POLITICA PER LA SICUREZZA DELLE INFORMAZIONI NEI SERVIZI CLOUD

La presente politica definisce i principi e le modalità attraverso cui l'organizzazione garantisce la sicurezza delle informazioni trattate nell'ambito dei servizi cloud, in coerenza con il proprio Sistema di Gestione della Sicurezza delle Informazioni e con le linee guida della norma ISO/IEC 27017. Essa si applica sia ai servizi cloud utilizzati internamente sia ai servizi gestiti erogati ai clienti, nel contesto di un modello operativo in cui l'organizzazione utilizza infrastrutture di terze parti e, al contempo, gestisce ambienti cloud per conto dei propri clienti.

La gestione della sicurezza nel cloud si basa sul principio della responsabilità condivisa, secondo cui i fornitori cloud sono responsabili della sicurezza dell'infrastruttura sottostante, mentre l'organizzazione è responsabile della configurazione, della gestione e della protezione degli ambienti e dei dati sotto il proprio controllo. In tale contesto, l'organizzazione adotta un approccio strutturato che integra i requisiti di sicurezza nelle attività di progettazione, configurazione e gestione dei servizi, assicurando che le misure tecniche e organizzative siano adeguate ai rischi e coerenti con le esigenze operative e normative.

La selezione dei fornitori cloud avviene attraverso un processo di valutazione basato sul rischio, che tiene conto della criticità dei servizi, della natura delle informazioni trattate e delle garanzie di sicurezza offerte, incluse le certificazioni e la documentazione tecnica disponibile. Considerata la frequente non negoziabilità delle condizioni contrattuali nei servizi cloud, l'organizzazione fonda le proprie decisioni su un'analisi approfondita delle caratteristiche dei servizi e sulle evidenze rese disponibili dai fornitori.

Nell'utilizzo dei servizi cloud, l'organizzazione mantiene il controllo delle configurazioni, degli accessi e delle misure di protezione dei dati, adottando principi quali il minimo privilegio e l'autenticazione adeguata al rischio. Particolare attenzione è riservata alla gestione degli accessi privilegiati, alla protezione delle informazioni in ambienti condivisi e alla valutazione degli impatti derivanti dalla localizzazione geografica dei dati e dai possibili trasferimenti tra giurisdizioni.

Nell'erogazione dei servizi ai clienti, l'organizzazione assume la responsabilità operativa per la sicurezza degli ambienti gestiti, garantendo la protezione dei dati, la separazione logica tra i diversi clienti e il controllo delle attività amministrative. Le attività sono svolte secondo

principi di sicurezza by design e by default e sono supportate da processi formalizzati per la gestione delle configurazioni, degli accessi e del ciclo di vita delle risorse.

La gestione degli incidenti di sicurezza avviene mediante un processo strutturato che consente di identificare, analizzare e gestire tempestivamente gli eventi, coordinando le attività con i fornitori cloud nei casi di loro competenza e assicurando adeguata comunicazione ai clienti interessati.

L'organizzazione assicura il monitoraggio continuo degli ambienti cloud e la verifica periodica dell'efficacia dei controlli adottati, utilizzando le evidenze raccolte per il miglioramento continuo delle misure di sicurezza. La politica costituisce inoltre riferimento per la definizione e l'applicazione dei controlli nell'ambito della Statement of Applicability, tenendo conto del modello di responsabilità condivisa e degli ambiti sotto il controllo diretto dell'organizzazione.

La presente politica è soggetta a riesame periodico da parte della Direzione al fine di garantirne la costante adeguatezza rispetto all'evoluzione del contesto tecnologico, operativo e normativo, nonché ai rischi associati ai servizi cloud utilizzati ed erogati.

Michele Rocchini

General Manager - System Line Srl

SYSTEM LINE srl
Sede: 50053 EMPOLI (FI)
Via 1° Maggio, 75
Tel. 0571.72329 - Fax 0571.74702
C.F. e P.IVA 03197970480