

MedLab S.p.A.

Policy di Cloud Computing Security

1	PREMESSA	2
1.1	CONTESTO DI RIFERIMENTO	2
1.2	AMBITO DEL DOCUMENTO	2
2	APPLICABILITÀ	3
2.1	DESTINATARI DEL DOCUMENTO	3
2.2	RESPONSABILITÀ DEL DOCUMENTO	3
3	DEFINIZIONI	3
4	RUOLI E RESPONSABILITÀ	5
4.1	UNITÀ CHIEF DATA & AI	6
4.2	UNITÀ CHIEF SERVICE	6
4.3	FUNZIONE RISK MANAGEMENT	6
4.4	FUNZIONE COMPLIANCE	7
4.5	LA FUNZIONE COMPLIANCE DELLA SOCIETÀ HA LA RESPONSABILITÀ DI PRESIDARE IL RISCHIO DI NON CONFORMITÀ ALLE NORME IN AMBITO CLOUD COMPUTING. UFFICIO BUSINESS CONTINUITY DI BANCA MEDIOLANUM	7
4.6	UNITÀ DI IT RISK & SECURITY DI BANCA MEDIOLANUM	7
4.7	DIVISIONE ACQUISTI DI BANCA MEDIOLANUM	7
4.8	DIVISIONE AFFARI LEGALI DI BANCA MEDIOLANUM	7
4.9	UFFICIO PRIVACY DI BANCA MEDIOLANUM	7
5	I PRINCIPI IN TEMA DI CLOUD COMPUTING SECURITY	7
5.1	CARATTERISTICHE ESSENZIALI DI UN SISTEMA CLOUD	7
5.2	MODELLI DI SERVIZIO	8
5.3	MODELLI DI DISTRIBUZIONE	8
5.4	PRINCIPI DI ESTERNALIZZAZIONE IN CLOUD	9
5.4.1	<i>Requisiti di esternalizzazione</i>	9
5.4.2	<i>Integrazione con i presidi e processi della Società</i>	10
5.5	PRINCIPALI AMBITI DI PRESIDIO	10
5.5.1	<i>Connettività</i>	10
5.5.2	<i>Identità ed Accessi privilegiati</i>	11
5.5.3	<i>Data Protection</i>	12
5.5.4	<i>Sicurezza Infrastrutturale</i>	13
5.5.5	<i>Eventi di Sicurezza e Gestione degli Incidenti</i>	15
5.6	EXIT STRATEGY	15
6	NORMATIVA DI RIFERIMENTO	16

1 PREMESSA

Scopo del presente documento è fornire una descrizione dei principi adottati da MedLab S.p.A. in tema di sicurezza relativa al Cloud Computing.

1.1 CONTESTO DI RIFERIMENTO

Il Cloud Computing, secondo la pubblicazione speciale del NIST 800-145, viene identificato come un modello per abilitare l'accesso ad una serie di risorse informatiche configurabili attraverso la rete (es. reti, server, dispositivi di storage, applicazioni oppure servizi) che possono essere messe a disposizione senza particolari difficoltà a livello gestionale o interazione tra provider di servizi.

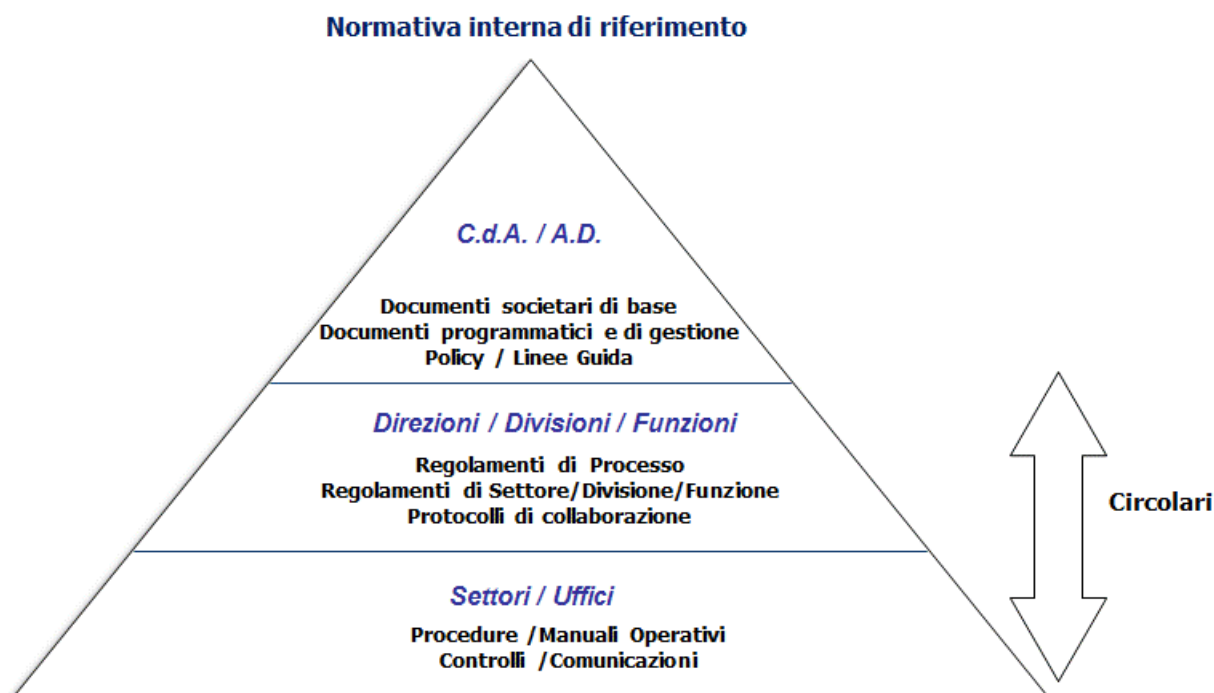
1.2 AMBITO DEL DOCUMENTO

La presente Policy descrive i principi ed i requisiti di sicurezza in tema di Cloud Computing di MedLab S.p.A. (di seguito anche la Società). I requisiti di cui sotto assumono particolare rilevanza in quanto la fruizione dei servizi offerti dalla Società si basano interamente su servizi di tipo Cloud.

I principi richiamati nella presente policy trovano quindi attuazione nei regolamenti di processo, nei quali saranno meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto degli adempimenti relativi alle normative. Tali regolamenti descriveranno più nel dettaglio le tematiche inerenti all'adozione del Cloud, al suo utilizzo e gli attori coinvolti, i loro ruoli e le responsabilità all'interno della Società.

Con riferimento alla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna", il presente documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente.

Figura 1. Modello della normativa aziendale



2 APPLICABILITÀ

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di MedLab S.p.A. e trova diretta applicazione all'interno della Società. I principi definiti si applicano a tutte le unità organizzative della Società incluse nel perimetro di intervento.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità dell'Unità Chief Data & AI.

3 DEFINIZIONI

Ai fini della presente Policy si intendono per:

CSP: un Cloud Service Provider è una organizzazione che mette a disposizione componenti di Cloud Computing ad altre organizzazioni.

CSC: un Cloud Service Client è un'organizzazione che utilizza componenti e/o risorse computazionali di Cloud Computing fornite da un CSP.

Disaster Recovery: l'insieme delle tecniche, delle tecnologie e delle modalità per ripristinare i servizi

informatici erogati da un Centro di Elaborazione Dati colpito da disastro e non più funzionante, su un Centro di Elaborazione Dati alternativo e fisicamente separato dal primo.

Hardening: il processo che mira, attraverso operazioni di configurazione specifica di un dato sistema e dei suoi componenti, a minimizzare l'impatto di possibili vulnerabilità, migliorandone quindi la sicurezza complessiva (ad esempio attraverso la riduzione della superficie di attacco e riconfigurazione dei servizi esistenti).

IMEL: Istituti di Moneta Elettronica, imprese che svolgono in via esclusiva l'attività di emissione di Moneta elettronica.

Incidente di sicurezza: ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es. frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi).

Informazione: nell'ambito della trasmissione e ricezione di comunicazioni o nozioni, ritenute utili o anche indispensabili per la definizione e l'attuazione dei processi aziendali, per informazione si intende il dato elettronico, il documento cartaceo ma anche le comunicazioni telefoniche o tramite videoconferenze o altri strumenti informatici e le conoscenze del personale.

Minimo privilegio (Least privilege): il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati, ovvero al suo ruolo.

Resilienza: capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura, in modo da garantire la disponibilità dei servizi erogati.

Rischio informatico (o rischio ICT): il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione. Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi reputazionali e strategici.

Segregation of duty (Segregazione dei ruoli): il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite.

Tecniche crittografiche: tecniche atte a garantire la riservatezza e l'integrità delle informazioni, rendendole illeggibili attraverso trasformazioni delle informazioni originali o la generazione di sequenze uniche di caratteri, basate sul contenuto delle informazioni stesse. Le tecniche crittografiche si basano sull'utilizzo di specifici algoritmi e utilizzano chiavi crittografiche con cui vengono elaborate le informazioni.

Verificabilità: la garanzia di poter ricostruire, all'occorrenza e anche a distanza di tempo, eventi connessi all'utilizzo del sistema informativo e al trattamento di dati.

Vulnerabilità Tecniche: punti deboli presenti all'interno di elaboratori e programmi / nella configurazione degli stessi, che potrebbero essere sfruttati da una potenziale minaccia per ottenere l'accesso a informazioni o per ostacolarne il funzionamento.

Funzione Operativa Importante (FOI): una funzione operativa per la quale risulta verificata almeno una delle seguenti condizioni:

- un'anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente:
 - i risultati finanziari, la solidità o la continuità dell'attività della Società ovvero
 - la capacità della Società di conformarsi alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza.
- riguarda attività sottoposte a riserva di legge;
- riguarda processi operativi delle funzioni aziendali di controllo o ha un impatto significativo sulla gestione dei rischi aziendali.

Funzioni Operative ICT: funzioni operative della Società riconducibili all'Information and Communication Technology.

Funzioni Operative non ICT: funzioni operative della Società non riconducibili all'Information and Communication Technology.

Esternalizzazione di Funzione Operativa Importante: cessione a soggetti interni al Gruppo, o a terzi, di una funzione che viene considerata essenziale o importante, in quanto un'anomalia nella sua esecuzione o la sua mancata esecuzione comprometterebbe gravemente la capacità della Società di continuare a conformarsi alle condizioni o agli obblighi della sua autorizzazione, o potrebbe causare un grave danno (anche reputazionale o operativo).

Exit Strategy: strategia da adottare, quando la Società decida di interrompere il rapporto con il Fornitore di una funzione esternalizzata, per sostituirlo con un altro fornitore o reinternalizzare la funzione.

ICT: Information and Communication Technology.

Key Risk Indicator (KRI): indicatore del livello di rischio di un'attività.

Organo con Funzione di Supervisione Strategica (OFSS): nel caso di MedLab S.p.A., si tratta del Consiglio di Amministrazione.

Service Level Agreement (SLA): accordo contrattuale sui livelli di servizio.

IaaS: Infrastructure as a Service (cfr. paragrafo 5.2).

PaaS: Platform as a Service (cfr. paragrafo 5.2).

SaaS: Software as a Service (cfr. paragrafo 5.2).

NIST: National Institute of Standard and Technology.

Infrastruttura Cloud: collezione di hardware e software necessaria ad abilitare le caratteristiche essenziali del Cloud. Essa può essere identificata come un contenitore a livello sia fisico che astratto. Il livello fisico è caratterizzato dalle risorse hardware necessarie per supportare i servizi Cloud forniti dal CSP e include componenti server, storage e di rete. Il livello astratto, invece, è caratterizzato dai software distribuiti attraverso il livello fisico, che manifesta le caratteristiche essenziali del Cloud. Idealmente, lo strato astratto si trova al di sopra di quello fisico.



Figura 2. Modello della struttura dell'ambiente Cloud

API: un'Application Programming Interface si può definire come un set di procedure atte all'espletamento di un dato compito: nella maggior parte dei casi questo termine comprende le librerie software di un linguaggio di programmazione.

4 RUOLI E RESPONSABILITÀ

Il modello organizzativo adottato da MedLab S.p.A. per la gestione della sicurezza in cloud prevede il coinvolgimento delle seguenti strutture della società stessa e delle strutture organizzative della Capogruppo Banca Mediolanum che svolgono in outsourcing servizi aziendali in virtù di apposito accordo di esternalizzazione.

4.1 UNITÀ CHIEF DATA & AI

L'unità Chief Data & AI garantisce, ispirandosi a criteri di funzionalità, efficienza e sicurezza, la gestione e lo sviluppo dei sistemi informativi e di comunicazione della Società.

In particolare, ha la responsabilità di:

- presidiare, con il supporto dell'unità IT Risk & Security di Banca Mediolanum, il governo dei Rischi IT e della IT Security in ambito Cloud Computing;
- verificare, con il supporto dell'unità IT Risk & Security di Banca Mediolanum, la coerenza dei presidi di sicurezza in ambito Cloud Computing con le policy approvate;
- analizzare, con il supporto dell'unità IT Risk & Security di Banca Mediolanum, i requisiti e validare le soluzioni architetturali e tecnologiche relativamente alla sicurezza informatica delle soluzioni basate su architetture Cloud;
- presidiare, con il supporto dell'unità IT Risk & Security di Banca Mediolanum, il monitoraggio, nel continuo, delle minacce applicabili alle risorse in cloud computing e monitorare/controllare i relativi programmi di mitigazione;
- verificare il corretto funzionamento dei servizi cloud anche al fine di garantire la capacità e la continuità operativa dei sistemi della Società;
- definire, governare e controllare le specifiche di Business Continuity ed il piano di Disaster Recovery della Società, predisporre e mantenere le infrastrutture cloud in linea con il suddetto piano;
- programmare, con il supporto del Business Continuity Office della Capogruppo, i test di Disaster Recovery in Cloud;
- presidiare, con il supporto dell'unità IT Risk & Security di Banca Mediolanum, il soddisfacimento dei principi di Sicurezza definiti dal presente documento per le fasi di analisi, progettazione, sviluppo, gestione e dismissione delle componenti infrastrutturali in cloud.

4.2 UNITÀ CHIEF SERVICE

L'Unità Chief Service per le attività trasversali alla Società e che coinvolgono uno o più CSP, partecipa alle riunioni dedicate a condividere tematiche inerenti al Cloud insieme a: da:

- Unità Chief Data & AI;
- Funzione Compliance;
- Unità IT Risk & Security di Banca Mediolanum;
- Ufficio Privacy di Banca Mediolanum.

Le riunioni si tengono ogni 15 giorni circa. L'obiettivo di queste riunioni è prendere decisioni in merito ad architetture e/o infrastrutture da adottare nell'ambito dell'erogazione dei servizi.

L'Unità Chief Service inoltre ha la responsabilità del presidio dei fornitori in ambito Cloud.

4.3 FUNZIONE RISK MANAGEMENT

La Funzione Risk Management della Società collabora con le unità IT Risk & Security di Banca Mediolanum e Chief Data & AI, deputate al presidio del rischio informatico e di sicurezza presso la Società, alla verifica dell'allineamento del profilo di rischio informatico alla soglia gestionale di propensione a tale rischio adottata dalla Società.

4.4 FUNZIONE COMPLIANCE

La funzione Compliance della Società ha la responsabilità di presidiare il rischio di non conformità alle norme in ambito Cloud computing.

4.5 UFFICIO BUSINESS CONTINUITY DI BANCA MEDIOLANUM

L'ufficio Business Continuity di Banca Mediolanum ha la responsabilità, in virtù dell'accordo di esternalizzazione di supportare operativamente il Consiglio di Amministrazione della Società nella stesura e aggiornamento del piano di continuità operativa aziendale e garantisce un presidio continuativo delle misure di continuità operativa.

4.6 UNITÀ DI IT RISK & SECURITY DI BANCA MEDIOLANUM

L'Unità IT Risk & Security della Divisione ICT di Banca Mediolanum, in virtù dell'accordo di esternalizzazione, supporta l'Unità Chief Data & AI nel:

- definire e gestire, nell'ambito del sistema di gestione della sicurezza delle informazioni (SGSI), i processi di attuazione e governo della sicurezza secondo le linee guida del Gruppo Bancario;
- accertare che, nell'ambito dei processi di progettazione, realizzazione e manutenzione dei servizi IT, i requisiti di sicurezza forniti siano rispettati, coerentemente con quanto stabilito dalle policy in ambito;
- concorrere ad eseguire le attività di Analisi del Rischio IT della Società, relativamente alla determinazione degli impatti sugli Scenari di Rischio dei servizi IT.

4.7 DIVISIONE ACQUISTI DI BANCA MEDIOLANUM

La Divisione Acquisti di Banca Mediolanum, in virtù dell'accordo di esternalizzazione, supporta il processo di selezione e negoziazione con i fornitori in ambito Cloud.

4.8 DIVISIONE AFFARI LEGALI DI BANCA MEDIOLANUM

La Divisione Affari Legali di Banca Mediolanum, in virtù dell'accordo di esternalizzazione, supporta il processo di predisposizione dei contratti con i fornitori di servizi in Cloud selezionati dalla Società.

4.9 UFFICIO PRIVACY DI BANCA MEDIOLANUM

L'ufficio Privacy di Banca Mediolanum, in virtù dell'accordo di esternalizzazione, partecipa al processo di selezione del fornitore di servizi in Cloud con particolare riferimento alla valutazione dei dati personali che verranno gestiti dal fornitore stesso.

5 I PRINCIPI IN TEMA DI CLOUD COMPUTING SECURITY

5.1 CARATTERISTICHE ESSENZIALI DI UN SISTEMA CLOUD

Il Cloud presenta alcune caratteristiche particolari:

- **On-demand self-service:** il cliente gestisce le risorse e la loro configurazione in modalità self-service, senza bisogno di intervento diretto da parte del fornitore;
- **Broad Network Access:** il servizio è erogato attraverso la rete e acceduto attraverso meccanismi standard, favorendo l'adozione di componenti eterogenei (ad es. smartphone) dal lato cliente;
- **Resource pooling:** il fornitore gestisce le risorse in pooling, assegnandole e riassegnandole ai diversi clienti al momento del bisogno. Questo modello eroga il servizio ad una specifica locazione fisica e la localizzazione dei Data Center del fornitore viene rappresentata ad un livello di astrazione elevato (ad es. un certo paese o regione);
- **Rapid elasticity:** le risorse possono essere acquisite e rilasciate dal cliente in modo rapido, permettendone il pronto adeguamento alle esigenze del cliente;
- **Measured Service:** l'assegnazione e l'utilizzo delle risorse avvengono in modo misurabile, ad un certo livello di astrazione (ad es. storage, capacità di calcolo, account attivi). L'uso delle risorse può essere monitorato, controllato e riportato, fornendo trasparenza sia al cliente che al fornitore.

5.2 MODELLI DI SERVIZIO

Sono definiti i modelli di servizio che caratterizzano le soluzioni Cloud (cfr. NIST), in particolare:

- **Software as a Service (SaaS):** permette al cliente di utilizzare le applicazioni del fornitore in un'infrastruttura Cloud. Le applicazioni sono accessibili tipicamente da diversi dispositivi del cliente, o attraverso un'interfaccia di programmazione. Il cliente non gestisce l'applicazione o l'infrastruttura, ma può operare su un insieme limitato di parametri di configurazione dell'applicazione;
- **Platform as a Service (PaaS):** fornisce al cliente una piattaforma su cui realizzare applicazioni attraverso linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il cliente non gestisce l'infrastruttura sottostante, compresi rete, server, sistemi operativi e storage, ma ha il controllo dell'applicazione ed eventualmente di alcuni parametri di configurazione dell'ambiente in cui è eseguita;
- **Infrastructure as a Service (IaaS):** fornisce al cliente capacità elaborativa, storage, connettività e altre risorse fondamentali, sulle quali il cliente può eseguire software, compresi sistemi operativi. Rientra in questo ambito ad esempio l'offerta di macchine virtuali. Il cliente non controlla l'infrastruttura sottostante, ma configura la capacità elaborativa, lo storage e le altre risorse; può inoltre avere il controllo di alcuni componenti di rete (ad es. firewall).

5.3 MODELLI DI DISTRIBUZIONE

Sono definite le modalità di erogazione che caratterizzano le soluzioni Cloud (cfr. NIST), in particolare:

- **Private Cloud:** l'infrastruttura Cloud viene messa a disposizione esclusivamente ad una singola organizzazione dove l'infrastruttura fisica può essere di proprietà della stessa o in gestione ad una terza parte. L'infrastruttura può essere all'interno o all'esterno della sede dell'organizzazione che ne usufruisce;
- **Community Cloud:** l'infrastruttura Cloud viene fornita esclusivamente ad una comunità di consumatori, che provengono da organizzazioni le quali condividono gli interessi ed i rischi a cui sono esposte. L'infrastruttura può essere di proprietà, gestite da una o più organizzazioni all'interno della comunità o esternalizzata a terze parti oppure da una

combinazione di essi. L'infrastruttura può essere all'interno o all'esterno delle sedi di proprietà della comunità;

- **Public Cloud:** l'infrastruttura Cloud viene fornita a più clienti o organizzazioni. Essa può essere di proprietà oppure in outsourcing ad una terza parte, ma deve essere situata nelle sedi dei CSP;
- **Hybrid Cloud:** l'infrastruttura Cloud si configura come una combinazione dei modelli di distribuzione sovra-descritti legati tra loro da tecnologie standard o di proprietà in grado di consentire la portabilità dei dati e delle applicazioni.

5.4 PRINCIPI DI ESTERNALIZZAZIONE IN CLOUD

Nella presente policy, ad integrazione di quanto già definito all'interno della "Policy di Gruppo in materia di esternalizzazione di funzioni aziendali" di Capogruppo, sono affrontate le specificità relative alle fasi di acquisizione e gestione di servizi in Cloud::

- **"Decisione di esternalizzare":** in questa fase, l'unità Chief Data & AI valuta l'opportunità di esternalizzare, analizza le opzioni disponibili sul mercato ed effettua, con supporto della Funzione Risk Management, una valutazione di rischio di dettaglio per i servizi offerti dai fornitori che rispettano i requisiti individuati. Questa fase include la predisposizione della documentazione da fornitore al Consiglio di Amministrazione per il relativo iter decisionale, che comprende anche la scheda di valutazione delle Funzioni Compliance e Risk Management;
- **"Selezione del fornitore":** a valle della decisione di esternalizzazione da parte del Consiglio di Amministrazione, l'unità Chief Data & AI, con il supporto della Divisione Acquisti di Banca Mediolanum che svolge in outsourcing il servizio di gestione degli Acquisti, avvia la selezione del fornitore fra quelli individuati nella fase precedente. In fase di selezione del fornitore la valutazione dei CSP da parte della Società si basa innanzitutto su verifica preliminare dei requisiti indicati dalle linee guida dettate da Banca d'Italia e dalla European Banking Authority (EBA). È stato identificato ed integrato un modello utile a valutare tutte le tematiche di Cloud security allo scopo di selezionare il CSP senza omettere alcun tipo di dettaglio. Il modello è strutturato secondo tre diverse fasi, descritte di seguito;
- **"Contrattualizzazione":** la Divisione Acquisti e della Divisione Affari Legali di Banca Mediolanum, in virtù dell'accordo di esternalizzazione di servizi aziendali, si occupano della predisposizione degli accordi quadro o dei contratti di fornitura, assicurando l'adeguatezza delle stesse alle necessità della Società, con il supporto dell'Unità Data & AI e se necessario dell'unità Chief Service;
- **"Monitoraggio e gestione delle funzioni aziendali esternalizzate":** che deve tener conto dei KPI e SLA definiti in sede contrattuale, valutandone il rispetto da parte del CSP, il quale si impegna a fornire reportistica periodica sull'andamento del servizio.

5.4.1 REQUISITI DI ESTERNALIZZAZIONE

Sono stati identificati specifici requisiti allo scopo di assicurare la sicurezza delle informazioni e delle strutture fisiche su cui esse verranno collocate del CSP. I requisiti sono stati identificati seguendo:

- le linee guida Cloud Security Alliance (CSA) fornite da EBA relative all'utilizzo dei servizi Cloud;
- i requisiti di esternalizzazione di Banca d'Italia contenuto nella Circolare riguardante le misure di sicurezza e presidi di controllo per i servizi informatici esternalizzati.

I requisiti di esternalizzazione definiti dalla Società riguardano le tematiche relative alla sicurezza nella sua totalità, che verranno richiesti al CSP come di seguito dettagliato:

- monitoraggio e sicurezza degli endpoint ed asset utilizzati per erogare i servizi;
- attività di controllo preassunzione, gestione dei profili utente e awareness in tema sicurezza per i dipendenti;
- controllo su attività di configurazioni di sicurezza, gestione cambiamenti e network security;
- implementazione di misure a protezione dei dati, siano essi in formato digitale oppure cartaceo, che riguardino la totalità del ciclo di vita (incluso la loro locazione, l'accesso a questi, il loro utilizzo e la loro eventuale distruzione);
- monitoraggio, reporting e correzione delle vulnerabilità;
- presenza di piani dettagliati di continuità operativa (che includano le fasi di backup & restore dei dati);
- modalità di comunicazione e gestione di incidenti di sicurezza informatica di qualsiasi entità;
- possibilità di effettuare attività di audit presso i CSP;
- sicurezza dei software in tutto il loro ciclo di vita (SSDLC);
- possibilità di migrazione semplice delle applicazioni, macchine virtuali e dei dati dall'ambiente del CSP ad un altro (strategia di uscita e piano di migrazione).

5.4.2 INTEGRAZIONE CON I PRESIDI E PROCESSI DELLA SOCIETÀ

A valle della selezione del CSP, viene prodotta un'analisi delle possibilità di integrazione dei servizi forniti dai provider stessi. L'analisi di cui sopra viene strutturata in due diverse fasi:

- verifica di come le capability dei provider si integrino con i sistemi e servizi della Società;
- verifica che i processi e presidi della Società siano efficaci ed in grado di trarre benefici dalle integrazioni con il Cloud.

5.5 PRINCIPALI AMBITI DI PRESIDIO

Sono stati individuati cinque ambiti di presidio che sono alla base della sicurezza dell'ambiente Cloud grazie alla quale la Società erogherà i propri servizi.



Figura 3. Modello della struttura dell'ambiente Cloud

5.5.1 CONNETTIVITÀ

Alla base dell'infrastruttura Cloud vi è la disponibilità di canali di connessione tra Società e CSP, in quanto senza una connessione il servizio non può essere erogato. Devono essere implementate da

parte del CSP misure di sicurezza idonee a garantire la sicurezza delle connessioni e degli scambi di dati attraverso l'ambiente Cloud. Inoltre, dovranno essere integrate delle zone di sicurezza che siano isolabili in caso di intromissione in modo da arginare possibili attacchi alla nascita.

5.5.2 IDENTITÀ ED ACCESSI PRIVILEGIATI

Considerando la facile fruizione delle risorse computazionali che deriva dall'implementazione di una infrastruttura Cloud, diviene fondamentale garantire la sicurezza delle identità digitali e degli accessi privilegiati. Il CSP deve avere implementato un'apposita policy che definisce le modalità di gestione delle utenze che accedono ai dati/servizi/informazioni del cliente e il relativo ciclo di vita. CSP e CSC devono assicurare che l'utilizzo delle risorse computazionali e non della Società sia subordinato all'inserimento di specifiche credenziali, in modo da garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite in Cloud.

I requisiti da seguire in tema di gestione delle identità digitali sono definiti da Capogruppo e rispettati dalla Società, la quale ha la responsabilità di fornire le utenze logiche. In particolare, si è ritenuto necessario integrare meccanismi di autenticazione forte (multi factor authentication) per chi accede alle risorse computazionali e non della Società, la quale ha la responsabilità del monitoraggio e dell'aggiornamento se necessario delle credenziali degli amministratori di sistema.

Considerando le tipologie di modelli di servizio descritte, CSP e CSC sono coinvolti secondo le seguenti matrici di responsabilità.


	Modello di Servizio		
	IaaS	PaaS	SaaS
	Software Level		
	MedLab	MedLab	MedLab
Utenze Applicative	Application Level		
	MedLab	MedLab	MedLab Provider
Utenze Amministrative	MedLab	MedLab	MedLab Provider
Configurazione Ambiente	MedLab	MedLab	Provider
Accesso Logico all'infrastruttura	Network Level		
	MedLab	Provider	Provider
Utenze Tecniche (NET)	Provider	Provider	Provider
Utenze Tecniche (HW)	Hardware Level		
	Provider	Provider	Provider

Figura 4. Gestione delle utenze

- Il CSP, nel modello SaaS, ha la responsabilità della gestione delle utenze tecniche di tutta l'infrastruttura sottostante l'applicazione, mentre il CSC gestisce le sole utenze applicative. Entrambi hanno corresponsabilità nella gestione delle utenze amministrative;
- il CSP, nel modello PaaS, ha la responsabilità delle utenze tecniche ed amministrative che accedono alla rete, ai server, ai sistemi operativi ed agli storage;
- il CSP, nel modello IaaS, ha la responsabilità della gestione delle utenze tecniche ed amministrative dell'infrastruttura di rete e dei meccanismi di controllo della stessa. Il CSC, invece, è responsabile delle utenze amministrative e non che hanno accesso ai sistemi operativi, agli storage, alle applicazioni e alle VLAN assegnate.

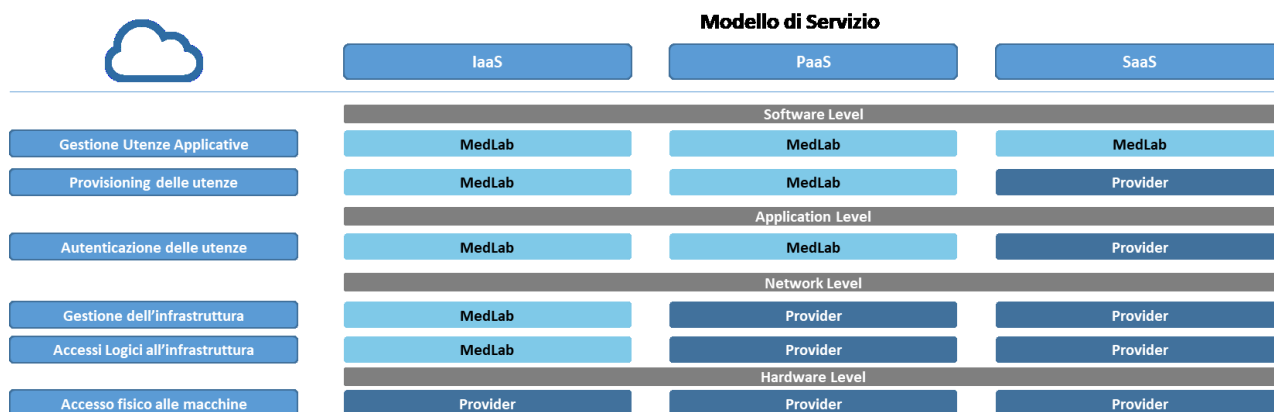


Figura 5. Gestione degli accessi logici

- Il CSP, in un modello di tipo SaaS, ha la responsabilità di gestire tutti gli aspetti relativi all'accesso alla rete, ai server e alle applicazioni presenti sull'infrastruttura Cloud. Considerando che tale modello è configurato come servizio rivolto direttamente agli utenti finali, l'accesso alle risorse deve avvenire in seguito ad un'autenticazione forte o altri meccanismi di log-in sicuro. In uno scenario di hosting come descritto, il CSP è responsabile di mettere a disposizione del CSC un'interfaccia utile a gestire le utenze e i log applicativi;
- il CSP, in un modello di tipo PaaS, è responsabile della gestione di tutti gli aspetti relativi al mantenimento dell'infrastruttura Cloud (sia fisica che virtuale), dei server e delle applicazioni presenti all'interno dell'infrastruttura stessa. Il CSP sarà inoltre responsabile della gestione degli accessi dei subfornitori nel caso in cui questi fossero necessari per lo sviluppo del servizio PaaS. Il CSC, in aggiunta a quanto verrà definito per il modello SaaS, è responsabile della gestione delle procedure di provisioning/deprovisioning e delle modalità di autenticazione delle utenze che hanno accesso alla piattaforma. In questo scenario, il CSC è ritenuto responsabile delle API, del software da esso implementato e che potrebbe avere ripercussioni sulla sicurezza degli accessi gestiti;
- il CSP, in un modello di tipo SaaS, è responsabile della gestione dell'accesso fisico alle macchine. Il CSC, invece, è responsabile della gestione degli accessi logici all'infrastruttura.

I diritti di accesso alle informazioni verranno definiti in base alla tipologia di servizio Cloud utilizzato. Il CSP dovrà garantire meccanismi e processi di gestione delle utenze e degli accessi logici secondo i principali standard di sicurezza internazionali (ad esempio ISO27001). La Società si riserva il diritto di richiedere al CSP le evidenze di tali misure di sicurezza in coerenza con quanto definito in sede di contratto.

Per quanto riguarda le utenze privilegiate e gli amministratori di sistema, anche sulle piattaforme Cloud dovranno essere garantiti gli standard di monitoraggio e controllo.

Dovranno essere quindi garantiti i principi dell'accountability, antiripudio delle azioni tracciate, least privilege, need to know e segregation of duties degli amministratori di sistema che utilizzando questi servizi.

5.5.3 DATA PROTECTION

In un contesto Cloud, in cui la fruizione delle risorse informatiche e computazionali è immediato e di facile utilizzo, diventa indispensabile la sicurezza in termini di integrità, confidenzialità e disponibilità dei dati in tutto il ciclo di vita a cui essi sono sottoposti. La protezione dei dati si può suddividere in

tre categorie principali: data accountability, data classification e data localization (in motion oppure at rest). Le responsabilità vengono suddivise in base alla tipologia di servizio come rappresentato nella seguente matrice.

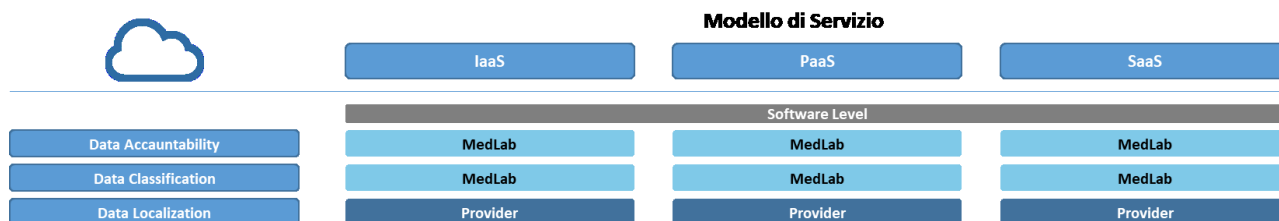


Figura 6. Sicurezza dei dati e ciclo di vita delle informazioni

Indipendentemente dalla tipologia di servizio, la localizzazione dei dati, in termini anche di accesso da utenze tecniche, gestione e messa in sicurezza del transito, è responsabilità del CSP che mantiene l'infrastruttura. La Società è ritenuta invece responsabile della classificazione dei dati, che avverrà secondo i principi dettati dalla policy di Sicurezza e dell'accountability, inclusa anche la "data remenance" ovvero la possibilità che alcuni dati residuali rimangano all'interno degli storage o nei cari supporti di memoria forniti dal CSP nonostante siano stati cancellati dal CSC. La Società si dovrà dotare di misure di sicurezza idonee relative alla gestione del dato in tutto il suo ciclo di vita e potrà richiedere al fornitore dimostrazione delle misure di sicurezza implementate da quest'ultimo riguardante questa tematica.

5.5.4 SICUREZZA INFRASTRUTTURALE

La sicurezza dell'infrastruttura rappresenta un elemento fondamentale per operare in maniera sicura in un ambiente Cloud. L'infrastruttura è composta da componenti fisiche e di rete, host e storage che costituiscono l'ambiente Cloud. Le misure di sicurezza fisica dei Datacenter e delle facilities che ospitano i servizi e le informazioni in Cloud del CSC sono svincolate dal modello di servizio utilizzato (SaaS, IaaS e PaaS) e sono responsabilità del CSP. Mentre di seguito viene rappresentata la matrice di responsabilità in tema di infrastruttura IT e virtualizzatori.

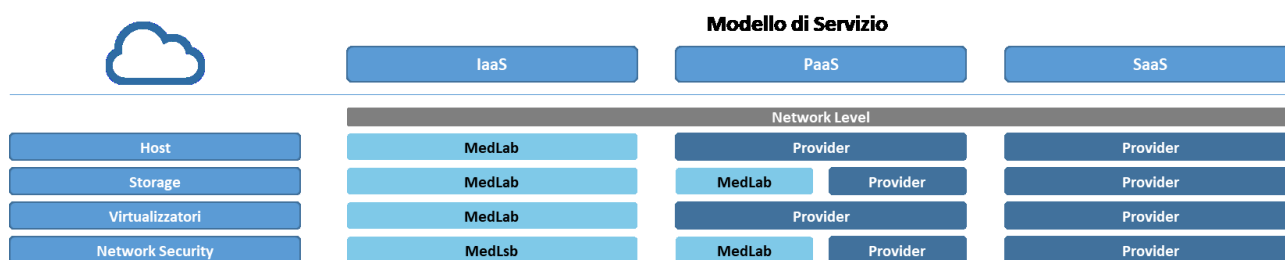


Figura 7. Sicurezza dell'infrastruttura IT e dei Virtualizzatori

Nel caso in cui il modello di servizio selezionato sia SaaS, il CSP è ritenuto responsabile anche della sicurezza dell'infrastruttura IT e dei Virtualizzatori implementando misure tecniche di difesa per il rilevamento e la risposta ad attacchi basati sulla rete associati a modelli anomali di traffico di ingresso e di uscita (es. DDoS), ad attacchi agli asset informatici, ad accessi e modifiche non autorizzate all'infrastruttura e per il monitoraggio dei sistemi. Inoltre, il CSP dovrà adottare soluzioni di sicurezza perimetrali (es. IPS, IDS, WAF) e se richiesto fornire report riguardanti le misure di sicurezza integrate al CSC. La differenza tra modello PaaS e SaaS risiede nella corresponsabilità da parte del CSC e del CSP nella gestione degli storage, nella gestione del network utilizzato per accedere ai servizi forniti dal CSP e delle misure di sicurezza ad essi applicate. Se invece il modello di servizio

è IaaS, essendo l'infrastruttura fornita al CSC che ne utilizza secondo le sue direttive le risorse, il CSC stesso è ritenuto responsabile dell'integrazione delle misure di sicurezza appena descritte.

Il CSP verrà ritenuto responsabile delle tematiche di continuità operativa secondo la seguente matrice.


	Modello di Servizio		
	IaaS	PaaS	SaaS
Business Continuity	MedLab	Provider	Provider
IT Resilience	MedLab	Provider	Provider
Backup	MedLab	Provider	Provider

Figura 8. Business continuity management e resilience

Per i modelli PaaS e SaaS la responsabilità dell'applicazione di misure atte a garantire la continuità operativa, la resilience e il backup è condivisa tra CSC e CSP. Il CSC ha il compito di acquistare ed attivare le funzionalità di business continuity e di disaster recovery; una volta attive il CSP sarà ritenuto accountable per la garanzia della corretta erogazione. Nel caso in cui il servizio erogato fosse del modello IaaS, il CSC ha la responsabilità di definire la strategia di business continuity e disaster recovery e nel caso in cui la soluzione fornita dal CSP non fosse ritenuta idonea, lo stesso CSC ha la responsabilità di integrare soluzioni alternative che ne rispettino i requisiti.

Nel caso di combinazioni di più CSP e/o modelli di servizio e si verifichi una situazione che possa compromettere uno di questi, è responsabilità del CSC dotarsi di misure tecniche ed organizzative utili a mantenere un livello di servizio adeguato.

Infine, per garantire la sicurezza delle infrastrutture Cloud è necessario declinare le responsabilità in tema di Vulnerability Assessment e gestione delle minacce. La matrice seguente ne declina le responsabilità.


	Modello di Servizio		
	IaaS	PaaS	SaaS
Incident Handling	MedLab	Provider	Provider
Comunicazione Incidenti	MedLab	Provider	Provider
Threat Intelligence	MedLab	Provider	Provider

Figura 9. Gestione delle vulnerabilità e delle minacce

Il CSC è tenuto a proteggere gli endpoint (personal computer, smartphone, tablet) che hanno accesso al Cloud, aggiornando antivirus, anti-malware, firewall e gestendo le patch in maniera corretta; egli è anche ritenuto responsabile della gestione delle vulnerabilità di tipo fisico che potrebbero coprire i dispositivi che accedono al Cloud. Nel modello di utilizzo PaaS, CSP e CSC detengono le stesse responsabilità del modello SaaS, tuttavia il CSC è responsabile della gestione delle vulnerabilità e delle minacce presenti sulle applicazioni implementate e distribuite sulla piattaforma PaaS. Nel modello IaaS, il CSP è responsabile della gestione delle vulnerabilità e delle minacce presenti nell'infrastruttura di Rete, mentre il CSC di quelle presenti nell'infrastruttura virtuale. Il CSC, infine, è responsabile della gestione corretta di tutti gli aspetti relativi alla gestione delle configurazioni di questi sistemi.

La Società, allo scopo di indirizzare tutte le vulnerabilità, promuove attività periodiche di Vulnerability Assessment/Penetration Testing. Le attività verranno fornite da Outsourcer esterni che saranno

variati periodicamente allo scopo di garantire l'efficacia del controllo.

La Società, inoltre, si avvarrà delle soluzioni Cloud Access Service Broker (CASB) fornite dai diversi fornitori, allo scopo di monitorare le attività che intercorrono tra la Società stessa e le varie soluzioni Cloud e assicurare l'applicazione puntuale delle policy di sicurezza.

5.5.5 EVENTI DI SICUREZZA E GESTIONE DEGLI INCIDENTI

La seguente matrice identifica le responsabilità in tema gestione degli incidenti di sicurezza e Cloud forensic:

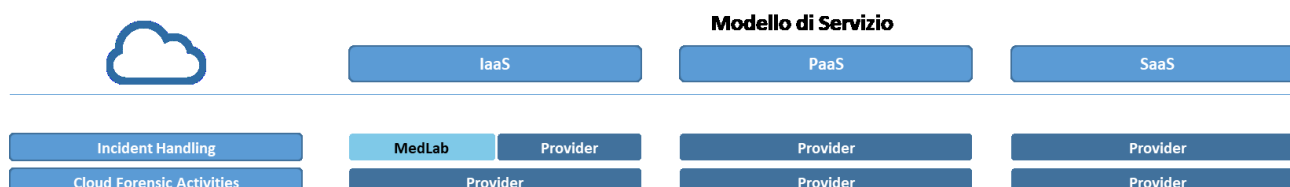


Figura 10. Responsabilità della gestione degli incidenti di sicurezza e Cloud Forensic

Il CSP deve definire ed implementare apposite misure di sicurezza in relazione al triage degli eventi di sicurezza allo scopo di assicurare una gestione tempestiva e completa degli incidenti. Il CSP deve fornire al CSC tempestiva notifica di incidente e i contatti del Referente del team di gestione degli incidenti da contattare in caso di rilevamento di incidente di sicurezza. Nel caso in cui l'incidente si rivelasse un "data breach", in conformità con il Regolamento UE 679/2016 il CSP è tenuto ad assistere e cooperare con il CSC titolare del trattamento, nel notificare eventuali breach alle Autorità di controllo e nel comunicarli agli interessati laddove necessario.

In particolare, gli eventi sono centralizzati e monitorati dai singoli fornitori (CSP compresi) che provvedono ad informare la Società in caso di incidente. Il processo di gestione operativa degli incidenti di sicurezza (siano essi di qualsiasi entità) si suddivide in due sotto-processi, che sono:

- gestione della crisi: processo di gestione della crisi successiva ad un incidente di varia entità, svolto da Banca Mediolanum in virtù dell'accordo di esternalizzazione;
- gestione operativa degli incidenti: processo atto a intraprendere contromisure e le necessarie attività di comunicazione (anche in accordo alle normative vigenti), in capo alla Società.

5.6 EXIT STRATEGY

In accordo con quanto definito dalle linee guida EBA, la Società deve pianificare ed implementare misure atte a mantenere la continuità dei propri servizi in caso si deteriori ad un grado inaccettabile oppure si compromettesse del tutto l'erogazione dei servizi da parte del CSP. Le misure di cui sopra devono essere composte anche da un piano di contingency e una strategia di uscita (exit strategy). In aggiunta a questo, la Società deve includere all'interno del contratto di esternalizzazione una clausola di gestione di terminazione ed uscita che permetta ai servizi erogati in Cloud di poter essere trasferite dal provider in uso ad un altro oppure di essere reincorporate all'interno della Società stessa.

La Società, in quanto esternalizza servizi in Cloud, deve assicurarsi di avere una strategia di uscita che, se necessario, non causi l'interruzione dell'erogazione dei propri servizi oppure abbia effetti in termini di compliance alle normative. Allo scopo di raggiungere questo obiettivo, la Società deve:

- sviluppare ed implementare strategie di uscita che siano comprensive, documentate e sufficientemente testate dove necessario;
- identificare soluzioni alternative e sviluppare piani di transizione in grado di trasferire le

attività esistenti e i dati utilizzati da un CSP nelle soluzioni alternative stesse in modo controllato e sufficientemente testato, tenendo conto delle problematiche relative alla locazione dei dati e il mantenimento della continuità operativa durante la fase di transizione;

- assicurare che l'accordo sull'esternalizzazione includa l'obbligo al CSP di supportare sufficientemente la Società allo scopo di trasferire le attività ad un altro CSP oppure in caso di terminazione dell'accordo.

Durante lo sviluppo delle strategie di uscita, la Società deve considerare di:

- sviluppare Key Risk Indicator (KRI) allo scopo di identificare livelli inaccettabili di servizio;
- produrre un'analisi degli impatti commisurata con i servizi esternalizzati allo scopo di identificare quali risorse, siano esse persone oppure asset, risultassero necessarie all'implementazione del piano di uscita e quanto tempo comporterebbe;
- assegnare ruoli e responsabilità per la gestione dei piani di uscita e di transizione dei servizi;
- definire i criteri di successo della transizione.

Infine, la Società deve includere indicatori che possono essere la base per l'avvio del piano di uscita durante il monitoraggio e la supervisione dei servizi esternalizzati al CSP.

6 NORMATIVA DI RIFERIMENTO

I principali riferimenti normativi e regolamentari in tema Cloud Computing Policy utilizzati per la stesura del presente documento, sono i seguenti:

- Circolare di Banca d'Italia 288 del 3 Aprile 2015 (2° aggiornamento del 27 Settembre 2016);
- ENISA, A Security and Resilience in Governmental Clouds;
- EU NIS Directive;
- EU-US Privacy Shield;
- GDPR (Regolamento UE 2016/679);
- ISO 27001:2013;
- NIST Cybersecurity Framework;
- Raccomandazioni EBA in tema di esternalizzazione Cloud;
- Cloud Security Alliance, Cloud Controls Matrix 3.0.1;
- COBIT 5;
- ENISA, A Security and Resilience in Governmental Clouds.