DOC. TECNICA AGORÀ

SOGI Scuola S.r.l.

Indice

Introduzione

Agorà è una piattaforma pensata per la didattica a distanza ed usufruibile dalle scuole Italiane. La piattaforma suddivide in varie aree che andremo a definire di seguito:

- **CALENDARIO -** Questa funzione permette al docente di vedere subito il carico domestico, quanto lavoro avrà lo studente e quante ore lo impegneranno.
- Presa la visione, il docente organizza il proprio lavoro, prenota una video lezione.
- **VIDEO LEZIONI -** Il docente invita la/le classi o singoli studenti ad accedere ad una video lezione.
- **COMPITI A DISTANZA -** Il docente assegna alla classe o a singoli alunni dei compiti da svolgere in autonomia. Il docente monitora la lettura o il compimento dell'esercizio.
- **VALUTAZIONI -** La valutazione deve dar la possibilità di raccogliere gli elaborati scritti, le chat con il docente, le video interrogazioni. L'Area "Valutazione" permette una video-interrogazione. Alla valutazione viene archiviato il documento e la discussione fatta con il docente/allievo.
- **CONDIVISIONE -** La funzione permette la condivisione file fra gli utenti della piattaforma.
- **IMPEGNI COLLEGIALI -** Tramite questa funzione possiamo organizzare: Consigli di classe, Riunione di staff, Collegio docenti e molti altre tipologie di riunioni tutte gestite tramite video call.
- **RICEVIMENTI -** I docenti possono organizzare i ricevimenti settimanali e generali con i genitori gestite tramite video call.
- **CHAT INTERNA -** Un sistema di chat interna che permette di dialogare tra gli utenti della piattaforma.
- **QUESTIONARI -** In quest'area possono essere generati questionari e quiz per dedicati agli alunni e al personale della scuola.

Certificazioni

I servizi SaaS Cloud offerti da **SOGI Scuola S.r.l.** (di seguito "SOGI Scuola") sono progettati e gestiti in accordo ai principali standard internazionali e *best practices* tra le quali:

- **ISO/IEC 27001** - Gestione della Sicurezza delle Informazioni
- **ISO/IEC 27017** - Controlli di sicurezza sul servizio cloud
- **ISO/IEC 27018** - Protezione dei dati personali nel cloud pubblico

SOGI Scuola si sottopone volontariamente a verifiche da parte di **Organismi di Certificazione terzi** ed **indipendenti** sulla propria organizzazione del servizio, al fine di fornire garanzie specifiche ed indipendenti.

Infrastruttura

I servizi sono erogati da **due Data Center in hosting**, situato ad Arezzo presso la sede Aruba S.p.A.

I Data Center utilizzati da SOGI Scuola, sono scelti secondo i più moderni standard in termini di affidabilità, prestazioni e sicurezza. Connessi ad Internet con 1 GBit/s, garantiscono una capacità trasmissiva triplo rispetto al fabbisogno effettivo, per assicurare continuità e qualità dei servizi.

Continuità e sicurezza dei Data Center

Il Data Center utilizzato da SOGI Scuola rispetta i **massimi standard di resilienza previsti** ha ottenuto il livello Rating 4 (former Tier IV) secondo la normativa ANSI/TIA 942-B-2017.

La certificazione ottenuta classifica la struttura ai massimi livelli previsti, assicurando **altissimi livelli di affidabilità** delle infrastrutture anche in presenza di gravi guasti grazie a livelli di ridondanza degli impianti che consentono di eseguire operazioni di manutenzione ordinaria senza la necessità di interrompere il servizio erogato.

Il Data Center è attrezzato per sopportare guasti in un qualsiasi punto dell'impianto senza causare downtime dell'infrastruttura oltre a garantire alti livelli di protezione nei confronti degli eventi fisici (come meglio dettagliato nel documento "*Policy di Sicurezza*" disponibile online).

Per conoscere tutte le misure di prevenzione adottate nelle rispettive strutture, protezioni passive, attive ed organizzative, si rimanda al documento dedicato "*Policy di Sicurezza*" aggiornato dall'Area Information Technology anch'esso pubblicato online.

Controlli crittografici

Nei servizi SaaS Cloud, i flussi di dati da/verso i sistemi ed i server esposti su Internet, sono protetti utilizzando un canale sicuro **SSL/HTTPS**, mediante opportuna configurazione sui server, tale da assicurare:

- **Autenticazione del server** (con chiave RSA da 4096 bit);
- **Cifratura della sessione** con un algoritmo di cifratura simmetrica considerato sufficientemente sicuro alla data, e con una chiave di sessione di almeno 256 bit.

Questo vale sia per i flussi originati in modo interattivo (Web browsing) sia quelli generati in modo automatico (per esempio Web services). Come algoritmo di cifratura simmetrica, si utilizza AES 256 bit.

Responsabilità condivisa e proprietà degli asset

SOGI Scuola ha identificato **le attribuzioni di proprietà per quanto riguarda infrastruttura, licenze, indirizzi IP, software forniti, dati e contenuti immessi dal cliente**, suddividendole per servizio/finalità secondo la seguente tabella:

Software Cloud SaaS Agorà	▪ L'infrastruttura è in hosting presso il provider che eroga il servizio (Aruba S.p.A.). ▪ Il software Cloud è di proprietà di SOGI Scuola che concede in licenza d'uso il servizio al cliente per tutta la durata della sua permanenza sulla piattaforma SOGI Scuola, come meglio descritto nelle Condizioni Generali di Contratto sottoscritte dal cliente in fase di acquisto. ▪ L'indirizzo IP del servizio SaaS fornito è di proprietà SOGI Scuola. ▪ Tutto il contenuto a livello di dati, informazioni e documenti forniti e/o condivisi o caricato dal cliente mediante il software SaaS rimangono di proprietà e sotto la responsabilità del cliente.
Assistenza Tecnica Social Customer Care	▪ Tutti gli asset fisici sono di proprietà di SOGI Scuola. ▪ L'attività di assistenza e supporto al cliente viene erogata tramite le seguenti modalità: (i) assistenza telefonica al numero dedicato del servizio SaaS; (ii) FAQ, (iii) Video-tutorial, (iv) webinar e (v) servizio di ticketing diretto per la segnalazione. ▪ Le linee telefoniche ed il centralino utilizzato sono di proprietà di SOGI Scuola. ▪ Gli indirizzi IP e le modalità di erogazione informatiche dell'assistenza sono di proprietà di SOGI Scuola.
Backup	▪ Tutti gli asset fisici sono di proprietà di SOGI Scuola. ▪ La licenza del software di backup compresi gli agenti installati sui server utilizzati dalla clientela è di proprietà di SOGI Scuola e viene garantita al cliente per tutta la durata della sua permanenza sulla piattaforma SOGI Scuola fino alla scadenza del Contratto con esso sottoscritto. ▪ Anche i dati, le informazioni e i documenti forniti e/o condivisi o caricati dal cliente mediante i software SaaS sono sottoposti a backup da parte di SOGI Scuola, sono quindi sotto la sua responsabilità e viene garantito al cliente per tutta la durata della sua permanenza sulla piattaforma SOGI Scuola fino alla scadenza del Contratto sottoscritto.
Cloud Monitoring	▪ Gli asset eroganti il servizio di monitoraggio sono di proprietà di SOGI Scuola. ▪ Le licenze dei software di monitoraggio dell'infrastruttura sono di proprietà SOGI Scuola. ▪ I dati, le informazioni e i documenti forniti e/o condivisi, memorizzati e visualizzati mediante il software SaaS, non sono monitorati, esaminati o verificati e sono di proprietà e sotto la responsabilità del cliente.

IAAS e CSP	▪ L'infrastruttura in hosting utilizzata per erogare il servizio è di proprietà del provider (Aruba S.p.A. per quello di Arezzo). ▪ Il provider è qualificato dall'Agenzia per l'Italia Digitale AgID come fornitore di servizi IaaS e Cloud Service Provider assicurando livelli di affidabilità e compliance prevista dalla normativa di riferimento. ▪ I dati, le informazioni e i documenti forniti e/o condivisi o introdotti nella piattaforma SaaS da parte del cliente sono di proprietà e sotto la responsabilità del cliente. ▪ L'utilizzo dell'infrastruttura IaaS e del relativo CSP è implicito nella licenza d'uso del servizio SaaS di SOGI Scuola concessa al cliente per tutta la durata della sua permanenza sulla piattaforma SOGI Scuola fino alla scadenza del Contratto sottoscritto.
Domain	▪ Il dominio dei servizi SaaS https://suite.sogiscuola.com è di proprietà di SOGI Scuola S.r.l.

Smaltimento sicuro dell'hardware

SOGI Scuola attua una specifica procedura di smaltimento per garantire che ogni dato presente negli storage che abbiano raggiunto il loro fine vita e che devono essere sostituiti e smaltiti sia completamente e definitivamente rimosso così come previsto dagli standard internazionali di riferimento ISO/IEC 27001 e Provvedimento del Garante Privacy del 13 ottobre 2008 "*Smaltimento e cancellazione sicura dei dati*".

Reversibilità e Cancellazione sicura dati e files

In base a quanto definito nel "*Contratto di nomina a responsabile del trattamento dei dati personali ai sensi dell'articolo 28, Regolamento (UE) 2016/679*" siglato dal Cliente, **le tempistiche di salvaguardia dei dati memorizzati nel sistema informativo aziendale sono di 90** (novanta) **giorni**.

La tempistica è da intendersi come tempo tecnico necessario per il completamento delle verifiche sui dati da restituire e cancellare, da compiersi in coordinamento con il Cliente.

Fermo restando quanto previsto, è fatto salvo il diritto di SOGI Scuola di trattare i dati anche successivamente alla data di cessazione del contratto al fine di ottemperare a specifici obblighi disposti dal diritto nazionale o dell'Unione, applicabile al Fornitore, nonché di conservare i dati, previa l'adozione di opportune misure di minimizzazione, **per finalità difensive e nei limiti dei termini stabiliti nel Registro dei Trattamenti** e di prescrizione previsti dal diritto nazionale in relazione alle controversie, potenziali o in essere, connesse all'erogazione dei servizi SaaS.

Così come previsto dalla propria procedura di reversibilità dei servizi SaaS, SOGI Scuola si assicura che lo spazio disco messo a disposizione dei clienti venga pulito al termine del tempo di salvaguardia concordato secondo le modalità descritte nella tabella che segue.

Dati presenti nei Software Cloud SaaS Agorà	Alla cessazione del contratto con il cliente, si interrompe ogni trattamento effettuato per mezzo del servizio SaaS utilizzato dal cliente. L'estrazione dei dati è indicativamente disponibile entro 24 (ventiquattro) ore, mentre la disattivazione completa del servizio avviene orientativamente in 5 (cinque) giorni lavorativi. I dati sono cancellati entro 60 (sessanta) giorni dalla data di cessazione del contratto siglato tra le parti e tale tempistica è da intendersi come tempo tecnico necessario per il completamento delle verifiche sui dati da restituire e da cancellare in coordinamento con il Cliente. Dopo i 60 (sessanta) giorni indicati i dati presenti nel database vengono cancellati in base a quanto definito nella Scheda del Registro dei Trattamenti (Allegato A) della Nomina a Resp. del Tratt. Dati sottoscritta dal cliente.
Log di accesso	Nell'infrastruttura vengono registrati i log di accesso di tutti gli utenti che usufruiscono del servizio Cloud SaaS. La maggior parte dei log vengono cancellati permanentemente dopo 12 mesi e non possono più essere recuperati. Solo pochissime tipologie di log invece rimangono permanentemente memorizzate.

Sviluppo Sicuro e testing

Gli ambienti di sviluppo di SOGI Scuola **sono chiusi e non accessibili** ad esclusione del personale SOGI Scuola formalmente autorizzato (Area Information Technology). I deploy vengono effettuati attraverso **procedure di progettazione e sviluppo degli applicativi web** e **rigorose linee guida di sviluppo sicuro**, atte ad assicurare il rispetto dei principi di *Privacy by Design* e *Privacy by Default*.

Ogni modifica/aggiornamento viene testato secondo fasi di test (di funzionalità, di sicurezza e di non regressione) predefinite e rigorose, il sistema di rilascio in produzione, oltre a richiedere la supervisione di figure di comprovata esperienza (Risk Owner ed Asset Owner), prevede una tracciatura delle attività e delle implementazioni svolte (Tracking System).

Infine, tanto per le attività di sviluppo e test è garantito un **ambiente sicuro e separato da quello di produzione**; le cui richieste di accesso vengono sottoposte a verifica e validazione.

Backup

Tutti i backup vengono effettuati la notte e salvati giornalmente presso un server ubicato nella sede di SOGI Scuola.

Giornalmente viene effettuato un backup completo del sistema compresi tutti i file caricati ed eliminati. Questa copia viene mantenuta per due giorni.

Il backup giornaliero dei database viene mantenuto per 15 giorni, dal sedicesimo giorno in poi viene mantenuta solo una copia settimanale, per un massimo di 52 settimane. Le prime 15 versioni giornaliere dei database vengono conservate anche sul server principale in modo da permettere una

riattivazione rapido nel caso si presentasse un problema ai database o per consentire al cliente di creare dei punti di ripristino per verificare lo stato dei dati nei precedenti 15 giorni.

Logging

SOGI Scuola raccoglie e conserva i **log dei server per assicurare** ai propri clienti **alti livelli di sicurezza** dei servizi SaaS erogati oltre che la **conformità normativa**. Tali log vengono periodicamente verificati dall'Area Information Technology di SOGI Scuola.

SOGI Scuola registra e conserva per le tempistiche definite nel precedente paragrafo "*Reversibilità e Cancellazione sicura dei dati e dei files*" i log applicativi nell'utilizzo del servizio SaaS.

Log degli Accessi ai Software Cloud SaaS Agorà	Il cliente può accedere in autonomina ai log degli accesi effettuati al servizio SaaS erogato da SOGI Scuola. I Log degli accessi alle piattaforme online sono conservati nel database per finalità difensive e nei limiti dei termini stabiliti nel Registro dei Trattamenti.
Log delle Attività	I Log delle operazioni svolte dagli utenti (sia interni - *dipendenti* - che esterni - *clienti* - a SOGI Scuola.) sono registrate nell'infrastruttura per un periodo di 12 (12) mesi, al termine di tale tempistica i Log vengono cancellati da una procedura automatica e non sono più accessibili. Oltre alle operazioni svolte, i Log delle Attività registrano anche l'utenza personale di colui che le ha compiute.

Comunicazione cifrata

Tutti i servizi SaaS di SOGI Scuola rivolti all'esterno utilizzano dei **canali di comunicazione cifrati** (ad esempio canale HTTPS, che è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti http e che viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti ed evitare diffusioni e modifiche non autorizzate).

Il seguente elenco descrive il dettaglio dei protocolli utilizzati su rete pubblica dei servizi SaaS Cloud:

Software Cloud SaaS Agorà	Il software SaaS Cloud di SOGI Scuola è accessibile solo previa autenticazione dell'utente e sono raggiungibili online tramite certificato cifrato SSL/HTTPS.
Assistenza Tecnica Social Customer Care	Tutte le attività di assistenza erogate nei confronti dei clienti consentono l'accesso a dati solo previa autenticazione da parte dell'operatore, registrazione delle operazioni svolte, autorizzazione formale da parte del cliente ed in caso di utilizzo di servizi di tele-assistenza crittografia delle sessioni AES (a 256 bit).
IAAS e CSP	L'accesso all'infrastruttura è possibile solo tramite connessione nominale VPN 2FA con autenticazione SHA-1 e cifratura a 256 bit

Sincronizzazione

Così come previsto dallo standard internazionale ISO/IEC 27001, tutti i sistemi Cloud SOGI Scuola utilizzano il sistema NTP per sincronizzare i propri orologi e mantenere coerenza degli eventi. La fonte autoritativa per la sincronizzazione dell'orologio è **INRiM** (https://www.inrim.it).

Il fuso orario su tutti i sistemi utilizzato è CEST su cui viene utilizzato GMT+1. Tutte le macchine virtuali dell'infrastruttura hanno fuso orario basato su CEST e utilizzano come fonte di sincronizzazione clock quella dell'Host su cui risiedono.

Sicurezza Organizzativa

In accordo alla propria **Politica SGSI**, SOGI Scuola assicura che tutti coloro che operano per l'erogazione dei servizi siano **adeguatamente formati e consapevoli dell'importanza del patrimonio informativo gestito**.

Questa misura applica in particolar modo per le nuove figure aziendali con i quali viene condivisa la politica adottata ed il rispetto dei termini previsti nello specifico accordo di riservatezza (*Non Disclosure Agreements*) per coloro svolgono funzioni di sviluppo e manutenzione dell'area IT. Per ciascuna area aziendale sono stati sviluppati programmi di formazione specifici, che vengono ripetuti e testati con cadenza periodica.

Per garantire la sicurezza dei propri servizi, SOGI Scuola controlla gli accessi ai dati ed ai sistemi e limita e monitora gli accessi ad essi.

Tra i principi adottati per la gestione della sicurezza organizzativa ci sono:

- "**need to know**" (Allegato B del D.Lgs. 196/2003) secondo il quale i soggetti che devono compiere attività di trattamento di informazioni sono autorizzati a trattare i soli dati essenziali allo svolgimento dell'attività attribuita;
- "**dual control**" per il quale sono stabilite alcune procedure operative che richiedono la compresenza di almeno due diversi operatori per la loro esecuzione, con particolare riferimento a figure senior dedicate quali Risk Owner ed Asset Owner;
- "**least privilege**" secondo il quale ad ogni operatore è concesso il privilegio minimo necessario per poter svolgere i propri compiti in modo da ridurre per quanto possibile il rischio di accesso/modifica/cancellazione degli asset e dei dati gestiti;
- "**privacy by design**" per il quale l'obiettivo già in fase di sviluppo dei servizi SaaS Cloud il tema del trattamento dei dati sia prioritario per garantire sicurezza e trasparenza oltre al fine ultimo di prevenire un problema;

- "**privacy by default**" secondo cui si debbano trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste (art. 5 p. 1 lett. b) e per il periodo strettamente necessario a tali fini (art. 5 p. 1 lett. c).

Nello specifico, caso in cui si renda necessario l'intervento di Amministratori di sistema SOGI Scuola sui sistemi Cloud, **è garantito che i privilegi di accesso siano forniti solo sulla base di specifiche procedure definite** e che tutte le attività siano eseguite secondo iter ed istruzioni predeterminate per le quali sia possibile mantenerne traccia.

Gestione delle vulnerabilità

SOGI Scuola riconosce che **la gestione delle vulnerabilità tecniche dei sistemi informatici rappresenti una delle attività cruciali per poter garantire la sicurezza dei propri servizi**: per questo motivo sono predisposte delle misure per ricercare, governare e risolvere le vulnerabilità tecniche individuate per evitare che possano comportare impatti negativi sul servizio e sui dati gestiti.

Il Resp. dell'Area Information Technology coadiuvata dall'Amministratore di Sistema compongono il gruppo deputato a eseguire **periodiche e regolari scansioni di vulnerabilità e penetration-test** sia sui servizi offerti alla clientela, sia sull'infrastruttura IT.

Gestione degli incidenti

SOGI Scuola 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.

SOGI Scuola ha individuato nello standard ISO/IEC 27001 i propri principi di riferimento per le attività di pianificazione e predisposizione ad una corretta e tempestiva risposta a eventuali eventi di sicurezza, anche con il supporto di una specifica squadra incaricata in base alla peculiarità della problematica riscontrata.

Gestione delle capacità e del cambiamento

Al fine di garantire la corretta consegna/erogazione del servizio **SOGI Scuola ritiene fondamentale monitorare le risorse a disposizione e adottare gli opportuni accorgimenti per lo sfruttamento ottimale** delle stesse.

A tal fine sono state individuate alcune risorse cui applicare un costante monitoraggio ed analisi delle capacità per poter permettere di assicurare la normale fruizione dei servizi.

I livelli di connettività, i livelli di occupazione delle risorse, lo spazio su disco ed il dimensionamento dell'infrastruttura sono monitorati con specifici strumenti di monitoraggio dell'Area Information Technology, il cui compito si estende anche al monitoraggio di qualsiasi evento anomalo.

Gli strumenti di monitoraggio permettono l'impostazione di controlli specifici per ciascun servizio, rilevando le anomalie e permettendo di anticipare le necessità di cambiamento.

I cambiamenti resi necessari dalle attività di monitoraggio e di gestione delle capacità oppure vengono gestiti in modo controllato per permettere di verificarne i risultati e di mantenere traccia delle attività svolte.

Policy di Sicurezza Logica e Fisica

Per conoscere in dettaglio **le politiche di sicurezza logica e fisica** adottate da SOGI Scuola nella propria infrastruttura presente nei due Data Center in housing si rimanda al documento dedicato "*Policy di Sicurezza*" disponibile per i propri stakeholder all'indirizzo online: (Allegato C).

Informazioni di contatto

In questo capitolo sono riportati i contatti telefonici ed e-mail per richiedere maggiori dettagli e/o delucidazioni sul presente documento e sul sistema di Sicurezza Informatica Aziendale.

Pippa Nicola

Tel. 0454935690
nicola.pippa@sogiscuola.it

Informazioni sulla società

SOGI Scuola S.r.l.

Via Gino Bozzini n. 5, 37135 Verona (VR)

Tel. 0454935690
www.sogiscuola.it