POLITICA SERVIZI IN CLOUD

PREMESSA

Il Cloud Computing sta trasformando il mondo dell'informatica all'interno delle aziende. La tecnologia Cloud consente infatti alle Aziende di ottenere le risorse di cui hanno bisogno senza l'esigenza di avere e mantenere una infrastruttura IT interna, riuscendo ad offrire dei servizi comunque sicuri, efficienti, rapidi e immediati, con risorse flessibili e garantendo scalabilità, qualora emergessero nuove esigenze.

L'utilizzo di queste risorse remote, non sotto diretto controllo NEXTER, aumenta però la responsabilità da parte NEXTER nel scegliere correttamente il fornitore di servizi di cui avvalersi per l'erogazione del proprio servizio.

Per erogare in maniera sicura il nostro servizio di "Sistemi di controllo degli accessi alle Zone a Traffico Limitato e relativi servizi erogati in cloud computing in modalità IaaS-SaaS", la nostra NEXTER ha deciso di avvalersi di cloud service providers riconosciuti a livello internazionale, che garantiscono la sicurezza nel trattamento delle informazioni a loro affidate e livelli di servizio senza interruzione di continuità, nel pieno rispetto delle best practices del settore.

La nostra NEXTER ha deciso di utilizzare questi fornitori di servizi cloud per aumentare le funzionalità e la disponibilità del servizio, in modo da migliorare la soddisfazione generale del cliente finale.

SCOPO E OBIETTIVI

I servizi cloud forniscono un accesso comodo e on-demand a un pool condiviso di risorse di elaborazione configurabili (ad esempio reti, server, storage, applicazioni e servizi). Lo scopo di questa politica è stabilire processi e procedure che dovranno rispettare i provider di servizi cloud a cui NEXTER si affida, le loro responsabilità e strategie di gestione per proteggere le applicazioni e i dati dei clienti forniti tramite l'utilizzo del servizio di "Sistemi di controllo degli accessi alle Zone a Traffico Limitato e relativi servizi erogati in cloud computing in modalità IaaS-SaaS".

CAMPO DI APPLICAZIONE

Questa policy si applica a tutto il personale, gli utenti e gli appaltatori NEXTER che creano, distribuiscono o supportano l'infrastruttura, le applicazioni e/o il software di sistema in un'infrastruttura basata su cloud, ospitata da providers esterni.

POLITICA SERVIZI CLOUD

La tecnologia cloud si è evoluta nel corso degli anni e consente oggi di offrire quasi tutte le risorse IT come servizio. Nella corretta scelta del cloud service provider da utilizzare, NEXTER adotta i seguenti processi e criteri, che devono essere seguiti quando valuterà offerte di servizi basati su cloud:

A. RESPONSABILITA'

Il PM, in coordinamento con il DGE, garantisce che tutte le offerte di servizi cloud vengano valutate e selezionate tramite un processo coerente e ripetibile.
Devono essere applicate le seguenti linee guida:

Risk Assessment – Un Risk Assesment interno deve essere effettuato per valutare affidabilità e sicurezza del cloud service provider. L'analisi deve identificare i rischi per l'NEXTER, e per i dati dei clienti che vengono trattati, processati, conservati dal cloud provider sulle proprie infrastrutture. E' necessario che venga effettuato un controllo del rispetto di standard e best practices da parte del cloud provider, nonchè preferenziale per la sua scelta risulterà la presenza di certificazioni del settore riconosciute.
Altro elemento preferenziale sarà la presenza di Disaster Recovery plan del cloud provider e la dichiarata ridondanza dei suoi sistemi per garantire il massimo livello di up-time del servizio.
Tali informazioni potranno essere rilevate tramite il sito web del cloud provider, tramite Data Processing Agreement o altro contratto che si andrà con esso a stipulare.

Parte di tale attività da parte di PM, in coordinamento con DGE, sarà quella di pianificare azioni di mitigazione e risposta nel caso comunque accadano eventi indesiderati con il cloud service provider, in modo da offrire il minimo disservizio al cliente finale.

Appalti e Contratti – Il AMM o il suo designato garantisce che tutte le politiche e le pratiche standard NEXTER in materia di appalti siano in vigore e seguite per quanto riguarda gli appalti generali.

Il modello di contratto standard NEXTER è utilizzato come base per tutte le relazioni con i fornitori di servizi. Tutti i termini specialistici relativi alla privacy dei dati dei clienti, al cloud computing e ai fornitori di terze parti devono essere applicati.

Ciò include, a titolo esemplificativo ma non esaustivo:

- Attività di due diligence, tra cui controlli sulla preparazione del personale, adeguata esperienza nel settore, presenza di assicurazione contro i danni a terzi.
- Garanzia che il personale del fornitore non violi le politiche, le procedure, gli accordi o i documenti correlati NEXTER.
- AMM NEXTER fornisce un punto di contatto principale per il fornitore responsabile della gestione della relazione, del Service Level Agreement (SLA) e garantisce che il fornitore operi in conformità a tutti i termini del contratto.
- Revisione periodica del personale autorizzato dei fornitori di servizi cloud, che lavorano sui sistemi parti del contratto e dei servizi eseguiti da ciascuno.
- La direzione NEXTER conserva copie di tutti gli accordi e della documentazione richiesta per ogni incarico a provider di servizi cloud.
- Tutti i contratti con i fornitori di servizi cloud devono includere:
    - Evidenza delle misure tecniche ed organizzative poste in essere dal cloud provider, i requisiti minimi di sicurezza pertinenti, compresi i controlli sull'elaborazione, l'accesso, la comunicazione, l'hosting e la gestione dei dati da parte del cloud provider affidatigli NEXTER. Ciò include la crittografia, i controlli di accesso, la prevenzione delle perdite e i controlli di

integrità per i dati scambiati per prevenire la divulgazione, l'uso, l'alterazione o la distruzione impropria dei dati.

- Clausole di riservatezza e privacy a protezione dei dati gestiti dal cloud provider.
- Accesso di sicurezza fisico da parte del personale del cloud provider basato su ruoli ben identificati, a sistemi, dati e applicazioni, che siano accettabili NEXTER.
- Sistemi e metodi di sicurezza adottati dal cloud provider a protezione dei dati affidatigli.
- Periodo massimo di data retention e procedure per la cancellazione delle informazioni presenti sui sistemi del cluod provider quando richiesto.
- Metodi accettabili per la restituzione, la distruzione o lo smaltimento delle informazioni memorizzate sulle risorse del fornitore alla fine dell'accordo.
- Garanzia che il fornitore di servizi deve utilizzare i dati affidatigli NEXTER solo per gli scopi espliciti definiti nel contratto.
- Accordo che qualsiasi informazione acquisita dal fornitore di servizi nel corso del contratto non può essere utilizzata per scopi diversi da quelli specificati nel contratto o divulgate ad altri senza eccezioni / condizioni scritte formali concordate dal proprietario dei dati e NEXTER.

B. REQUISITI DEL CLOUD SERVICE PROVIDER

Il AMM o il suo designato garantisce che ciascun fornitore di servizi rispetti i seguenti processi e procedure:

Accesso a dati personali – Al personale del cloud provider è inibito l'accesso a dati riservati, identificati come dati personali o sensibili, che vengono trattati sui suoi sistemi. E' consentito il trattamento solo per quelle

operazioni autorizzate quali l'esecuzione di attività di Disaster Recovery, qualora il sito dove viene effettuato il trattamento sia da ripristinare operativamente. Qualsiasi attività di trattamento termina alla cessazione della fornitura dei servizi, con obbligo di restituzione da parte del cloud provider delle informazioni presenti sui loro sistemi e successiva cancellazione immediata.

Comunicazione Incidenti di Sicurezza – Il fornitore deve segnalare immediatamente qualsiasi incidente di sicurezza correlato a compromissioni di dati fisici o logici al AMM NEXTER incaricato, ed intraprendere poi tutte le azioni necessarie per mitigare in futuro il ripresentarsi di tali rischi di sicurezza, dando opportuna evidenza delle misure applicate.

Termine del servizio – Il fornitore deve garantire che tutti i dati trattati per conto di NEXTER siano raccolti e restituiti NEXTER stessa e fornire una certificazione scritta di distruzione dei dati entro un periodo concordato.

Audit – Ai fornitori può essere richiesto di sottoporsi ad audit periodici per la sicurezza delle informazioni da parte di NEXTER. Nel caso il cloud provider non sia disponibile, è richiesto che fornisca evidenza che venga sottoposto ad audit periodicamente da parte di organizzazioni terze.

Data Breaches – Il cloud provider deve informare NEXTER entro ventiquattro (24) ore dalla scoperta di una violazione della sicurezza ad uno dei suoi sistemi che gestisce dati personali conferiti da NEXTER. A seguito di tale notifica, NEXTER si riserva il diritto, ma non l'obbligo, di risolvere il contratto con il fornitore di servizi cloud. Il cloud provider sosterrà tutti i costi sostenuti per porre rimedio alla violazione, i suoi clienti e le spese correlate relative all'incidente.

GESTIONE DOCUMENTALE E PROCEDURE

Per questa politica operativa verranno prodotte procedure documentate ed evidenze, da rendersi disponibili anche per richieste in fase di audit, sulle scelte effettuate riguardanti i cloud service providers utilizzati per l'erogazione del servizio, come parte dei processi operativi interni NEXTER.

A titolo di esempio:

- Conservazione della documentazione contrattuale per gli attuali fornitori di provider di servizi cloud e di eventuali precedenti;
- Documentazione interna relativa ai processi di valutazione dei rischi e ai componenti di mitigazione per i cloud providers utilizzati, sia attualmente che eventuali precedenti.

VIOLAZIONI

I destinatari della presente politica, se trovati in violazione delle norme presentate, possono essere ad azioni disciplinari, fino alla risoluzione del contratto di lavoro inclusa, nei casi previsti dalla legge.

COMUNICAZIONE

Questa politica deve essere distribuita a tutto il personale di NEXTER coinvolto nei servizi IT cloud, relativi al servizio di "Sistemi di controllo degli accessi alle Zone a Traffico Limitato e relativi servizi erogati in cloud computing in modalità IaaS-SaaS" ed eventualmente agli appaltatori che utilizzano le risorse informative di tale servizio, solamente se necessario.

VERSIONI

Versione	Data	Descrizione	Approvato da
0.1	04/04/2023	Prima emissione	DG - Cavalli Pierpaolo