



Scheda tecnica del servizio SicraWEB EVO

su Google Cloud Platform

Indice

Sommario

1) Cluster Kubernetes Autopilot Google - posizionamento e ridondanza	3
2) Database - posizionamento e ridondanza	3
3) Storage repository dati - posizionamento e ridondanza	3
4) Documento Google di compliance al GDPR	3
5) Qualificazione SicraWEB EVO ACN	4
6) Monitoraggio Uptime	4
7) Disponibilità ambiente di test	4
8) Qualificazione dei servizi del CSP Google	4
9) Crittografia	6
10) Geolocalizzazione IP pubblico 34.149.78.52	7
11) VPN e accesso diretto ai dati per integrazioni o scambio dati con altri software/sistemi	7
12) Requisiti minimi richiesti di banda in upload/download	7
13) SLA: Uptime, RPO/RTO (Policy backup	8
14) Assistenza	8

Di seguito le informazioni tecniche relative all'erogazione del servizio SicraWEB EVO su infrastruttura Google Cloud Platform

Fornitore: Google Cloud Italy S.r.l.

Data inizio validità: 05/02/2025

Data fine validità: 04/02/2028

1) Cluster Kubernetes Autopilot Google - posizionamento e ridondanza

Modalità: Autopilot

Tipo di località: Singola region

Regione: Milano (europe-west8)

Zone nodo predefinite: europe-west8-a, europe-west8-b, Europe-west8-c

Security: La sicurezza è gestita da Google, vedi informazioni sulla sicurezza al link

<https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview?hl=it>

2) Database - posizionamento e ridondanza

Versione Istanza: CloudSQL Enterprise

Regione: Milano (europe-west8)

Disponibilità: elevata su più zone (HA)

Primaria: europe-west8-b

Secondaria: una disponibile diversa dalla primaria (europe-west8-a, europe-west8-c)

3) Storage repository dati - posizionamento e ridondanza

Tipologia: Bucket Standard, Dual Region

Regioni: primaria Milano (europe-west8), secondaria Francoforte (europe-west3)

Numero versioni per file: 3

4) Documento Google di compliance al GDPR

Google Cloud e il Regolamento generale sulla protezione dei dati (GDPR)

<https://cloud.google.com/privacy/gdpr?hl=it>

Riservatezza dei dati del cliente garantita con Google Cloud

https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf?hl=it

Google si impegna a rispettare le leggi vigenti in materia di protezione dei dati

<https://business.safety.google/intl/it/compliance/>

ISO 27018 (Privacy nel cloud)

scaricabile link seguente

<https://cloud.google.com/security/compliance/compliance-reports-manager#/ReportType=Certificate>

5) Qualificazione SicraWEB EVO ACN

Sicraweb EVO ha un livello di qualificazione QC1: <https://www.acn.gov.it/portale/w/sa-3836>

6) Monitoraggio Uptime

E' disponibile una dashboard per consentire al cliente il monitoraggio dell'uptime in base ai livelli di servizio ACN.

7) Disponibilità ambiente di test

E' disponibile un servizio aggiuntivo per l'attivazione di uno o più ambienti di test dedicati al cliente.

8) Qualificazione dei servizi del CSP Google

I servizi Google sono individuabili nel catalogo cloud di acn.gov.it al seguente indirizzo:

<https://catalogocloud.acn.gov.it>

Segue elenco servizi Google certificati da ACN

1) Infrastruttura dei servizi cloud: <https://www.acn.gov.it/portale/w/in-271>

2) Servizi Cloud qualificati di tipo Infrastructure as a Service.

IA-4058;Google Cloud VMware engine - GCVE;IaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si

IA-3956;Backup & DR;IaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si

IA-356;Cloud VPN;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-3822;VPC Service Controls;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-295;Persistent Disk;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-5335;Cloud Load Balancing;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-2521;Cloud HSM;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-293;Compute Engine;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-2319;Cloud External Key Manager;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-357;Cloud Interconnect;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-3821;Cloud Router;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-366;Cloud NAT;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-294;Cloud Storage;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-367;Cloud Key Management Service;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

IA-358;Cloud DNS;IaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

3) Servizi Cloud qualificati di tipo Platform as a Service.

PA-3962;Cloud Speech-to-Text;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4065;Vertex AI Gemini API;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4063;Service Directory;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4070;Vertex AI Platform;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3958;Cloud Firestore;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3957;Certificate Authority Service;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4055;Dialogflow;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4067;Sensitive Data Protection - precedentemente chiamato Cloud Data Loss Prevention;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4069;Vertex AI Search e Conversation - Vertex AI agent Builder;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3954;Access context Manager;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3961;Cloud Run;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3953;Access Approval;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3955;Apigee;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4060;Organization Policy Service;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4062;Resource Manager API;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4068;Vertex AI Imagen - AI Image Generator;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4064;Traffic Director/Cloud Service Mesh;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3960;Cloud Monitoring;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3959;Cloud IDS;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-4057;Document AI;PaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 PA-3829;Access Transparency;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-298;DataFlow;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-372;Cloud Spanner;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-3013;Network Connectivity Center;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-283;Google Kubernetes Engine;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-2519;Cloud Composer;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-299;Dataproc;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-3009;Virtual Private Cloud;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-284;Cloud SQL;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-297;BigQuery;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-2514;Artifact Registry;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-3830;Identity-Aware Proxy;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-275;Cloud Bigtable;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-273;Cloud Logging;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 PA-300;Pub/Sub;PaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

4) Servizi Cloud qualificati di tipo Software as a Service.

SA-4044;Cloud Vision API OCR;SaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 SA-4061;reCaptcha enterprise;SaaS;Google Cloud Italy S.r.l.;""QC2"";2024-07-10;2025-07-10;Si
 SA-689;Identity and Access Management;SaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si
 SA-690;Workspace;SaaS;Google Cloud Italy S.r.l.;""QC2"";2025-03-25;2028-03-25;Si

I datacenter utilizzati garantiscono la compliance al principio Do No Significant Harm (DNSH) con ISO 14001

Datacenter Milano (europe-west8)

Certificato depositato e accessibile pubblicamente presso ACCREDIA, l'Ente di Accreditamento Nazionale.

Sul sito Accredia e cercando per Certificato numero IT22/00000664 si trovano la prova del possesso del certificato ISO14001 per i 3 datacenter Google della Region di Milano:

- Santo Stefano Ticino (MI) - Lombardia
- Cassina De' Pecchi (MI) - Lombardia
- Rozzano (MI) - Lombardia

Datacenter Francoforte (europe-west3)

Certificato depositato presso DEKRA Certification GmbH, non pubblicato online ma possiamo fornire il documento di certificazione, a richiesta.

Sul sito datacenters.com nella pagina dedicata al datacenter Francoforte2 è riportata la compliance ISO14001.

Sul sito di CyrusOne nella pagina del datacenter Francoforte2 è possibile scaricare il pdf delle specifiche con indicata la compliance ISO14001.

9) Crittografia

I dati all'interno di Google Cloud sono criptati sia "at rest" che "in transit".

Tutte le componenti coinvolte dall'applicativo SicraWEB EWO sono criptate.

Kubernetes: Traffico HTTPS criptato con certificato

Database: i dati sono criptati con crittografia a 256 bit (AES-256)

Bucket: i bucket sono criptati, non accessibili pubblicamente

Backup: viene creato un bucket criptato, separato da quello di produzione e non accessibile pubblicamente

Tutti i dati a livello di archiviazione vengono criptati tramite DEK, che utilizzano AES-256 per impostazione predefinita. Al seguente link viene fornita documentazione in merito

<https://cloud.google.com/storage/docs/encryption/default-keys?hl=it>

Le chiavi DEK sono a loro volta criptate tramite KEK che utilizzano AES-256. Al seguente link viene fornita documentazione in merito

https://cloud.google.com/docs/security/encryption/default-encryption?hl=it#key_management

La chiavi di crittografia sono gestite da Google.

10) Geolocalizzazione IP pubblico 34.149.78.52

Nazione	Regione	Città
United States of America 	Missouri	Kansas City

Il servizio SicraWEB EVO è basato sul modello “Network Premium” che sfrutta un’ampia rete in fibra di proprietà di Google, gli indirizzi della rete Premium sono annunciati da tutti i PoP Google (Point of Presence) e l’accesso avviene nel punto più vicino all’utente che intende accedere ai servizi. Il fatto che l’indirizzo sia annunciato su tutti i PoP Google (indirizzo di tipo anycast) non rende attendibili gli strumenti che localizzano gli indirizzi IP. In particolare la localizzazione effettuata da tali indirizzi non corrisponde alla localizzazione dei servizi (esempio: localizzazione IP negli USA, ma servizi in Europa). Il traffico dal POP Google arriva al datacenter dove sono ospitati i dati/servizi direttamente attraverso la rete globale a bassa latenza e alta affidabilità di Google, questo metodo di routing riduce al minimo la congestione e massimizza le prestazioni riducendo il numero di hop tra gli utenti finali e i PoP più vicini.

Panoramica di Network Service Tiers:

<https://cloud.google.com/network-tiers/docs/overview?hl=it>

Our Edge Network

<https://peering.google.com/?hl=it#/>

11) VPN e accesso diretto ai dati per integrazioni o scambio dati con altri software/sistemi

Per garantire la sicurezza dei servizi non è consentito l’uso di VPN e accessi diretti ai dati da origini esterne al perimetro SicraWEB EVO su Google Cloud.

Eventuali necessità devono essere analizzate ed implementate mediante l’utilizzo di strumenti adeguati, esempio:

- Interfaccia API
- Servizio aggiuntivo che prevede l’utilizzo di bucket nel quale posizionare database e files che l’ente può scaricare e gestire in autonomia.

Ogni richiesta di integrazione è da valutare con il settore di competenza.

12) Requisiti minimi richiesti di banda in upload/download

- 0.5Mbit/s sincroni per postazione Socr@web
- latenza inferiore a 50ms
- il corretto funzionamento del servizio è garantito solo se eseguito da un browser e un sistema operativo supportati dai rispettivi produttori

13) SLA: Uptime, RPO/RTO (Policy backup)

Maggioli si impegna a garantire il livello di servizio “SL1-Disponibilità del servizio” come da specifica ACN

- UPTIME su base mensile del 99,0%
La mancata disponibilità dei servizi dovuta ad interventi di manutenzione programmata non viene conteggiata come disservizio. La manutenzione programmata riguarda tutte le attività

svolte regolarmente dal Fornitore per mantenere e innovare le infrastrutture tramite le quali viene erogato il Servizio.

- i seguenti valori massimi di RPO/RTO: 12h/48h.
Dove per RPO (Recovery Point Objective) si intende il tempo massimo che intercorre tra l'avvenimento del disastro e l'ultimo salvataggio dei dati che possono essere ripristinati e per RTO (Recovery Time Objective) il tempo massimo che intercorre tra l'avvenimento del disastro e il ripristino dell'operatività di un sistema o di un processo. La retention del backup giornaliero è pari a 7 giorni.

14) Assistenza

Il servizio è operativo nei seguenti orari:

Descrizione	Copertura oraria
Ricevimento richieste di assistenza: <ul style="list-style-type: none"> ● Telefono 0541.628.380 ● Portale Web https://assistenza.maggioli.it 	Lunedì – Venerdì: 08:30 -17:30 Sabato: 08:30-12:30 (Festivi: esclusi) 24h x 7 tramite il portale web
Esecuzione intervento di assistenza a cura del personale tecnico per assistenza sull'uso delle funzionalità applicative.	Lunedì – Venerdì: 08:30 -17:30; Festivi: esclusi
Esecuzione intervento di assistenza a cura del personale tecnico per segnalazioni sull'erogazione del servizio Saas.	Lunedì – Venerdì: 08:00 - 18:00; Festivi: esclusi

Le richieste di assistenza sono gestite in relazione alla loro criticità secondo le seguenti tempistiche:

Codice priorità	Descrizione	Tempi di presa in carico	Tempi di risoluzione
G1	Incident Anomalia Bloccante (**): L'intero servizio è indisponibile agli utenti.	1 ora lavorative	4 ore lavorative (*)
G2	Incident Anomalia Grave: Malfunzionamento di procedure primarie del sistema che risultano indisponibili o gravemente degradate.	8 ore lavorative (*)	16 ore lavorative (*)
G3	Incident Anomalia Media: Malfunzionamento di procedure secondarie del sistema che risultano indisponibili o parzialmente degradate.	8 ore lavorative (*)	32 ore lavorative (*)
R	Richiesta Assistenza Applicativa	5 giorni lavorativi	

(*) Il rispetto dei livelli di servizio è garantito nel 90% dei casi su base mensile, al netto di eventuali interventi e/o informazioni e/o attività in carico al Cliente.

(**) I malfunzionamenti di tipo bloccante (G1), dovranno essere attivati esclusivamente mediante contatto telefonico all'operatore del servizio, al fine di garantire la massima tempestività nella risoluzione del problema.