PROTOCOLLO SERVIZI IN CLOUD

1 Introduzione 2
2 Definizione ed illustrazione dei ruoli e responsabilità 2
3 Individuazione logistica dei Server 2
4 Etichettatura delle Informazioni 2
5 Gestione degli Accessi 3
6 Limitazione degli Accessi 3
7 Crittografia 3
8 Change Management 3
9 Servizio di backup 3
10 Raccolta e Monitoraggio Log 3
11 Sincronizzazione degli orologi 3
12 Gestione delle Vulnerabilità 3
13 Gestione degli Incidenti 4
14 Protezione delle Registrazioni 4
15 Audit Tecnici 4
16 Rimozione degli Asset 4
17 Monitoraggio del Cloud 5
18 Sicurezza delle Reti 5
19 Divulgazione delle Informazioni 5
20 Data Breach 5
21 Restituzione, Trasferimento e Smaltimento di dati personali 5
22 Accordi di Riservatezza 5

1 Introduzione

Il presente documento, che è parte integrante del contratto di servizio fornito in modalità SaaS, redatto dalla Sautech Srl (di seguito sempre definita solo come Organizzazione), descrive i requisiti specifici da soddisfare ed una dettagliata informativa al cliente sulle modalità di gestione delle attività in conformità a quanto previsto dalle linee guida ISO IEC 27017:2015 e ISO IEC 27018:2019.

L'Organizzazione fornisce servizi software in modalità SaaS. Per l'erogazione di detti servizi è utilizzato un provider certificato che garantisce ai clienti dell'Organizzazione la completa disponibilità dei loro dati e la necessaria ed assoluta riservatezza, integrità degli stessi.

2 Definizione ed illustrazione dei ruoli e responsabilità

Per tutte le attività descritte la struttura funzionale e dirigenziale dell'Organizzazione fa capo alle figure di Security Manager, Responsabile SGSI e al Team Security Manager, aventi responsabilità specifiche in materia di sicurezza delle informazioni. Inoltre, il Responsabile Commerciale occupa il ruolo di interfaccia operativa tra l'Organizzazione e il cliente, in materia di sicurezza del cloud.

L'interfaccia principale è il Customer Care per quanto attiene le funzionalità del software fornito in modalità SaaS.

Il Responsabile del trattamento dei Dati (GDPR) ed il Security Manager sono invece le funzioni preposte nell'Organizzazione per l'elaborazione dei dati personali (PII) prevista nei contratti, inoltre l'Organizzazione ha individuato al proprio interno del reparto Produzione i punti di contatto con il cliente; eventuali elaborazioni delle PII (ad esempio per motivi di assistenza e manutenzione), sono svolte dagli incaricati interni.

3 Individuazione logistica dei Server

L'Organizzazione utilizza per i propri servizi in cloud infrastrutture all'interno del territorio nazionale italiano o europeo (Data Center Aruba ubicati a Arezzo, Data Center CDLAN ubicati a Caldera Park (MI)).

Aruba è certificata per i servizi di "Progettazione e fornitura servizi di Cloud Computing e Cloud Storage, Hosting, Housing e Colocation, Posta Elettronica, Domini Internet, Sicurezza Informativa e Disaster Recovery" secondo la norma **ISO IEC 27001:2022** con estensione alle linee guida 27017:2015 e 27018:2019.

CDLAN è certificata per i servizi di "Erogazione e assistenza di Colocation (Data Center), Cloud computing e Cloud storage, Hosting, Telecomunicazioni dati e voce" secondo la norma **ISO/IEC 27001:2022** con estensione alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

L'Organizzazione, nell'eventualità di dover effettuare modifiche di change location sui servizi cloud attivati verso altri Data Center ubicati all'interno della UE, comunicherà tale variazione ai clienti con un preavviso di almeno 15 giorni, così come comunicherà per iscritto altre formalizzazioni che potranno riguardare eventuali espansioni infrastrutturali.

4 Etichettatura delle Informazioni

Laddove dai requisiti contrattuali o laddove si reputi necessario, l'Organizzazione rende noto al cliente le funzionalità dei servizi rivenduti su cloud che consentano un'adeguata etichettatura delle informazioni presenti sul cloud. Detta classificazione consente di regolamentare l'accesso alle sole funzioni che ne hanno l'autorità.

5 Gestione degli Accessi

L'Organizzazione regola l'accesso all'applicazione e ai sistemi con modalità differenti a seconda dei servizi offerti, per cui con il Rappresentante del Cliente viene generata un'utenza "Administrator" che individuerà una propria password. L'Administrator del Cliente potrà invitare gli utenti che provvederanno alla registrazione delle anagrafiche associate al Cliente. L'Administrator del Cliente può provvedere alla disabilitazione dell'utente.

L'utente registrato può provvedere autonomamente alla cancellazione (deregistrazione: si parla solo di cancellazione logica).

Per autenticare gli utenti l'Organizzazione assegna un codice di accesso, nome utente e password, la quale viene generata automaticamente, e per questa sarà richiesta la modifica già al primo accesso.

L'Utente avendo la possibilità di modificare autonomamente le password, consente in maniera tempestiva di intervenire nei casi di dubbi circa eventuali corruzioni o compromissioni di password, come i casi di divulgazioni involontarie.

6 Limitazione degli Accessi

Le limitazioni di accesso alle informazioni su cloud sono concordate in fase contrattuale con il Cliente.

7 Crittografia

Nel servizio cloud i flussi di dati da e verso i sistemi ed i server esposti su internet sono protetti utilizzando un canale sicuro TLS mediante opportuna configurazione sui server.

8 Change Management

Per quanto attiene le eventuali modifiche al servizio cloud ed ai sistemi che lo compongono, l'Organizzazione provvederà tempestivamente a comunicarle ai clienti, fornendo i tempi di esecuzione delle variazioni così da minimizzarne gli impatti che potrebbero derivarne.

9 Servizio di backup

Il servizio di Backup è assicurato da Sautech. In ogni caso l'organizzazione esegue dei test per assicurarsi della regolarità delle operazioni affidate. I tempi di conservazione sono definiti contrattualmente con il cliente.

10 Raccolta e Monitoraggio Log

Le registrazioni dei log applicativi sono rese disponibili ai clienti dall'Organizzazione, inoltre le modifiche alle informazioni personali vengono storicizzate e conservate con i log delle modifiche effettuate, così che i clienti possano consultarli o chiederne all'Organizzazione una "traduzione".

11 Sincronizzazione degli orologi

L'Organizzazione per sincronizzare tutti gli orologi e mantenere coerenza degli eventi sul cloud utilizza il sistema NTP, la fonte autoritativa per la sincronizzazione dell'orologio è "INRiM" (http://www.inrim.it). Il fuso orario su tutti i sistemi utilizzato è CEST ad eccezione di UK su cui viene utilizzato GMT+1, tutte le Virtual Machine fornite hanno fuso orario basato su CEST e utilizzano come fonte di sincronizzazione clock quella dell'host su risiede.

12 Gestione delle Vulnerabilità

L’Organizzazione predispone tutte le misure per ricercare, governare e risolvere le vulnerabilità tecniche individuate per evitare che possano comportare impatti negativi sul servizio e sui dati gestiti.

Sono definiti un team e delle risorse per eseguire periodiche e regolari scansioni di vulnerabilità e penetration test.

L'Organizzazione esegue semestralmente (o in caso di modifiche e/o richieste specifiche) test di vulnerabilità sugli applicativi; in caso di esiti negativi, provvede ad adottare le necessarie azioni correttive. Considerata la riservatezza di tali informazioni, l'esito dei test non è divulgato all'esterno.

13 Gestione degli Incidenti

L’Organizzazione ha definito una specifica procedura per poter permettere un approccio organizzato e regolato alla gestione degli incidenti come parte della propria strategia di sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza e ai punti di debolezza.

Gli incidenti di sicurezza delle informazioni devono essere segnalati al più presto possibile inviando un’email a cyberalert@sautechgroup.com. Tutte le segnalazioni pervenute saranno gestite da apposito team che valuterà se classificarle come incidente relativo alla sicurezza delle informazioni, rispondendo coerentemente a quanto previsto dalla procedura interna.

È a cura del Cliente sensibilizzare i propri dipendenti affinché forniscano informazioni relative al tipo di dati, alle informazioni, alla data e ora in cui si è verificato l'incidente e la posizione logica dei dati.

Se l'incidente di sicurezza delle informazioni è in relazione alle informazioni personali il Responsabile del Trattamento dei dati, oltre alle figure sopra richiamate, deve essere informato.

Il livello di impatto di un incidente di sicurezza delle informazioni sarà determinato secondo la strategia di gestione del rischio stabilita da RSGSI, con il Security Manager ed il Responsabile del trattamento dei dati.

Il RSGSI manterrà una copertura del processo di gestione degli incidenti in relazione ad identificazione, valutazione, gestione e monitoraggio degli incidenti di sicurezza delle informazioni, compresa la raccolta di qualsiasi prova che potrebbe essere richiesta per l'analisi come prova forense.

14 Protezione delle Registrazioni

L’Organizzazione gestisce le registrazioni dei dati dei clienti (database) applicando le prassi di sicurezza previste dalle policies vigenti (https, cifratura del canale, ecc.). Inoltre, per la validazione delle soluzioni implementate, l’Organizzazione esegue con regolarità test di vulnerabilità.

15 Audit Tecnici

L’Organizzazione, avendo un sistema di gestione conforme alla ISO IEC 27001 e alle linee guida 27017-27018 esegue regolarmente Audit tecnici.

16 Rimozione degli Asset

Alla chiusura di un contratto con l’Organizzazione la piattaforma ferma i servizi del cliente ma non esegue la cancellazione effettiva. Dopo 15 giorni dall’avvenuta disconnessione, gli asset del cliente presenti sui sistemi vengono cancellati definitivamente e non possono più essere recuperati. Eventuali Indirizzi di rete pubblica assegnati al cliente tornano liberi e possono essere immediatamente riassegnati ad altri clienti.

La cancellazione avviene attraverso API messe a disposizione dal fornitore del software di virtualizzazione (microsoft e vmware). I servizi saranno disabilitati, i dati backuppati e conservati localmente a cura dell'Organizzazione, per un arco di tempo in linea con la normativa vigente, per eventuali controversie.

17 Monitoraggio del Cloud

L'Organizzazione effettua il monitoraggio dei servizi cloud con gli strumenti messi a disposizione da Aruba; eventuali parametri di monitoraggio stabiliti in fase contrattuale saranno forniti a cura del Security Manager. Le modifiche alle informazioni personali sono storicizzate ed un log delle modifiche effettuate viene conservato dall'applicazione.

18 Sicurezza delle Reti

Le reti virtuali sono definite dall'Organizzazione e messe a disposizione su base contrattuale. I requisiti di configurazione sono definiti in funzione dei parametri di sicurezza desiderati.

19 Divulgazione delle Informazioni

A meno che non sia necessaria per soddisfare requisiti contrattuali non è prevista alcuna divulgazione di PII. L'eventuale divulgazione può avvenire solo verso dipendenti, fornitori o subappaltatori. In questi due ultimi casi l'Organizzazione richiede un espresso consenso da parte del Cliente, con esclusione di richieste legalmente vincolanti da parte delle autorità preposte (es. Autorità Giudiziaria).

Nei casi in cui avvenga un incidente che causa la divulgazione delle PII (es. data breach), la notifica al Responsabile Trattamento Dati sarà segnalata prima possibile, telefonicamente o di persona.

Qualsiasi divulgazione di PII deve essere registrata dal Responsabile Trattamento Dati nel registro di divulgazione delle PII. Tale documento deve comprendere quali informazioni personali sono state divulgate, da chi, a chi e a che ora.

Nei casi in cui la divulgazione è richiesta da autorità preposte, il riferimento legale utilizzato per autorizzare la divulgazione deve essere incluso nella registrazione.

20 Data Breach

È previsto l'intervento del Responsabile Trattamento Dati per la gestione del Data Breach in caso di eventi tracciabili di accesso non autorizzato alle PII o accesso non autorizzato alle apparecchiature o alle strutture di elaborazione che comportano perdita, divulgazione o alterazione delle PII.

21 Restituzione, Trasferimento e Smaltimento di dati personali

Il Responsabile Trattamento Dati dell'Organizzazione, deve garantire che la conservazione delle PII avvenga solo per il tempo necessario al raggiungimento delle finalità contrattuali.

Per quanto riguarda l'acquisizione, lo sviluppo e la manutenzione dei sistemi informativi, devono essere stabiliti requisiti per garantire che i file e i documenti creati nel normale corso delle operazioni, elaborazioni, vengano eliminati non appena tali file e documenti non siano più necessari. Le PII detenute eventualmente in formato cartaceo sono distrutte mediante la distruggi documenti presente in azienda.

22 Accordi di Riservatezza

L'Organizzazione ha definito al proprio interno appositi accordi di riservatezza con il personale che opera in qualità di incaricato al trattamento sui servizi in Cloud forniti al cliente. Di norma non si producono stampe cartacee di materiali contenenti PII, eventuali stampe sono distrutte immediatamente dopo l'utilizzo. Gli

interventi di assistenza, eseguiti su richiesta del cliente sono tracciabili mediante richieste dai Clienti (la piattaforma di ticketing, mail, registro) e non danno luogo ad archiviazioni di dati personali.

Le e-mail utilizzate dall'Organizzazione viaggiano su canale crittografato sia in ingresso che in uscita, garantendo in tal modo che eventuali dati personali trasmessi (sebbene la policy aziendale vieti la trasmissione di PII mediante e-mail) lo facciano in modo sicuro.

Laddove l'organizzazione operi su PII del cliente, richiede formalmente una nomina a incaricata del trattamento, coperta dai vincoli di cui al regolamento 2016/679.

Sautech non fa uso di subappaltatori per l'elaborazione dei dati.