



POLITICA INTEGRATA QUALITÀ E SICUREZZA DELLE INFORMAZIONI

1. Il Nostro Impegno e la Visione Strategica

Advinser S.r.l. è un partner tecnologico specializzato nell'offerta di soluzioni software Tailor Made, Business Intelligence e System Integration per i settori Fashion & Luxury, Manifatturiero e Utilities.

L'Alta Direzione riconosce che il successo e la crescita sostenibile dipendono dalla capacità dell'azienda di garantire, in modo coerente, l'eccellenza dei servizi erogati (Qualità) e la massima protezione delle informazioni trattate (Sicurezza delle Informazioni), con particolare attenzione ai servizi cloud forniti ai Clienti.

Per questo, Advinser adotta e mantiene un Sistema di Gestione Integrato (SGI) conforme ai requisiti delle norme:

- ISO 9001:2015 – Sistemi di Gestione per la Qualità
- ISO/IEC 27001:2022 – Sistemi di Gestione per la Sicurezza delle Informazioni
- ISO/IEC 27017:2021 – Controlli di sicurezza per servizi cloud
- ISO/IEC 27018:2020 – Protezione dei dati personali nei servizi cloud

Attraverso il SGI garantiamo il rispetto di tutti i requisiti applicabili, dei requisiti contrattuali e normativi, dei controlli specifici richiesti per l'erogazione di servizi in cloud, nonché il raggiungimento degli obiettivi e il miglioramento continuo delle performance.

L'Alta Direzione si impegna inoltre a fornire risorse adeguate (umane, tecnologiche ed economiche) per garantire l'efficacia del Sistema e per sostenere l'evoluzione dei servizi cloud e dei processi aziendali.

2. Campo di Applicazione del Sistema di Gestione Integrato

Il Sistema di Gestione Integrato (SGI) di Advinser si applica a tutte le attività e i processi relativi a:

"Progettazione, realizzazione e fornitura di soluzioni software e sistemi enterprise, con erogazione in modalità Software as a Service (SaaS) e on-premise."

Il campo di applicazione include:

- sviluppo software personalizzato
- soluzioni proprietarie in cloud
- servizi di Business Intelligence
- integrazioni applicative e sistemi enterprise
- gestione documentale

- trattamento, gestione e protezione dei dati personali dei Clienti
- controllo della sicurezza delle informazioni nei servizi cloud forniti

Sono inoltre inclusi i controlli specifici richiesti dalle norme ISO/IEC 27017 (sicurezza per cloud provider e cloud customer) e ISO/IEC 27018 (protezione dei dati personali nei servizi cloud pubblici, ove applicabile).

3. Principi Guida per la Qualità

Advinser mira a essere un punto di riferimento per l'innovazione tecnologica, assicurando che ogni progetto superi le aspettative del Cliente.

Per raggiungere questo obiettivo, ci focalizziamo sull'approccio per processi e sulla gestione del rischio in tutte le fasi coperte dal Campo di Applicazione: dalla comprensione del bisogno iniziale del Cliente alla progettazione, dallo sviluppo all'implementazione e all'assistenza.

Questo include la valutazione proattiva dei rischi e delle opportunità che possono influire sull'efficacia dei nostri servizi.

Promuoviamo una cultura della Qualità che parte dalla Leadership e si estende al Coinvolgimento di tutto il personale, incoraggiando la competenza tecnica, l'uso di metodologie di sviluppo aggiornate e la costante attenzione ai dettagli per garantire la conformità e la performance dei sistemi che realizziamo.

4. Principi Guida per la Sicurezza delle Informazioni

Data la natura del nostro business, che implica l'accesso e la gestione di dati critici di produzione, finanziari e di Business Intelligence dei nostri Clienti, la Sicurezza delle Informazioni è una priorità assoluta all'interno del Campo di Applicazione definito.

Il nostro impegno è assicurare le tre proprietà fondamentali dell'informazione gestita nei servizi SaaS e on-premise:

- **Riservatezza:** Impedendo l'accesso, l'uso o la divulgazione non autorizzata delle informazioni proprietarie dei Clienti e di Advinser.
- **Integrità:** Mantenendo l'accuratezza e la completezza dei dati e dei sistemi
- **Disponibilità:** Garantendo la continuità operativa e l'accesso affidabile alle informazioni e ai servizi da parte degli utenti autorizzati.

Impegni aggiuntivi specifici per ISO/IEC 27017 e ISO/IEC 27018

Advinser si impegna inoltre a garantire:

- l'adozione di controlli specifici per la sicurezza nei servizi cloud, come previsti dalla ISO/IEC 27017 (per esempio segregazione delle funzioni cloud provider/cloud customer, gestione sicura delle VM, protezione delle API, obblighi contrattuali di sicurezza);
- la protezione dei dati personali trattati come cloud provider, secondo i principi della ISO/IEC 27018, tra cui:
- limitazione delle finalità di trattamento
- divieto di utilizzo dei dati per marketing o profilazione non autorizzata
- gestione sicura degli incidenti e delle violazioni dei dati personali

- minimizzazione dei log che contengono dati personali
- gestione dei diritti dell'interessato
- trasparenza nei sub-fornitori e nelle localizzazioni dei dati

Advinser si impegna rigorosamente a rispettare tutti gli obblighi legali e contrattuali relativi alla sicurezza, in particolare il Regolamento Generale sulla Protezione dei Dati (GDPR) per i dati personali trattati. Attraverso una continua valutazione del rischio, definiamo controlli adeguati (tecnici, fisici e organizzativi) per prevenire incidenti di sicurezza e assicurare la resilienza in caso di evento avverso.

La gestione del rischio informa costantemente la progettazione e l'applicazione dei controlli tecnici, organizzativi e fisici necessari a prevenire incidenti o interruzioni e ad assicurare resilienza operativa e disponibilità dei servizi cloud.

5. Contesto, Parti Interessate e Miglioramento

Questa Politica è sviluppata tenendo conto del contesto specifico di Advinser, delle esigenze delle nostre Parti Interessate (in primis i Clienti nei settori chiave, i dipendenti, i fornitori di tecnologia e le Autorità regolatorie) e dei rischi ambientali e tecnologici specifici del settore IT.

La Politica è comunicata, compresa e implementata a tutti i livelli dell'organizzazione. Essa costituisce il quadro di riferimento per la definizione e il monitoraggio degli Obiettivi misurabili di Qualità e di Sicurezza delle Informazioni.

L'Alta Direzione si impegna a rivedere la Politica periodicamente, in occasione del Riesame del SGI, per garantire che rimanga sempre appropriata e allineata alle strategie di crescita e alle evoluzioni tecnologiche di Advinser.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI NEI RAPPORTI CON I FORNITORI

1. PREMESSA

Lo scopo del presente documento è quello di definire i requisiti di sicurezza delle informazioni nei rapporti con i Fornitori al fine di mitigare i rischi associati all'accesso agli asset di ADVINSER SRL da parte di soggetti esterni.

La presente politica trova applicazione in tutti i rapporti con i fornitori e coi partner che hanno un coinvolgimento sulla sicurezza delle informazioni nel processo di approvvigionamento e/o erogazione dei prodotti e servizi.

2. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

ADVINSER SRL implementa e mantiene un Sistema di Gestione per la sicurezza delle Informazioni in accordo ai requisiti specificati nella norma ISO/IEC 27001:2022, con estensioni ISO 27017 e ISO 27018 e nel Regolamento UE 2016/679, in modo da garantire:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetture associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione;
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

La mancanza di adeguati livelli di sicurezza delle informazioni può comportare il danneggiamento dell'attività di ADVINSER SRL, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine dell'azienda e della filiera sottostante.

La Direzione di ADVINSER SRL è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con l'azienda nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.

Per questi motivi la Direzione di ADVINSER SRL promuove tutte le azioni necessarie affinché i processi e le attività siano orientati al raggiungimento dei seguenti obiettivi:

- Identificare le esigenze di sicurezza tramite l'analisi dei rischi al fine di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo;
- Attuare le azioni necessarie per mitigare i rischi individuati e le misure di sicurezza più idonee;
- Garantire la massima sicurezza delle informazioni dei clienti, in termini di riservatezza, disponibilità e integrità;
- Dare continuità operativa ai servizi critici anche a seguito di gravi incidenti;
- Tutelare i diritti e gli interessi di tutti coloro che interagiscono con l'azienda (clienti, dipendenti, collaboratori, terze parti, ecc.);
- Salvaguardare gli interessi degli investitori e dei partners;
- Garantire un livello di servizio eccellente.

I Fornitori devono assicurare che tutto il personale operanti per il raggiungimento dei suindicati obiettivi di sicurezza nella gestione delle informazioni e impieghino le tecnologie più adeguate a garantire il rispetto della presente politica.

3. REQUISITI DI SICUREZZA PER LA TRASMISSIONE DELLE INFORMAZIONI

Lo scambio di documenti e informazioni tra ADVINSER SRL e il Fornitore deve avvenire in modo controllato e sicuro in accordo al sistema di classificazione ed etichettatura adottato dall'azienda e al quale il Fornitore deve adeguarsi.

Tale sistema prevede in particolare i seguenti livelli di classificazione delle informazioni:

1. di dominio pubblico (non necessitano di alcuna etichettatura)
2. ad uso interno
3. riservato (o confidenziale)

Nel caso si debbano discutere o scambiare informazioni confidenziali tra ADVINSER SRL e il Fornitore, o tra un Fornitore e terzi, le parti devono prima assicurarsi di aver sottoscritto un Accordo di riservatezza o di non divulgazione.

Per le informazioni digitalizzate la trasmissione deve avvenire attraverso, posta elettronica o PEC con utilizzo del protocollo TLS; nel corpo del messaggio di posta elettronica deve essere presente un'intestazione standardizzata in cui si avverte della confidenzialità/riservatezza del messaggio; gli allegati di posta elettronica possono essere cifrati con password per assicurare maggiore protezione alle Informazioni Riservate ritenute più critiche (es. dati personali particolari o giudiziari).

Le informazioni riservate che sono comunicate in forma verbale devono essere considerate tali nel momento in cui il soggetto che le comunica le indicherà come "riservate" all'altra parte.

Il fornitore si impegna ad attuare soluzioni per la protezione delle informazioni da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate.

In caso di necessità di accesso agli asset di ADVINSER SRL da parte del Fornitore, lo stesso dovrà essere preventivamente autorizzato e informato delle modalità di utilizzo degli stessi, cui dovrà attenersi scrupolosamente e sarà soggetto ai controlli previsti dalle politiche di sicurezza di ADVINSER SRL.

Per i Fornitori associati ai servizi e ai prodotti della filiera di fornitura per l'ICT, il Fornitore deve impegnarsi a rispettare i requisiti di ADVINSER SRL per affrontare i rischi relativi alla sicurezza delle informazioni, richiedendo preventivamente a ADVINSER SRL la copia delle policy applicabili.

4. MONITORAGGIO E RIESAME DEI SERVIZI EROGATI DAL FORNITORE

Al fine di assicurare il controllo su tutti gli aspetti di sicurezza relativi alle informazioni critiche o alle strutture di elaborazione delle informazioni, ADVINSER SRL monitora i livelli di prestazione del servizio erogato e ricevuto dal Fornitore al fine di verificare il rispetto degli accordi. Potranno essere condotti audit ai propri Fornitori, congiuntamente al riesame dei rapporti di fornitura.

5. GESTIONE DEI CAMBIAMENTI AI SERVIZI

Nel caso di cambiamento alla fornitura dei servizi da parte dei fornitori/partner, devono essere prontamente comunicate a ADVINSER SRL che rivedrà le procedure di qualifica e che riprenderà in esame gli aspetti legati alla sicurezza delle informazioni all'interno degli accordi.

6. GESTIONE DEGLI ACCESSI ALLA RETE ED AI SERVIZI DI RETE

Qualora il servizio richiesto al Fornitore richieda di operare all'interno della rete ADVINSER SRL, allo stesso verrà fornito l'accesso con le seguenti modalità e solo per i servizi ai quali sono stati specificatamente autorizzati dai singoli accordi con ADVINSER SRL:

- Il Fornitore dovrà comunicare il nominativo degli operatori che saranno preventivamente approvati da ADVINSER SRL per operare sulla rete;

- Agli stessi verrà assegnata una credenziale di autenticazione composta da userID e password da modificare al primo accesso.

7. CONTROLLO DEI LOG

L'utente (operatore del Fornitore) è soggetto al controllo dei Log da parte del personale ICT di ADVINSER SRL.

8. GESTIONE PASSWORD

Gli utenti (operatori del Fornitore) si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso indicati all'interno di questo documento.

Le password devono essere lunghe almeno otto caratteri, non devono contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente, devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole, non devono essere uguale alle precedenti.

La password deve essere obbligatoriamente modificata ogni sei mesi; nel caso di trattamento di dati personali particolari e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.

La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno o all'esterno dell'organizzazione.

Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, rispondere ad e-mail sospette e/o cliccare sui link durante la navigazione web o dallo stesso messaggio di posta ricevuto, al fine di contrastare possibili frodi informatiche (es. phishing, furto di identità, ecc.).

Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account.

Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà segnalarlo a personale IT di ADVINSER SRL. Per la conservazione sicura delle credenziali di accesso si consiglia di evitare la memorizzazione su documenti cartacei o in file conservati all'interno della postazione di lavoro.

9. ACCESSI FISICI

ADVINSER SRL ha predisposto un sistema di controllo perimetrale per l'accesso alla sede, agli uffici e ai locali in cui si trattano informazioni.

L'accesso è consentito solo al personale autorizzato, per cui se il Fornitore ha necessità di accedere agli uffici o ai locali della sede di ADVINSER SRL deve disporre di autorizzazione specifica e rispettare le misure di sicurezza fisica ed ambientale applicate.

10. COMUNICAZIONE EVENTI DI SICUREZZA

Ogni segnalazione di vulnerabilità, eventi ed incidenti di sicurezza rilevati nel corso delle attività svolte dal Fornitore deve essere comunicata in modo formale anche per il tramite della posta elettronica al referente del contratto di ADVINSER SRL per la successiva gestione e risoluzione della problematica.

11. CESSAZIONE RAPPORTI CON IL FORNITORE

Nell'ipotesi di cessazione dei rapporti con il fornitore/partner, gli aspetti sulla sicurezza delle informazioni dovranno essere gestiti conformemente a quanto contrattualizzato tra le parti.

12. SANZIONI

Il mancato o il ritardato adempimento di quanto previsto dalla presente politica aziendale e/o dal contratto stipulato tra le parti, che dovesse provocare dei danni di natura economica, finanziaria e di immagine alla ADVINSER SRL e alla filiera sottostante, comporterà il conseguente obbligo di risarcimento in favore di ADVINSER SRL, oltre alle eventuali sanzioni amministrative pecuniarie e/o penali previste dal Regolamento GDPR 2016/679 e/o dalla normativa vigente.

13. CONDIVISIONE POLITICA

La Politica nei rapporti coi fornitori/partner viene resa disponibile sul sito aziendale ed eventuali variazioni verranno notificate via email.

14. AGGIORNAMENTO

La Politica è mantenuta costantemente aggiornata ed allineata con gli indirizzi strategici della Direzione. In occasione del Riesame della Direzione ne viene verificata l'adequatezza

POLITICA DI SICUREZZA DELLE INFORMAZIONI NELL'EROGAZIONE DI SERVIZI CLOUD

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche aziendali specifiche, parti integranti della politica generale del SGI definita dalla Direzione di ADVINSER S.R.L., relativamente al servizio Cloud, per la protezione dei dati globali, inclusi i dati personali applicando le best practices definite dagli standard ISO 27017 e ISO 27018.

Lo scopo di questa politica pertanto è descrivere i principi generali di sicurezza nell'ambito dei servizi in cloud che ADVINSER S.R.L. ha fatto propri, al fine di garantire una sicurezza delle informazioni, conservate e/o

gestite su piattaforme in cloud pubblici, di livello almeno pari ai principi generali espressi nella sua politica generale di sicurezza e, in presenza di dati personali, conformi alla normativa vigente.

2. PERIMETRO ORGANIZZATIVO

La presente policy si applica a tutto il personale dipendente di ADVINSER S.R.L. e a tutti i soggetti che collaborano con la stessa.

La policy si applica inoltre a tutti i processi più in generale e a tutte le risorse coinvolte nella gestione delle informazioni trattate dalla società.

Nel documento, i termini "fornitore di servizi cloud" o "CSP", acquistano una duplice valenza a seconda del contesto. Quando la policy verrà applicata a servizi di cui ADVINSER S.R.L. è cliente, con i suddetti termini ci si riferirà al fornitore di tali servizi. Quando verrà applicata a servizi erogati da ADVINSER S.R.L., ci si riferirà all'azienda.

3. TERMINI E DEFINIZIONI

- Asset o Bene – Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (es. beni fisici, software, informazioni e dati, ...).
- Cloud – Un insieme di servizi ICT accessibili on-demand e in modalità self-service tramite tecnologie Internet, basati su risorse condivise, caratterizzati da rapida scalabilità e dalla misurabilità puntuale dei livelli di performance, in modo da poter essere pagati in base al consumo.
- Cloud Privato – Piattaforma basata su Cloud gestita internamente per erogare servizi e non aperta alla disponibilità di soggetti terzi.
- Cloud Pubblico – Piattaforma basata su Cloud che eroga servizi a più soggetti non connessi tra di loro.
- Cloud Ibrido – Soluzione tecnologica che prevede l'impiego combinato di Cloud Pubblico e Cloud Privato.
- CSP – (Cloud Service Provider) Un'entità (privata o pubblica) che fornisce piattaforme, infrastrutture, applicazioni, servizi di sicurezza o di archiviazione basati su cloud a un'altra entità/organizzazione solitamente a pagamento.
- Disponibilità – Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata (ISO/IEC 13335-1:2004).
- Hardening – Insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.
- IaaS – (Infrastructure-as-a-Service) Infrastruttura erogata in modalità di servizio. Risorse hardware virtualizzate vengono messe a disposizione, affinché l'utilizzatore possa creare e gestire, secondo le proprie esigenze, una propria infrastruttura sul cloud senza preoccuparsi di dove siano allocate le risorse
- SaaS – Il Software as a Service è un modello di distribuzione del software basato su cloud in cui il provider di servizi cloud sviluppa e mantiene il software applicativo cloud, fornisce aggiornamenti software automatici e mette il software a disposizione dei propri clienti via Internet basato sul pay-as-you-go.
- Integrità – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata (ISO/IEC 13335-1:2004).
- Log - Il log è un sistema di registrazione di avvenimenti significativi. I file che contengono queste annotazioni sono detti file di log e potrebbero essere identificati anche come i file delle registrazioni, per cui il log è non è altro che un registro.
- Responsabile del Trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; Riservatezza – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO/IEC 13335-1:2004).
- Snapshot – Copia dello stato di una macchina virtuale in un determinato momento.

- Titolare del Trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

4. CONTESTO REGOLATORIO DI RIFERIMENTO

- ISO 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- ISO 27017:2021 – Codice di pratica per i controlli di sicurezza delle informazioni basati su ISO / IEC 27002 per i servizi cloud
- ISO 27018:2020 – Codice di pratica per la protezione delle informazioni personali (PII) in cloud pubblici che agiscono come processori PII
- GDPR Reg. UE 679/2016 e legislazione nazionale

5. POLITICA DI SICUREZZA DI GESTIONE SERVIZIO CLOUD

ADVINSER S.R.L. eroga anche servizi di cloud computing in modalità SaaS (Software-as-a-Service) in quanto i servizi all'utente finale sono erogati tramite applicazioni basate sul Web. Il modello SaaS è un metodo per la distribuzione di applicazioni software tramite Internet, dove i provider di servizi cloud ospitano tali applicazioni software al fine di consentire l'uso delle stesse a tutti i client connessi.

ADVINSER S.R.L., nell'utilizzare la infrastruttura IAAS a supporto dei propri processi, acquisisce il ruolo di Cloud Service Customer.

Il Cloud ADVINSER S.R.L. può essere erogato al Cliente tramite:

1. Creazione di un'istanza per ogni cliente sul server cloud di ADVINSER S.R.L., situato presso AWS S.p.A.

Nell'ambito dell'erogazione e/o gestione di servizi cloud ADVINSER S.R.L. prende in considerazione i requisiti di seguito descritti.

- Gestione del Cloud: lo spostamento di dati nel cloud può richiedere un riallineamento significativo di ruoli e responsabilità all'interno dell'organizzazione e/o nei confronti dei suoi fornitori. Per questo motivo è necessario definire puntualmente i ruoli tanto relativamente all'erogazione del servizio quanto alla gestione delle relazioni con i fornitori di servizi cloud.

Il personale con responsabilità dirette relativamente ai servizi su cloud pubblico è formato sulle tecnologie cloud, sulle disposizioni in materia di trattamento di dati personali.

- Separazione degli ambienti virtuali: ADVINSER S.R.L. adotta un'architettura multi-tenant con forte isolamento logico tra i dati e gli ambienti di ogni Cliente. Ogni Cliente opera sulla propria istanza virtuale logica, con controllo degli accessi e meccanismi di segregazione dei dati che impediscono l'accesso incrociato tra i dati di diversi Clienti.

- Gestione delle identità digitali: la gestione delle identità digitali è una componente essenziale per garantire la sicurezza dei dati nel cloud computing. ADVINSER S.R.L. garantisce una loro corretta gestione durante tutto il ciclo.
- Gestione dei Log: ADVINSER S.R.L. dispone delle necessarie informazioni relative ai log di monitoraggio e garantisce l'accesso ai soli utenti autorizzati. I log delle attività svolte dai clienti sull'applicazione vengono loggati sul Database
- Sicurezza delle applicazioni Web: il cloud è, in genere, un ambiente aperto. Questo aspetto aumenta significativamente l'esposizione agli attacchi. Per questa ragione ADVINSER S.R.L. sottopone a controlli suppletivi le applicazioni web che si interfacciano con ambienti Cloud pubblici.
- Disaster Recovery: sui dati conservati in Cloud, ADVINSER S.R.L. effettua verifiche puntuali per garantire la loro disponibilità anche in caso di disastro.
- Indagini informatiche: In caso di richiesta legale vincolante da parte di autorità governative per la divulgazione dei PII del Cliente, ADVINSER S.R.L. si impegna a notificare tempestivamente il Cliente, a meno che tale notifica non sia proibita dalla legge applicabile.

Per garantire la massima trasparenza e conformità normativa nella gestione della sicurezza, ADVINSER S.R.L. si impegna a definire, documentare e conservare tutte le politiche e le linee guida di sicurezza amministrativa.

- Trattamento dei dati personali: i ruoli e le responsabilità nell'ambito del trattamento dei dati personali conservati riportati all'interno del Registro dei Trattamenti dei ADVINSER S.R.L.

Nel seguito vengono descritte le principali attività necessarie per recepire i requisiti sopra riportati.

1. RUOLI E RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

Per consentire un'efficace attività di gestione dei servizi cloud ADVINSER S.R.L. assicura che:

- Il personale con responsabilità dirette relativamente ai servizi su cloud è formato sulle tecnologie cloud, sulle disposizioni in materia di trattamento di dati personali.
- Nel caso di acquisizione di servizi cloud sul mercato, sulla gestione dei fornitori sono definiti e documentati i diversi ruoli e responsabilità per il personale responsabile della gestione del servizio cloud, sono formalizzati Quality Technical agreement per assicurare il livello del servizio erogato, sono inoltre sottoscritti NDA a garanzia della sicurezza e riservatezza delle informazioni.
- Tali ruoli sono condivisi anche con i clienti quando ADVINSER S.R.L. opera in qualità di CSP. Mediante le condizioni specifiche del servizio cloud SaaS sono state identificate le responsabilità del CPS e del Cliente finale.

L'identità del Responsabile del trattamento, è la seguente:

ADVINSER S.R.L.

Sede legale e operativa: Via Martiri della libertà 1- 53041 Asciano (SI)

Contatti: e-mail mail@advinser.it

Telefono: [+39 0577 1911900](tel:+3905771911900)

Il controllo della gestione in sicurezza dell'infrastruttura Cloud è assicurato da un team di tecnici specialisti composto da risorse interne all'organizzazione ADVINSER S.R.L. e da fornitori esterni qualificati.

Per informazioni di dettaglio:

- Team per la sicurezza – isirt@advinser.it
- DPO - dpo@advinser.it

7. SEDE GEOGRAFICA TRATTAMENTO DEI DATI

I servizi cloud di ADVINSER S.R.L. sono hostati su AWS S.p.A, dotate dei più alti standard di sicurezza disponibili sul mercato e residenti in server farm geograficamente distribuite nel rispetto delle policy di business del prodotto e delle normative vigenti.

Per informazioni di dettaglio:

- Team per la sicurezza – isirt@advinser.it

8. GESTIONE DEGLI ASSET E CLASSIFICAZIONE DELLE INFORMAZIONI

L'accesso agli asset del cliente avviene in relazione alle disposizioni contrattuali ed in conformità con le disposizioni legislative.

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, ADVINSER S.R.L. si impegna ad informare costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza dei dati e di privacy applicate.

Questi impegni includono:

- Accesso e proprietà: il cliente conserva il pieno controllo dei propri contenuti. La proprietà dei dati rimane al cliente.
- Divulgazione dei contenuti dei clienti: ADVINSER S.R.L. non divulga i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale;
- Controlli di Sicurezza: ADVINSER S.R.L. adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e confidenzialità.

9. GESTIONE ACCESSI UTENTE

Il Servizio SaaS offerto da ADVINSER S.R.L. è un'applicazione web accessibile via browser. Tra le soluzioni disponibili vi sono piattaforme SaaS come MES, Quality-Control, NFT Platform e MainFlow per la gestione di ticket, asset e contratti.

All'accesso, l'utente inserisce le credenziali fornite da ADVINSER S.R.L.; al primo login è previsto il cambio obbligatorio della password. Dopo il login, viene mostrata la homepage della piattaforma, con una dashboard e un menu laterale per navigare tra le varie sezioni disponibili.

Il Cliente è responsabile della gestione degli account dei propri utenti: tramite il pannello di amministrazione può creare, modificare o eliminare utenti, assegnare ruoli e privilegi, e revocare l'accesso in qualsiasi momento. È inoltre possibile concordare con ADVINSER S.R.L. la gestione delegata degli account utenti, nel caso in cui serva un supporto diretto da parte loro.

Alla cessazione del contratto, i dati del Cliente saranno conservati per un periodo stabilito per consentirne l'esportazione. Su richiesta del Cliente, o su sollecito di ADVINSER S.R.L., questi dati possono essere restituiti tramite download su OneDrive o similare piattaforma di sharing dati, in base al volume dei dati da consegnare.

10. GESTIONE DELLE CREDENZIALI

La piattaforma assicura una gestione sicura di tutte le credenziali, incluse le password degli utenti.

A tal fine, ci impegniamo a fornire meccanismi tecnici che impongano l'uso di password complesse e uniche, a non memorizzare mai le password in chiaro e a supportare l'autenticazione a più fattori (MFA) per un ulteriore livello di protezione. Le nostre procedure di ripristino delle password sono progettate per garantire che solo gli utenti autorizzati possano recuperare l'accesso ai propri account. Spetta al cliente e al suo personale la responsabilità di mantenere la riservatezza delle credenziali, di non condividerle e di segnalare tempestivamente qualsiasi sospetto di compromissione.

11. VIRTUALIZZAZIONE SUI SISTEMI ACQUISITI SUL MERCATO

La maggior parte dei controlli di separazione logica non sono fisici. ADVINSER S.R.L. opera per garantire, nell'ambiente virtuale, un livello di sicurezza della separazione dei sistemi almeno analogo a quello degli ambienti fisici.

Per consentire un'efficace protezione dei sistemi virtuali:

- in fase di valutazione del fornitore sono valutate le politiche di sicurezza adottate prestando particolare attenzione all'adozione di standard e best practice riconosciuti.
Le politiche, a titolo esemplificativo, contemplano i seguenti aspetti:
- disabilitazione (o rimozione) di tutte le interfacce, porte, servizi e dispositivi non strettamente necessari;
- configurazione con principi di sicurezza delle informazioni di tutte le interfacce di rete virtuali e le aree di archiviazione;
- limiti sull'utilizzo delle risorse della VM;
- hardening (adozione di politiche di sicurezza) di tutti i sistemi operativi e delle applicazioni in esecuzione all'interno della macchina virtuale;
- validazione dell'integrità delle operazioni di gestione delle chiavi crittografiche;
- assicura che i seguenti controlli siano applicati:
- accesso agli access log amministrativi;

- registrazione di tutti i log.
- ADVINSER S.R.L., identifica l'elenco completo dei suoi fornitori coinvolti nella gestione del cloud per l'erogazione del servizio contrattualizzato. Nel caso vi siano anche dati personali (PII), ADVINSER S.R.L. assicura l'adempimento di quanto previsto dalla normativa vigente sul trattamento dei dati personali. Il cliente in qualsiasi momento può acquisire informazioni sull'elenco completo dei fornitori coinvolti facendone specifica richiesta alla mail mail@advinser.it.

12. SEPARAZIONE DEGLI AMBIENTI

La separazione dei diversi sistemi logici che coesistono su una infrastruttura Cloud è una delle principali misure per garantire la riservatezza e l'integrità dei dati memorizzati oltre che la sicurezza di tutta l'infrastruttura di erogazione del servizio.

ADVINSER S.R.L implementa una segregazione logica degli ambienti, assicurando che i dati e le risorse di ciascun cliente siano isolati e non accessibili ad altri clienti.

Pur operando talvolta sullo stesso sistema multi-tenant, le funzionalità del servizio impediscono che altri utenti possano inavvertitamente o intenzionalmente visualizzare o modificare i dati di un altro. Questa segregazione logica degli ambienti è un requisito fondamentale per la sicurezza e la conformità normativa, in quanto assicura che il cliente mantenga il controllo totale e la riservatezza dei propri dati sensibili.

Le credenziali e i diritti di accesso sono gestiti in modo sicuro per prevenire conflitti o abusi. Il cliente è responsabile della corretta gestione degli account del proprio personale e della tempestiva revoca degli accessi non più necessari.

Il fornitore esterno di cloud service dovrà fornire a ADVINSER S.R.L., se richiesto, tutto il supporto necessario a verificare che tale segregazione sia garantita anche quando venissero richiesti elementi di segregazione addizionali nel rispetto delle proprie politiche.

13. GESTIONE DELLE IDENTITÀ DIGITALI

La gestione delle identità digitali deve rispettare quanto previsto nel documento "POL.03_Politica controllo accessi"

14. GESTIONE DEI LOG

Quando ADVINSER

S.R.L. utilizza servizi di Cloud Pubblico di terzi, deve rispettare quanto previsto nella procedura di riferimento per i sistemi in gestione e concordare con il fornitore le caratteristiche dei log necessari.

Nel caso ADVINSER S.R.L. operi in qualità di CSP, il servizio deve garantire ai suoi clienti la possibilità di definire

puntualmente i requisiti di monitoraggio in particolare per quanto riguarda tutte le operazioni che richiedono privilegi amministrativi.

15. BACKUP

I dati del Cliente vengono sottoposti a backup completi giornalieri che vengono poi depositati su un server dedicato. I dati sono recuperabili per 4 settimane.

16. SICUREZZA DELLE APPLICAZIONI WEB

Nel caso di servizi cloud acquisiti sul mercato, ADVINSER S.R.L. ha a disposizione un team (TEAM ISIRT) per gestire gli incidenti di sicurezza e adottare delle linee guida per lo sviluppo delle applicazioni Web che garantisca almeno le misure della PRO.09_Procedura Sviluppo Sicuro e della PRO.05_Procedura di gestione della continuità operativa.

17. DISASTER RECOVERY

I piani di continuità operativa e disaster recovery (BCDR) sono testati annualmente per assicurare la loro efficacia e tempi di recupero (RTO) e punti di recupero (RPO) definiti.

18. INDAGINI INFORMATICHE

Ai clienti dei servizi cloud verrà garantito il massimo supporto, nel rispetto della normativa vigente, nel caso questi avviassero delle indagini sui servizi acquisiti.

Nel caso di servizi cloud acquisiti sul mercato, per consentire un'efficace attività di investigazione, deve essere concordata, con il fornitore qualificato per i servizi cloud, la modalità per la richiesta di dati necessari ad indagini interne ovvero a seguito di richiesta alle autorità legali competenti.

19. REQUISITI CONTRATTUALI

L'adozione dei servizi sul cloud a mercato possono comportare maggiori rischi rispetto all'integrità, riservatezza e disponibilità dei dati. Per questa ragione, i contratti che hanno come oggetto la fornitura di servizi su Cloud Pubblico, devono almeno prevedere:

- Una dichiarazione di "NDA - Non Disclosure Agreement";
- l'espressa dichiarazione che il cliente conserverà il diritto "esclusivo" alla proprietà dei dati per tutta la durata dell'accordo. La proprietà include tutte le copie dei dati disponibili presso il CSP, comprese eventuali copie dei supporti di backup;
- l'espresso divieto per il CSP di utilizzare i dati delle agenzie statali per marketing e/o pubblicità o qualsiasi altro scopo secondario non autorizzato;
- l'indicazione del paese(i) in cui è accettabile che i dati vengano conservati;

- che la normativa sulla protezione dei dati personali applicabile sia conforme alla normativa europea;
- il Service Level Agreement (SLA) del servizio;
- l'obbligo da parte del CSP di informare senza ingiustificato ritardo in merito a qualsiasi violazione dei dati, sia questa confermata o sospetta;
- l'obbligo per il CSP di eliminare completamente qualsiasi traccia di dati/informazioni, al termine dell'Accordo, da tutti i suoi sistemi;
- le modalità con cui il CSP restituirà i dati al termine dell'accordo.

I requisiti di cui sopra andranno rispettati anche nella contrattualizzazione di servizi quando ADVINSER S.R.L. opera in qualità di CSP verso i suoi clienti.

20. PRIVACY E TRATTAMENTO DEI DATI PERSONALI

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, il cliente del servizio Cloud, in qualità di Titolare o Responsabile del trattamento, provvede a nominare il CSP, quale Responsabile o Sub- Responsabile del trattamento, con un atto formale.

ADVINSER S.R.L. si impegna a monitorare costantemente lo scenario in continua evoluzione di regolamenti e leggi riguardanti la privacy al fine di identificare i cambiamenti e determinare gli strumenti di cui i clienti potrebbero avere necessità per le esigenze di conformità, in funzione delle loro applicazioni.

ADVINSER

S.R.L. si impegna ad informare costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza dei dati e di privacy applicate.

Questi impegni includono:

- **Accesso e proprietà:** il cliente conserva il pieno controllo dei propri contenuti. La proprietà dei dati rimane al cliente;
- **Divulgazione dei contenuti dei clienti:** ADVINSER S.R.L. non divulgherà i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale;
- **Controlli di Sicurezza:** ADVINSER S.R.L. adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e confidenzialità.

21. MODALITA' DI AGGIORNAMENTO

Eventuali modifiche ai contenuti del presente documento sono comunicate ai clienti attraverso gli applicativi con accesso ad Internet o al servizio Cloud ADVINSER

S.R.L. oppure, segnalate mediante il documento di rilascio alla prima release del software successiva alla modifica di cui in discorso.

La Versione aggiornata del presente documento è comunque sempre consultabile al sito internet <https://advinser.it/> in calce alla Home Page.