# *POL 523a*

# *Politica di Erogazione dei Servizi in Cloud*

**ATTENZIONE:**

- Il presente documento è disponibile in copia originale nella rete aziendale.
- Ogni copia cartacea si ritiene copia di lavoro **non controllata**.
- È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

Rev 02 del 26/08/2024

Classificazione: PUBBLICO

| INDICE DELLE REVISIONI | | | | | |
|---|---|---|---|---|---|
| VERSIONE | DATA | OGGETTO | REDATTO | VERIFICATO | APPROVATO |
| 01 | 06.04.2023 | Prima emissione | COO | RSGI | CEO |
| 02 | 26.08.2024 | Aggiornamento e separazione delle politiche di Erogazione e d'Uso dei Servizi in Cloud | Michele Gobbo | RSGI | CEO |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# *Sommario*

# 1. Introduzione

Lo scopo del presente documento è quello di descrivere i principi generali definiti da LARUS al fine di erogare servizi in modalità Cloud.

Il Cloud Computing è generalmente accettato come composto dai seguenti tipi di servizi:

- **Software-as-a-Service (SaaS)**: la fornitura di un'applicazione ospitata da utilizzare come parte di un processo aziendale. L'hosting di solito include tutti i componenti di supporto per l'applicazione come hardware, software operativo, database ecc.
- **Platform-as-a-Service (PaaS)**: vengono forniti hardware e software di supporto come sistema operativo, database, piattaforma di sviluppo, server Web ecc., ma non applicazioni aziendali
- **Infrastructure-as-a-Service (IaaS)**: vengono forniti solo componenti hardware fisici o virtuali

L'esatta combinazione di controlli che si applicano a ciascuno dei modelli di cui sopra varierà in base all'ambito concordato dei servizi Cloud forniti. Ciò sarà indicato all'interno del contratto firmato prima dell'inizio della fornitura dei servizi Cloud.

La presente politica si applica a tutto il personale interno, alle terze parti che collaborano alla erogazione dei servizi nonché di tutti gli utilizzatori dei servizi proposti.

La presente politica è diffusa a tutti i soggetti sia interni che esterni interessati nonché sarà oggetto di riesame annuale.

# 2. Attività

Questo documento è strutturato attorno ai controlli stabiliti nell'allegato A dello standard ISO/IEC 27001 per la sicurezza delle informazioni. Le informazioni fornite hanno lo scopo di riflettere un livello di dettaglio adeguatamente utile sulle difese di sicurezza dell'organizzazione, senza divulgare dettagli che potrebbero essere utili per un utente malintenzionato. Ulteriori dettagli possono essere disponibili su richiesta per il Cliente autorizzato ai sensi di un accordo di non divulgazione.

LARUS opera da protagonista nel mercato dell'Information Technology & Communication con la proposta e fornitura della soluzione Galileo.XAI.

Le competenze espresse da LARUS derivano da anni di esperienza in progetti privati e pubblici.

Gli obiettivi etici principali di LARUS sono:

- avere, sempre, un rapporto di correttezza nei riguardi del Cliente e dei fornitori che sono entrambi visti come partner strategici;

- creare un'azienda in cui l'aggiornamento tecnologico sia tale da evitare l'obsolescenza culturale e con l'ambizione di utilizzare sempre le tecnologie più avanzate che il mercato informatico è in grado di mettere a disposizione.

In tale ottica riconoscendo l'importanza strategica delle risorse umane, dei dispositivi informatici, delle infrastrutture e del patrimonio delle informazioni, LARUS ha deciso di tutelarne la salvaguardia in tutte le fasi dei processi aziendali considerando l'Information Security uno strumento che permette la condivisione sicura delle informazioni, il miglioramento delle prestazioni rese ai Clienti e della propria immagine.

## 2.1 Politiche di sicurezza delle informazioni

Le politiche di sicurezza delle informazioni di LARUS sono scritte per tenere conto delle esigenze specifiche della fornitura di servizi Cloud, tra cui:

- Ampio uso della virtualizzazione
- La natura multi-tenant dei nostri servizi
- Rischi da insider autorizzati
- Protezione dei dati dei Clienti nel Cloud
- La necessità di una comunicazione efficace con i nostri Clienti

Tutte le politiche sono controllate dalla versione, autorizzate e comunicate a tutti i dipendenti e appaltatori interessati.

Obiettivi di LARUS sono quindi:

- mantenimento della certificazione del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni con estensione ai controlli ISO/IEC 27017 e ISO/IEC 27018;
- rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il rischio residuo a livelli accettabili;
- definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (Business Continuity);
- riduzione delle vulnerabilità dei propri asset aziendali da minacce quali virus, software nocivo ecc. tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:
    - sistemi hardware e software (personal computer, workstation, server, apparecchiature di rete, sistemi di comunicazione elettronica);
    - informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);
    - servizi (posta elettronica e accessi al CSP);
- caratterizzazione della propria offerta di servizi ai Clienti con la garanzia della salvaguardia delle informazioni condivise mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in LARUS e/o definite in sede contrattuale.

## 2.2 Organizzazione della sicurezza delle informazioni

I ruoli e le responsabilità per la gestione dell'ambiente Cloud sono chiaramente definiti come parte della negoziazione del contratto in modo che le aspettative del Cliente siano adeguatamente allineate con il modo in cui il servizio verrà erogato.
Inoltre, viene in LARUS stabilita e mantenuta una chiara divisione delle responsabilità tra i nostri fornitori, compresi i fornitori di servizi Cloud che forniscono servizi di supporto.
LARUS opera da diverse aree geografiche e adotta un approccio di zona per l'archiviazione dei dati dei Clienti in modo che siano sempre ubicati nel paese o nei paesi richiesti dal Cliente.

LARUS al fine di proteggere le informazioni dei Clienti archiviate e gestite in Cloud, in conformità dello standard ISO/IEC 27017:2015, considera:

- le informazioni archiviate nell'ambiente del Cloud cui il Cliente può avere accesso e che sono gestite dal Provider del Cloud (CSP);
- gli asset mantenuti sul Cloud, come le applicazioni;
- i processi in multi-tenant che si possono svolgere nel Cloud virtuale;
- gli utenti del Cloud ed il contesto in cui essi utilizzano il servizio;
- gli amministratori del servizio Cloud dei Clienti che hanno un accesso privilegiato;
- la localizzazione geografica del Provider del Cloud ed i Paesi in cui quest'ultimo può archiviare i dati relativi al Cloud (anche temporaneamente);
- i requisiti base di sicurezza delle informazioni applicabili alla progettazione ed alla implementazione del servizio Cloud;
- i rischi derivanti da addetti ai lavori autorizzati;
- procedure per il controllo degli accessi;
- comunicazioni con il Cliente durante il change management;
- allineamento e sicurezza degli ambienti virtuale e cloud;
- accesso ai dati del Cliente del servizio Cloud e loro protezione;
- gestione del ciclo di vita dell'account del Cliente;
- comunicazione di Data Breach e linee guida per la condivisione delle informazioni, per aiutare le investigazioni.

LARUS mette in pratica una Privacy Policy descrivendo le modalità con cui tratta i dati personali nell'ambito della erogazione del servizio di Cloud Computing, anche alla luce degli obblighi imposti dal Regolamento UE 2016/679.

LARUS in qualità di erogatore del servizio SaaS assicura che vengano soddisfatte le seguenti condizioni:

- i dati archiviati sui server rimangono sempre di proprietà del Cliente;

- impone adeguati controlli di accesso e garantisce che i dati in transito e il caricamento o il trasferimento di file siano protetti con protocolli di crittografia;
- concede al Cliente la possibilità di scaricare una copia dei dati di cui il Cliente stesso è titolare in qualsiasi momento durante la vigenza del contratto previa adeguata richiesta e dichiara con la massima trasparenza il luogo fisico dove risiedono i dati;
- fornisce al Cliente la possibilità di monitorare periodicamente le prestazioni del servizio e il rispetto del contratto.

Relativamente allo Standard ISO/IEC 27018 LARUS garantisce l'implementazione dei controlli richiesti per il trattamento di dati personali implementando adeguate misure di protezione, nel rispetto dei seguenti requisiti:

- Scelta e Consenso: agevolazione dell'esercizio dei diritti di accesso, rettifica e/o cancellazione da parte dell'interessato, attraverso le indicazioni specificate nel contratto.
- Finalità del trattamento: le finalità del trattamento sono rese note nel contratto di servizio.
- Minimizzazione dei dati: file e documenti temporanei sono cancellati o distrutti entro un periodo specificato e documentato.
- Limitazione all'uso, alla conservazione e alla divulgazione: Non avviene la divulgazione di dati personali a terze parti. La richiesta di divulgazione di dati personali da parte di autorità amministrative o giudiziarie è notificata al Cliente in maniera tempestiva, ove consentito dalla legge.
- Trasparenza: il ricorso a subappaltatori da parte del fornitore del servizio Saas è reso noto al Cliente prima del loro utilizzo. Le disposizioni per l'utilizzo dei subappaltatori sono riportate in chiaro nel contratto tra il fornitore del servizio Saas e il Cliente informandolo in modo tempestivo di eventuali modifiche previste in questo senso.
- Accountability: in caso di violazioni che comportano perdite, diffusione o modifica dei dati personali (data breach), effettua la notifica tempestivamente al Cliente attraverso un processo interno di Incident Management.
- Conformità alla privacy: il fornitore del servizio Saas indica i Paesi in cui sono conservati i dati, anche derivanti dall'utilizzo di subappaltatori e indica specifici accordi contrattuali applicati in merito al trasferimento internazionale di dati. Il provider informa tempestivamente il Cliente di eventuali modifiche previste a tale riguardo.

## 2.3 Sicurezza delle risorse umane

Un programma completo di formazione sulla sensibilizzazione viene fornito su base continuativa a tutti i dipendenti per sottolineare la necessità di proteggere adeguatamente i dati del Cloud dei Clienti.

## 2.4 Gestione delle risorse

La funzionalità viene fornita ove possibile all'interno dei nostri servizi Cloud per consentire ai nostri Clienti di riflettere i propri schemi di classificazione ed etichettatura delle informazioni.

È in atto una procedura controllata per la restituzione e la rimozione delle risorse dei Clienti Cloud quando appropriato. Questa procedura è progettata per garantire la protezione dei dati dei Clienti e in particolare delle informazioni di identificazione personale (PII).

## 2.5 Controllo di accesso

LARUS fornisce procedure di accesso sicuro per qualsiasi account richiesto dal Cliente del servizio Cloud per gli utenti sotto il suo controllo.

## 2.6 Crittografia

LARUS protegge la riservatezza delle informazioni critiche elaborate, trasmesse e ricevute attraverso l'impiego della crittografia. I contenuti dei dati "cifrati" (per i quali è stata impiegata la crittografia) sono resi incomprensibili a coloro che vi accedano senza disporre della relativa autorizzazione.

## 2.7 Sicurezza fisica e ambientale

I data center utilizzati per ospitare l'hardware che supporta i nostri servizi Cloud non sono identificati al pubblico e sono deliberatamente progettati per presentare un profilo basso nel loro ambiente immediato.

LARUS effettua lo smaltimento sicuro o il riutilizzo delle risorse quando non sono più richieste dal Cliente Cloud. Ciò garantisce che i dati dei Clienti non siano messi a rischio. Inoltre, viene effettuata la valutazione del rischio e vengono attuate misure tecniche e organizzative per ridurre al minimo i rischi identificati.

## 2.8 Sicurezza delle operazioni

I backup crittografati degli ambienti del Cliente vengono eseguiti con frequenza giornaliera e vengono conservati per un periodo predefinito di sette giorni. I backup vengono archiviati in una posizione separata off-site rispetto alla posizione principale dei dati del Cliente a una distanza considerata sufficiente a rappresentare una ragionevole precauzione di continuità aziendale. I campioni di backup vengono verificati periodicamente per confermarne l'integrità. Il ripristino dal backup può essere richiesto dal Cliente a partire dal giorno successivo all'esecuzione del backup.

LARUS sottoscrive accordi di riservatezza o di non divulgazione con i suoi dipendenti e collaboratori.

I registri delle attività e delle transazioni vengono registrati nell'ambiente Cloud e possono essere consultati su richiesta dal Cliente anche per attività di monitoraggio. Questi includono i dettagli di login/logout, accesso ai dati e modifiche/cancellazioni.

Tutti gli orologi del sistema e del dispositivo all'interno dell'ambiente Cloud sono sincronizzati (tramite server designati) con un'origine dell'ora esterna, i cui dettagli sono disponibili su richiesta.

L'ambiente Cloud del Cliente è soggetto a regolare scansione delle vulnerabilità utilizzando strumenti standard del settore. Le patch di sicurezza critiche vengono applicate in conformità con le raccomandazioni dei produttori di software.

Le attività operative ritenute critiche e, in alcuni casi, irreversibili (come la cancellazione dei server virtuali) sono soggette a procedure appositamente controllate che assicurano un adeguato controllo prima del completamento. Raccomandiamo inoltre al Cliente di mettere in atto le proprie procedure in queste aree.

LARUS fornisce la garanzia che ogni volta che lo spazio di archiviazione dei dati viene assegnato a un servizio Cloud, tutti i dati che precedentemente risiedevano su tale spazio di archiviazione sono stati resi inintelligibili.

## 2.9 Sicurezza delle comunicazioni

LARUS considera:

- il divieto di utilizzo di supporti e dispositivi di memorizzazione portatili;
- limitazione della creazione di materiale cartaceo (comprese le stampe che contengono dati personali);
- smaltimento sicuro dei materiali cartacei;
- crittografia dei dati che vengono trasmessi sulle reti pubbliche;
- utilizzo di ID univoci per il Cliente Cloud;
- gestione degli ID utente e divieto di assegnazione ad altri di quelli non utilizzati o scaduti;
- stesura e aggiornamento sistematico di un registro degli utenti che accedono al sistema e dei relativi profili di accesso;

## 2.10 Acquisizione, sviluppo e manutenzione del sistema

Vengono utilizzate procedure e pratiche di sviluppo sicuro in LARUS, inclusa la separazione degli ambienti di sviluppo, test e produzione, tecniche di codifica sicure e test completi di accettazione della sicurezza.

## 2.11 Rapporti con i fornitori

Nella fornitura di determinati servizi, LARUS si avvale di fornitori di servizi Cloud peer in un accordo di catena di fornitura. Questi fornitori sono soggetti ad una verifica preventiva delle loro misure di sicurezza.

LARUS mostra evidenza dei controlli minimi di sicurezza nei contratti con Clienti e subappaltatori e garantisce la conformità rispetto alle condizioni contrattuali concordate con i fornitori e con i Clienti.

## 2.12 Gestione degli incidenti di sicurezza delle informazioni

LARUS, laddove ritenga necessario ed opportuno, può informare il Cliente di un evento di sicurezza delle informazioni anche prima che venga determinato se debba essere trattato come un incidente. Allo stesso modo, il Cliente può segnalare gli eventi di sicurezza al nostro servizio di assistenza dove verranno registrati e verrà decisa l'azione appropriata. Informazioni sullo stato di avanzamento di tali eventi possono essere ottenute presso il servizio di assistenza.

LARUS segnalerà gli incidenti di sicurezza delle informazioni al Cliente in cui ritiene che i dati siano o saranno interessati, non appena ragionevolmente possibile e condividerà tutte le informazioni sull'impatto e sull'indagine dell'incidente che riterrà appropriate per la sua risoluzione efficace e tempestiva. In ogni caso verrà nominato un responsabile della gestione dell'incidente che fungerà da punto di contatto, comprese le questioni relative all'acquisizione e alla conservazione delle prove digitali, se necessario.

## 2.13 Gestione della sicurezza delle informazioni e della continuità operativa

LARUS pianifica e verifica regolarmente la sua risposta a vari tipi di incidenti dirompenti che potrebbero influire sul servizio Cliente Cloud. L'architettura dei nostri servizi Cloud è progettata per ridurre al minimo la probabilità e l'impatto di un tale incidente e vengono fatti tutti gli sforzi ragionevolmente possibili per evitare qualsiasi impatto sui servizi Cloud dei Clienti.

## 2.14 Conformità

La giurisdizione legale del servizio Cloud fornito dipenderà dal paese in cui viene stipulato il contratto. Laddove i dati personali siano conservati, LARUS rispetterà i requisiti della normativa applicabile in materia di privacy e protezione dei dati.

I record raccolti da LARUS come parte della sua fornitura del servizio Cloud saranno soggetti a protezione in conformità con il nostro schema di classificazione delle informazioni e con la normativa vigente in tema di privacy e protezione dei dati (il Regolamento generale per la protezione dei dati personali 2016/679 o General Data Protection Regulation o GDPR).

I servizi Cloud di LARUS sono certificati secondo lo standard internazionale ISO/IEC 27001 per la sicurezza delle informazioni e vengono verificati su base annuale di sorveglianza. Rispettiamo inoltre il codice di condotta ISO/IEC 27017 per i controlli di sicurezza delle informazioni nel Cloud e il codice di condotta ISO/IEC 27018 per la protezione delle informazioni di identificazione personale nel Cloud.