Il presente estratto sintetizza il contenuto della politica sul cloud adottata e definisce come l'organizzazione governa la sicurezza delle informazioni nei servizi cloud, in coerenza con il SGSI e con le linee guida ISO/IEC 27017, estendendo i principi della ISO/IEC 27001/27002 al contesto specifico.
Si applica sia ai servizi cloud utilizzati internamente sia ai servizi SaaS erogati ai clienti, coinvolgendo dipendenti, utenti terzi come i consulenti e i fornitori che trattano, ospitano o trasmettono dati aziendali.
La selezione dei provider di terze parti avviene sulla base della classificazione dei dati e della criticità degli asset, e richiede requisiti stringenti su sicurezza, portabilità e chiusura del servizio, tutela della privacy, localizzazione dei server e trasferimenti transfrontalieri, raccolta delle evidenze digitali, backup e disaster recovery, gestione dei cambiamenti e livelli di servizio; sono privilegiati i fornitori con attestazioni come ISO 27001 con estensione 27017 o SOC 2 Type II, oggetto di verifiche periodiche.

L'organizzazione, nell'ambito dei servizi cloud, opera in una doppia veste: come Cloud Service Customer utilizza IaaS/PaaS di terzi per le proprie applicazioni, assumendo la responsabilità di sistemi operativi, configurazioni, applicazioni e dati; come Cloud Service Provider progetta ed eroga servizi SaaS, integrando requisiti di sicurezza by design e by default lungo l'intero ciclo di vita.
Nel primo caso, la politica considera i rischi legati all'accesso potenziale del provider e alla multi-tenancy, imponendo controlli su accessi privilegiati, autenticazione forte, principio del minimo privilegio, baseline di configurazione e classificazione dei dati, con clausole contrattuali chiare e verifiche dell'adeguatezza delle misure dei fornitori.
Nel secondo, prevede segregazione rigorosa tra tenant, tracciatura e controllo degli accessi amministrativi, processi formali di change management e gestione del ciclo di vita degli account dei clienti, oltre a misure tecniche come cifratura, controllo accessi e monitoraggio continuo.

La gestione degli incidenti segue un processo strutturato di identificazione, risposta, ripristino e analisi post-evento, con coordinamento verso i provider IaaS/PaaS secondo le responsabilità contrattuali e comunicazioni tempestive ai clienti quando necessario. Il monitoraggio dell'efficacia dei controlli, gli audit e le azioni correttive assicurano il miglioramento continuo. La policy è allineata con la SoA per giustificare l'applicabilità dei controlli ISO nel cloud ed è soggetta a riesame periodico della Direzione, con approvazione formale e comunicazione delle modifiche alle parti interessate.

1 settembre 2025
Alessio Lucarotti