

Termini di servizio della piattaforma Cloud privato Unimib

Il presente documento è stato redatto dai Sistemi Informativi di concerto con il Titolare del Trattamento Dati e il Responsabile alla Protezione dei Dati dell'Università degli Studi di Milano-Bicocca al fine di conseguire gli obiettivi di *privacy-by-design* e *privacy-by-default* così come previsti dal Regolamento generale sulla protezione dei dati UE 2016/679 (GDPR).

Descrizione del servizio

I Sistemi Informativi offrono, nell'ambito delle finalità strategiche di Ateneo di Didattica, Ricerca e Terza Missione, una piattaforma cloud privata basata su tecnologia VMware vRealize Automation.

Per ogni gruppo di lavoro viene reso disponibile sulla piattaforma di Cloud privato Unimib un ambiente di lavoro isolato, definito da un insieme di risorse di calcolo (memoria, CPU, storage), da una rete privata e da una lista di membri che ne potranno disporre, definito logicamente come *spazio cloud privato*. Ogni spazio cloud privato coincide con un *Gruppo di business* all'interno della piattaforma di Cloud privato Unimib.

Dal portale Cloud privato Unimib gli utenti abilitati potranno creare e gestire le proprie macchine virtuali in maniera autonoma nei limiti delle risorse assegnate e monitorarne i relativi costi.

Parti coinvolte

La piattaforma Cloud privato Unimib vede coinvolti:

- il personale tecnico-informatico dell'Area Sistemi Informativi che ha nominato come responsabile di progetto il Capo Area dei Sistemi Informativi e i suoi collaboratori afferenti al Settore Sistemi e Servizi di Rete
- il responsabile dello spazio cloud privato, nella persona del responsabile scientifico interno della ricerca che effettua la richiesta tramite l'apposito modulo online, e i responsabili aggiuntivi da esso indicati nel relativo registro nell'ambito dell'attività di gestione dello spazio cloud privato.

Ruoli e responsabilità delle parti coinvolte

La responsabilità dei Sistemi Informativi copre tutti gli aspetti di continuità operativa, di sicurezza dell'infrastruttura di virtualizzazione, di connettività di rete e di provisioning delle risorse.

Al personale docente e ricercatore incaricato spettano gli obblighi normativi derivanti dalla gestione dello spazio cloud privato.

L'Area Sistemi Informativi nella persona del Capo Area, e il personale docente e ricercatore per il tramite del responsabile scientifico interno della ricerca, sono responsabili per quanto di propria competenza di fronte al Titolare del trattamento dei dati di questo Ateneo. La compromissione delle funzionalità legate all'utilizzo dell'infrastruttura e/o delle macchine virtuali in gestione sono da imputarsi per quanto di competenza alle singole strutture.

Tutte le parti coinvolte agiscono nell'ambito dei principi di buon andamento della Pubblica Amministrazione, mettendo in atto tutte le strategie necessarie a tale scopo.

Modalità di creazione delle macchine virtuali

Una volta creato lo spazio cloud privato, le macchine virtuali possono essere generate autonomamente dal personale appartenente al progetto di ricerca tramite il portale Cloud privato Unimib, a partire dai modelli a catalogo forniti dai Sistemi Informativi.

Questi modelli rispettano i requisiti degli standard di sicurezza europei ed internazionali vigenti e vengono mantenuti aggiornati nel corso del tempo, così da offrire sempre il massimo livello di sicurezza.

Aspetti relativi all'accesso

Come opzione predefinita le macchine virtuali vengono create in un ambiente isolato accessibile esclusivamente agli aventi diritto attraverso la piattaforma web Cloud privato Unimib o tramite VPN dedicata.

In questo modo non sarà possibile nessun tipo di comunicazione indesiderata (dolosa o accidentale) con le macchine virtuali appartenenti ad altri spazi cloud privati.

Qualora fosse necessario i Sistemi Informativi provvederanno alla pubblicazione di servizi all'esterno tramite indirizzi ip pubblici dedicati ai singoli progetti di ricerca.

La gestione avviene tramite strumenti che consentono ai tecnici di riconfigurare l'ambiente senza avere accesso diretto alla rete privata, nel rispetto della riservatezza dei dati e dei servizi su di essa veicolati.

Obblighi delle parti coinvolte

Al fine di assecondare l'attività di ricerca e compatibilmente con quanto disposto dalle normative vigenti, i Sistemi Informativi non hanno accesso alle macchine virtuali create dai membri degli spazi cloud privati né agli applicativi in esecuzione sulle macchine stesse, ai dati in esse contenuti (di qualsiasi tipo) e alle reti private assegnate, garantendo così agli utenti la più ampia autonomia e riservatezza. L'eventuale delega alla gestione delle macchine virtuali da parte dei Sistemi Informativi viene accordata solo in seguito di parere positivo del dirigente dell'Area Sistemi Informativi, fatto salvo che ogni attività eseguita dal personale dei Sistemi Informativi viene opportunamente tracciata secondo gli obblighi di legge.

Inoltre si dispone quanto segue:

- è responsabilità del personale dell'Area Sistemi Informativi:
 - prendere in carico le richieste pervenute tramite l'apposito *Modulo di richiesta di uno spazio cloud privato*
 - garantire adeguate misure di sicurezza per la parte di infrastruttura hardware, software e di rete, secondo quanto indicato dal regolamento (UE) 2016/679 e secondo quanto specificato nel documento relativo all'attuazione delle misure minime di sicurezza ICT approvato da questo Ateneo in data 21/12/2017 e successive modifiche
- il responsabile dello spazio cloud privato deve:
 - garantire adeguate misure di sicurezza rispetto al sistema operativo e ai software installati, nonché ai dati trattati nelle macchine virtuali, secondo quanto disposto dalle misure minime di sicurezza ICT e quanto definito dal Regolamento generale sulla protezione dei dati UE 2016/679 (GDPR)
 - garantire la corretta gestione dei log di sistema, dei servizi e degli applicativi installati nelle VM, e la loro conservazione *non oltre i 180 giorni*
 - trattare eventuali dati personali registrati nelle macchine virtuali secondo i principi stabiliti dall'articolo 5 del regolamento (UE) 2016/679, rendendoli anonimi o pseudo-anonimi dove possibile

- tenere un registro aggiornato delle persone che accedono allo spazio cloud privato, alle macchine virtuali e ai servizi da esse erogate e dei privilegi/livelli di accesso a essi rilasciati
 - avere cura di mantenere le utenze di accesso nominative, sicure e riservate
- tutto il personale operante nell'ambito dello spazio cloud privato si impegna a:
 - seguire le istruzioni ricevute dal responsabile scientifico interno della ricerca in merito alla normativa nazionale ed europea sul trattamento dei dati personali
 - non utilizzare per scopi (anche istituzionali) diversi da quelli necessari all'espletamento delle funzioni o delle cariche sopra indicate i dati oggetto di trattamento, neppure in forma anonima o aggregata, se non previa comunicazione dell'informativa ai diretti interessati e sottoscrizione del consenso da parte degli stessi
 - garantire quanto sopra descritto anche dopo la scadenza di utilizzo delle macchine virtuali richieste.