialmente idonee a contenere dati dei clienti o informazioni personali, sono trattate come se tali dati fossero effettivamente presenti.

Le operazioni di distruzione o bonifica sono eseguite in conformità alle policy di sicurezza aziendale e, ove applicabile, agli standard tecnici riconosciuti.

Le evidenze delle attività di smaltimento sono conservate a fini di verifica e audit.

2.2. MODELLO DI RESPONSABILITÀ CONDIVISA (SSRM)

Il SSRM definisce chiaramente le aree di responsabilità tra Fornitore e Cliente.

Il Fornitore è responsabile della sicurezza dell'infrastruttura cloud, mentre il Cliente gestisce la sicurezza delle applicazioni e dei dati caricati.

Il modello è conforme alle linee guida di ISO/IEC 27001:2022 e ISO/IEC 27018:2025.

2.2.1. MODELLO SSRM (SHARED SECURITY RESPONSIBILITY MODEL) PER FORNITORE DI SERVIZI SaaS

Il presente paragrafo definisce le responsabilità condivise tra GIES e i Clienti in materia di sicurezza delle informazioni, protezione dei dati personali e conformità normativa, in coerenza con le best practice di settore.

RESPONSABILITÀ DEL FORNITORE SaaS

Il Fornitore SaaS si impegna a garantire la sicurezza dell'infrastruttura e della piattaforma secondo i seguenti punti:

1. Sicurezza dell'infrastruttura

Gestione e protezione dei data center, dei server fisici e delle reti utilizzate per fornire il servizio.
Implementazione di misure di sicurezza fisica e logica, inclusi firewall, IDS/IPS, e protezione DDoS

2. Crittografia dei dati

Crittografia dei dati in transito e a riposo utilizzando algoritmi avanzati (es. AES-256).
Gestione sicura delle chiavi di crittografia, a meno che diversamente specificato da contratto.

3. Patch e aggiornamenti

Applicazione regolare di patch di sicurezza e aggiornamenti del software per garantire la protezione contro vulnerabilità note.

4. Backup e Disaster Recovery

Esecuzione di backup periodici e implementazione di piani di Disaster Recovery con tempi di recupero garantiti.

5. Conformità normativa

Garantire la conformità agli standard di sicurezza riconosciuti a livello nazionale. Supportare il Cliente nel rispetto delle normative nazionali (con specifico riferimento a quelle per la PA).

6. Monitoraggio e logging

Fornire strumenti di monitoraggio delle attività e accesso ai log di sicurezza.
Segnalazione tempestiva di incidenti di sicurezza rilevati sull'infrastruttura.

RESPONSABILITÀ DEL CLIENTE

Il Cliente è responsabile della gestione e protezione dei propri dati e dell'uso sicuro del servizio SaaS, come segue:

1. Gestione degli accessi e delle identità

- *Configurare correttamente i controlli di accesso e le politiche di sicurezza interne.*
- *Utilizzare funzionalità proprie di autenticazione a più fattori (MFA) e Single Sign-On (SSO).*

2. Protezione dei dati

- *Garantire che i dati caricati nel sistema siano conformi alle normative vigenti.*
- *Effettuare backup periodici dei dati specifici, se non coperti dal Fornitore.*

3. Configurazione del servizio

- *Personalizzare e configurare il servizio SaaS in modo sicuro, secondo le indicazioni del Fornitore che può mettere a disposizione dopo la contrattualizzazione.*

4. Monitoraggio delle attività

- *Monitorare le attività degli utenti e rispondere tempestivamente a eventuali anomalie di utilizzo degli utenti.*

5. Conformità normativa

- *Assicurare la conformità normativa nella gestione dei dati propri e dei propri clienti, in particolare rispetto al GDPR.*

2

RESPONSABILITÀ CONDIVISE

Alcuni aspetti della sicurezza possono richiedere la collaborazione tra Fornitore e Cliente:

1. Gestione delle chiavi di crittografia

- *In scenari dove il Cliente gestisce le proprie chiavi (es. Bring Your Own Key - BYOK), entrambe le parti devono collaborare per garantire la sicurezza.*

2. Gestione degli incidenti

- *Collaborazione nella rilevazione, gestione e risoluzione di incidenti di sicurezza.*
- *Comunicazione tempestiva di eventuali violazioni dei dati entro i termini previsti dalla normativa.*

3. Audit e valutazioni di Sicurezza

- *Possibilità di condurre audit congiunti o di fornire documentazione comprovante la conformità a standard di sicurezza.*

4. Formazione sulla sicurezza

- *Il Fornitore fornisce risorse e strumenti per la formazione, mentre il Cliente è responsabile della formazione continua dei propri utenti.*

LIMITAZIONI DI RESPONSABILITÀ

Il Fornitore SaaS non sarà ritenuto responsabile per:

1. Incidenti di sicurezza derivanti da una configurazione errata da parte del Cliente;
2. Accessi non autorizzati dovuti a credenziali deboli o condivise;
3. Perdite di dati derivanti da errori del Cliente nel backup o nella gestione delle informazioni.

RISOLUZIONE DELLE CONTROVERSIE

In caso di controversie relative alla sicurezza o alla gestione dei dati, le parti si impegnano a risolverle in via amichevole.

In caso di mancato accordo, le controversie saranno risolte in sede giudiziale secondo la normativa vigente in materia di contratti pubblici.

MODIFICHE CONTRATTUALI

Eventuali modifiche al presente SSRM devono essere concordate per iscritto tra le parti e allegate al contratto principale.

2.2.2. SEGREGAZIONE DELLE RISORSE

GIES mette in atto adeguate politiche al fine di ottenere l'isolamento delle risorse in cui sono presenti dati dei clienti.

Dove possibile, vengono messi in atto automatismi per eliminare le informazioni create a seguito di altre elaborazioni.

L'accesso da parte di personale aziendale ai dati, anche in sola lettura, è regolamentato secondo il criterio "least privilege" per il quale a ogni operatore è concesso il privilegio minimo necessario per poter svolgere i propri compiti.

2.2.3. MULTITENANCY E ACCESSO ALLE RISORSE DEL CLIENTE

Le caratteristiche di tenancy dell'ambiente SaaS fornito da GIES sono definite tra queste modalità:

- ***Ambiente single-tenant:***
  - *Il Cliente è proprietario in esclusiva di una porzione delle risorse hardware fornite da GIES;*
  - *l'ambiente software è dedicato esclusivamente al Cliente;*

- ***Ambiente multi-tenant:***
  - *l'ambiente è in condivisione con più utenti;*
  - *la separazione delle risorse avviene a livello software: ogni utente è separato dagli altri da ACL di accesso che isolano i vari tenant tra di loro;*

Le persone che possono accedere alle risorse del Cliente sono quelle individuate nel team di lavoro dedicato.

GIES garantisce al Cliente la possibilità di censire e mappare i diversi profili e le diverse autorizzazioni per l'accesso corretto ai servizi, conformemente ai requisiti prescritti da Regolamento Cloud ACN.

Inoltre, per una maggiore comprensione dei diversi utenti e privilegi sono stati redatti appositi manuali per i diversi servizi erogati.
Per maggiori informazioni sulle caratteristiche del servizio SaaS, è possibile attivare una richiesta di supporto al Canale di Assistenza Tecnica.

2.3. COMPLIANCE CON ISO/IEC 27001:2022 E ISO/IEC 27018

Il servizio è certificato ISO/IEC 27001:2022 per la gestione della sicurezza delle informazioni e ISO/IEC 27018:2025 per la protezione dei dati personali nel cloud.

Inoltre, il Fornitore è certificato ISO/IEC 20000-1:2018 per garantire la fornitura di servizi IT di alta qualità.

Gli audit annuali confermano la conformità a questi standard.

PROCESSO DI CHANGE MANAGEMENT

3

3.1. POLITICHE E PROCEDURE

Il processo di Evoluzione del software (Change Management) segue una politica strutturata per gestire modifiche pianificate e non pianificate. Ogni richiesta di modifica è soggetta a un processo di valutazione del rischio, pianificazione dettagliata e approvazione formale.
Le procedure adottate tengono conto dei cambiamenti dell'infrastruttura cloud o degli applicativi ivi ospitati. GIES metterà in atto procedure di notifica ai clienti dei cambiamenti che è intenzionata a eseguire o che sono già stati effettuati.
Dove necessario, saranno inclusi nelle procedure di notifica dettagli relativi a:

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

Inoltre, GIES notifica ai clienti qualsiasi cambiamento eseguito o programmato dal fornitore dello IaaS sottostante, che dovesse avere impatto sui servizi cloud pubblicati.

La frequenza di aggiornamento del servizio cloud qualificato è almeno mensile, in ottemperanza delle prescrizioni previste nel Regolamento Cloud ACN.

3.2. STANDARD ISO/IEC 20000-1 e ISO/IEC27001

Le procedure sono conformi agli standard ISO/IEC 20000-1:2018 e ISO/IEC 27001:2022, garantendo che ogni modifica sia gestita in modo da minimizzare l'impatto sui servizi e sugli utenti finali.

3.3. COMUNICAZIONE DEI CAMBIAMENTI

Le modifiche rilevanti vengono comunicate agli stakeholders con un preavviso minimo di 30 giorni.
La comunicazione include i dettagli del cambiamento, l'impatto previsto e le azioni richieste.

LOGGING E MONITORING

4

Al fine di mantenere la sicurezza e integrità dei dati, e nel rispetto delle Politiche aziendali, si informa che GIES ha messo in atto una serie di azioni riguardanti la gestione e il monitoraggio dei log di accesso e che tali log possono essere utilizzati come testimonianza nel processo di gestione degli incidenti relativi alla sicurezza delle informazioni.

4.1. LOGGING

Il log dettagliato degli accessi e delle operazioni eseguite nel sistema, sia amministrative che operative, viene storicizzato su sistema fisicamente separato in modalità criptata AES-256 non esposto e non modificabile, accessibile a specifici operatori:

- **Il periodo di conservazione (retention) massimo dei log è di 1 anno mentre il periodo minimo è di 6 mesi;**
- **Salvo dove non altrimenti possibile, sono messe in atto azioni al fine di evitare l'inclusione di PII all'interno dei log.**

I log delle attività vengono raccolti e archiviati in modo sicuro per un periodo massimo di 12 mesi.

Le informazioni registrate includono accessi, modifiche ai dati e tentativi di accesso non autorizzati. Il sistema garantisce inoltre il costante monitoraggio delle risorse e il controllo degli accessi al servizio SaaS.

Per maggiori informazioni sulla raccolta dei log nelle procedure SaaS GIES, è possibile contattare il Canale di Assistenza Tecnica.

4.2. COMPLIANCE CON ISO/IEC 27017

I Servizi implementano pratiche di logging e monitoring conformi agli standard ISO/IEC 27017:2015, garantendo la protezione e l'integrità delle informazioni gestite nel cloud.

GESTIONE DEGLI INCIDENTI E PROCEDURE DI COMUNICAZIONE

5

GIES, per rispondere e gestire adeguatamente eventuali incidenti di sicurezza, implementa procedure e azioni che coprono tutte le fasi dell'incidente, nel rispetto dei principi di protezione dei dati personali fin dalla progettazione e per impostazione predefinita (Privacy by Design e Privacy by Default), ai sensi dell'articolo 25 del Regolamento UE 2016/679.

5.1. PIANO DI GESTIONE DEGLI INCIDENTI

GIES ha definito controlli e procedure per poter permettere un approccio organizzato e regolato alla gestione degli incidenti come parte della propria strategia di sicurezza delle informazioni.
Qualora si verifichino incidenti relativi alla sicurezza informatica di gravità tale che sia presente un rischio elevato per i diritti e le libertà fondamentali degli interessati, GIES si occuperà di comunicare l'accaduto al Cliente nel minor tempo possibile.
Il piano di gestione degli incidenti si basa su un approccio proattivo e reattivo, garantendo che questi vengano identificati, gestiti e risolti tempestivamente. La gestione degli incidenti viene effettuata seguendo le metodologie aziendali sulla base di criticità e tipologie di impatto.
Per segnalazioni relative a eventi sulla sicurezza informatica, fare riferimento alla sezione Contatti.

5.2. NOTIFICA E COMUNICAZIONE AGLI STAKEHOLDERS

In caso di incidente, i clienti vengono notificati entro un periodo massimo di 24 ore dal rilevamento dell'evento.
Le notifiche includono informazioni dettagliate sull'incidente, le azioni correttive adottate e il tempo stimato per la risoluzione.
La comunicazione avviene attraverso canali scritti. I riferimenti al paragrafo *CONTATTI*.
Il canale utilizzato per la comunicazione e le caratteristiche di quest'ultima saranno definite da GIES in base alla tipologia di violazione.
Il referente che sarà contattato da GIES in caso di incidente è il firmatario dell'affidamento, fatta eccezione in caso di delega alla notifica e comunicazione, di cui al paragrafo 7.3. *DELEGA ALLA GESTIONE DEGLI ACCESSI*.

5.3. RIFERIMENTI ALLA NORMA ISO/IEC 27001:2022

Le procedure di gestione degli incidenti sono allineate alla norma ISO/IEC 27001:2022 e al Regolamento UE 2016/679 (GDPR), garantendo un approccio sistematico e standardizzato alla rilevazione, analisi, contenimento e recupero dagli incidenti.
Tutti i dettagli relativi alla gestione degli incidenti sono presenti nelle Politiche aziendali, fornite su richiesta del Cliente.

AUDIT

6

GIES, in qualità di fornitore di servizi cloud, consente al Cliente l'effettuazione di audit periodici, nel rispetto delle modalità e delle tempistiche stabilite nel contratto.

6.1. AUDIT

Il firmatario dell’affidamento può avanzare richieste di audit per verificare la conformità ai termini dello SLA e alle normative applicabili.
Gli audit possono includere verifiche dei sistemi, processi e infrastrutture utilizzate per l’erogazione del servizio.

6.2. REQUISITI NORMATIVI E STANDARD ISO/IEC 27001 E 27018

Il Fornitore è certificato secondo gli standard ISO/IEC 27001:2022 e ISO/IEC 27018:2025, che garantiscono la conformità a elevati livelli di sicurezza per i servizi cloud. Gli audit possono essere condotti da enti terzi qualificati o direttamente dal Cliente previa notifica scritta da inviare tramite il Canale di Assistenza Tecnica.

6.3. LIMITAZIONI ALL'ESECUZIONE DI AUDIT

Quando l’esecuzione di audit individuali da parte dei clienti non è praticabile o potrebbe compromettere la sicurezza complessiva dell’infrastruttura, GIES mette a disposizione evidenze indipendenti e aggiornate - come certificazioni, rapporti di audit e attestazioni di conformità - a garanzia della trasparenza e dell’efficacia del proprio sistema di gestione della sicurezza delle informazioni.

MODALITÀ DI GESTIONE DEGLI ACCESSI E CESSAZIONE DEL SERVIZIO PER LA SUITE BABYLONWEB

7

GIES si impegna a fornire le modalità di attivazione e cessazione del servizio adottando politiche di dismissione e di portabilità dei dati, osservando le best practices previste dalle vigenti norme AGID e ACN.
Il processo di attivazione decorre dalla sottoscrizione contrattuale e prevede l'attivazione entro 7 giorni dell'istanza applicativa, l'abilitazione dei servizi acquisiti e la trasmissione delle credenziali temporanee di primo accesso unicamente agli utenti indicati, secondo le modalità previste nei paragrafi che seguono.

7.1. REGISTRAZIONE E CANCELLAZIONE

Il servizio è accessibile esclusivamente tramite autenticazione. Le credenziali di primo accesso sono create da GIES e consegnate tramite canale sicuro al referente del Cliente, successivamente alla sottoscrizione del contratto, previa richiesta da parte dell'ente.
La creazione delle credenziali di primo accesso avverrà successivamente alla sottoscrizione del contratto con GIES, seguendo queste modalità:

1. Le richieste di attivazione di nuove credenziali devono essere inviate via email al Canale di Assistenza Tecnica;
2. Il firmatario dell'affidamento si occuperà di fornire a GIES la lista degli utenti, il loro indirizzo email, nome e cognome, ruolo e permessi dei moduli in uso all'Ente;
3. Eventuali richieste di creazione di nuovi utenti, provenienti da soggetti diversi dal firmatario dell'affidamento, saranno prese in considerazione solo se avanzate da figure di ruolo gerarchico superiore rispetto a quello del firmatario dell'affidamento.

GIES si impegna a processare le richieste di nuovi accessi ai servizi SaaS secondo le tempistiche definite nella "*Tabella 1 – SLA Assistenza*", successivamente esplicata.

Qualora ci fosse la necessità di visionare una versione di prova (demo) dell'applicativo SaaS prima della sottoscrizione del contratto, saranno create credenziali esclusivamente dedicate a questo scopo su un'ambiente dedicato, previa apposita richiesta da parte dell'ente.

È compito del Cliente prendere in carico le credenziali di primo accesso e procedere immediatamente con la variazione della relativa password.

È dovere del Cliente attuare tutte le buone norme sulla conservazione in sicurezza delle credenziali di accesso ai servizi SaaS GIES.

Qualora si avesse il sospetto della compromissione delle credenziali di accesso, il Cliente è tenuto a eseguire tempestivamente la variazione della password in autonomia o aprendo una richiesta di supporto che dovrà pervenire esclusivamente al Canale di Assistenza Tecnica.
Qualora l'utente non ricordi lo username di accesso è tenuto a contattare l'Assistenza con la medesima modalità, oppure a usufruire delle funzionalità di Recupero Password messe a disposizione dalla piattaforma BabylonWeb.

GIES non sarà ritenuta responsabile per qualsiasi inconveniente derivato dall'utilizzo non autorizzato delle credenziali di accesso ai servizi SaaS GIES fornite al cliente.

7.2. GESTIONE AUTONOMA DEGLI ACCESSI

Il firmatario dell'affidamento può richiedere al Canale di Assistenza Tecnica l'abilitazione a gestire in autonomia le proprie utenze all'interno della suite BabylonWeb: in tal caso il personale dell'ente sarà formato all'uso della Console Amministratore che consentirà di eseguire la gestione di tutte le utenze in uso al Cliente. Al termine della formazione la gestione delle utenze sarà completamente delegata al cliente. Da questo momento le eventuali richieste in merito alla configurazione delle utenze, dovranno essere rivolte agli addetti dell'ente formati all'uso della Console Amministratore della suite BabylonWeb.

7.3. DELEGA ALLA GESTIONE DEGLI ACCESSI

L'ente può discrezionalmente delegare un soggetto diverso dal firmatario dell'affidamento per l'inoltro delle richieste di gestione degli utenti; per effettuare ciò l'ente può scegliere di procedere secondo una delle seguenti modalità:

1. Ogni richiesta che pervenga dal delegato deve riportare esplicito riferimento alla delega e il firmatario dell'affidamento deve essere inserito in copia conoscenza (CC).

2. L'ente può richiedere a GIES il *"modello standard di delega delle responsabilità e dei ruoli"* che sarà utilizzato come documentazione di dettaglio per la corretta gestione dei permessi e dei ruoli concessi ai referenti dell'ente nei confronti di GIES. Tale documento è da intendersi come una comunicazione ufficiale che incarica il personale dell'ente delle responsabilità indicate nel presente documento; tramite questa comunicazione sarà possibile identificare le eventuali figure sostitute del referente firmatario dell'affidamento e quanti altri per competenza.

Quanto viene indicato nei paragrafi successivi al presente fa riferimento alle modalità in uso qualora l'ente non abbia adottato:

- *Una gestione autonoma degli accessi, di cui al paragrafo 7.2. GESTIONE AUTONOMA DEGLI ACCESSI; in tal caso si rimanda alle politiche di gestione che l'ente ha deciso di adottare.*

- *Delega alla gestione degli accessi, di cui al presente paragrafo; in tal caso il soggetto al quale si fa riferimento sarà il delegato indicato secondo le modalità sopra indicate.*

7

7.4. CANCELLAZIONE A SEGUITO DI CESSAZIONE CONTRATTUALE

Alla cessazione del contratto, GIES provvede tempestivamente alla disattivazione degli account SaaS utilizzati dal Cliente.

7.5. BLOCCO E SOSPENSIONE CREDENZIALI

GIES provvede al blocco delle credenziali di accesso alla piattaforma di un utente, con le modalità di seguito descritte:

1. Il blocco può essere richiesto dal titolare delle credenziali, dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore, al fine di impedire l'accesso alla piattaforma da parte dell'utente;
2. Il blocco può inoltre avvenire automaticamente, a seguito di ripetuti tentativi di accesso alla piattaforma falliti dall'utente;
3. Il blocco riguarda sia l'accesso alla piattaforma, sia l'uso di API autenticate di interscambio dati;
4. Il blocco è da intendersi permanente fino a contraria comunicazione da parte dell'Ente.

GIES provvede alla sospensione delle credenziali di accesso secondo le modalità di seguito descritte:

1. Le richieste di sospensione devono essere inviate via email indicando la data di fine sospensione e avranno effetto dal momento dell'avvenuta evasione della richiesta fino alla data indicata;
2. La sospensione può essere richiesta dal titolare delle credenziali, dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore;
3. La sospensione può inoltre avvenire automaticamente, a seguito di aggiornamenti del quadro amministrativo di gestione;
4. Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

Le richieste di sblocco e di riattivazione delle credenziali devono pervenire nelle modalità di seguito descritte:

1. Nel caso in cui il blocco o la sospensione delle credenziali sia stato richiesto dall'utente stesso, potrà essere lo stesso utente titolare delle credenziali a richiederne lo sblocco o la riattivazione;
2. Nel caso in cui il blocco o la sospensione delle credenziali sia stato richiesto dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore, lo sblocco o la riattivazione potranno essere richieste esclusivamente da tali figure.
3. Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

Tutte le richieste descritte nella sezione devono pervenire esclusivamente via email al Canale di Assistenza Tecnica.

7.6. GESTIONE DEI PERMESSI DEGLI UTENTI

GIES provvede alla gestione delle richieste di aggiunta o rimozione dei permessi assegnati agli utenti della piattaforma, al fine di garantire la tracciabilità e la sicurezza delle attività svolte all'interno del servizio SaaS, secondo le modalità di seguito descritte:

1. Le richieste di aggiunta o rimozione dei permessi devono essere inviate via email al Canale di Assistenza Tecnica;

2. Il firmatario dell'affidamento deve fornire a GIES l'elenco degli utenti interessati, specificando per ciascuno il ruolo, le operazioni consentite e i moduli o menu da abilitare o disabilitare.

3. Eventuali richieste di aggiunta di permessi provenienti da soggetti diversi dal firmatario dell'affidamento saranno prese in considerazione solo se avanzate da figure di ruolo gerarchico superiore.

4. La richiesta di rimozione dei permessi di un utente può essere presentata dall'utente stesso, dal firmatario dell'affidamento o da un suo superiore.

Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

7.7. POLITICHE DI DISMISSIONE

Il processo di disattivazione parziale o totale del servizio viene deciso da GIES a seconda dei termini contrattuali; decorsi 90gg dal termine contrattuale o a seguito di esplicita richiesta del Cliente, GIES procederà con la disattivazione del servizio.

Alla cessazione del contratto, il fornitore si impegna a garantire la disponibilità dei dati del Cliente per un periodo di almeno 90 giorni al fine di consentire una transizione agevole.

I dati vengono eliminati definitivamente al termine del periodo di conservazione (90gg), in conformità con le linee guida di ISO/IEC 27001:2022.

7

7.8. CESSAZIONE DEL SERVIZIO

Le politiche di cessazione rispettano le best practices descritte in ISO/IEC 27001:2022 per la sicurezza delle informazioni e la continuità operativa, assicurando un processo di transizione sicuro e trasparente.

MODALITÀ DI GESTIONE DEGLI ACCESSI E CESSAZIONE DEL SERVIZIO PER L'APPLICATIVO ROSS 1000

8

GIES si impegna a fornire le modalità di attivazione e cessazione del servizio adottando politiche di dismissione e di portabilità dei dati, osservando le best practices previste dalle vigenti norme AGID e ACN.
Il processo di attivazione decorre dalla sottoscrizione contrattuale e prevede l'attivazione entro 7 giorni dell'istanza applicativa, l'abilitazione dei servizi acquisiti e la trasmissione delle credenziali temporanee di primo accesso unicamente agli utenti indicati, secondo le modalità previste nei paragrafi che seguono.

8.1. REGISTRAZIONE E CANCELLAZIONE

Il servizio è accessibile esclusivamente tramite autenticazione. L'autenticazione può essere o standard (username e password) e/o tramite autenticazione SPID.

Le credenziali di primo accesso possono essere relative a diversi ruoli e profilazioni. I profili sono generalmente due: "supervisore" (il più alto dal punto di vista gerarchico) e il profilo "struttura". In fase iniziale, prima di opportuna formazione, possono essere creati utenti supervisori da GIES, le cui credenziali vengono consegnate tramite canale sicuro al referente del Cliente, successivamente alla sottoscrizione del contratto, previa richiesta da parte dell'ente.
La creazione delle credenziali di primo accesso avverrà successivamente alla sottoscrizione del contratto con GIES, seguendo queste modalità:

1. Le richieste di attivazione di nuove credenziali devono essere inviate via email al Canale di Assistenza Tecnica;
2. Il firmatario dell'affidamento si occuperà di fornire a GIES la lista degli utenti, il loro indirizzo email, nome e cognome, ruolo e permessi dei moduli in uso all'Ente;
3. Eventuali richieste di creazione di nuovi utenti, provenienti da soggetti diversi dal firmatario dell'affidamento, saranno prese in considerazione solo se avanzate da figure di ruolo gerarchico superiore rispetto a quello del firmatario dell'affidamento.

GIES si impegna a processare le richieste di nuovi accessi ai servizi SaaS secondo le tempistiche definite nella "*Tabella 1 – SLA Assistenza*" successivamente esplicata.

Qualora ci fosse la necessità di visionare una versione di prova (demo) dell'applicativo SaaS prima della sottoscrizione del contratto, saranno create credenziali esclusivamente dedicate a questo scopo su un'ambiente dedicato, previa apposita richiesta da parte dell'ente.

È compito del Cliente prendere in carico le credenziali di primo accesso e procedere immediatamente con la variazione della relativa password.

È dovere del Cliente attuare tutte le buone norme sulla conservazione in sicurezza delle credenziali di accesso ai servizi SaaS GIES.

Qualora si avesse il sospetto della compromissione delle credenziali di accesso, il Cliente è tenuto a eseguire tempestivamente la variazione della password in autonomia o aprendo una richiesta di supporto che dovrà pervenire esclusivamente al Canale di Assistenza Tecnica.

8.2. GESTIONE AUTONOMA DEGLI ACCESSI

A seguito di opportuna formazione la gestione delle utenze sarà completamente delegata al cliente.
Da questo momento le eventuali richieste in merito alla configurazione delle utenze, dovranno essere rivolte agli addetti dell'ente formati all'uso della relativa console di ROSS 1000.

8.3. DELEGA ALLA GESTIONE DEGLI ACCESSI

L'ente può discrezionalmente delegare un soggetto diverso dal firmatario dell'affidamento per l'inoltro delle richieste di gestione degli utenti; per effettuare ciò l'ente può scegliere di procedere secondo una delle seguenti modalità:

1. Ogni richiesta che pervenga dal delegato deve riportare esplicito riferimento alla delega e il firmatario dell'affidamento deve essere inserito in copia conoscenza (CC).

2. L'ente può richiedere a GIES il "*modello standard di delega delle responsabilità e dei ruoli*" che sarà utilizzato come documentazione di dettaglio per la corretta gestione dei permessi e dei ruoli concessi ai referenti dell'ente nei confronti di GIES. Tale documento è da intendersi come una comunicazione ufficiale che incarica il personale dell'ente delle responsabilità nel presente documento indicate; tramite questa comunicazione sarà possibile identificare le eventuali figure sostitute del referente firmatario dell'affidamento e quanti altri per competenza.

Quanto viene indicato nei paragrafi successivi al presente fa riferimento alle modalità in uso qualora l'ente non abbia adottato:

- *Una gestione autonoma degli accessi, di cui al presente paragrafo.*
  In tal caso si rimanda alle politiche di gestione che l'ente ha deciso di adottare.

- *Delega alla gestione degli accessi, di cui al presente paragrafo 8.3 DELEGA ALLA GESTIONE DEGLI ACCESSI.*
  In tal caso il soggetto al quale si fa riferimento sarà il delegato indicato secondo le modalità sotto indicate.

Qualora l'utente non ricordi lo username di accesso è tenuto a contattare l'Assistenza con la medesima modalità, oppure a usufruire delle funzionalità di Recupero Password messe a disposizione dalla piattaforma ROSS 1000.

GIES non sarà tenuta responsabile per qualsiasi inconveniente derivato dall'utilizzo non autorizzato delle credenziali di accesso ai servizi SaaS GIES fornite al cliente.

8.4. CANCELLAZIONE A SEGUITO DI CESSAZIONE CONTRATTUALE

Alla cessazione del contratto GIES provvede alla disattivazione degli account SaaS utilizzati dal Cliente.

8.5. BLOCCO E SOSPENSIONE CREDENZIALI

GIES provvede al blocco delle credenziali di accesso alla piattaforma di un utente, con le modalità di seguito descritte:

- Il blocco può essere richiesto dal titolare delle credenziali, firmatario dell'affidamento o da una figura di ruolo gerarchico superiore al firmatario dell'affidamento, al fine di impedire l'accesso alla piattaforma da parte dell'utente;
- Il blocco può inoltre avvenire automaticamente, a seguito di ripetuti tentativi di accesso alla piattaforma falliti dall'utente;
- l blocco riguarda sia l'accesso alla piattaforma, sia l'uso di API autenticate di interscambio dati.
- Il blocco è da intendersi permanente fino a contraria comunicazione da parte dell'Ente.

Le richieste di sblocco delle credenziali devono pervenire nelle modalità di seguito descritte:

- Nel caso in cui il blocco delle credenziali sia stato richiesto dall'utente stesso, potrà essere lo stesso utente titolare delle credenziali a richiederne lo sblocco;
- Nel caso in cui il blocco delle credenziali sia stato richiesto dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore, lo sblocco potrà essere richiesto esclusivamente da una di tali figure.
- Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

GIES provvede alla limitazione delle credenziali di accesso secondo le modalità di seguito descritte:

- Le richieste di limitazione devono essere inviate via email indicando la data di fine attività;
- La limitazione può essere richiesta dal titolare delle credenziali, dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore;
- La limitazione può inoltre avvenire automaticamente, a seguito di aggiornamenti del quadro amministrativo di gestione;
- Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

Le richieste di riattivazione delle credenziali devono essere trasmesse nelle modalità di seguito descritte:

- Nel caso in cui la limitazione sia stata richiesta dall'utente titolare delle credenziali, potrà essere lo stesso utente a richiederne la riattivazione;
- Nel caso in cui la limitazione delle credenziali sia stata richiesta dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore, la riattivazione potrà essere richiesta esclusivamente da tali figure.

Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

Tutte le richieste descritte nella sezione devono pervenire esclusivamente via email all'indirizzo dell'Assistenza del Turismo **giesturismo@gies.sm**

8.6. GESTIONE DEI PERMESSI DEGLI UTENTI

GIES provvede alla gestione delle richieste di aggiunta o rimozione dei permessi assegnati agli utenti della piattaforma, al fine di garantire la tracciabilità e la sicurezza delle attività svolte all'interno del servizio SaaS, secondo le modalità di seguito descritte:

- Le richieste di aggiunta o rimozione dei permessi possono essere avanzate esclusivamente dal firmatario dell'affidamento del servizio o da una figura di ruolo gerarchico superiore e devono essere inviate via email all'indirizzo dell'Assistenza del Turismo: **giesturismo@gies.sm**

8

- Il firmatario dell'affidamento deve fornire a GIES l'elenco degli utenti interessati, specificando per ciascuno il ruolo, le operazioni consentite e i moduli o menu da abilitare o disabilitare.
- Eventuali richieste di aggiunta di permessi provenienti da soggetti diversi dal firmatario dell'affidamento saranno prese in considerazione solo se avanzate da figure di ruolo gerarchico superiore.
- La richiesta di rimozione dei permessi di un utente può essere presentata dal firmatario dell'affidamento o da un suo superiore.
- Le richieste provenienti da soggetti diversi da quelli sopra indicati saranno ritenute non autorizzate e pertanto respinte.

8.7. POLITICHE DI DISMISSIONE

Il processo di disattivazione parziale o totale del servizio viene deciso da GIES a seconda dei termini contrattuali; decorsi 90 gg dal termine contrattuale o a seguito di esplicita richiesta del Cliente, GIES procederà con la disattivazione del servizio.
Alla cessazione del contratto, il fornitore si impegna a garantire la disponibilità dei dati del Cliente per un periodo di almeno 90 giorni al fine di consentire una transizione agevole.
I dati vengono eliminati definitivamente al termine del periodo di conservazione (90gg), in conformità con le linee guida di ISO/IEC 27001:2022.

8.8. CESSAZIONE DEL SERVIZIO

Le politiche di cessazione rispettano le best practices descritte in ISO/IEC 27001:2022 per la sicurezza delle informazioni e la continuità operativa, assicurando un processo di transizione sicuro e trasparente.

PORTABILITÀ DEI DATI

9

Il Cliente ha il diritto di richiedere una copia completa dei propri dati in un formato standard e interoperabile, garantendo la facilità di migrazione verso altri fornitori.
Per questo genere di richieste è necessario che da parte del firmatario dell'affidamento o da una figura di ruolo gerarchico superiore a esso, pervenga richiesta scritta via email al Canale di Assistenza Tecnica.
Il processo e le politiche di portabilità rispettano le best practices di ISO/IEC 27001:2022.
Al termine del contratto tra GIES e il Cliente, quest'ultimo riceverà copia completa dei dati a chiusura del servizio, in formati concordati con il Cliente (es. CSV, MDB, SQL Server, ecc..).

9.1. ESPORTAZIONE DEI DATI

GIES mette a disposizione degli utenti abilitati dell'Ente diverse modalità di esportazione dei dati.

Le modalità di esportazione disponibili sono le seguenti e sono descritte in dettaglio nelle sezioni successive:

1. Esportazioni autonome dell'utente
   L'utente può esportare in autonomia i dati visualizzati nelle griglie della piattaforma in vari formati;

2. Esportazione tramite query
   Comprendono query e business intelligence creabili dall'utente, o modelli predisposti da GIES al fine di consentire all'utente l'esportazione dei dati desiderati;

3. Esportazioni specifiche richieste a GIES
   Comprendono query o query parametrizzate predisposte da GIES su richiesta dell'Ente, al fine di consentire l'esportazione di dati formattati secondo esigenze specifiche;

4. Esportazione dell'intera banca dati dell'Ente
   Può essere effettuata da GIES su richiesta dell'Ente, secondo le modalità indicate nella sezione "*9.1.3. ESPORTAZIONE INTERA BANCA DATI*". Tutte le esportazioni vengono eseguite nel rispetto delle policy di sicurezza e riservatezza dei dati previste da ACN.

9.1.1. ESPORTAZIONE AUTONOMA DEI DATI

La procedura mette a disposizione dell'utente strumenti per l'esportazione autonoma dei dati. È inoltre possibile richiedere l'esportazione dei dati tramite API, in conformità ai requisiti ACN.

Ogni operazione di esportazione è associata all'utenza che l'ha eseguita, allo scopo di tenere traccia delle azioni eseguite dagli utenti.

9.1.2. ESPORTAZIONE DEI DATI SECONDO SPECIFICHE RICHIESTE

Qualora l'Ente necessiti di esportare dati non ottenibili tramite gli strumenti sopra descritti, può richiedere a GIES la realizzazione di tracciati specifici inviando una richiesta via email al Canale di Assistenza Tecnica.

Le richieste dovranno essere inviate dal firmatario dell'affidamento o da una figura di ruolo gerarchico superiore.

L'ente può discrezionalmente delegare un soggetto diverso dal firmatario dell'affidamento: in tal caso ogni richiesta che pervenga dal delegato deve riportare esplicito riferimento alla delega e il firmatario dell'affidamento deve essere inserito in copia conoscenza (CC).

Le richieste prive di tale requisito non saranno considerate autorizzate e pertanto saranno respinte.

A seguito della ricezione della richiesta, GIES valuterà la fattibilità fornendo riscontri all'Ente su tempi e metodi di realizzazione.

9.1.3. ESPORTAZIONE INTERA BANCA DATI

L'Ente che ha in essere rapporti contrattuali con GIES in corso di validità, che prevedono l'erogazione o l'utilizzo del servizio SaaS, può richiedere l'esportazione dell'intera banca dati: per procedere in tal senso è necessario che da parte del firmatario dell'affidamento o da una figura di ruolo gerarchico superiore, pervenga richiesta scritta all'indirizzo del Canale di Assistenza Tecnica.

L'ente può discrezionalmente delegare un soggetto diverso dal firmatario dell'affidamento: in tal caso ogni richiesta che pervenga dal delegato deve riportare esplicito riferimento alla delega e il firmatario dell'affidamento deve essere inserito in copia conoscenza (CC).

Le richieste provenienti da soggetti diversi non saranno considerate autorizzate e pertanto saranno respinte.
Il database contenente l'intera banca dati sarà consegnato all'Ente in un file compresso e protetto, la cui password sarà inviata tramite email al richiedente e il file sarà reso accessibile mediante opportuna piattaforma di trasferimento, tramite apposito link di download inviato in risposta alla richiesta.

Il file così condiviso sarà disponibile per il download per un periodo massimo di 3 giorni lavorativi dal momento della comunicazione di avvenuta condivisione; qualora i dati non vengano scaricati entro tali termini, l'Ente dovrà procedere nuovamente a richiedere l'esportazione.
GIES conserverà una copia dei dati trasmessi all'Ente fino a 30 giorni dalla data di trasmissione.

Non saranno forniti altri formati o utilizzati altri canali rispetto agli standard in uso a GIES. Le modalità di conservazione dei dati applicate da GIES saranno le medesime previste dalle vigenti norme ACN.

9.1.4. ADOZIONE DI STANDARD APERTI

Allo scopo di consentire la migrazione da un altro Fornitore SaaS o servizio SaaS, GIES garantisce al Cliente la possibilità di importare i dati all'interno del servizio SaaS tramite formati pubblici e aperti.
GIES si rende disponibile alla condivisione della documentazione su apposita richiesta del Cliente, fornendo manuali di gestione delle interfacce API.

TRATTAMENTO DEI DATI PERSONALI

10

GIES può trattare PII al fine unico di eseguire il lavoro concordato con il Cliente in sede contrattuale. GIES è responsabile delle PII che risiedono sui propri servizi SaaS, e sarà sua responsabilità e garantisce la loro protezione, integrità e disponibilità.
GIES assicura che tutti coloro che operano nell'ambito dell'erogazione dei servizi siano adeguatamente formati al rispetto delle norme GDPR.
Sono inoltre pianificati programmi periodici di formazione e verifica interna del personale.

10.1. PROTEZIONE DEI DATI PERSONALI

La protezione delle PII raccolte dal sistema avviene con criptazione dell'archivio dati, secondo le indicazioni sullo sviluppo sicuro di AGID.
Nell'ambito del servizio di assistenza, GIES si impegna a non divulgare a terzi PII senza l'esplicito consenso del Cliente, salvo nei casi in cui la comunicazione sia richiesta dalla legge o da un'autorità competente.
L'utilizzo di PII in ambito di test e demo degli applicativi è vincolato alla stretta osservanza di regole al fine di evitare la divulgazione involontaria delle PII.
I dati contenenti PII utilizzati nell'ambito di test vengono storicizzati in location sicura e segregata oppure eliminati appena terminata l'esigenza della loro conservazione o allo scadere del contratto con il titolare del trattamento.
Il servizio si impegna a garantire la protezione dei dati personali attraverso:

1. Crittografia dei dati a riposo e in transito;
2. Controlli di accesso basati sui ruoli (RBAC) per limitare l'accesso alle informazioni sensibili;
3. Valutazioni di impatto sulla protezione dei dati (DPIA), in conformità con l'articolo 35 del GDPR, per identificare e mitigare rischi associati al trattamento dei dati;
4. Osservanza dei principi di Privacy By Design & By Default per adottare tutte le misure più adeguate al contesto *ex ante* ed *ex post* il trattamento.

10.2. COMPLIANCE CON GDPR E ISO/IEC 27001:2022

Il servizio garantisce:

1. Procedure trasparenti per la gestione dei diritti degli interessati (accesso, rettifica, cancellazione, portabilità);
2. Processi di audit periodici per garantire il rispetto delle normative;
3. Trattamento dei dati personali in accordo con principi di minimizzazione e proporzionalità.

Nel caso di richieste fatte nell'ambito di procedimenti giudiziari, GIES si impegna a darne tempestiva informazione al Cliente ove ciò non sia precluso da disposizioni normative o da provvedimenti dell'autorità.

METODO DI EROGAZIONE DEL SERVIZIO DI ASSISTENZA

11

GIES adotta un modello di assistenza centralizzato, che garantisce la gestione unificata delle richieste di supporto del Cliente e il monitoraggio continuo delle performance del servizio. Per effettuare una segnalazione, il Cliente dovrà contattare l'Assistenza GIES attraverso uno dei canali ufficiali indicati nella sezione apposita denominata "*13.1 CONTATTI ASSISTENZA*". Qualora la richiesta venga inviata via email, è consigliato indicare un oggetto e una descrizione coerente con la problematica riscontrata, al fine di velocizzare le operazioni di identificazione e risoluzione del problema.

Ogni richiesta ricevuta viene tracciata tramite l'assegnazione di un codice identificativo, che sarà inviato in risposta all'indirizzo email di colui che ha contattato l'Assistenza. Il codice identificativo consente al Cliente di interagire con l'Assistenza e di ricevere da essa eventuali riscontri in merito alla segnalazione. L'analisi e l'evoluzione della problematica saranno discusse tramite email e tutte le interazioni saranno tracciate tramite il codice identificativo; allo scopo di ciò è fondamentale che ogni risposta ricevuta dal Cliente sia pervenuta all'Assistenza in risposta all'email che ha aperto la segnalazione o successive.

Dopo aver ricevuto la richiesta l'Assistenza GIES avvia una fase di analisi preliminare volta a identificare la natura del problema, verificando la completezza e la chiarezza delle informazioni fornite dal Cliente e richiedendo se necessari ulteriori approfondimenti: se la problematica risulta chiara, l'addetto dell'Assistenza assegnerà al tecnico competente la richiesta e a partire da quel momento decorrerà il tempo di risposta previsto dalle SLA.

L'addetto che si occuperà della richiesta fornirà risposta alla stessa e attenderà eventuale risposta da parte del Cliente entro 72 ore. Trascorso questo termine, la segnalazione verrà considerata chiusa con causale "**mancata risposta da parte del Cliente**". Qualora il tecnico incaricato ritenga siano necessarie ulteriori informazioni o chiarimenti contatterà il Cliente e, in questo caso, il conteggio del tempo di risposta previsto dalle SLA sarà sospeso fino al ricevimento delle informazioni richieste, per poi riprendere al momento della ricevuta risposta da parte del Cliente.

Individuate le cause del problema l'Assistenza procederà con le fasi di risoluzione che possono essere di varia tipologia:

1. Risoluzione tramite correzione sul dato.
   È possibile un intervento sui dati, in modo che possa essere ripristinato il corretto funzionamento del sistema e la ripresa delle attività da parte del Cliente, agendo sulle informazioni imputate senza necessità di intervento sulle logiche del software;
2. Risoluzione tramite correzione immediata del software, fix
   Qualora sia presente un errore sulle logiche di funzionamento del software, gli addetti GIES possono adoperare delle correzioni immediate in modo che tali logiche diano il risultato atteso. Tali correzioni vengono assoggettate a tempi di rilascio di fix correttivi:
3. Risoluzione tramite correzione del software, aggiornamento di versione
   Qualora sia presente una mancanza all'interno delle logiche di funzionamento del software, gli addetti GIES possono provvedere all'integrazione di tali logiche, che andranno a evolvere il sistema stesso generando quindi una nuova versione. Tale versione sarà assoggettata a tempi di rilascio più lunghi.

Nel caso in cui il problema venga risolto attraverso quanto descritto nei punti 1. e 2. di cui sopra, la segnalazione sarà ritenuta risolta e saranno applicati i tempi descritti nel paragrafo "*Livelli di servizio di assistenza*" per la risoluzione della stessa.
Rimane onere del segnalatore l'eventuale ripresa della segnalazione qualora la problematica risulti non essere completamente risolta, o si ripresentasse nuovamente in un altro scenario. GIES offre la possibilità ai propri Clienti di visualizzare una dashboard dedicata contenente informazioni e statistiche su ticket aperti e chiusi. Per accedere a tale dashboard è necessario fare richiesta all'Assistenza.

LIVELLI DI SERVIZIO DI ASSISTENZA

12

I Livelli di Servizio (SLA) adottati da GIES sono i seguenti:

1. SLA di disponibilità del Servizio. GIES ha definito che gli applicativi SaaS sono disponibili con availability del 99.5 % su base mensile;

2. SLA di rispetto dei tempi di prima risposta, presa in carico e risoluzione delle richieste.

Il servizio di supporto è fornito in lingua italiana e inglese dalle ore 08:00 alle ore 18:00 dal lunedì al venerdì.

GIES si impegna a dare una prima risposta, a prendere in carico e a risolvere le segnalazioni dei Clienti, dal lunedì al venerdì, dalle 09:00 alle 13:00 e dalle 14:30 alle 17:30, esclusi i festivi italiani, secondo le tempistiche definite nella "*Tabella 1 - SLA Assistenza*", espresse in ore lavorative e definite in base alla natura del problema e alla tipologia di intervento richiesto; le tipologie di richiesta sono così distinte:

1. RDA – Richiesta di Assistenza;

2. GUS – Richiesta di Gestione Utenti Software;

3. RED – Richiesta Export Dati.

Tipologia	Descrizione	Classificazione risoluzione	Priorità	Tempo di risposta massimo (h)	Tempo di presa in carico massimo (h)	Tempo di risoluzione massimo (h)
RDA	Intero sistema indisponibile	Ripristino del sistema	Urgente	1	1	2
RDA	Funzionalità critiche indisponibili, con immediato impatto sull'operatività degli utenti	Correzione immediata del software	Alta	4	7	37
RDA	Funzionalità non critiche indisponibili, senza immediato impatto sull'operatività degli utenti	Correzione sul dato	Normale	7	15	150
		Correzione in nuova versione	Bassa	21	42	300
RDA	Richiesta di assistenza generica o chiarimenti	Invio di informazioni o risposte	Bassa	21	42	300
GUS	Richiesta di registrazione e cancellazione nuovi utenti	Registrazione e cancellazione utenti	Urgente	7	-	52
			Bassa	14	-	104
GUS	Richiesta di blocco o sospensione di utenti	Blocco o sospensione degli utenti	Urgente	7	-	52
			Bassa	14	-	104
GUS	Richiesta di gestione dei permessi degli utenti	Gestione dei permessi degli utenti	Urgente	7	-	52
			Bassa	14	-	104
RED	Richiesta di esportazione dei dati secondo specifiche richieste	Esportazione dei dati	Urgente	7	-	52
			Bassa	14	-	104
RED	Richiesta di esportazione dell'intera banca dati	Esportazione dell'intera banca dati	Urgente	7	-	52
			Bassa	14	-	104

Tabella 1 - SLA Assistenza

Si precisa che i tempi di risoluzione decorrono dal momento in cui la problematica viene identificata.

Per le richieste di tipologia GUS e RED, il livello di priorità sarà indicato dall'Agente dell'Assistenza incaricato della risoluzione della richiesta.

Per le specifiche richieste riguardo ai tempi SLA si rimanda ai singoli contratti in essere con il Cliente.

GIES adotta questi specifici SLA con l'obiettivo di misurare il livello di qualità del Servizio offerto.

Tali livelli sono definiti attraverso KPI oggettivi e misurabili, che rappresentano i parametri di riferimento per la valutazione delle prestazioni del Servizio.

Per assicurare il costante rispetto dei KPI associati agli SLA, le misurazioni vengono effettuate e monitorate in modo continuativo tramite strumenti e software dedicati; in nessun caso saranno prese in considerazione misurazioni dei KPI effettuate per mezzo di strumenti diversi dai sistemi predisposti da GIES.

Si precisa inoltre che, nell'ambito dei KPI, non vengono conteggiati i periodi di indisponibilità del Servizio dovuti a interventi di manutenzione programmata da GIES.

Il Cliente, al fine di verificare il rispetto degli SLA da parte di GIES, può richiedere un report riepilogativo dettagliato contenente i dati relativi al monitoraggio dei KPI di proprio interesse.

La richiesta dovrà pervenire inviando un'email al Canale di Assistenza Tecnica.
GIES si impegna a inviare il report entro 10 giorni lavorativi dal momento della ricezione della richiesta.

A decorrere dalla data di trasmissione del report, il Cliente dispone di 10 giorni di tempo per comunicare a GIES eventuali contestazioni in merito al mancato rispetto dei livelli di servizio SLA, utilizzando il medesimo canale attraverso il quale il report è stato trasmesso.

Alla ricezione della notifica di presunto disservizio, al fine di valutare la fondatezza della contestazione, GIES avvierà una verifica interna grazie all'analisi dei dati in proprio possesso.

12

Al termine dell'attività di verifica, GIES comunicherà al Cliente l'esito di quest'ultima e conseguentemente l'accoglimento o il rigetto della contestazione presentata.

REFERENTI E CONTATTI

13

13.1. CONTATTI ASSISTENZA

Per problematiche inerenti a errori sul software, incidenti sulla sicurezza sui servizi SaaS erogati da GIES, richieste inerenti la gestione delle utenze e degli accessi sui servizi SaaS erogati da GIES, è possibile contattare l'Assistenza inviando una email ai seguenti indirizzi:

1. Per BabylonWeb: **assistenza@gies.sm**
2. Per il ROSS 1000: **giesturismo@gies.sm**

13.2. ALTRI CONTATTI

Per informazioni sul trattamento dei dati:

1. Inviare una email all'indirizzo **privacy@gies.sm**
2. Chiamare al numero di telefono **+39 0549 999 497**

Per segnalare presunta violazione della altrui proprietà intellettuale inviare una email all'indirizzo **documenti@gies.sm**

Per richieste relative ad audit o riesami relativi alla sicurezza delle informazioni, inviare una email all'indirizzo **sistemi@gies.sm**

Ai sensi del Regolamento UE 2016/679 (GDPR), GIES ha nominato come DPO: ICTLC S.p.A. contattabile ai seguenti recapiti:

1. Telefono: **+ 39 0284 247 194**
2. E-mail: **DPO-outsourcing@ictlc.com**
3. PEC: **ictlc@pec.it**

La presente informativa e tutte le policy relative alla sicurezza delle informazioni sono conservate da GIES per un periodo minimo di 5 anni.


gies