Condivisione delle responsabilità per il controllo delle risorse e la sicurezza nei servizi cloud di tipo IaaS

Applico Digital Lab (di seguito anche ADL) è un fornitore di infrastrutture e servizi cloud**;** opera, gestisce e controlla tutti i componenti, dal sistema operativo host e dalla virtualizzazione, alla sicurezza degli impianti in cui opera il servizio.
Nel modello di distribuzione cloud IaaS, i **Clienti** (*Consumer*) controllano l'architettura e la protezione delle applicazioni e dei dati che vengono introdotti nell'infrastruttura, mentre il **Fornitore** (*Provider*) ha la responsabilità di fornire i servizi su un'infrastruttura estremamente sicura e controllata e di offrire una gamma di funzioni di sicurezza supplementari.

1 Accesso amministrativo

ADL fornisce i Servizi Cloud mediante data center di sua proprietà. ADL definisce i servizi di rete e le architetture di sistema, nonché i requisiti hardware e software. Il Cliente accede ai servizi cloud tramite tunnel VPN IPsec o un tunnel VPN SSL sulla rete internet pubblica consentendo la gestione delle risorse in remoto e in modo sicuro nella rete privata di ADL.
ADL potrà accedere all'ambiente dei servizi del Cliente per svolgere le attività indispensabili ai fini della prestazione dei Servizi Cloud oggetto del contratto, ivi compresa la fornitura dei servizi di supporto. ADL consente l'accesso ai sistemi del Cliente solo a personale esperto e vincolato da impegni contrattuali di integrità e riservatezza. Tali accessi saranno tracciati dai sistemi di logging di ADL.

2 Orario di operatività

I Servizi Cloud sono disponibili 24 ore su 24, 7 giorni su 7, 365 giorni l'anno, ad eccezione dei periodi di manutenzione del sistema e di aggiornamento tecnologico, nonché nei casi previsti dal documento di Offerta Tecnico Economica e dalle Condizioni di fornitura inclusi i livelli di servizio concordati (SLA – Service Level Agreement).

3 Nomina a Responsabile Esterno al Trattamento dei dati Personali

In accordo con il Cliente, ADL viene nominata Responsabile Esterno al Trattamento dei Dati Personali (articolo 28 del GDPR) in quanto fornitore di servizi. ADL è disponibile a fornire assistenza per gli articoli da 15 a 22 e da 32 a 36 del GDPR, nei limiti della natura del trattamento e delle informazioni a sua disposizione.
Per qualsiasi informazione e chiarimento, scrivere a privacy@applicodigitallab.it.

4 Gestione della Sicurezza e livelli di certificazione

ADL progetta, realizza e gestisce infrastrutture e servizi cloud IaaS, in conformità con i principali standard internazionali e buone pratiche di cui mantiene aggiornante le seguenti certificazioni e linee guida:

- ISO 9001;
- ISO/IEC 27001;
- ISO/IEC 27017;
- ISO/IEC 27108.

5 Revisione annuale indipendente

ADL sottopone a controlli e audit l'infrastruttura tecnologica ed i processi interni, da parte di organismi di certificazione accreditati da ACCREDIA (l'Ente Italiano di Accreditamento), al fine di fornire garanzie specifiche ed indipendenti.

6 Proprietà delle risorse

ADL mette a disposizione un'infrastruttura idonea alla costituzione di applicazioni ad elevata disponibilità, dove siano evitabili singoli punti di guasto.
L'infrastruttura IT erogante il servizio, tra cui:

- Server,
- Sistemi di archiviazione informazioni (storage),
- Sistemi di monitoraggio e controllo delle apparecchiature,
- Router e switch per gestire il traffico dati,
- Indirizzi IP,
- Gruppi di continuità per garantire la continuità operativa,
- Sistemi di sicurezza (come, ad esempio, i sistemi di sicurezza antincendio)

è di proprietà di ADL.
Le licenze eventualmente fornite sono di proprietà di ADL e vengono concesse in uso al Cliente per la durata del contratto.

> *Responsabilità e Raccomandazioni per il Cliente*
> Il Cliente è proprietario e responsabile del software installato sulla piattaforma messa a disposizione da ADL. Ogni software utilizzato dal Cliente nell'ambito del Servizio dovrà essere un software originale, munito di apposita licenza d'uso, comunque compatibile con le specifiche e prescrizioni eventualmente comunicate da ADL. Tutto il contenuto di dati trattati sulla piattaforma rimane di proprietà e responsabilità del cliente.

7 Gestione dell'obsolescenza tecnologica

ADL implementa specifiche procedure di smaltimento sicuro dell'hardware utilizzato per archiviare i dati introdotti dal Cliente. Sono attuate pratiche standard per garantire la rimozione definitiva dei dati introdotti sul supporto hardware.

8 Cancellazione dei dati e dei files temporanei

ADL, secondo quanto definito contrattualmente, provvede alla cancellazione e rimozione di tutti i dati presenti sulla propria infrastruttura ivi compresi i dati del servizio di backup eventualmente incluso.

Responsabilità e Raccomandazioni per il Cliente

Il Cliente è responsabile di analizzare che le informazioni messe a disposizione dal fornitore ADL, riguardo lo smaltimento degli asset presenti sul sistema cloud.

9 Principali aree di intervento per sicurezza

ADL, in qualità di fornitore di servizi cloud è consapevole che assicurare la riservatezza, integrità e protezione dei dati e delle risorse utilizzate è un aspetto prioritario da condividere con il Cliente, in un modello di responsabilità di seguito meglio specificato.
Di norma, ADL è responsabile del servizio IaaS che eroga e non dei sistemi e applicazioni installate dal Cliente, dei dati introdotti dal Cliente durante l'utilizzo del servizio cloud.
Complessivamente, ADL è responsabile della protezione fisica e ambientale e sugli aspetti infrastrutturali resi disponibili.

Responsabilità e Raccomandazioni per il Cliente

Il Cliente è proprietario dei dati e, come tale, è responsabile delle autorizzazioni di accesso e del controllo. Il Cliente è anche responsabile del livello dell'applicazioni installate in termini di controllo di accesso, protezione e configurazione, cifratura, e così via.

Schema di raggruppamento delle principali responsabilità di sicurezza

Livello	Cloud IaaS
Dati trattati e loro classificazione	Responsabilità del Cliente
Applicazioni installate, identificazione, autorizzazione, e verifica degli endpoint	Responsabilità del Cliente
Sistemi Operativi e loro hardering	Responsabilità del Cliente
Tecnologia di Virtualizzazione	**Responsabilità del Fornitore**
Server fisici	**Responsabilità del Fornitore**
Dispositivi di Storage	**Responsabilità del Fornitore**
Network e isolamento	**Responsabilità del Fornitore**
Fisico e ambientale	**Responsabilità del Fornitore**

10 Organizzazione della sicurezza

ADL si è dotata di una infrastruttura idonea per la fornitura del servizio cloud e del relativo supporto operativo. Sono adottate e mantenute aggiornate policy e procedure che regolano il servizio e prevedono una regolare valutazione e mitigazione dei rischi attraverso un efficace sistema di misure fisiche, logiche ed operative di seguito riepilogate.

11 Sicurezza Fisica e perimetrale

Le sedi aziendali di ADL dispongono di misure avanzate di protezione, attiva e passiva nonché organizzativa. Il sito che ospita il Data Center ha livelli multipli di protezione, attrezzati con sistemi di: controlli accessi, differenziato per aree sensibili, sistemi antintrusione, allarmi remotizzati, armadi che ospitano i sistemi protetti da gabbie fisiche con serrature a chiave, impianti di continuità elettrica, rilevazione fumi, spegnimento incendi e antiallagamento tali da proteggere i sistemi.
ADL eroga i servizi da Data Center proprietari, progettati seguito ad un'analisi dei rischi per assicurare continuità e qualità, applicando misure di prevenzione fisiche, tecniche ed organizzative.

12 Sicurezza del personale

ADL ha definito chiaramente ruoli e responsabilità per gestire l'implementazione dei controlli di sicurezza. Tutto il personale coinvolto all'interno dell'infrastruttura è sensibilizzato, anche attraverso percorsi formativi specialistici, sulle loro responsabilità nel garantire il rispetto della privacy e procedure di sicurezza, dei requisiti legali e normativi, durante la gestione delle attività di trattamento del patrimonio informativo gestito.
Il personale dipendente ed i fornitori coinvolti hanno sottoscritto Accordi di non divulgazione e di Riservatezza per la protezione dei dati.

Responsabilità e Raccomandazioni per il Cliente

È responsabilità del Cliente formare il proprio personale addetto all'utilizzo dei servizi cloud forniti ed alla corretta gestione dati personali, sulla base di specifici requisiti (compresi, eventualmente, le altre parti interessate).

13 Sicurezza dell'infrastruttura tecnologica

ADL è responsabile dell'installazione e il funzionamento di qualsiasi dispositivo hardware ed altri sistemi utilizzati per fornire servizi cloud, inclusa la configurazione necessaria alla fornitura, proteggendoli dai più comuni cyber attacchi. La rete e gli apparati sono aggiornati con patch di sicurezza raccomandate e necessarie ad escludere le intrusioni ed accessi non autorizzati.
ADL offre un servizio per la protezione/mitigazione dagli attacchi DDoS (Distributed Denial of Service) più comuni e frequenti verso la rete e il livello di trasporto, con la possibilità di personalizzare la funzionalità.
I servizi cloud, sono gestiti attraverso azioni di supporto, gestione e configurazione tali da garantire le seguenti funzionalità basilari:

I. Gestione sistemistica della piattaforma hardware;
II. Installazione degli aggiornamenti sistemistici delle componenti installate;
III. Gestione operativa della piattaforma software di monitoraggio a tutti i livelli e di Cloud Computing per il networking, server, storage, backup.

Sono messi in atto i seguenti meccanismi:

- Segregazione degli ambienti infrastrutturali e applicativi per garantire l'isolamento dei singoli ambienti dei Clienti utilizzando soluzioni di virtualizzazione;
- Sicurezza delle comunicazioni tra rete pubblica mediante protocolli di cifratura;
- Apparati e sistemi per contrastare i più comuni attacchi su Internet, gestiti da staff tecnico specializzato;
- Validazione della configurazione di sicurezza con test periodici sull'infrastruttura fisica e virtuale fornita (vulnerability assessment e penetration test);
- Hardering degli hypervisor, delle VM fornite sotto forma di immagini e aggiornamento delle patch di sicurezza;
- Tutti i sistemi cloud utilizzano un sistema di NTP per sincronizzare i propri orologi e mantenere coerenza degli eventi. Tutte le VM fornite utilizzano come fonte di sincronizzazione clock quella dell'host in cui risiede;
- ADL mette a disposizione un'infrastruttura idonea alla costituzione di applicazioni ad elevata disponibilità dove siano evitabili singoli punti di guasto, nei seguenti termini: del tipo: architettura server basata su tecnologia di virtualizzazione VMWare con ridondanza per garantire una adeguata tolleranza ai guasti. In caso di guasto (failure) di un nodo, il software di gestione dell'ambiente virtuale è in grado di ridistribuire i carichi di lavoro su altri nodi ;
- Ridondanza degli apparati

Responsabilità del Cliente e Raccomandazioni

Sarà cura del Cliente installare sui sistemi utilizzati misure adeguate di protezione e/o di sicurezza dei propri dati (antivirus, firewall per applicazioni etc.), idonee anche a evitare danni ai dati di terzi, e comunque nel rispetto di quanto disposto dalle normative vigenti. Il Cliente riconosce che la mitigazione (protezione dagli attacchi DDoS) fornita da ADL non lo dispensa, in nessun caso, dall'onere di provvedere all'adozione di misure atte a garantire la sicurezza del proprio Servizio, ad esempio installando strumenti di sicurezza (firewall, etc.), procedendo al regolare aggiornamento del sistema, salvando i propri dati e controllando la sicurezza delle proprie applicazioni (script, codici, etc…).

14 Sicurezza logica e controllo accessi

ADL pone molta attenzione nella gestione delle utenze e dei relativi profili di accesso. Per questo scopo, qualora si renda necessario l'intervento di amministratori di sistema sui sistemi cloud, limita l'accesso alle informazioni ed ai servizi erogati secondo i criteri di "need to access" ovvero alle effettive e legittime necessità operative di ciascun soggetto, e "least privilege" per il quale ogni operatore è concesso il privilegio minimo necessario per poter svolgere i propri compiti. Sono emesse specifiche politiche in merito alla corretta gestione dei profili di accesso di tipo amministrativo (dell'infrastruttura di virtualizzazione e della console di gestione) e separazione organizzativa in modo che tutte le attività siano eseguite secondo un processo definito per le quali sia possibile mantenerne traccia.

ADL raccomanda al Cliente che l'accesso al pannello di controllo dei servizi è personale ed a non diffondere i propri dati di accesso.

Responsabilità e Raccomandazioni per il Cliente

Il Cliente è responsabile per l'uso e la configurazione del sistema di gestione di controllo degli accessi fornito da ADL e per l'assegnazione dei corretti diritti di accesso al personale che ritiene adeguato. Il Cliente è responsabile della corretta conservazione delle credenziali di accesso ai servizi, dell'eventuale utilizzo improprio o malevolo di tali credenziali, anche se effettuato da terzi (ad esempio partner tecnologici).

14 Sicurezza operativa

ADL si impegna a garantire la continuità e la prevenzione blocchi dei servizi erogati secondo quanto concordato nei termini e condizioni contrattuali di riferimento. ADL ha implementato nell'ambito della propria organizzazione apposite procedure di seguito indicate:

- Gestione e monitoraggio degli eventi di sicurezza e procedura di escalation a fronte di fault o anomalie che hanno un impatto rilevante sull'operatività aziendale;
- Procedure per la gestione degli incidenti per garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio;
- Gestione controllata dei cambiamenti di qualunque modifica al sistema, e della capacità degli apparati e delle infrastrutture, per garantire il mantenimento nel tempo di un'adeguata prestazione del Sistema anche al variare delle condizioni tecniche, funzionali e di utenza;
- Procedure di creazione, gestione e manutenzione di Backup e Restore delle informazioni, del software e delle immagini dei sistemi e sottoposti a test periodici.

Responsabilità e Raccomandazioni per il Cliente

È cura del Cliente la facoltà di eseguire in autonomia il backup dei propri dati per l'intera durata del contratto e per il successivo intervallo eventualmente indicato nei termini e condizioni contrattuali. In tutti i casi il Cliente è responsabile di validare il contenuto e l'allineamento dei suoi dati e il rispetto delle prescrizioni normative a seguito di eventuali attività di ripristino da backup che ADL comunicherà.

16 Sicurezza dei dati

Il Cliente ha il diritto e la possibilità di conoscere dove i loro dati si trovano ed eventualmente poter decidere se tenerli o cancellarli. I dati del Cliente sono archiviati e processati esclusivamente all'interno del Data Center di ADL, gestiti e localizzati in territorio italiano, in conformità alle disposizioni vigenti in ambito privacy e protezione dati.

Il personale di ADL **non accede e non controlla** i dati ed i contenuti introdotti dai Clienti durante fruizione dei servizi. L'accesso alle risorse del Cliente è consentito esclusivamente per garantire i servizi oggetto del contratto, e in esso dettagliati.

Il cliente potrà depositare dati e oggetti digitali di proprietà, nello spazio associato ai servizi in uso. ADL non esegue trattamenti (tantomeno per finalità di marketing diretto o pubblicitarie) sui dati che il Cliente inserisce nello spazio associato al servizio

utilizzato. Tipicamente, nei servizi cloud, le transazioni di dati sono protetti utilizzando la configurazione di canali sicuri mediante cifratura della sessione.

ADL offre la possibilità di cifrare tutti i dati sottoposti a backup prima del trasferimento e la possibilità di aggiungere opzionalmente ulteriori livelli di cifratura.
Eventuali archivi cartacei sono gestiti in ottemperanza alle disposizioni di privacy previste in materia di trattamento dei dati senza l'ausilio di strumenti informatici.
ADL si impegna a garantire che apparecchiature, dati e applicazioni non vengano portati all'esterno del perimetro aziendale senza preventiva autorizzazione. Sono previste misure di sicurezza per gli asset aziendali collocati o trasportati all'esterno delle sedi di ADL, previa attenta valutazione dei rischi.

Responsabilità e Raccomandazioni per il Cliente

ADL non risponde pertanto degli eventuali danni causati a terzi da parte di hardware e software di proprietà del Cliente e dovuti alla mancanza di tali misure minime di sicurezza. Il Cliente si impegna altresì a comunicare senza ritardo ADL dell'eventuale accesso non autorizzato al proprio sistema di accesso al Servizio ovvero a comunicare ogni violazione della sicurezza del Servizio che dovesse riscontrare. Inoltre le Parti dichiarano fin d'ora che faranno fede nei loro rapporti esclusivamente i Log di ADL conservati secondo legge, anche in ordine alle attività effettuate dal Cliente, ovvero da terzi dallo stesso autorizzati, nell'ambito del Servizio.

17 Registrazione eventi (logging)

I sistemi forniti sono configurabili mediante meccanismi che consentono il tracciamento ed il costante monitoraggio degli accessi e, ove necessario delle attività svolte dalle diverse tipologie di utenze (es Amministratori di Sistema).
ADL, raccoglie e conserva i log dei server per gli accessi privilegiati ai sistemi in osservanza ai requisiti legali. Sono disponibili per il Cliente i log applicativi da loro prodotti nell'utilizzo dei servizi, ovvero da terzi dallo stesso autorizzati.

Responsabilità e Raccomandazioni per il Cliente

È un impegno del Cliente analizzare le informazioni messe a disposizione da ADL ed implementare e gestite ulteriori sistemi di monitoraggio e registrazione nell'utilizzo dei servizi, in base alle necessità.

18 Segnalazione di vulnerabilità

ADL si impegna a garantire che i suoi sistemi IT siano sicuri, dati e applicazioni sono protetti e sono accessibili solo agli utenti autorizzati.

Responsabilità e Raccomandazioni per il Cliente

Prima di utilizzare i servizi cloud, gli utenti dell'ambiente devono valutare se l'uso è appropriato e seguire le linee guida in questo documento per limitare il rischio imposto sui dati trattati. È cura del Cliente identificare eventuali vulnerabilità tecnologiche di sua responsabilità definendo le modalità di gestione.
Il Cliente deve segnalare eventi di potenziali vulnerabilità di sicurezza:

A. Comunicando privatamente ad Applico Digital Lab i dettagli di una sospetta vulnerabilità tramite service desk;
B. Fornendo i dettagli completi della sospetta vulnerabilità in modo che il team addetto alla sicurezza di Applico Digital Lab possa convalidare e riprodurre il problema.

Ultimo aggiornamento
25/04/2020

Il fornitore di servizi cloud
Applico Digital Lab Srl