# Documento informativo sulla Sicurezza delle Informazioni per i servizi Cloud

## 1. Introduzione

Il presente documento, redatto in linea con la ISO 27001:2024 con le estensioni previste dalla ISO 27017:2021, ha lo scopo di fornire ai clienti la descrizione delle principali misure tecniche e organizzative adottate da Mediaus S.r.l. per la protezione delle informazioni nell'ambito dell'erogazione dei servizi cloud, in particolare quelli SaaS.

Le misure descritte sono definite e mantenute in coerenza con il Sistema di Gestione per la Sicurezza delle Informazioni e tengono conto del modello di responsabilità condivisa proprio dei servizi cloud, nel quale Mediaus s.r.l. opera in qualità di fornitore di servizi SaaS avvalendosi di infrastrutture IaaS o PaaS di terze parti.

Il documento ha finalità informativa e consente ai clienti di comprendere le principali caratteristiche di sicurezza del servizio, nonché la ripartizione delle responsabilità e le modalità di gestione dei rischi.

## 2. Modello di responsabilità

Il modello di responsabilità in essere prevede il coinvolgimento di tre tipologie di soggetti: Mediaus, cloud provider e cliente. A seconda del ruolo svolto nella progettazione, erogazione e fruizione del servizio SaaS, si differenziano le loro responsabilità.

Mediaus s.r.l. identifica e gestisce gli asset rilevanti per l'erogazione del servizio, al fine di garantirne un'adeguata protezione in relazione ai rischi associati. Mediaus S.r.l. assicura la segretezza e la sicurezza dell'archiviazione dei dati, ma non risponde della correttezza, della conformità e della esattezza dei dati inseriti, la cui responsabilità incombe sul cliente.

Mediaus s.r.l. assicura che il personale coinvolto nell'erogazione del servizio sia adeguatamente formato e sensibilizzato in materia di sicurezza delle informazioni, attraverso attività periodiche di formazione e aggiornamento, al fine di garantire un comportamento coerente con le politiche di sicurezza adottate.

La sicurezza del servizio è gestita secondo un modello di responsabilità condivisa, nel quale Mediaus s.r.l. è responsabile della sicurezza applicativa, della gestione del servizio SaaS e della protezione dei dati trattati, mentre il fornitore IaaS/PaaS è responsabile della sicurezza dell'infrastruttura/piattaforma sottostante.

Mediaus s.r.l. definisce e assegna ruoli e responsabilità in materia di sicurezza delle informazioni nell'ambito della propria organizzazione, al fine di garantire una gestione efficace e coordinata delle misure di sicurezza adottate.

Mediaus S.r.l., in qualità di fornitore del Servizio SaaS, definisce e mantiene ruoli, competenze e responsabilità connesse ai processi di progettazione, sviluppo ed erogazione del Servizio, applicando i principi di segregazione delle mansioni (*segregation of duties*), privilegio minimo (*least privilege*) e controllo duale (*dual control*), coerentemente con quanto stabilito dal provider.

Nell'ambito dei processi operativi del Servizio, le attività sono strutturate in sequenze procedurali eseguite da soggetti differenti, al fine di evitare che il controllo dell'intero processo sia attribuito a un singolo individuo.

I diritti di accesso a locali, apparati, dati e funzionalità sono attribuiti al personale addetto esclusivamente nella misura necessaria all'espletamento delle mansioni assegnate, in applicazione del principio del privilegio minimo.

I cloud provider selezionati documentano e comunicano le proprie capacità di sicurezza, i ruoli e le responsabilità applicabili al servizio erogato, nonché le responsabilità che restano in capo al cliente; tali informazioni sono recepite e incorporate nei documenti interni, nella matrice di responsabilità e nei contratti. La protezione degli hypervisor e dei componenti del piano di controllo dell'infrastruttura è responsabilità del fornitore IaaS/PaaS e viene verificata da Mediaus S.r.l. attraverso attestazioni e report indipendenti, mentre la progettazione del servizio assicura l'utilizzo di controlli di isolamento e segmentazione coerenti con le buone pratiche.

**Tabella di responsabilità per i prodotti SaaS di Mediaus**

| Ambito | Responsabilità |
|---|---|
| Infrastruttura/Piattaforma Cloud | Provider |
| Piattaforma di virtualizzazione | Provider |
| Protezione fisica dei Data center | Provider |
| Controlli di sicurezza fisica e logica | Provider |
| Monitoraggio, gestione e sicurezza dell'infrastruttura | Provider |
| Applicazioni | Mediaus |
| Dati caricati sul servizio | Cliente |
| Configurazioni applicative | Mediaus |
| Gestione utenti finale | Mediaus |
| Sicurezza di rete | Provider |
| Sicurezza dell'infrastruttura | Provider |
| Monitoraggio e logging | Provider |
| Gestione degli accessi privilegiati | Provider |

### 3. Gestione degli accessi e delle identità

L'accesso al servizio è consentito esclusivamente agli utenti autorizzati. La gestione degli utenti e dei relativi diritti di accesso è effettuata dal cliente mediante funzionalità dedicate.

L’assegnazione dei diritti di accesso avviene sulla base di ruoli definiti, al fine di garantire che ciascun utente disponga esclusivamente delle autorizzazioni necessarie allo svolgimento delle proprie attività.

Sulla base dell’analisi del rischio effettuata dal cliente, possono essere implementati meccanismi di autenticazione coerenti con il livello di rischio conseguente. Per gli utenti con privilegi amministrativi è prevista l’attivazione dell’autenticazione a più fattori.

Le credenziali sono gestite in modo da garantirne la riservatezza e non sono accessibili in chiaro.

All’attivazione del Servizio, MEDIAUS provvede alla creazione delle utenze necessarie; le credenziali possono essere modificate in autonomia dagli Utenti autorizzati dal Cliente. Al termine della procedura di registrazione al Servizio, il Cliente ottiene l'assegnazione di un Nome Utente o user ID e di una password riservati (Dati di Accesso o account) dei quali il Cliente stesso è unico ed esclusivo responsabile, anche in ordine alle attività realizzate tramite il loro utilizzo. Il Cliente, pertanto, si impegna a:

a) comunicare immediatamente a MEDIAUS qualsiasi utilizzo non autorizzato della propria password o del proprio account nonché qualsiasi altra violazione delle regole di sicurezza di cui venga a conoscenza;

b) uscire dal proprio account al termine di ogni sessione. MEDIAUS non potrà in alcun modo essere ritenuta responsabile per eventuali danni derivanti dal mancato rispetto della presente regola.

Il Cliente è consapevole che, al fine di regolare l'accesso al Servizio, la propria autenticazione è rimessa esclusivamente alla verifica dell'account del Nome Utente e della Password utilizzati dallo stesso. Il Cliente è quindi responsabile della custodia e del corretto utilizzo del proprio account, del Nome Utente e della password per accedere al Servizio, nonché di ogni conseguenza dannosa o pregiudizio che dovesse derivare, a carico di MEDIAUS ovvero di terzi, a seguito del non corretto utilizzo, dello smarrimento, sottrazione e/o compromissione della riservatezza dell'account, del Nome Utente e della password utilizzata dal Cliente. Ogni Prodotto SaaS include funzionalità per la registrazione delle utenze e la loro disattivazione/annullamento secondo i profili autorizzativi definiti dal Cliente.

Tutte le operazioni effettuate per il tramite dell'account, del Nome Utente e della password utilizzati dal Cliente comportano l'automatica attribuzione allo stesso delle operazioni condotte e delle richieste effettuate, senza eccezioni di sorta. Il Cliente riconosce e prende atto che MEDIAUS potrà sempre produrre, quale prova delle operazioni effettuate dal Cliente e - più in generale - dei rapporti con il Cliente stesso, anche mezzi di prova ricavabili dai sistemi e dalle procedure informatiche utilizzate da MEDIAUS per regolare l'accesso al Servizio.

Il Cliente potrà comunicare i Dati di Accesso esclusivamente ai propri dipendenti che debbano utilizzare tali Dati in esecuzione delle loro mansioni. Non appena il Cliente dovesse avere conoscenza di un uso di tali Dati non conforme a quanto contrattualmente previsto dovrà immediatamente segnalare l’evento a MEDIAUS. Al ricevimento di tale segnalazione, MEDIAUS potrà disabilitare l’accesso al servizio. In tal caso la riattivazione del servizio verrà effettuata solo dopo il ricevimento da parte di MEDIAUS di apposita comunicazione scritta del Cliente.

**4. Logging e monitoraggio**

Le risorse e i servizi sono organizzati secondo criteri di segregazione logica, al fine di garantire l'isolamento tra ambienti, utenti e componenti del sistema.

I log sono protetti da accessi non autorizzati e alterazioni e sono conservati per un periodo coerente con le esigenze operative, di sicurezza e di conformità normativa.

L'accesso alle informazioni di log è limitato ai soggetti autorizzati.

Se richiesto, Mediaus S.r.l. mette a disposizione dei clienti capacità di logging pertinenti al proprio tenant. Al riguardo, i sistemi in essere permettono la registrazione, la memorizzazione e l'analisi dei log, in particolare:

- Accessi al sistema
- Disponibilità dei sistemi
- Anomalie operative
- Performance delle risorse
- Operazioni amministrative
- Attività privilegiate
- Eventi di sicurezza

I clienti sono informati su eventi rilevanti che possono compromettere il servizio. Le comunicazioni vengono effettuate tempestivamente tramite mail ai referenti di progetto.

I sistemi adottano meccanismi di sincronizzazione temporale basati su fonti affidabili, al fine di garantire la coerenza degli eventi registrati e supportare le attività di monitoraggio, analisi e gestione degli incidenti.

**5. Backup e continuità operativa**

Le risorse utilizzate per l'erogazione del servizio sono monitorate e gestite al fine di garantire adeguati livelli di capacità e prestazioni, anche in funzione della scalabilità delle soluzioni cloud adottate e per prevenire incidenti di sicurezza riconducibili a carenze di risorse, quali indisponibilità, degradi di servizio o malfunzionamenti dei controlli di sicurezza.

Qualora siano necessarie attività straordinarie di adeguamento della capacità che possano influire temporaneamente sulle prestazioni o sulla disponibilità, i clienti sono informati mediante i canali ufficiali con indicazione della finestra operativa.

Sono effettuati backup periodici dei dati, con frequenza giornaliera e retention definita. I backup sono conservati su infrastrutture separate rispetto ai sistemi primari.

I backup sono protetti mediante misure di sicurezza adeguate al fine di prevenire accessi non autorizzati, alterazioni o perdite di dati.

Per quanto riguarda i prodotti SaaS, la struttura dei backup, i controlli, la verifica, i test, sono a carico di Mediaus che garantisce al Cliente la conservazione configurabile del backup (esempio: backup

incrementali giornalieri degli ultimi 7 giorni; backup settimanali per 3 mesi), possibilità di ripristino granulare, protezione in base alle sue esigenze. I sistemi di backup prevedono sistemi di notifica in caso di problemi.

Il Cliente può decidere in autonomia le proprie politiche di backup; non dispone dei backup eseguiti da Mediaus, ma ne può richiedere copia in qualsiasi momento. Esistono ulteriori snapshot automatiche delle vm rese immutabili nel datacenter secondario del provider per una settimana.

| ATTIVITÀ | MEDIAUS | CLIENTE |
|---|---|---|
| Progettazione ed esecuzione backup | Progetta ed esegue i backup dei prodotti SaaS, assicurandone il corretto funzionamento. | |
| Controlli, verifiche e test backup | Effettua controlli, verifiche e test periodici per assicurare l'affidabilità dei backup. | |
| Conservazione configurabile | Garantisce la conservazione secondo parametri concordati. | Concorda i parametri di conservazione previsti dal contratto. |
| Ripristino granulare | Fornisce la possibilità di ripristino granulare come da accordi contrattuali. | Richiede il ripristino quando necessario secondo le modalità contrattuali. |
| Protezione dei backup | Applica i livelli di protezione concordati per i backup. | |
| Copertura delle componenti | Include nei backup le componenti funzionali del servizio, la gestione utenti e le componenti architetturali secondo le procedure aziendali. | |
| Notifiche di anomalia | Attiva sistemi di notifica automatica in | Riceve le notifiche, prende atto e segue le istruzioni |

| | | |
|---|---|---|
| | caso di problemi relativi ai backup. | contrattuali se previste. |
| Snapshot orarie e immutabilità | Esegue snapshot automatiche orarie, le consolida in quattro a fine giornata e le rende immutabili nel data center secondario per una settimana. | |
| Accesso e richieste di copia | Non concede accesso diretto ai backup; fornisce copia su richiesta secondo contratto. | Non accede direttamente ai backup; può richiederne copia secondo le modalità contrattuali. |
| Politiche di backup del cliente | | Definisce in autonomia le proprie politiche di backup interne (esportazioni, copie locali) per ciò di cui è direttamente responsabile. |

Mediaus S.r.l. definisce inoltre livelli di disponibilità dei servizi in funzione delle caratteristiche delle soluzioni offerte e delle infrastrutture utilizzate. Tali livelli sono disciplinati nei rapporti contrattuali con i clienti e possono prevedere specifici obiettivi di disponibilità su base mensile, che, a seconda del servizio, si attestano in ogni caso indicativamente fino al 97%.

Sono implementate, per i servizi cloud, procedure di disaster recovery che prevedono:

- Replica geografica dei sistemi critici
- Piani di ripristino documentati
- Test periodici di DR

Definizione di RTO e RPO per i servizi erogati.

## 6. Classificazione delle informazioni

Le informazioni gestite internamente sono soggette, ove applicabile, a meccanismi di etichettatura coerenti con il sistema di classificazione adottato, al fine di garantirne una gestione e protezione adeguata lungo il ciclo di vita.

Mediaus s.r.l. adotta un sistema di classificazione delle informazioni basato su policy interne di sicurezza, al fine di garantire un'adeguata protezione in funzione della sensibilità delle informazioni trattate.

Per quanto riguarda i dati inseriti nel servizio, la classificazione delle informazioni è di responsabilità del cliente, che definisce il livello di protezione necessario in relazione alle proprie esigenze e al contesto di utilizzo. Al riguardo, i prodotti SaaS offerti prevedono per il cliente la possibilità di classificare o etichettare le informazioni e le risorse associate, attivabile in base alle specifiche progettuali.

## 7. Isolamento e segregazione in ambienti multi-tenant

Il servizio è progettato per ambienti multi-tenant e adotta meccanismi di segregazione logica per garantire l'isolamento tra i clienti e tra ambienti distinti. L'isolamento copre i livelli dati, applicazioni virtualizzate, sistemi operativi, storage e rete, mediante configurazioni dedicate del perimetro, segmentazione, separazione degli spazi di archiviazione e scoping dei dati a livello di tenant. Le attività di amministrazione interna di Mediaus S.r.l. sono mantenute separate dalle risorse utilizzate dai clienti, applicando il principio del minimo privilegio, canali di gestione dedicati e controlli di accesso indipendenti.

## 7. Crittografia

Mediaus s.r.l. adotta un approccio strutturato all'utilizzo della crittografia per la protezione dei dati, in coerenza con le proprie politiche di sicurezza.

I dati sono protetti in transito mediante protocolli sicuri (es. HTTPS/TLS) e a riposo mediante meccanismi di cifratura dello storage.

La gestione delle chiavi crittografiche è affidata al fornitore IaaS, selezionato anche in funzione delle modalità di gestione delle chiavi e delle garanzie di sicurezza offerte.

L'utilizzo della crittografia è disciplinato da criteri e policy interne che definiscono le modalità di applicazione in funzione dei rischi e della natura delle informazioni trattate.

La gestione delle chiavi crittografiche è effettuata secondo modalità che garantiscono adeguati livelli di sicurezza lungo il ciclo di vita delle stesse, anche quando tale gestione è demandata al fornitore IaaS o PaaS.

## 8. Restituzione, rimozione e cancellazione dei dati alla cessazione

Alla cessazione del rapporto contrattuale, il cliente può richiedere l'esportazione dei propri dati del servizio in formati documentati, secondo le modalità descritte nella documentazione del servizio.

Completate le attività di restituzione, Mediaus S.r.l. procede alla disattivazione del tenant e alla rimozione degli asset del cliente dai sistemi applicativi di produzione.

L'organizzazione assicura che i periodi di conservazione dei dati definiti dai clienti siano implementati e rispettati nei sistemi applicativi di produzione. Eventuali persistenze residue nei sistemi di backup, gestiti direttamente o tramite fornitori di infrastruttura cloud, sono limitate al tempo strettamente necessario per esigenze di continuità operativa, non eccedente i cicli tecnici di retention, e non consentono l'accesso o il riutilizzo dei dati per finalità operative.

La cancellazione è effettuata mediante metodologie conformi alle buone pratiche di sicurezza delle informazioni e adeguate alle caratteristiche dell'infrastruttura sottostante, assicurando l'impossibilità di recupero non autorizzato dei dati.

Il perimetro degli asset interessati comprende i dati del cliente del servizio cloud (contenuti applicativi, configurazioni del tenant e allegati), nonché i dati derivati dal servizio pertinenti al tenant del cliente, come descritto nella documentazione del servizio.

Le tempistiche e le fasi del processo (disattivazione, esportazione dati, rimozione da produzione, cancellazione da backup/archivi) sono definite, documentate e comunicate al cliente, e possono essere oggetto di evidenze su richiesta.

**9. Gestione delle vulnerabilità**

L'infrastruttura cloud è soggetta ad un processo continuo di vulnerability management da parte del provider, ove le vulnerabilità critiche sono gestite con priorità elevata. I prodotti SaaS, ove sia richiesto dalle normative o dal cliente, sono sottoposti a Vulnerability Assessment o Penetration Test.

Mediaus S.r.l. adotta criteri di hardening per le macchine virtuali e i componenti di sistema impiegati nell'erogazione del servizio, assicurando che siano abilitati esclusivamente porte, protocolli e servizi necessari e che siano implementate adeguate misure tecniche, quali protezioni anti-malware ove pertinenti, logging e monitoraggio.

**10. Gestione delle modifiche**

Le modifiche al servizio sono gestite mediante un processo strutturato che prevede la classificazione delle modifiche, l'analisi degli impatti, la valutazione dei rischi, l'esecuzione di test, l'approvazione da parte delle funzioni competenti e la completa tracciabilità delle attività svolte.

Il processo di gestione delle modifiche considera anche gli impatti sui dati e sui servizi dei clienti, inclusi gli effetti su disponibilità, integrità e sicurezza delle informazioni trattate.

Le modifiche sono classificate in base alla loro criticità e tipologia (ordinaria, significativa, urgente) e sono gestite secondo livelli di controllo proporzionati al rischio.

Le modifiche sono comunicate ai clienti secondo criteri proporzionati alla loro criticità. In particolare, le modifiche non urgenti con impatto significativo sono comunicate con un preavviso minimo di 10 giorni lavorativi, mentre le modifiche urgenti possono essere implementate senza preavviso, con successiva informazione al cliente.

L’organizzazione tiene conto delle modifiche introdotte dai fornitori di servizi infrastrutturali (IaaS/PaaS) utilizzati per l’erogazione del servizio, valutandone gli impatti sul servizio SaaS e assicurando la comunicazione ai clienti nei casi in cui tali modifiche possano influire sui servizi erogati o sui dati trattati.

Mediaus S.r.l. identifica le operazioni critiche la cui esecuzione, in caso di errore, può comportare danni non recuperabili agli asset trattati nel servizio, e disciplina tali operazioni mediante procedure formalizzate, approvate, tracciate e soggette a supervisione e controllo degli accessi. A titolo esemplificativo, rientrano tra le operazioni critiche l’installazione, la modifica e la cancellazione di componenti virtualizzati e risorse (ad esempio server, reti e storage), le procedure di cessazione del servizio e le attività di backup e ripristino.

Su richiesta, Mediaus S.r.l. mette a disposizione dei clienti la documentazione di riferimento relativa a tali operazioni critiche, al fine di consentire una corretta valutazione dell’impatto e il coordinamento delle attività.

**11. Sviluppo sicuro**

Il servizio è sviluppato secondo principi di sicurezza integrati nel ciclo di vita del software.

I requisiti di sicurezza sono definiti nelle fasi di progettazione e sviluppo e sono mantenuti lungo tutte le fasi del ciclo di vita.

Mediaus s.r.l. adotta linee guida per lo sviluppo sicuro al fine di garantire la protezione delle informazioni e la resilienza del servizio.

Le attività di sviluppo sono disciplinate da linee guida e policy interne che definiscono i principi di sviluppo sicuro adottati.

Ove richiesto dal cliente, è possibile esporgli le opzioni di configurazione relative alle macchine virtuali o ai componenti sottostanti, le impostazioni raccomandate di hardening, le porte/protocolli/servizi da mantenere abilitati, e le misure tecniche disponibili, al fine di supportare l’adozione di configurazioni sicure.

**12. Gestione dei fornitori**

Mediaus s.r.l. adotta criteri e principi per la selezione e gestione dei fornitori, al fine di garantire che i servizi erogati da terze parti siano coerenti con i requisiti di sicurezza delle informazioni.

I requisiti di sicurezza applicabili ai fornitori sono definiti e formalizzati nell’ambito dei rapporti contrattuali.

I fornitori sono valutati sulla base di requisiti di sicurezza, affidabilità e conformità e sono oggetto di monitoraggio e riesame periodico; vengono scelti quelli in possesso delle certificazioni UNI EN ISO 9001:2015, UNI EN ISO 27001:2022 con estensione alle linee guida ISO/IEC 27017:2021. I data center dei fornitori sono localizzati in Unione Europea, in particolare in Italia, Spagna e Francia, e sono tutti Tier IV.

Le modifiche rilevanti ai servizi forniti da terze parti sono valutate al fine di analizzarne l'impatto sulla sicurezza delle informazioni e sulla continuità del servizio.

Sono considerati i rischi derivanti dalla catena di fornitura ICT, inclusi eventuali fornitori indiretti.

I fornitori cloud sono considerati parte integrante della catena di fornitura e i relativi rischi sono gestiti in funzione dell'impatto sui servizi erogati.

**12. Gestione degli incidenti**

Sono definite procedure per la gestione degli incidenti di sicurezza delle informazioni.

Sono individuati ruoli e responsabilità per garantire una risposta efficace e coordinata.

Gli eventi possono essere segnalati tramite canali dedicati sia da parte degli utenti interni sia da parte dei clienti.

Le evidenze relative agli incidenti sono raccolte, conservate e protette al fine di supportare le attività di analisi e, ove necessario, eventuali esigenze legali o forensi.

**13. Conformità normativa**

Mediaus s.r.l. identifica e mantiene, ove applicabile, contatti con le autorità competenti in materia di sicurezza delle informazioni e protezione dei dati, al fine di garantire la corretta gestione di eventuali eventi che richiedano il coinvolgimento di soggetti istituzionali.

Mediaus s.r.l. identifica e monitora i requisiti normativi e regolamentari applicabili al servizio.

Sono tutelati i diritti di proprietà intellettuale relativi al software e sono rispettati i diritti di terzi.

I registri e le informazioni rilevanti sono protetti al fine di garantirne l'integrità e la disponibilità.

L'utilizzo della crittografia avviene in conformità alle normative applicabili.

**14. Miglioramento continuo**

La sicurezza delle informazioni è oggetto di riesami periodici, anche da parte di soggetti indipendenti rispetto alle attività operative.

Mediaus S.r.l. si impegna a mantenere e migliorare nel tempo le misure di sicurezza adottate, in funzione dell'evoluzione tecnologica, dei rischi emergenti e del contesto normativo.