Documento di Responsabilità Condivisa per i Servizi Cloud

Premessa

Il presente documento descrive la ripartizione delle responsabilità tra il Fornitore di Servizi Cloud (Nordcom in seguito indicato come “FSC”) e il Cliente in riferimento alla sicurezza, gestione, conformità e accesso ai dati e alle risorse in un ambiente cloud.

Responsabilità del Fornitore di Servizi Cloud (FSC)

Le responsabilità di FSC, suddivise per i diversi ambiti di appartenenza, sono descritte qui di seguito. Non sussistono altre responsabilità in capo al FSC salvo quelle di seguito espressamente indicate.

Sicurezza dell'infrastruttura:

- Sicurezza fisica dei data center, inclusi sistemi di controllo accessi e protezione perimetrale.
- Sicurezza virtuale dell'infrastruttura cloud, con implementazione di firewall, sistemi di rilevamento delle intrusioni e tecnologie di prevenzione delle intrusioni.
- Sicurezza dei sistemi di archiviazione, con crittografia dei dati a riposo e in transito.
- Gestione delle vulnerabilità e patching tempestivo di software e sistemi.
- Monitoraggio continuo della sicurezza dell'infrastruttura e dei sistemi.

Disponibilità del servizio:

- Garanzia di uptime del servizio cloud secondo gli eventuali livelli di servizio concordati nel contratto.
- Implementazione di sistemi di disaster recovery e piani di ripristino per garantire la continuità del servizio in caso di eventi di down.
- Comunicazione trasparente al Cliente in caso di interruzioni del servizio o manutenzione programmata.

Protezione dei dati:

- Implementazione di misure di sicurezza adeguate (come descritte in contratto/nomina) per proteggere i dati del Cliente da accessi non autorizzati, uso improprio, divulgazione, modifica o distruzione.

- Crittografia dei dati del Cliente a riposo e in transito su richiesta espressa del Cliente e previo accordo specifico sul punto.
- Controllo degli accessi ai dati del Cliente basato su ruoli e privilegi.
- Gestione degli incidenti di sicurezza informatica e notifica tempestiva al Cliente in caso di violazioni o intrusioni.

Conformità normativa:

- Rispetto delle normative applicabili in materia di protezione dei dati e sicurezza informatica (iGDPR e la ISO/IEC 27001).
- Formazione del personale del FSC sulle normative applicabili.
- Audit periodici per verificare la conformità del FSC alle normative citate.

Responsabilità del Cliente

Le responsabilità del cliente possono variare in funzione della declinazione del servizio (PAAS, SAAS, IAAS) come sotto riportato. Di seguito le responsabilità principali e sempre sussistenti.

Sicurezza dei dati:

- Configurazione di accessi sicuri al servizio cloud, con autenticazione multifattoriale e password robuste.
- Gestione delle credenziali di accesso con adeguate misure di sicurezza.
- Protezione dei dati sensibili con crittografia e controlli di accesso granulari.
- Formazione del personale del Cliente sulle best practice di sicurezza informatica.

Conformità alle normative:

- Rispetto delle normative applicabili in materia di protezione dei dati e sicurezza informatica, in particolare per quanto riguarda la gestione dei dati personali (GDPR).
- Nomina di un Data Protection Officer (DPO) se necessario.
- Adozione di misure tecniche e organizzative adeguate per proteggere i dati personali.

Gestione delle applicazioni e dei dati (non applicabile in caso di appartenenza alla declinazione SAAS):

- Installazione, configurazione e manutenzione delle proprie applicazioni in ambiente cloud.

- Gestione e backup dei propri dati in conformità alle best practice di sicurezza.
- Monitoraggio delle prestazioni e dell'utilizzo delle proprie applicazioni.
- Risoluzione dei problemi tecnici relativi alle proprie applicazioni.

Accesso e utilizzo del servizio:

- Utilizzo del servizio cloud in modo conforme al contratto con FSC e suoi fornitori e alle normative applicabili.
- Rispetto delle policy di utilizzo del FSC e di eventuali limiti di utilizzo del servizio.
- Notifica tempestiva al FSC di qualsiasi attività sospetta o anomala rilevata in ambiente cloud.

Salva diversa previsione in contratto, si riporta sotto uno schema sintetico della distribuzione delle responsabilità in funzione della tipologia di servizio cloud erogato.

	On-prem	IAAS	PAAS	SAAS
Contenuti				
Policy di accesso				
Sicurezza applicazioni web				
Gestione credenziali di accesso/identità4				
Autenticazione				
Sicurezza network				
Sistema operativo				
Audit log				
Network				
Storage and encryption				
Hardware				
Responsabilità del CLIENTE				
Responsabilità del FORNITORE				