L'acquisto di servizi cloud nel settore pubblico

Manuale con testo di esempio di una RDO nell'ambito di un Accordo quadro per il cloud

Versione 2: febbraio 2022

Avvisi

Il presente documento viene fornito esclusivamente a scopo informativo. Non è stato redatto in base ai requisiti di legge delle procedure di appalto pubblico di alcuna particolare regione. I clienti di servizi cloud sono tenuti a condurre autonomamente una valutazione delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi offerti dal fornitore di servizi cloud. Il presente documento non produce nessuna garanzia o dichiarazione, né impegni contrattuali, condizioni o assicurazioni.

I documenti e i testi di esempio non devono essere interpretati come consulenze legali, istruzioni o consigli. I clienti cloud sono tenuti a rivolgersi a un consulente legale di fiducia per chiarire le proprie responsabilità ai sensi del diritto applicabile nel Paese dove l'azienda opera. Il CISPE declina espressamente qualsiasi garanzia o responsabilità o richiesta risarcitoria conseguente a, o in relazione a, informazioni contenute nel presente documento.

Informazioni sul CISPE

Il CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) è un'associazione di categoria indipendente senza scopo di lucro. Nel rappresentare i fornitori di infrastrutture e servizi cloud in Europa, collaboriamo con gli operatori del settore e con i legislatori al fine di offrire indicazioni e consigli sui servizi cloud e sul ruolo che questi ultimi occupano nel comparto, nella vita pubblica e nella società in generale.

La nostra associazione è in costante espansione e include aziende che operano in tutti i Paesi dell'UE e con sedi legali in ben 16 Paesi europei. La nostra è un'associazione aperta alle aziende, con l'unico requisito che almeno uno dei servizi offerti dall'azienda abbia ottenuto la dichiarazione di conformità al Codice di condotta CISPE sulla protezione dei dati. Il nostro ruolo consiste nel:

- Promuovere i vantaggi delle politiche "cloud first" (cloud al primo posto) negli appalti pubblici dell'UE e degli Stati membri dell'UE
- Coinvolgere il settore delle infrastrutture cloud per raggiungere la neutralità climatica entro il 2030
- Promuovere l'adozione di requisiti di sicurezza e di standard tecnici uniformi in tutta l'UE
- Sostenere i requisiti di riservatezza generali tramite un Codice di condotta sulla protezione dei dati
- Assicurare che il mercato delle infrastrutture cloud nell'UE sia aperto, competitivo e libero da vincoli (lock-in)
- Impedire l'imposizione ingiustificata di obblighi di monitoraggio dei contenuti nel quadro giuridico dell'UE

Il compito dei nostri associati è fornire e gestire "gli elementi costitutivi dell'IT", senza i quali la pubblica amministrazione, gli enti pubblici e le imprese non potrebbero realizzare i propri sistemi ed erogare servizi essenziali a miliardi di cittadini. A tal fine, contribuiamo allo sviluppo di tecnologie e servizi altamente innovativi, che inglobano l'intelligenza artificiale (IA), gli oggetti connessi, i veicoli a guida autonoma e il 5G, fino ad arrivare alle tecnologie di prossima generazione per la connettività cellulare.

Codice di condotta per i servizi di infrastrutture cloud

Il Codice di condotta CISPE sulla protezione dei dati, lanciato pubblicamente a settembre 2016, è antecedente all'entrata in vigore del Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea. In linea con i severi requisiti del GDPR, il codice aiuta i fornitori di infrastrutture cloud ad applicare la conformità alla protezione dei dati; offre, altresì, un quadro di riferimento solido per aiutare i clienti a selezionare i fornitori di servizi cloud e ad affidarsi ai loro servizi. Il Codice di Condotta CISPE è stato validato dal Comitato europeo per la protezione dei dati (EDPB) a maggio 2021 e approvato dall'Autorità francese per la protezione dei dati (CNIL) in qualità di Autorità Competente a giugno 2021. https://www.codeofconduct.cloud/

Patto per la neutralità climatica dei data center

Alla fine del 2019, il CISPE si è impegnato con la Commissione Europea a sviluppare una serie di parametri e un'iniziativa di autoregolamentazione finalizzate a garantire la neutralità climatica dei data center entro il 2030. Questa iniziativa, sviluppata insieme alla European Data Center Association (EUDCA) e ad altre associazioni di categoria e attori del mercato dei data center, è stata

lanciata a gennaio 2021 con il nome di "Climate Neutral Data Center Pact" (Patto per la neutralità climatica dei data center) https://www.climateneutraldatacentre.net/

Iniziativa Fair software

Insieme all'associazione dei CIO francesi, CIGREF, e con il supporto di altre associazioni di categoria di CIO e fornitori in tutta Europa, il CISPE ha lanciato i Dieci Principi per una gestione delle licenze software equa e corretta per gli utenti del cloud; si tratta di un insieme di best practice rivolte alle aziende che vogliono spostarsi nel cloud per favorire lo sviluppo, l'innovazione e la flessibilità e che chiedono ai fornitori di software la garanzia di termini di licenza equi chiaramente definiti.
https://www.fairsoftware.cloud/

GAIA-X

Il CISPE è stato uno dei ventidue membri fondatori di GAIA-X, l'iniziativa europea per creare un ecosistema digitale aperto, trasparente e sicuro. In quanto tale, il CISPE si è impegnato sin dall'inizio nella visione e nei principi dell'organizzazione GAIA-X; il suo Segretario generale è stato rieletto a giugno 2021 per far parte del consiglio di amministrazione. Alcuni strumenti citati nel manuale, come il Codice di condotta CISPE sulla protezione dei dati e il Codice di condotta SWIPO IaaS, sono utili per dimostrare la conformità ai principi GAIA-X. https://www.gaia-x.eu

Il CISPE e il settore pubblico

Il CISPE partecipa attivamente al dibattito pubblico europeo, promuovendo una migliore comprensione del ruolo, del contributo e del potenziale del comparto delle infrastrutture cloud in Europa.

I modelli di acquisto della pubblica amministrazione dovrebbero condizionare l'adozione e l'utilizzo del cloud computing. Tuttavia, l'acquisizione dei servizi cloud differisce dalle forme più tradizionali di acquisizione di tecnologie note al settore pubblico. Il meccanismo degli appalti va ripensato. A questo scopo, il CISPE incoraggia i legislatori europei a sviluppare un approccio più ambizioso e lungimirante su scala UE, basato su iniziative politiche "cloud first" che stimolino la crescita del mercato unico delle infrastrutture cloud nell'UE e assicurino il conseguimento degli obiettivi di crescita del mercato unico digitale (Digital Single Market, DSM).

Lo scopo del presente manuale è fornire indicazioni utili agli enti pubblici, per assisterli nell'acquisizione dei servizi cloud.

Ulteriori informazioni

Associati CISPE: https://cispe.cloud/members
Consiglio direttivo: https://cispe.cloud/board-of-directors
Servizi di cloud computing dichiarati ai sensi del Codice di condotta CISPE:
https://www.codeofconduct.cloud/public-register/

Indice

v2: febbraio 2022

Sommario e scopo del presente manuale

Lo scopo del presente **Manuale per l'acquisto di servizi cloud** è assistere i clienti che desiderano acquistare i servizi cloud tramite una procedura di appalto competitiva, denominata **Richiesta di Offerta (RDO, ovvero "Request for Proposal", RFP) di servizi cloud**, i quali sono tuttavia privi delle competenze necessarie per redigere autonomamente un Accordo quadro per il cloud (Cloud Framework Agreement).

Il presente documento viene fornito esclusivamente a scopo informativo. Non è stato sviluppato in base ai requisiti di legge delle procedure di appalto pubblico di alcun particolare Paese o regione.

Il manuale contiene, inoltre, il testo di esempio per definire i criteri di selezione degli **ordini a chiamata** ("call off") o delle **mini-gare**, qualora gli acquisti avvengano al di fuori di un Accordo quadro per il cloud. Il manuale è suddiviso in capitoli che riflettono la struttura di una Richiesta di Offerta (RDO) generica per il settore IT. Una RDO generica e il testo di esempio per definire i criteri di selezione sono accompagnati da commenti utili per comprendere cosa distingue una RDO per il cloud da una RDO per il settore IT tradizionale.

A seguito della pubblicazione della Strategia cloud della Commissione europea che guida le istituzioni e le agenzie europee nel percorso di modernizzazione della propria infrastruttura IT attraverso un approccio cloud-first, il CISPE ha consegnato il manuale alla Commissione europea a luglio 2019 in occasione dell'evento *"Come trasformare la pubblica amministrazione attraverso una politica cloud intelligente"*.

La **versione 2** del presente manuale include nuove linee guida in materia di protezione dei dati (paragrafo 2.3.1.1), cambio di fornitori di servizi cloud e portabilità dei dati (paragrafo 2.3.1.2), termini e condizioni del software (paragrafo 2.5.2), sostenibilità nel cloud (paragrafo 3.6) e una valutazione tecnica in tempo reale nell'Appendice B aggiornata.

*Con **"servizi cloud"** si intendono tutte le tecnologie destinate al cloud e i servizi correlati a cui un utente finale potrebbe dover accedere. Sono compresi i servizi di consulenza/professionali/gestiti che supportano ed eseguono la migrazione al cloud e che supportano i carichi di lavoro nel cloud, oltre all'infrastruttura cloud stessa e ai servizi marketplace per il cloud, ad esempio i prodotti Software come servizio (SaaS).*

L'affermazione del cloud computing come scelta preferenziale per l'IT nel settore pubblico rappresenta anche l'occasione per ammodernare le strategie di appalto esistenti. Grazie alle procedure di acquisto incentrate sul cloud, gli enti pubblici possono sfruttare appieno i vantaggi del cloud (ad esempio, l'accesso immediato alle innovazioni, l'aumento di velocità e agilità, il miglioramento della posizione di sicurezza e della governance della conformità) lavorando, nel contempo, a un piano di efficientamento e taglio dei costi.

Le tradizionali procedure di appalto del settore IT finalizzate all'acquisto di hardware, software e data center non possono essere applicate direttamente all'acquisto di servizi cloud. Un modello cloud prevede un approccio completamente diverso rispetto ad argomenti quali la determinazione del prezzo, la governance dell'appalto, i termini e le condizioni, la sicurezza, i requisiti tecnici, gli accordi sul livello del servizio (SLA) e così via. Per questa ragione, l'utilizzo delle procedure di appalto esistenti riduce o annulla i vantaggi offerti dal cloud.

Uno degli strumenti migliori per l'acquisizione efficiente dei servizi cloud nel settore pubblico è un Accordo quadro per il cloud: l'assegnazione a più operatori economici di un menu di cloud, dal quale i potenziali acquirenti (affiliati alla centrale di committenza) potranno scegliere le tecnologie cloud e i servizi correlati più idonei alle proprie esigenze. Gli "accordi quadro", in quanto strumenti dei contratti cloud, consentono di acquistare i servizi cloud in modo efficiente e conveniente; gli acquirenti e gli enti utilizzatori finali possono così accedere a una gamma completa di servizi cloud e, all'atto pratico, sfruttare appieno i vantaggi del cloud: agilità, benefici di una grande economia di scala, scalabilità per aumentare la disponibilità a un costo più basso, ampiezza di funzionalità, velocità di innovazione, capacità di adattamento a nuove realtà geografiche.

Nota: il presente documento affronta il tema dell'acquisto di tecnologie cloud Infrastruttura come servizio (IaaS) e Piattaforma come servizio (PaaS), così come fornite da un *CISP (Cloud Infrastructure Service Provider, fornitore di infrastrutture e servizi cloud)*. È possibile acquistare le suddette tecnologie cloud direttamente da un CISP oppure indirettamente, tramite un rivenditore del CISP. *Nel caso di distributori di servizi marketplace per cloud (PaaS e SaaS) e di servizi di consulenza per cloud, si rendono necessarie ulteriori riflessioni sulla RDO.*

Inoltre, si prega di considerare che il presente documento non tratta tutti gli aspetti legati alla predisposizione di un Accordo quadro completo per l'appalto di servizi cloud. Vi sono molti altri documenti, redatti da analisti ed esperti del settore, che affrontano i temi relativi al cloud, ad esempio le best practice per gli appalti, il budget per il cloud, la governance del cloud, ecc. Invitiamo caldamente i lettori a tenere conto di tali documenti e consigli durante lo sviluppo di una strategia generale finalizzata all'appalto di servizi cloud.
La Tabella 1 riporta uno schema del Manuale delle richieste di offerta (RDO) di servizi cloud e l'indicazione dei capitoli dove è possibile trovare il testo di esempio per ogni argomento.

Tabella 1. Capitoli del Manuale delle richieste di offerta (RDO) di servizi cloud

Capitolo	Panoramica e testi di esempio di RDO
1.0 Panoramica di un Accordo quadro per il cloud	Una panoramica generale del modello di Accordo quadro per il cloud (LOTTI, modalità di partecipazione e appalto)

Capitolo	Panoramica e testi di esempio di RDO
2.0 Panoramica della RDO di servizi cloud	Testo di esempio di una RDO generica che include i paragrafi riportati sotto; include anche i commenti che spiegano la logica alla base di una RDO di servizi cloud e lo stile utilizzato.
2.1 Predisposizione della RDO di servizi cloud	2.1.1 Introduzione e obiettivi strategici 2.1.2 Tempistica delle risposte a una RDO 2.1.3 Definizioni 2.1.4 Descrizione dettagliata del modello di acquisto e concorrenza nell'ambito dell'Accordo quadro 2.1.5 Requisiti minimi del candidato - Amministrativi
2.2 Requisiti tecnici	2.2.1 Requisiti minimi 2.2.2 Confronto tra fornitori 2.2.3 Appalto
2.3 Sicurezza	2.3.1 Requisiti minimi 2.3.1.1 Protezione dei dati 2.3.1.2. Cambio di fornitori di servizi cloud e portabilità dei dati 2.3.2. Confronto tra fornitori 2.3.3 Appalto
2.4 Prezzi	2.4.1 Requisiti minimi 2.4.2 Confronto tra fornitori
2.5 Schema/Termini e condizioni per l'esecuzione dell'appalto	2.5.1 Termini e condizioni 2.5.2 Termini e condizioni del software 2.5.3 Come scegliere l'aggiudicatario migliore 2.5.4 Onboarding e offboarding
3.0 Best Practice/Lezioni apprese	3.1 Governance del cloud 3.2 Budget per il cloud 3.3 Comprendere il modello di business dei partner 3.4 Cloud broker 3.5 Approvvigionamento/ricerca di mercato antecedente la RDO 3.6 Sostenibilità
Appendice A - Requisiti tecnici per il confronto tra offerenti	Un elenco di requisiti tecnologici generici per il cloud con riferimento agli ordini a chiamata o alle mini-gare
Appendice B – Valutazione tecnica in tempo reale	Un testo di esempio per dimostrare il punteggio di un prodotto tecnologico per il cloud (le demo del cloud fanno parte dell'ordine a chiamata o della mini-gara)

1.0 Panoramica di un Accordo quadro per il cloud

Se ben strutturato, un Accordo quadro per il cloud può agevolare l'acquisto dei servizi cloud, beneficiando sia le amministrazioni pubbliche sia i fornitori di servizi cloud che vi partecipano. Di seguito i principali vantaggi di un Accordo quadro per il cloud ben strutturato:

- Collaborazione
    - Quando più enti collaborano all'assegnazione di ordini con requisiti simili, si ottengono comodità, efficienza e riduzione dei costi, oltre a una procedura semplificata degli ordini. Si stabilisce un metodo efficace per aggregare più enti pubblici che hanno un comune fabbisogno di tecnologie e di servizi cloud correlati, ad esempio le soluzioni per il marketplace e la consulenza.
- Gamma completa di servizi cloud
    - Può comprendere, al suo interno, tutti i servizi di consulenza/professionali/gestiti necessari per supportare ed eseguire la migrazione al cloud e per supportare i carichi di lavoro nel cloud, le tecnologie cloud fornite dal CISP e i servizi marketplace.
    - È possibile acquistare le tecnologie cloud direttamente da un CISP oppure indirettamente, tramite un rivenditore autorizzato.
- Governance dell'appalto
    - Allinea diverse tipologie di enti/acquirenti a una serie comune di termini e condizioni, e all'aggiudicazione di un unico appalto principale, anziché tanti appalti diversi per ciascun ente.
    - I vantaggi sono importanti anche per i fornitori, in quanto si stabilisce una norma comune per la procedura di acquisto, i termini e le condizioni e il meccanismo degli ordini. Ciò evita la presenza di procedure diverse per ogni ente pubblico.
    - Si garantisce la flessibilità. La creazione, l'approvazione e la gestione di un appalto efficace per il cloud nell'ambito delle policy e dei regolamenti attuali della pubblica amministrazione sono attività che richiedono sperimentazione e la capacità di adattarsi velocemente. È di gran lunga più vantaggioso creare un Accordo quadro che consenta al settore pubblico e ai fornitori cloud di lavorare insieme per migliorare l'appalto (contrattualmente, meccanicamente ed efficientemente). Un appalto pluriennale poco efficiente e non suscettibile di modifiche può causare un danno agli utenti finali dell'ente pubblico, alle stazioni appaltanti e ai fornitori cloud.
- Scelta
    - Offre agli acquirenti l'opportunità di scegliere tra svariati CISP qualificati e aumenta il livello dei servizi cloud e dei servizi correlati, ad esempio il marketplace PaaS/SaaS cloud e le consulenze cloud.
    - Consente di controllare il numero dei fornitori ammessi in un Accordo quadro attraverso la debita verifica dei requisiti di ciascun aggiudicatario.

Un Accordo quadro per l'acquisto di servizi cloud funziona al meglio se include le tecnologie IaaS/PaaS essenziali fornite dal CISP, un marketplace PaaS/SaaS e i servizi di consulenza accessibili agli utenti finali dell'amministrazione pubblica in caso di necessità, consentendo la pianificazione, la transizione, l'utilizzo e la gestione di un carico di lavoro nel cloud. Pertanto, una RDO di servizi cloud efficace ai fini della predisposizione di un Accordo quadro per il cloud dovrebbe essere suddivisa nei 3 lotti descritti di seguito:

- 1° LOTTO - TECNOLOGIE CLOUD
  Tecnologie cloud acquistate direttamente da un CISP o tramite un rivenditore autorizzato del CISP.

- 2° LOTTO - MARKETPLACE
  Accesso a un marketplace di servizi PaaS e SaaS.

- 3° LOTTO - CONSULENZA CLOUD
  Servizi di consulenza correlati al cloud (formazione, servizi professionali, servizi gestiti ecc.) e supporto tecnico.

*Come accennato in precedenza, il presente documento si concentra specificamente sull'acquisto di tecnologie cloud IaaS e PaaS (**1° LOTTO**), così come fornite da un CISP (acquistate direttamente dal CISP o tramite un rivenditore del CISP). Per i fornitori del 2° e 3° LOTTO di una RDO di servizi cloud sono richieste qualifiche distinte.*

La Figura 1 riporta il quadro generale di una RDO di servizi cloud ben strutturata, suddivisa in tre lotti. Una RDO strutturata in tal senso può sfociare in un Accordo quadro per il cloud, assicurando agli enti pubblici l'agilità (sia tecnica sia contrattuale), la visibilità e il controllo sulla spesa e sull'utilizzo del cloud e la disponibilità di tutti i servizi cloud necessari per costruire e mantenere le soluzioni richieste.

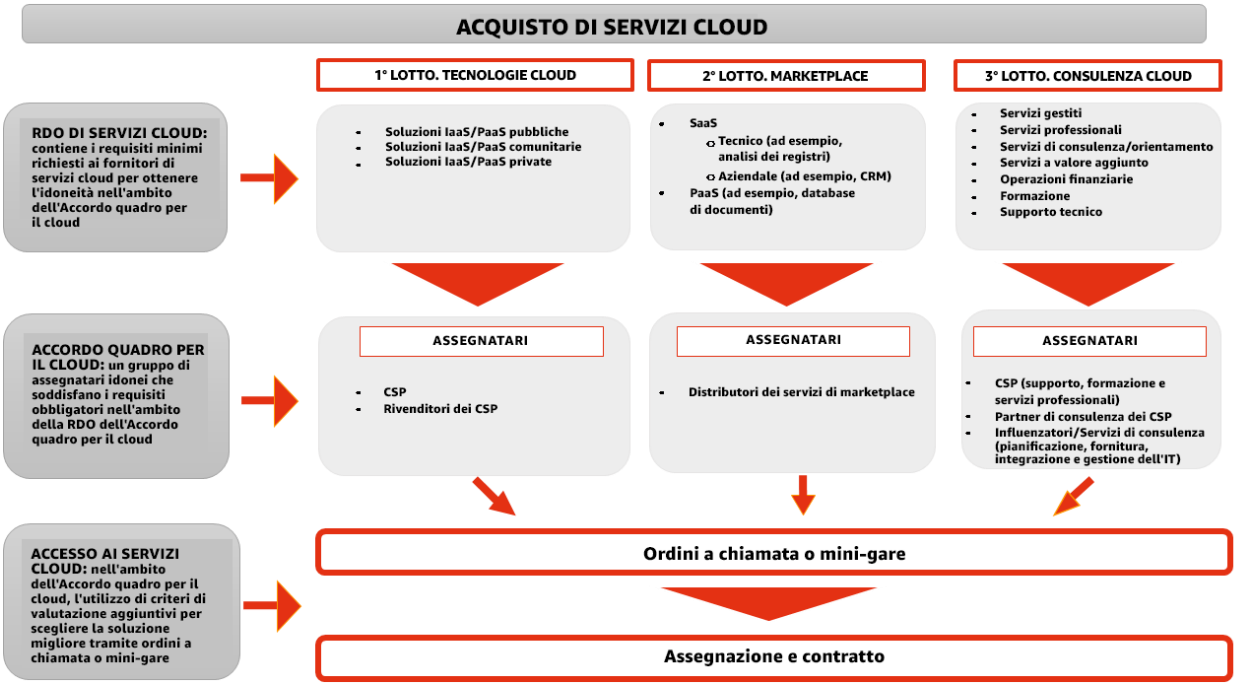

Figura 1. Una RDO di servizi cloud ben strutturata è suddivisa in 3 lotti. Ogni lotto include le Categorie o i "tipi di offerte" specifiche, per assicurare la conformità tecnica e contrattuale ai requisiti dell'utente finale quando gli acquisti avvengono al di fuori dell'Accordo quadro per il cloud.

Si prega di considerare che:

- Ogni lotto è aperto a più aggiudicazioni.
- Il 3° LOTTO può essere aggiudicato tramite un'altra RDO o, eventualmente, tramite un contratto esistente di fornitura di servizi di consulenza.

Categorie del 1° LOTTO

Gli Accordi quadro per il cloud efficaci impongono ai CISP di descrivere il modello di cloud da essi offerto, suddiviso in base alle categorie di ciascun lotto. Consigliamo di fare riferimento agli standard di settore per il cloud computing (Caratteristiche essenziali del cloud secondo il NIST) per quanto riguarda le definizioni di cloud **pubblico**, cloud **comunitario** e cloud **privato**. Con un Accordo quadro per il cloud così strutturato, la stazione appaltante e gli enti pubblici possono scegliere, tra i vari modelli cloud, quello più adatto alle rispettive esigenze.

A proposito delle definizioni fornite dal NIST per i singoli modelli cloud del 1° LOTTO (IaaS/PaaS pubblico, IaaS/PaaS comunitario e IaaS/PaaS privato), *vedere il paragrafo **2.1.3** Definizioni*.

Scelta tra ordini a chiamata e mini-gare

I criteri di qualificazione di una RDO di servizi cloud devono includere gli elementi essenziali e gli standard minimi; non possono includere standard secondari/opzionali. Con l'aggiunta di standard supplementari, superiori agli standard di base dei fornitori dotati dei requisiti, si rischia di escludere dalla gara d'appalto alcuni fornitori, limitando così le opzioni a disposizione degli acquirenti.

Dopo l'emissione della RDO e la conseguente predisposizione dell'Accordo quadro per il cloud, gli enti pubblici che sono parte dell'Accordo quadro possono effettuare "ordini a chiamata" per ottenere i servizi cloud necessari in base alle proprie esigenze. Inserendo un ordine a chiamata nell'ambito dell'Accordo quadro, gli acquirenti possono correggere o aggiungere dei requisiti tecnici relativi all'ordine a chiamata specifico, senza rinunciare ai vantaggi offerti dall'Accordo quadro.

Se necessario, è possibile indire una mini-gara per individuare il fornitore migliore per un determinato carico di lavoro o progetto. Si parla di mini-gara quando un cliente amplia ulteriormente la concorrenza nell'ambito dell'accordo quadro attraverso l'invito, rivolto a tutti i fornitori di un determinato lotto, a rispondere a una serie di requisiti. Il cliente invita tutti i fornitori qualificati del lotto a presentare un'offerta. Per tale ragione, è importante che gli aggiudicatari di una RDO di servizi cloud siano in possesso dei requisiti minimi: ciò garantisce uno standard elevato di opzioni nell'ambito di ciascun lotto.

Merita sottolineare l'importanza di disporre di ***termini e condizioni contrattuali distinti*** *per ogni lotto di cui alla precedente Figura 1. L'adozione di un unico approccio indifferenziato per appaltare tutti i lotti potrebbe infatti causare problemi di fattibilità e compatibilità tecnica.*

2.0 Panoramica della RDO di servizi cloud

Il presente capitolo descrive il modello e l'ambito di applicazione di una RDO di servizi cloud: gli obiettivi strategici, i partecipanti, le definizioni, la tempistica e i requisiti amministrativi minimi. È opportuno ribadire che il presente manuale si concentra in modo specifico sul 1 LOTTO: TECNOLOGIE CLOUD.

2.1 Predisposizione della RDO di servizi cloud

Invitiamo caldamente gli enti pubblici a chiarire esattamente gli obiettivi e i requisiti fondamentali già nell'introduzione alla RDO di servizi cloud.

2.1.1 Introduzione e obiettivi strategici

Ai fini della chiarezza degli obiettivi strategici, è buona norma dichiarare quanto segue già nell'introduzione della RDO di servizi cloud: **(1)** gli obiettivi commerciali e i vantaggi che l'ente intende perseguire attraverso il cloud; **(2)** lo schema dell'Accordo quadro (chi compra, chi opera, chi decide il budget ecc.); **(3)** la piena comprensione del modello di responsabilità condivisa tra ente pubblico e fornitori di servizi cloud (CISP), un fattore fondamentale ai fini dell'acquisto e dell'utilizzo dei servizi cloud in forma efficace, e **(4)** la relazione che si instaura tra i fornitori di servizi cloud (CISP), i distributori di servizi marketplace, i partner di consulenza, le amministrazioni aggiudicatrici/stazioni appaltanti, nonché gli utenti finali dell'ente pubblico. Attraverso la definizione di questi quattro punti, l'ente può sviluppare una RDO perfettamente rispondente alle proprie esigenze e, altresì, garantire che clienti e fornitori comprendano chiaramente il contenuto dei documenti finali della RDO.

La RDO di servizi cloud persegue una finalità diversa rispetto a una classica RDO del settore IT. La tecnologia cloud non è semplicemente un sostituto dell'informatica classica, ma introduce un modo completamente nuovo di utilizzare la tecnologia. Le RDO di servizi cloud ben strutturate possono aiutare gli enti pubblici a sfruttare rapidamente i vantaggi del cloud.

Quando si parla di "good practice" con riferimento agli acquisti di servizi cloud, il punto di partenza migliore è, senz'altro, una spiegazione chiara del modello di responsabilità condivisa. Il modello di responsabilità condivisa[1] è utilizzato perlopiù quando si parla di sicurezza e conformità del cloud, ma la delineazione delle responsabilità si applica a tutti gli aspetti delle tecnologie cloud. In una RDO di servizi cloud è necessario dichiarare quali aspetti sono di competenza del CISP in un ambiente cloud e quali aspetti restano, invece, di competenza del cliente. Ad esempio, il CISP mette a disposizione le funzionalità di monitoraggio delle risorse e delle applicazioni eseguite nel cloud, *ma* l'utilizzo concreto di tali funzionalità messe a disposizione dal CISP è responsabilità del cliente. Questo perché un CISP con milioni di clienti che opera su vasta scala non può occuparsene.

Inoltre, i clienti cloud devono comprendere come la rete di partner del CISP possa aiutarli a utilizzare il cloud e a gestire le proprie responsabilità. Ad esempio, un fornitore di servizi gestiti

[1] Vedere il capitolo 5 del Codice di condotta CISPE per i fornitori di servizi di infrastruttura cloud: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

(MSP) per il cloud può aiutare un cliente a configurare e a utilizzare le funzionalità di monitoraggio messe a disposizione dal CISP per soddisfare i propri requisiti di conformità e audit specifici.

In sintesi, le responsabilità nel modello cloud si declinano come segue:

Il CISP mette a disposizione la tecnologia cloud

Il cliente utilizza la tecnologia cloud

Le **società di consulenza**, se presenti, aiutano il cliente ad accedere alla tecnologia cloud e a sfruttarla al meglio

*Le **"società di consulenza"** sono aziende di servizi gestiti/professionali che aiutano i clienti a progettare, strutturare, costruire, migrare e gestire i propri carichi di lavoro e le applicazioni nel cloud. Tali società includono integratori di sistemi, consulenti strategici, agenzie, fornitori di servizi gestiti (MSP) e rivenditori a valore aggiunto (VAR).*

Acquistare i servizi cloud è un po' come fare la spesa in una ferramenta. Un negozio di ferramenta può fornire tutto il materiale e tutti gli strumenti necessari per un determinato progetto. Il progetto può riguardare la costruzione di un armadietto, di una piscina o addirittura di una casa intera: è il cliente a decidere. Al momento dell'acquisto del materiale e degli strumenti, il commesso della ferramenta può dare delle indicazioni basate sulla sua esperienza, ma non può andare a casa del cliente a realizzare il lavoro. Ecco quindi le opzioni possibili:

1. Acquistare il materiale e gli strumenti e mettersi al lavoro per realizzare il proprio progetto.
2. Acquistare il materiale e gli strumenti e affidare il lavoro ad altri.
3. Affidare il lavoro ad altri e chiedere di includere nell'offerta complessiva anche il materiale e gli strumenti necessari.

Se un ente possiede internamente le competenze necessarie per costruire e gestire autonomamente le soluzioni e l'ambiente cloud, dovrà soltanto accedere alle tecnologie cloud e agli strumenti standardizzati messi a disposizione dal CISP (direttamente dal CISP o tramite un rivenditore del CISP; vedere il **1° LOTTO**). Le applicazioni software SaaS e PaaS necessarie dovrebbero essere disponibili su un marketplace cloud (**2° LOTTO**). Se occorre ulteriore assistenza in materia di consulenza, migrazione, implementazione e/o gestione, entra in gioco la rete di partner del CISP (**3° LOTTO**).

Testo di esempio di una RDO: introduzione e obiettivi strategici

Il cloud computing garantisce agli enti pubblici l'accesso rapido a un'ampia gamma di risorse IT flessibili, a basso costo, pagate in base al consumo. Gli enti possono procurarsi le risorse più adatte, in termini di tipologia e dimensione, per sviluppare idee innovative o per garantire l'operatività del proprio reparto IT, evitando investimenti importanti in prodotti hardware e/o contratti di licenza software a lungo termine.

*L'**<ENTE>** ha la necessità di accedere a questi tipi di tecnologie cloud in commercio per rispondere alle proprie esigenze aziendali, nel contesto di un ampio spettro di enti affiliati.*

L'obiettivo principale della presente RDO è l'aggiudicazione di un ***<ACCORDO QUADRO>*** *in forma parallela e non esclusiva a un numero massimo di* ***<x>*** *fornitori, che rappresentano diverse tecnologie cloud e servizi correlati.*

1. ***1° LOTTO****. Fornitore di servizi cloud (CISP) o rivenditori del CISP per l'acquisto di tecnologie cloud.*
2. ***2° LOTTO.*** *Fornitori di servizi marketplace.*
3. ***3° LOTTO.*** *Fornitori di servizi di consulenza che offrono ulteriori competenze per agevolare la migrazione alle offerte del CISP e l'utilizzo delle stesse.*

Per quanto riguarda il ***1° LOTTO****, gli operatori economici che partecipano alla gara d'appalto (CISP o rivenditori del CISP) sono tenuti a dimostrare la modalità in cui la propria offerta soddisfa i seguenti obiettivi:*

- ***Agilità:*** *mettere le risorse IT a disposizione degli utenti finali entro pochi minuti, anziché nell'arco di settimane o mesi.*
- ***Innovazione:*** *garantire l'accesso immediato alle tecnologie più innovative disponibili sul mercato.*
- ***Costi:*** *passare dagli investimenti in conto capitale alle spese variabili (da spese in conto capitale a spese operative). In altre parole, pagare solo ciò che si consuma.*
- ***Bilancio:*** *visualizzare i dati sulla fatturazione e sul consumo sia a livelli granulari sia di riepilogo, per avere una panoramica dei modelli di spesa nel tempo e una previsione di spesa per il futuro.*
- ***Elasticità:*** *ottenere un abbassamento dei costi variabili grazie alle economie di scala di alto livello fornite dal cloud.*
- ***Capacità:*** *capire le esigenze in termini di capacità dell'infrastruttura, evitando di tirare a indovinare.*
- ***Dismissione dei data center:*** *porre l'attenzione sulle attività utili ai cittadini, anziché allestire rack voluminosi e accumulare server che occupano spazio e consumano energia.*
- ***Sicurezza:*** *formalizzare la progettazione degli account, rendendo le risorse più visibili e verificabili ed eliminando i costi per la protezione degli impianti e dell'hardware fisico.*
- ***Responsabilità condivisa:*** *ridurre gli oneri operativi grazie al fatto che il CISP opera, gestisce e controlla tutti i componenti, dal sistema operativo host e dalla virtualizzazione, alla sicurezza degli impianti in cui opera il servizio.*
- ***Automazione:*** *integrare l'automazione nell'architettura cloud per aumentare la scalabilità in modo sicuro, rapido ed economicamente conveniente.*
- ***Governance del cloud:*** *(1) iniziare con un inventario completo di tutte le risorse IT; (2) gestire tutte le suddette risorse centralmente e (3) predisporre degli avvisi su utilizzo/fatturazione/sicurezza ecc., tutti dotati di funzionalità di localizzazione delle risorse, gestione dell'inventario, gestione delle modifiche, gestione e analisi dei registri, visibilità generale e governance del cloud.*
- ***Controllo:*** *ottenere piena visibilità sulle modalità di utilizzo dei servizi IT e sulle aree che possono essere perfezionate ai fini di sicurezza, affidabilità, prestazioni e costi.*
- ***Reversibilità:*** *fornire strumenti e servizi di portabilità per agevolare la migrazione da/verso l'infrastruttura del CISP, riducendo al minimo i vincoli contrattuali del fornitore (vendor lock-in) e rispettando il codice (o i codici) di condotta del settore.*

- ***Protezione dei dati:*** *capacità di dimostrare la conformità al Regolamento generale sulla protezione dei dati (GDPR) tramite l'adozione di un codice di condotta specifico per i servizi di infrastrutture cloud, ovvero il Codice di condotta CISPE sulla protezione dei dati.*
- ***Trasparenza:*** *garantire ai clienti il diritto di conoscere l'ubicazione delle infrastrutture utilizzate per l'elaborazione e l'archiviazione dei propri dati (area urbana).*
- ***Neutralità climatica:*** *i clienti dovrebbero collaborare con i CISP che adottano misure specifiche e comprovate per raggiungere gli obiettivi di neutralità climatica entro il 2030 e sono firmatari del Patto per la neutralità climatica dei data center. In questo modo, i clienti stessi potranno raggiungere i propri obiettivi di neutralità climatica.*

2.1.2 Tempistica delle risposte a una RDO

In fase di redazione dell'Accordo quadro per il cloud e della RDO di servizi cloud correlata, è buona prassi indicare agli offerenti la tempistica della gara di appalto. Maggiore sarà il coinvolgimento del settore, maggiori saranno le garanzie che tutte le parti interessate comprendano chiaramente i requisiti della RDO e l'adeguatezza di tutti servizi dei fornitori al modello dei servizi cloud.

La tempistica di una RDO non può prescindere dalle leggi locali e dagli obblighi giuridici; pertanto, l'elenco fornito di seguito va inteso come una guida alle best practice e non come norma da applicare obbligatoriamente alle attività e alle tempistiche.

Testo di esempio di una RDO: tempistica della risposta

La tempistica di una RDO di servizi cloud è la seguente:

Tempistica di una RDO di servizi cloud
• *Pubblicazione della richiesta di informazioni (RFI, Request for Information):* • *Risposta alla RFI:* • *Pubblicazione della bozza della richiesta di offerta (RDO):* • *Termine di presentazione della bozza della risposta alla richiesta di offerta (RDO):* • *Fase di consultazione di mercato: <tempistica>* • *Pubblicazione della RDO di preselezione:* • *Risposta alla RDO di preselezione:* • *Pubblicazione della RDO:* • *Fase 1 Termine di presentazione dei quesiti:* • *Fase 1 Risposte:* • *Fase 2 Termine di presentazione dei quesiti:* • *Fase 2 Risposte:* • *Termine di presentazione della risposta alla RDO:* • *Periodo dedicato alle richieste di precisazioni sull'offerta:* • *Periodo di trattativa:* • *Data di aggiudicazione prevista:* • *Aggiudicazione dell'appalto:* • *Durata dell'appalto (opzioni di proroga):*

La tempistica di una RDO non può prescindere dalle leggi locali e dagli obblighi giuridici; pertanto, l'elenco fornito di seguito va inteso come una guida alle best practice e non come norma da applicare obbligatoriamente alle attività e alle tempistiche.

2.1.3 Definizioni

La RDO di servizi cloud deve includere un elenco dettagliato delle definizioni. L'elenco deve includere i ruoli dei fornitori (ad esempio, fornitore di servizi cloud, rivenditore cloud, fornitore partner), i concetti tecnologici di carattere generale (calcolo, archiviazione, IaaS/PaaS, SaaS) e altri elementi fondamentali del contratto. Di seguito un esempio di definizioni:

Testo di esempio di una RDO: definizioni

Le definizioni di cloud computing fornite di seguito sono indicate dal National Institute of Standards and Technology (NIST).[2]

- ***Infrastruttura come servizio (IaaS).*** *Capacità di fornire al consumatore le funzionalità di elaborazione, archiviazione, rete e le altre risorse informatiche fondamentali affinché il consumatore possa implementare ed eseguire il software in modo arbitrario, inclusi sistemi operativi e applicazioni. Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante, ma controlla i sistemi operativi, l'archiviazione e le applicazioni implementate e, ove possibile, esercita un controllo limitato sulla scelta dei componenti delle reti (ad esempio, firewall host).*

- ***Piattaforma come servizio (PaaS).*** *Capacità di garantire al consumatore l'implementazione, nell'infrastruttura cloud, di applicazioni acquisite o create dal consumatore stesso, mediante linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante (rete, server, sistemi operativi e archiviazione), ma controlla le applicazioni implementate e, se possibile, le impostazioni di configurazione per l'ambiente di hosting delle applicazioni.*

- ***Software come servizio (SaaS).*** *Capacità di garantire al consumatore l'utilizzo delle applicazioni del fornitore che sono eseguite nell'infrastruttura cloud. L'accesso a tali applicazioni è consentito da diversi dispositivi client, tramite un'interfaccia Thin Client come un browser Web (ad esempio, e-mail basata sul Web) o tramite l'interfaccia di un programma. Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante (rete, server, sistemi operativi e archiviazione) e neppure le funzionalità delle singole applicazioni, con la sola possibile eccezione di alcune e limitate impostazioni di configurazione delle applicazioni specifiche dell'utente.*

- ***Cloud pubblico.*** *L'infrastruttura cloud è a disposizione per il libero uso da parte del pubblico. Il proprietario, gestore od operatore può essere un'azienda, un'istituzione accademica o la pubblica amministrazione, o una combinazione delle tre. L'infrastruttura risiede presso la sede del fornitore di servizi cloud.*

- ***Cloud comunitario.*** *L'infrastruttura cloud viene messa a disposizione esclusiva di una specifica comunità di consumatori da parte di enti che hanno un interesse comune (ad esempio una missione, dei requisiti di sicurezza, delle politiche e delle considerazioni sulla conformità). Il proprietario, gestore od operatore dell'infrastruttura possono essere uno o più enti presenti nella comunità, un soggetto terzo o una combinazione di questi. L'infrastruttura può risiedere o meno presso la sede dei soggetti di cui sopra.*

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- ***Cloud ibrido.*** *L'infrastruttura cloud è composta da due o più infrastrutture cloud distinte (private, comunitarie o pubbliche) che rimangono entità univoche e distinte, ma legate da una tecnologia standardizzata o proprietaria che consente la portabilità di dati e applicazioni (ad esempio, espansione del cloud per il bilanciamento del carico tra i cloud).*

- ***Cloud privato.*** *L'infrastruttura cloud viene messa a disposizione esclusiva di un unico ente che comprende più consumatori (ad esempio, varie unità operative di un'azienda). Il proprietario, gestore od operatore può essere l'ente stesso, un soggetto terzo o una combinazione di questi. L'infrastruttura può risiedere o meno presso la sede del soggetto di cui sopra.*

2.1.4 Descrizione dettagliata del modello di acquisto e concorrenza nell'ambito dell'Accordo quadro

Come già sottolineato, gli enti pubblici devono individuare il modello in base al quale l'accordo quadro agirà da meccanismo di acquisto delle tecnologie cloud e dei servizi correlati di implementazione e gestione. Tale aspetto deve essere chiarito nella RDO di servizi cloud, cosicché i fornitori di tecnologie cloud, le organizzazioni che forniscono servizi di consulenza, i distributori marketplace e i soggetti acquirenti conoscano perfettamente i rispettivi ruoli.

Nel definire l'ambito di applicazione dell'accordo quadro, così come gli ordini a chiamata e le mini-gare conseguenti, gli enti devono considerare quanto segue:

- Chi sarà responsabile dell'integrazione e dei servizi gestiti che comportano l'uso delle tecnologie cloud, come da contratto.
- Esiste l'esigenza di affidarsi a un rivenditore CISP/partner in grado di fornire servizi a valore aggiunto al di là del mantenimento delle relazioni contrattuali con il CISP, ad esempio la fornitura di servizi di fatturazione consolidata e l'accesso diretto e puntuale ai dati relativi a fatturazione e consumo associati all'uso dei servizi del fornitore di servizi cloud?
- Esiste l'esigenza di avere a pieno servizio un rivenditore a valore aggiunto, un integratore di sistemi o un fornitore di servizi gestiti, o qualsiasi altra forma di servizi di manodopera IT?

È importante sottolineare che un CISP non è né un integratore di sistemi (SI) né un fornitore di servizi gestiti (MSP). Molti clienti del settore pubblico avranno bisogno di un CISP per i propri servizi IaaS/PaaS e di un SI o MSP a cui esternalizzare le attività concrete (“hands on keyboard”) di pianificazione, migrazione e gestione. Nella Figura 2 sono illustrati i ruoli e le responsabilità in un modello di servizi cloud.

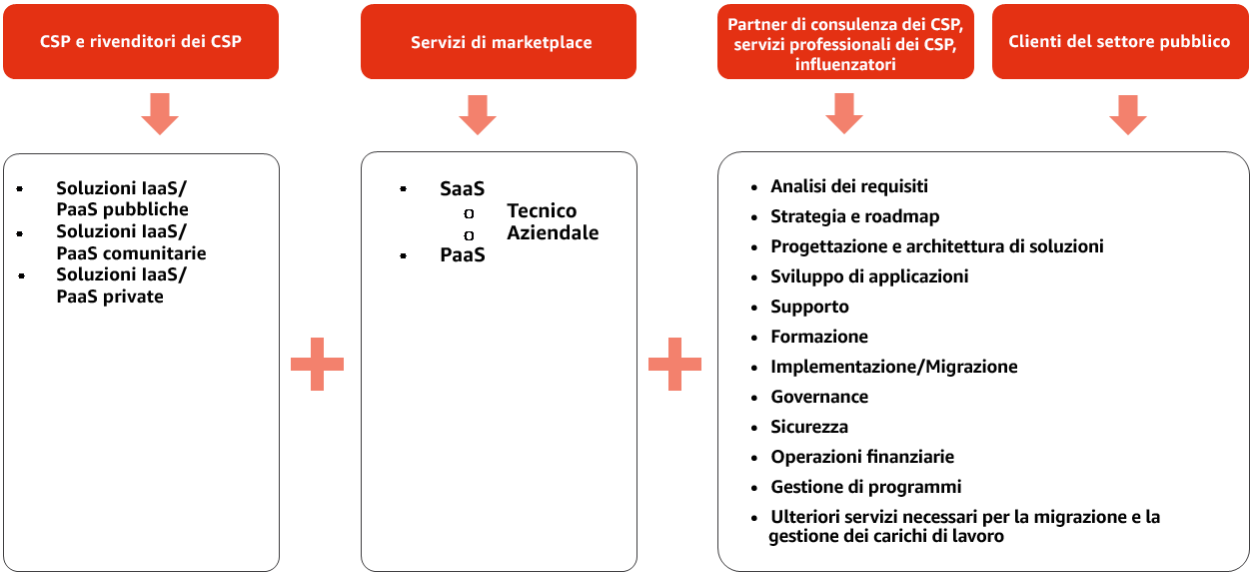

Figura 2. Una RDO di servizi cloud dovrebbe fornire agli utenti finali una lista completa dei servizi cloud da essi richiesti. I clienti del settore pubblico avranno bisogno di un CISP per le tecnologie cloud e, se necessario, di un marketplace per i prodotti PaaS e SaaS. Il cliente potrà quindi decidere in quale misura partecipare all'erogazione dei servizi cloud e quante attività esternalizzare a una società di consulenza/un SI/un MSP ecc.

Il testo di esempio sotto riportato è redatto in base ai ruoli e alle responsabilità descritti nella Figura 2. Un Accordo quadro per il cloud e la RDO di servizi cloud associata devono consentire agli acquirenti di valutare adeguatamente le offerte di ciascun fornitore e di scegliere i servizi necessari per il carico di lavoro/progetto specifico. Questo traguardo può essere raggiunto suddividendo i servizi in lotti, come già accennato, e spiegando chiaramente come si devono svolgere gli ordini a chiamata e le mini-gare nell'ambito dell'accordo quadro.

Testo di esempio di una RDO: modello di acquisto

*Il presente contratto fungerà da strumento di acquisto dell'**Accordo quadro**. Il presente Accordo quadro per il cloud conterrà il numero di **lotti** definito dall'<**ENTE**> per le tecnologie cloud e i servizi/prodotti correlati del marketplace, i servizi di consulenza, i servizi professionali di integrazione di sistema/servizi gestiti/di migrazione, la formazione e il supporto definiti dall'<**ENTE**> e potrà essere utilizzato da più acquirenti autorizzati e affiliati all'<**ENTE**>. Ciò consente di semplificare la procedura della gara d'appalto e, contestualmente, di ottimizzare le economie di scala.*

Una volta sottoscritto, il presente Accordo quadro consente a un ente di acquistare le specifiche tecnologie cloud e i servizi cloud desiderati, nel momento in cui l'ente ne ha bisogno, diversamente da quanto accade nelle gare d'appalto singole. Tale approccio riduce i requisiti amministrativi e semplifica enormemente la gara d'appalto dal punto di vista della complessità e dei tempi.

*L'Accordo quadro avrà una durata massima di **<X>** anni, compresi eventuali rinnovi. La durata massima di un ordine a chiamata nell'ambito di un Accordo quadro è normalmente di **<x>** mesi, prorogabili per **<x>** mesi e, successivamente, per ulteriori **<x>** mesi, mediante le eventuali e pertinenti approvazioni interne finalizzate alla concessione della proroga. Ciascun **ordine a chiamata** deve necessariamente riportare la durata dello stesso.*

*L'ACCORDO QUADRO è suddiviso in **3 (tre) lotti**.*

1. *1° LOTTO - TECNOLOGIE CLOUD. Fornitura completa di tecnologie cloud (direttamente dal CISP, dal rivenditore o dal RAV, ovvero rivenditore a valore aggiunto nell'ambito di servizi/assistenza):*
    i. *Servizi IaaS e PaaS: menu di tecnologie cloud per calcolo, archiviazione, reti, database, analisi dei dati, servizi applicativi, implementazione, gestione, sviluppo, Internet of Things (IoT), ecc. Include dei pacchetti di soluzioni basate sulla tecnologia cloud, come DR/COOP, archiviazione, Big Data e strumenti di analisi, DevOps, ecc.*
2. *2° LOTTO - MARKETPLACE. Fornitura completa di servizi/prodotti PaaS e SaaS, ad esempio contabilità, CRM, progettazione, HR, GIS (Sistema informativo geografico) e mappatura, HPC, BI, gestione dei contenuti, analisi dei registri ecc.*
3. *3° LOTTO - CONSULENZA CLOUD. Fornitura completa di servizi di consulenza (servizi gestiti, servizi professionali, servizi di consulenza/orientamento, servizi a valore aggiunto, operazioni finanziarie, supporto tecnico) correlati alla migrazione e all'utilizzo del cloud. Questi servizi possono includere: pianificazione, progettazione, migrazione, gestione, supporto, controllo della qualità, sicurezza, formazione ecc.*

I fornitori possono presentare offerte per più lotti.

I fornitori potranno presentare offerte corredate di prezzi in un formato a loro scelta.

CONCORRENZA NELL'AMBITO DELL'ACCORDO QUADRO E AGGIUDICAZIONE DEGLI APPALTI

ORDINI A CHIAMATA

Gli enti pubblici che sono parte dell'Accordo quadro possono ricorrere agli "ordini a chiamata" per i servizi di cui hanno bisogno, al momento opportuno. Inserendo un ordine a chiamata nell'ambito dell'accordo quadro, gli acquirenti possono correggere o aggiungere dei requisiti tecnici per l'ordine a chiamata specifico, senza dover rinunciare ai vantaggi offerti dall'Accordo quadro.

Gli appalti aggiudicati tramite l'Accordo quadro forniranno una cronologia delle attività (audit trail) molto chiara per quanto riguarda i requisiti applicati alla selezione del fornitore per ogni lotto. Gli acquirenti finali terranno traccia di tutte le comunicazioni avvenute con i fornitori, comprese eventuali consultazioni preliminari di mercato, richieste di precisazioni, e-mail e discussioni faccia a faccia.

1. DEFINIZIONE DEI REQUISITI DI UN ORDINE A CHIAMATA E APPROVAZIONE INTERNA DELL'ACQUISTO

Tutti gli acquirenti finali che hanno diritto ad utilizzare l'Accordo quadro creeranno dei gruppi misti (costituiti da utenti finali aziendali, esperti di acquisti e tecnici) per redigere un elenco dei prodotti/servizi indispensabili e di prodotti/servizi desiderati. Questi requisiti semplificheranno la scelta del lotto/dei lotti pertinenti e del fornitore/dei fornitori più qualificati. Nel definire i requisiti, gli acquirenti dovranno considerare:

- *i fondi disponibili per l'uso del servizio*
- *i requisiti tecnici e i requisiti della procedura di appalto del progetto*
- *i criteri a fondamento della scelta*

2. RICERCA DEI SERVIZI

Nell'ambito dell'Accordo quadro, gli acquirenti potranno consultare un catalogo online dedicato (un portale sul quale saranno elencati tutti gli aggiudicatari qualificati in base all'Accordo quadro, con i rispettivi servizi) per trovare i prodotti/servizi rispondenti alle proprie esigenze specifiche. Dovranno scegliere i lotti pertinenti e, successivamente, cercare i servizi.

3. ESAME E VALUTAZIONE DEI SERVIZI

Nell'ambito dell'Accordo quadro, gli acquirenti potranno esaminare le descrizioni dei servizi e individuare i servizi rispondenti alle proprie esigenze sulla base dei requisiti e del budget. Tutte le descrizioni dei servizi devono includere:

- *Un documento contenente le definizioni dei servizi o i link alle definizioni dei servizi*
- *Un documento contenente i termini e le condizioni*
- *Un documento contenente i prezzi (i link ai prezzi pubblici sono ammessi a condizione che, su richiesta, sia disponibile un documento/listino prezzi completo)*

Il prezzo corrisponderà al costo della configurazione più comune del servizio. Tuttavia, il prezzo viene normalmente fissato in base al volume; pertanto, gli acquirenti devono consultare sempre il documento con i prezzi del fornitore o un suo listino pubblico e, con l'aiuto degli strumenti idonei, calcolare il prezzo effettivo di ciò che acquistano, nonché il valore globale per l'acquirente (ad esempio, servizi di ottimizzazione con conseguente taglio dei costi).

Nell'ambito dell'Accordo quadro, gli acquirenti possono interagire con i fornitori per chiedere chiarimenti circa la descrizione di un servizio, i termini e le condizioni applicati, i prezzi o il modello/documento che definisce il servizio. È necessario mantenere traccia di tutte le interazioni con i fornitori.

4. SCELTA DI UN SERVIZIO E AGGIUDICAZIONE DI UN APPALTO

Fornitore unico

Qualora vi sia un solo fornitore che soddisfa tutti i requisiti, quest'ultimo sarà l'aggiudicatario dell'appalto.

Fornitori multipli

Se l'elenco viene ristretto a un determinato numero di servizi, la scelta dell'acquirente dovrà ricadere sull'offerta economicamente più vantaggiosa (MEAT, Most Economically Advantageous Tender). Per conoscere i criteri della valutazione basata sul principio MEAT, vedere la tabella seguente. Gli acquirenti possono decidere le caratteristiche specifiche da utilizzare e in quale misura utilizzarle.

È opportuno considerare che l'acquirente potrebbe dover:

- *Considerare le combinazioni di più fornitori*
- *Chiedere informazioni specifiche su sconti per azienda o per volume e sui servizi di ottimizzazione dei costi offerti dai fornitori*

La valutazione dei fornitori deve essere sempre onesta e trasparente. La scelta deve ricadere sull'offerta più idonea e i fornitori/servizi non dovranno essere esclusi senza un'adeguata verifica dei requisiti del progetto.

Tabella 2. Valutazione basata sul principio MEAT

Criteri di aggiudicazione
Costo dell'intero ciclo di vita: *rapporto costi/benefici, prezzo e costi di esercizio*
Valore tecnico e idoneità funzionale: *copertura, capacità di rete e prestazioni, come specificato nei livelli di servizio pertinenti*
Gestione post-vendita dei servizi: *help desk, documentazione, funzione di gestione degli account e continuità del rifornimento di una serie di servizi*
Caratteristiche non funzionali

MINI-GARE

Se necessario, è possibile indire una mini-gara per individuare il fornitore migliore per un determinato carico di lavoro o progetto. Si parla di mini-gara quando un cliente amplia ulteriormente la concorrenza nell'ambito dell'accordo quadro attraverso l'invito, rivolto a tutti i fornitori di un determinato lotto, a rispondere a una serie di requisiti. Il cliente inviterà tutti i fornitori qualificati, nell'ambito del lotto, a presentare un'offerta. Nei capitoli seguenti sono riportate ulteriori informazioni comparative riguardanti aspetti tecnici, sicurezza e prezzo/valore.

CONTRATTO

*Sia l'acquirente che il fornitore devono sottoscrivere una copia del contratto prima dell'utilizzo del servizio. La durata massima di un Accordo quadro è normalmente di **<x>** mesi, prorogabili per **<x>** mesi e, successivamente, per ulteriori **<x>** mesi, mediante le eventuali e pertinenti approvazioni interne finalizzate alla concessione della proroga.*

Una copia dell'accordo dovrà essere sottoscritta da tutte le parti interessate (l'acquirente e il fornitore) prima dell'utilizzo del servizio.

2.1.5 Requisiti minimi del candidato - Amministrativi

L'uso di un linguaggio semplice e chiaro per definire i criteri di qualificazione dell'Accordo quadro contribuirà a evitare la presentazione di offerte da parte dei tradizionali fornitori di hardware o data center che offrono una soluzione classica facendola passare per "cloud". Chi parteciperà alla RDO dovrà dimostrare di soddisfare i requisiti amministrativi minimi degli offerenti.

Come già sottolineato, il presente documento si sofferma in modo specifico sul **1° LOTTO - TECNOLOGIE CLOUD.** Tuttavia, sono state aggiunte delle informazioni anche sul **2° LOTTO - MARKETPLACE** e sul **3° LOTTO - CONSULENZA CLOUD** qualora esse siano utili a chiarire il contesto generale dal punto di vista dei requisiti e dell'ambito di applicazione della RDO. Ad esempio, è importante includere i criteri di qualificazione minimi di un rivenditore CISP/MSP/integratore di sistemi/consulente ecc. per garantire che il soggetto (1) sia direttamente affiliato al CISP in qualità di rivenditore o partner commerciale; (2) sia autorizzato dal CISP a rivendere a soggetti terzi l'accesso diretto alle offerte del CISP e (3) sia in possesso di una certificazione rilasciata dal medesimo CISP che ne attesti competenze ed esperienza.

Testo di esempio di una RDO: requisiti amministrativi minimi dell'offerente

Il presente Accordo quadro aggiudicherà appalti a fornitori multipli per le categorie seguenti. Il fornitore deve essere un CISP commerciale, un rivenditore terzo di un CISP, un distributore di servizi marketplace e/o un fornitore di servizi per l'utilizzo di un CISP (ad esempio consulenze, servizi di migrazione, servizi gestiti, operazioni finanziarie ecc.). Individuare i ruoli per i quali si presenta l'offerta:

1° LOTTO

____ - Fornitore diretto (CISP) di servizio cloud pubblico (IaaS + PaaS)

____ - Fornitore diretto (CISP) di servizio cloud comunitario (IaaS + PaaS)

____ - Fornitore diretto (CISP) di servizio cloud privato (IaaS + PaaS)

____ - Rivenditore CISP terzo (in grado di garantire l'accesso diretto alle offerte cloud online dei CISP).

- *Indicare l'offerta del CISP per la quale l'offerente rivende l'accesso diretto al servizio: _____*
- *Allegare una lettera in cui il CISP attesta che l'offerente è autorizzato a rivendere le offerte del CISP: _____*

2° LOTTO

____ - Fornitore diretto di servizi marketplace eseguiti su infrastrutture di un CISP (PaaS e/o SaaS)

____ - Distributore di servizi marketplace eseguiti su infrastrutture di un CISP (PaaS e/o SaaS)

3° LOTTO

____ - CISP che offre servizi professionali

____ - Fornitore di supporto tecnico per il CISP

____- Partner del CISP che offre servizi per l'utilizzo o l'operatività sulle infrastrutture di un CISP

____- Influenzatore/consulente che offre servizi per l'utilizzo o l'operatività sulle infrastrutture di un CISP

Indicare il tipo di offerta:

- *Servizi gestiti di carichi di lavoro sulle infrastrutture di un CISP (SI/NO): _____*
  - *Indicare le aree di specializzazione, se pertinenti: _____*
- *Servizi professionali (SI/NO): _____*
- *Consulenza - Formazione (SI/NO): _____*
- *Consulenza - Strategia (SI/NO): _____*
- *Consulenza - Migrazione (SI/NO): _____*
- *Consulenza - Governance del cloud (SI/NO): _____*
- *Consulenza - Operazioni finanziarie (SI/NO): _____*
- *Consulenza - Altro (specificare): _____*

Indicare il CISP o i CISP per conto dei quali si forniscono i servizi: _____
Allegare una lettera del CISP che conferma l'incarico al partner in conformità al modello del CISP: _____

REQUISITI AMMINISTRATIVI MINIMI PER IL 1° LOTTO

Fornitore di servizi cloud (CISP)
Per potersi qualificare come CISP, il soggetto offerente deve rispettare i requisiti seguenti.

Criteri di qualificazione proposti al CISP	*Motivazione*
Informazioni sull'organizzazione (ad esempio: ragione sociale, struttura giuridica, n° di registro imprese/codice DUNS, n° di partita IVA ecc.)	
Dimensioni dell'azienda, capacità economica e finanziaria[3]	*Il cliente può stabilire se il CISP sarà in grado di onorare il contratto d'appalto.*
Motivi che determinano l'esclusione (ad esempio, attività criminali e fraudolente ecc.)	
Casi di studio/Referenze dei clienti (specificare il numero/tipo richiesto)	*Il cliente ha la capacità di valutare se l'esperienza del CISP garantisce l'erogazione dei servizi richiesti.*
Responsabilità sociali d'impresa	*Queste dovrebbero essere informazioni di pubblico dominio fornite dal CISP.*
Impegni e pratiche di pubblico dominio a favore della sostenibilità	*Il cliente può verificare se il CISP si è impegnato a gestire la propria azienda nel rispetto dell'ambiente*
Il CISP deve dimostrare di avere investito nell'innovazione e di avere sviluppato nuovi servizi e funzionalità utili negli ultimi 5 anni, in particolare per quanto riguarda PaaS, machine learning e analisi dei dati, Big Data, servizi gestiti e funzionalità di ottimizzazione dell'utilizzo del cloud. Per dimostrare il punto di cui sopra, è possibile presentare dei changelog o dei feed di aggiornamento di pubblico dominio.	*Il CISP dimostra il proprio impegno alla realizzazione di nuovi prodotti per i clienti; dimostra il proprio impegno al costante aggiornamento e miglioramento dei propri prodotti. Ciò consente ai clienti di mantenere un'infrastruttura IT sempre all'avanguardia, senza ricorrere a nuovi investimenti.*

Rapporto del rivenditore/partner con il CISP

*L'**<ENTE>** richiede che il contraente principale sia direttamente affiliato al CISP in qualità di rivenditore o partner commerciale; sia autorizzato dal CISP a rivendere a soggetti terzi l'accesso diretto alle offerte del CISP; sia in possesso di una certificazione rilasciata dal CISP medesimo che ne attesti competenze ed esperienza. In questo modo, l'**<ENTE>** è esonerato dall'incombenza di verificare i termini e i servizi associati all'ulteriore livello di subappalto tra il primo contraente dell'**Accordo quadro** e il CISP. Inoltre, tale requisito riduce la complessità derivante da ulteriori livelli di rivendita qualora (1) l'**<ENTE>** esegua la propria "due diligence" per garantire che le responsabilità rispetto ai servizi forniti siano ripartite chiaramente e (2) l'**<ENTE>** svolga quotidianamente attività che comportano il consumo dei servizi cloud.*

2.2 Requisiti tecnici

Una RDO di servizi cloud deve aumentare il livello delle aspettative, imponendo ai CISP di fornire le tecnologie cloud standardizzate che consentono al cliente di crearsi la propria soluzione personalizzata. Come accennato in precedenza, la distinzione tra ciò che è standardizzato e ciò che è personalizzato ha un rilievo decisivo nell'ambito di una RDO di servizi cloud. I CISP offrono servizi standardizzati a milioni di clienti; pertanto, le personalizzazioni in una RDO di servizi cloud devono

[3] Nota: nelle RDO di servizi cloud sono richieste le informazioni societarie generali, non il numero di dipendenti o l'organigramma dell'azienda. Dal punto di vista della tecnologia cloud, non c'è correlazione tra la garanzia delle prestazioni del servizio e il numero di dipendenti. Al contrario, nelle RDO di servizi cloud contano di più le dimensioni complessive dell'azienda in rapporto ai requisiti (dimensioni adeguate), nonché l'esperienza e le prestazioni dimostrate.

incentrarsi su soluzioni e risultati al di sopra degli standard e non sui metodi, sulle infrastrutture o sui componenti hardware sottostanti con cui vengono offerti i servizi cloud utili per la realizzazione delle soluzioni.

2.2.1 Requisiti minimi

Le tradizionali procedure di appalto del settore IT si basano spesso su requisiti commerciali sviluppati dopo una lunga serie di sessioni di lavoro, che documentano il modo in cui l'ente/l'amministrazione lavora. Definire tali requisiti con esattezza è, nella migliore delle ipotesi, un'impresa complicata. Se l'impresa va in porto, tutte le sessioni dedicate alla definizione dei requisiti documenteranno lo storico del processo aziendale che, di per sé, potrebbe rivelarsi già antiquato e inefficiente. Se, successivamente, i requisiti entrano a far parte di una RDO a cui il CISP deve attenersi, l'unica possibilità consiste in una soluzione personalizzata. Un modello simile non è compatibile con gli appalti per il cloud.

Gli enti pubblici devono individuare chiaramente i propri obiettivi aziendali e le proprie esigenze dal punto di vista delle prestazioni. Tuttavia, essi non devono utilizzare un linguaggio prescrittivo in una RDO, ossia devono evitare di dettare la progettazione e la funzionalità del sistema. Al contrario, l'ente dovrebbe ambire a concludere l'affare migliore sul mercato. Anziché valutare offerte relative a centinaia o migliaia di requisiti prescrittivi – che comunque non garantirebbero l'efficienza dei servizi –, gli enti dovrebbero fissare dei criteri di valutazione. Tali criteri stabiliscono la misura in cui le tecnologie e i servizi correlati soddisfano o superano gli obiettivi aziendali, soddisfano le aspettative in termini di prestazioni e permettono di adattare le regole aziendali attraverso la configurazione.

Nelle RDO di servizi cloud devono figurare le domande giuste in funzione delle soluzioni migliori. Dal momento che in un modello cloud non si acquistano risorse materiali, molti requisiti previsti per i tradizionali appalti dei data center non sono pertinenti. ***Riciclando le domande valide per i data center si otterranno, inevitabilmente, risposte valide per i data center****. Tale circostanza impedisce, di fatto, ai CISP di presentare un'offerta, oppure comporta appalti strutturati talmente male che i clienti del settore pubblico non potranno usufruire pienamente di tutti i vantaggi offerti dal cloud.*

Una RDO di servizi cloud deve concentrarsi sui requisiti imprescindibili di un CISP e sui servizi cloud, garantendo così fornitori altamente qualificati per il 1° LOTTO. I requisiti non devono essere eccessivamente prescrittivi, per non limitare l'accesso della pubblica amministrazione a un'ampia gamma di CISP qualificati.

Testo di esempio di una RDO: caratteristiche del fornitore di servizi cloud

Vedere anche i requisiti amministrativi minimi di un CISP con riferimento al 1° LOTTO

Criteri di qualificazione proposti al CISP	*Motivazione*
Infrastruttura	
L'infrastruttura del CISP deve prevedere almeno 2 cluster di data center. Ogni cluster deve essere costituito da almeno 2 data center con connessione a bassa latenza, per garantire le distribuzioni e le implementazioni in modalità attivo/attivo a disponibilità elevata degli scenari DR-BC (Disaster Recovery e Business Continuity). I data center in ogni cluster devono essere fisicamente isolati l'uno dall'altro e indipendenti in caso di guasto.	*Il CISP deve mettere a disposizione un'infrastruttura idonea alla costruzione di applicazioni ad elevata disponibilità, dove siano evitabili i singoli punti di errore.*
Il CISP deve mettere a disposizione regioni isolate logicamente e geograficamente. È severamente vietato al CISP replicare i dati dei clienti al di fuori delle suddette regioni.	*Secondo quanto previsto dai requisiti di residenza dei dati, il cliente esercita pieno controllo sul luogo in cui si trovano i propri dati.*
Il CISP deve assicurare la connettività diretta, dedicata e privata tra i propri data center.	*La connettività privata è un requisito essenziale ai fini della costruzione di un'infrastruttura ibrida sicura.*
Il CISP deve mettere a disposizione un numero sufficiente di meccanismi, tra i quali rientra la crittografia dei dati in transito.	*Il cliente può esigere che nessun dato transiti in forma non crittografata.*
Certificazioni minime del CISP	
Il CISP deve possedere la certificazione ISO 27001	*La verifica, la certificazione e l'accreditamento da parte di un soggetto terzo confermano che il cliente è in grado di offrire dei servizi in linea con i livelli di benchmark (e in particolare la piattaforma) in termini di qualità, sicurezza e affidabilità. È richiesto un numero minimo di certificazioni.*
Il CISP deve essere conforme al Codice di condotta CISPE sulla protezione dei dati, al fine di fornire funzionalità e servizi che possano essere utilizzati in conformità al GDPR e che consentano ai clienti di creare applicazioni conformi al GDPR.	*Il cliente deve essere in grado di creare o eseguire applicazioni in conformità al GDPR.*
Il CISP deve produrre le relazioni delle verifiche condotte da soggetti terzi, come SOC 1 e 2 (che coprono i luoghi e i servizi utilizzati dai clienti finali), per assicurare trasparenza nei controlli e nelle procedure del CISP.	*Il CISP deve garantire trasparenza circa il modo in cui l'applicazione viene utilizzata e gestita. I report SOC (System and Organization Controls) sono funzionali all'ottenimento della fiducia e della trasparenza.*
Il CISP deve aderire al Patto per la neutralità climatica dei data center	*Il Patto per la neutralità climatica dei data center vede i CISP impegnati a raggiungere la neutralità climatica entro il 2030, consentendo, pertanto, all'utente di sostenere i propri obiettivi di sostenibilità. I fornitori con oltre 250 dipendenti a tempo pieno (non le PMI) sono tenuti a sottoporsi a verifiche da parte di revisori di terze parti*
Il CISP deve aderire al codice di condotta SWIPO IaaS sulla portabilità dei dati	*Il codice di condotta SWIPO IaaS sulla portabilità dei dati garantisce che i servizi soddisfano i requisiti dell'art. 6 "Portabilità dei dati" del Regolamento sulla libera circolazione dei dati non personali.*

Caratteristiche del servizio	
L'infrastruttura del CISP deve essere accessibile tramite le interfacce API e una console di gestione basata sul Web.	*L'accesso autonomo e le interfacce API sono uno standard obbligatorio per i fornitori CISP, i quali devono favorire il più possibile l'accesso disintermediato dell'utente e del fornitore stesso.*
Il CISP deve offrire una serie basilare di Servizi, tra i quali: archiviazione di oggetti, database relazionale gestito, database non relazionale gestito, bilanciatori del carico gestiti, monitoraggio e dimensionamento automatico integrato.	*Il semplice fatto di offrire macchine virtuali non è sufficiente per qualificarsi come fornitore di servizi cloud. I fornitori di servizi cloud devono offrire un insieme di servizi PaaS e IaaS in grado di migliorare e accelerare le applicazioni del cliente.*
Il CISP deve consentire al cliente di cambiare liberamente l'utilizzo e la configurazione dei propri servizi o di spostare i dati da/verso l'infrastruttura del CISP (offerta self-service).	*L'accesso ai servizi e ai dati in modalità self-service è un requisito imprescindibile per garantire la totale indipendenza del cliente.*
Il CISP ha l'obbligo di fornire la fatturazione dei propri servizi in base al consumo.	*La fatturazione in base al consumo consente al cliente di ottimizzare i costi dei carichi di lavoro, riducendo al minimo i rischi e sfruttando al meglio le applicazioni di breve durata e le Proof of Concept (prove di fattibilità) del CISP.*
Sicurezza dei dati e del sistema	
Il CISP deve lasciare al cliente il pieno controllo dei propri dati, assicurando a quest'ultimo la libertà di scegliere dove conservare i dati (area urbana); il CISPE deve, altresì, garantire che nessun dato del cliente sia spostato, tranne nel caso di iniziativa da parte cliente stesso.	*Il cliente deve poter controllare: dove vengono conservati i suoi dati; come viene gestito l'accesso ai contenuti; l'accesso degli utenti ai servizi e alle risorse.*
Le caratteristiche del servizio del CISP devono lasciare al cliente il pieno controllo delle relative policy di sicurezza, incluse riservatezza, integrità e disponibilità dei dati e dei sistemi.	*Il cliente deve essere in grado di definire e applicare i propri standard di sicurezza all'interno di tutti i carichi di lavoro. Non basta confidare nel fatto che il fornitore "farà ciò che è giusto" con i dati del cliente.*
Controllo dei costi	
Il CISP deve approntare meccanismi e strumenti tali da consentire al cliente di monitorare le spese nel corso del tempo. Tali strumenti devono prevedere la segmentazione basilare dei costi per carico di lavoro, servizio e account.	
Il CISP deve offrire gli strumenti adeguati per avvisare il cliente ogniqualvolta si verifichi il superamento della soglia dei costi.	
Il CISP deve inviare al cliente delle fatture dettagliate. La struttura della fattura permette di segmentare i costi in base a carico di lavoro, ambiente e account.	

Inoltre, il CISP è tenuto a rispondere alle domande seguenti riguardanti i requisiti tecnici.

SOLUZIONI
Il CISP deve dimostrare in quale modalità potrà fornire modelli predefiniti e soluzioni software che sono ospitati o integrati nella sua infrastruttura per le soluzioni seguenti:

- *Archiviazione*
- *DevOps*
- *Sicurezza/Conformità*
- *Big Data e strumenti di analisi dei dati*
- *Applicazioni aziendali*
- *Telecomunicazioni e reti*
- *Applicazioni geospaziali*
- *IoT*
- *[Altro]*

Fornire una panoramica di come è stato utilizzato il CISP per i carichi di lavoro seguenti:

- *Ripristino di emergenza*
- *Sviluppo e collaudo*
- *Archiviazione*
- *Backup e ripristino*
- *Big Data*
- *Calcolo ad alte prestazioni (HPC)*
- *Internet of Things (IoT)*
- *Siti Web*
- *Serverless Computing*
- *DevOps*
- *Distribuzione di contenuti*
- *[Altro]*

2.2.2 Confronto tra fornitori

Oltre ai requisiti minimi, in una RDO di servizi cloud è importante indicare anche i criteri per il confronto delle tecnologie del CISP nell'ambito di una valutazione competitiva.

Le RDO di servizi cloud devono indicare le funzionalità cloud necessarie all'ente, nella consapevolezza che il cliente ha il pieno utilizzo delle suddette funzionalità per costruire la propria soluzione. Le funzionalità che vanno oltre gli standard forniti dal CISP (ad esempio soluzioni già sviluppate attraverso i sistemi del CISP o funzioni di automazione) possono essere utilizzate per un'analisi più significativa delle "opzioni a valore aggiunto" o del "miglior rapporto qualità-prezzo" in una RDO di servizi cloud.

Le amministrazioni pubbliche spesso sollecitano la competizione tra gli offerenti applicando criteri di valutazione quali il miglior rapporto qualità-prezzo, l'offerta economicamente più vantaggiosa (MEAT) o il prezzo più basso. Nella fase di pianificazione di questa componente della RDO di servizi cloud, le amministrazioni pubbliche devono assumere un approccio che tenga conto delle peculiarità del cloud. A titolo di esempio, è importante comprendere che un semplice confronto tra le voci incluse nelle proposte dei fornitori di servizi cloud (ad esempio, calcolo o archiviazione) non è un metodo efficace per confrontare le offerte. Al contrario, è consigliabile focalizzare l'attenzione sulle soluzioni generali, come quelle illustrate nel paragrafo ***2.2.1***. Le amministrazioni

pubbliche potranno quindi prendere in esame i requisiti specifici del cloud, come quelli elencati nell'*Appendice A - Requisiti tecnici per il confronto tra* offerenti.

Nella RDO vanno indicate le caratteristiche essenziali del cloud che sono necessarie per costruire la soluzione cloud. A questo scopo, le amministrazioni pubbliche possono fare riferimento alle caratteristiche essenziali del cloud descritte dal National Institute of Standards and Technology (NIST), nonché alle relazioni di analisti di terze parti, per avere la certezza che il CISP disponga dell'offerta per il cloud "più idonea" e che sia in grado di operare su larga scala.

Testo di esempio di una RDO: confronto tra fornitori

*I CISP sono tenuti a rispondere a TUTTE le domande sui requisiti tecnici dell'**Appendice A**.*

I candidati devono essere in possesso degli attributi descritti di seguito e devono spiegare la modalità in cui la rispettiva offerta di servizi cloud soddisfa le cinque caratteristiche essenziali del cloud computing[4].

1) ***Self-Service on demand**: il candidato deve garantire di poter provvedere unilateralmente alla fornitura delle risorse informatiche (ad esempio, tempo del server e archiviazione in rete) secondo necessità e in modo automatico, senza l'obbligo di interagire direttamente con ciascun fornitore di servizi. Il candidato deve garantire che la fornitura dei servizi avvenga unilateralmente (cioè senza la verifica o l'approvazione del fornitore) attraverso il processo di ordinazione. Spiegare in che modo la propria offerta, o l'offerta che si rappresenta, è compatibile con quanto sopra esposto.*

2) ***Accesso ininterrotto alla rete**: il candidato deve offrire opzioni multiple di connettività alla rete; una di esse deve essere obbligatoriamente basata su Internet. Spiegare in che modo la propria offerta, o l'offerta che si rappresenta, è compatibile con quanto sopra esposto.*

3) ***Pool di risorse:** il CISP del candidato deve fornire le risorse informatiche sotto forma di pool, in modo da servire più consumatori tramite un modello multi-tenant, con risorse virtuali diverse che vengono assegnate e riassegnate in modo dinamico, in base alla domanda del consumatore. L'utente può specificare la posizione a un livello superiore di astrazione (ad esempio, Paese, regione o data center). Il candidato deve supportare il dimensionamento di queste risorse entro pochi minuti, od ore, dalla richiesta di provisioning. Spiegare in che modo la propria offerta, o l'offerta che si rappresenta, è compatibile con quanto sopra esposto.*

4) ***Elasticità rapida**: il CISP del candidato deve supportare il provisioning e il de-provisioning del servizio (dimensionamento verso l'alto o il basso), rendendo il servizio disponibile nei tempi minimi prescritti (massimo "x" ore) dalla richiesta di provisioning. Il candidato deve supportare le rettifiche della fatturazione causate da tali richieste di provisioning che arrivano giornalmente, provvedendo a ciò con frequenza oraria o giornaliera.*

5) ***Servizio misurato**: il candidato deve dare visibilità all'utilizzo del servizio tramite un pannello di controllo online o uno strumento elettronico analogo.*

Inoltre, il CISP deve:

- *Essere un leader affermato nella fornitura di servizi cloud, secondo la definizione del Quadrante magico di Gartner per i servizi IaaS[5]*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

- *Fornire le relazioni svolte da analisti di terze parti, riconosciuti nel settore, in cui si attestino le capacità e l'affidabilità dei CISP.*

Infine, i CISP saranno messi a confronto tra loro con riferimento agli scenari previsti nell'Appendice B.

2.2.2.1 Accordi sul Livello di Servizio (SLA)

I CISP forniscono degli accordi sul livello di servizio (SLA) commerciali e standardizzati a milioni di clienti, pertanto non sono in grado di offrire accordi SLA personalizzati, come accade in un modello di data center on-premise. Tuttavia, i clienti dei CISP (spesso assistiti dai partner dei CISP) possono utilizzare il cloud sfruttando al meglio gli accordi SLA commerciali di un CISP e così soddisfare, se non addirittura superare, i propri requisiti specifici.

Le RDO di servizi cloud devono garantire che i CISP offrano le funzionalità e le istruzioni necessarie per un utilizzo ottimale dei rispettivi servizi e accordi SLA commerciali; in questo modo, i singoli utenti finali sono messi nelle condizioni di soddisfare i requisiti di prestazioni e disponibilità.

Testo di esempio di una RDO: Accordi sul Livello di Servizio (SLA)

Fornire informazioni, unitamente ai link corrispondenti, circa l'approccio dei CISP agli accordi SLA.

*L'**<ENTE>** dovrà tenere presenti gli accordi SLA del CISP e implementare i carichi di lavoro e le applicazioni più importanti in modo tale che l'operatività degli stessi non venga meno in caso di mancato rispetto dell'accordo SLA.*

*L'**<ENTE>** è tenuto a mantenere gli accordi SLA opportuni associati a qualsiasi apparecchiatura di proprietà dell'**<ENTE>** o ai servizi gestiti dall'**<ENTE>** utilizzati congiuntamente al CISP.*

*Il CISP deve mettere a disposizione dell'**<ENTE>** funzionalità che forniscano a quest'ultimo visibilità costante e report sulle prestazioni operative degli accordi SLA, nonché best practice documentate che consentano un utilizzo ottimale dell'infrastruttura del CISP per strutturare servizi duraturi, affidabili ed efficienti in termini di prestazioni.*

2.2.3 Appalto

I termini e le condizioni del CISP devono riflettere il modello di funzionamento dei servizi cloud (non si tratta di acquistare risorse materiali; inoltre, i CISP operano su grande scala, fornendo servizi standardizzati). Di conseguenza, è essenziale che i termini e le condizioni del CISP siano incorporati e applicati nella misura più ampia possibile. Per ulteriori informazioni su termini e condizioni, e sull'appalto, vedere il paragrafo *2.5*.

2.2.3.1 Servizi nuovi e migliorati

I CISP offrono delle prestazioni attraverso un servizio. A differenza delle tradizionali soluzioni on-premise, che comportano aggiornamenti e contratti di manutenzione soggetti a scadenza, i fornitori di servizi cloud forniscono semplicemente il servizio standardizzato. Per far sì che il modello cloud raggiunga economie di scala, le modifiche e gli aggiornamenti dell'infrastruttura sottostante vengono estesi a tutti gli utenti, non a singoli utenti; dopodiché, i clienti medesimi scelgono i servizi in base al proprio concreto utilizzo. La continuità del servizio è più elevata rispetto ai sistemi on-premise del passato; in più, i fornitori di servizi cloud aggiungono costantemente servizi nuovi o migliorati, che i clienti possono utilizzare a proprio piacimento.

Qualora non sia possibile aggiungere servizi nuovi o migliorati del CISP dopo la scadenza del termine per la presentazione di una RDO, gli enti pubblici non avranno la possibilità di avvalersi delle nuove funzionalità finché non verrà rilasciata una nuova versione dell'Accordo quadro. Pertanto, si consiglia vivamente di fornire una gamma, quanto più possibile ampia, dei servizi descritti nell'Accordo quadro, così da consentire l'aggiunta di eventuali nuovi servizi del CISP anche dopo la scadenza del termine per la presentazione delle offerte. È possibile che la legislazione UE in materia di appalti pubblici ponga dei limiti all'introduzione nell'Accordo quadro di nuovi servizi, materialmente diversi, del CISP. Tuttavia, eventuali aggiornamenti e nuove versioni dei servizi, che non sono ritenuti modifiche materiali, potrebbero essere ammessi senza provocare eventuali contestazioni all'appalto.

Testo di esempio di una RDO: servizi nuovi e migliorati

*Il CISP deve fornire una soluzione economicamente vantaggiosa che sfrutta sia le tecnologie di virtualizzazione affidabili e consolidate, sia le tecnologie di nuova generazione costantemente aggiornate. L'**<ENTE>** riconosce e accetta quanto segue: le tecnologie cloud possono essere fornite, sotto forma di servizio condiviso, all'**<ENTE>** e ad altri clienti del CISP tramite un codice sorgente (codebase) condiviso e/o un ambiente comune; il CISP può, di tanto in tanto, cambiare, aggiungere/eliminare funzioni, caratteristiche, prestazioni o altri aspetti dei servizi cloud e, qualora dette modifiche/aggiunte/eliminazioni abbiano effettivamente luogo, le specifiche tecniche del servizio cloud saranno aggiornate di conseguenza.*

*L'ambito del presente ordine di consegna comprende tutti i servizi esistenti, nuovi o migliorati del CISP **CHE RIENTRANO NELL'AMBITO DELL'ACCORDO QUADRO**. I servizi cloud forniti dal CISP ai clienti commerciali saranno messi a disposizione dell'**<ENTE>**.*

2.2.3.2 Vendor lock-in/Reversibilità

La tecnologia cloud riduce il "vendor lock-in" (la dipendenza da un singolo fornitore) poiché non vengono acquistate risorse materiali e i clienti possono decidere di spostare i propri dati da un fornitore di servizi cloud a un altro, in qualsiasi momento.

Eppure, quando si acquistano servizi cloud, persiste inevitabilmente un certo grado di "vendor lock-in". Poiché non tutti i cloud sono uguali, un CISP potrebbe offrire servizi e funzionalità che un altro semplicemente non è in grado di offrire; di conseguenza, diminuisce la possibilità di usufruire di quei servizi mediante un altro fornitore. Un approccio prudente consiste nel richiedere al CISP di fornire le funzionalità e i servizi necessari per uscire dal cloud del CISP medesimo, allegando la documentazione necessaria per l'utilizzo di tali servizi, quale ragionevole "strategia di uscita". Infatti, è impossibile che un CISP conosca la configurazione specifica con cui il cliente utilizza i servizi standardizzati del CISP. Per questa ragione, il CISP non può offrire un piano di uscita personalizzato.

Consultare il paragrafo 2.3.1.2 sui codici di condotta del settore per gestire la "portabilità dei dati" e il "cambio di fornitori di servizi cloud" in conformità alle disposizioni dell'articolo 6 del Regolamento UE sulla libera circolazione dei dati non personali.

Testo di esempio di una RDO: onboarding e offboarding

*L'**<ENTE>** è alla ricerca di offerte che forniscano una strategia di uscita ragionevole ed evitino il lock-in. L'**<ENTE>** non sta acquistando risorse materiali e il CISP dovrà consentire la possibilità di innalzamento e abbassamento dello stack IT. Il CISP fornirà gli strumenti e i servizi per la portabilità in modo tale da agevolare la migrazione da/verso la piattaforma del CISP, riducendo al minimo il lock-in. La documentazione che descrive l'uso degli strumenti e dei servizi di portabilità fornita dal CISP fungerà da piano di uscita ragionevole.*

*Il CISP non può esigere impegni minimi **obbligatori** o contratti a lungo termine **obbligatori**.*

*I dati archiviati presso un fornitore di servizi possono essere esportati dal cliente in qualsiasi momento. Il CISP deve consentire all'**<ENTE>** di spostare i dati, secondo necessità, da/verso l'archiviazione del CISP. Il CISP deve, inoltre, consentire il download delle immagini della macchina virtuale e la loro portabilità verso un nuovo fornitore di servizi cloud. L'**<ENTE>** può esportare le immagini della propria macchina e utilizzarle in modalità on-premise o presso un altro fornitore (nel rispetto delle limitazioni di licenza del software).*

2.3 Sicurezza

Le responsabilità relative a sicurezza e conformità sono condivise tra il CISP e i suoi clienti. In questo modello, i clienti dei servizi cloud controllano l'architettura e la protezione delle applicazioni e dei dati inseriti nell'infrastruttura; dal canto loro, i CISP hanno la responsabilità di fornire i servizi su un'infrastruttura estremamente sicura e controllata e di offrire una gamma di funzioni di sicurezza supplementari molto ampia. In questo modello, il livello delle responsabilità del CISP e del cliente dipende dal modello di implementazione cloud (IaaS/PaaS/SaaS) e i clienti devono avere la piena cognizione delle rispettive responsabilità nell'ambito di ciascun modello.

È essenziale comprendere tale modello di responsabilità condivisa per poter predisporre una buona RDO di servizi cloud. Gli enti pubblici devono sapere quali sono le proprie responsabilità, quali sono le responsabilità del CISP e in quali casi possono risultare utili i consulenti/gli ISV partner e le soluzioni da essi offerte.

2.3.1 Requisiti minimi

In tema di sicurezza del cloud, la parola chiave è **funzionalità**. Gli enti pubblici devono essere esigenti con i CISP e pretendere che i CISP forniscano funzionalità di sicurezza tali da garantire ai clienti l'assolvimento dei propri compiti nell'ambito del modello di responsabilità condivisa. Come illustrato nell'elenco di seguito, il CISP è chiamato a fornire una funzionalità standardizzata. In questo modo, il cliente può usufruirne per rendere sicuro il proprio ambiente cloud specifico.

- ***Fornire** firewall di rete e **funzionalità** firewall delle applicazioni Web per creare reti private e per controllare l'accesso a istanze e applicazioni.*
- ***Fornire opzioni** di connettività che supportano le connessioni private o dedicate dall'ufficio del cliente o dall'ambiente on-premise del cliente.*
- ***Fornire** le **funzionalità** per implementare una strategia di difesa profonda e contrastare gli attacchi DDoS (Distributed Denial of Service).*
- *Fornire **funzionalità** di crittografia dei dati nei servizi di archiviazione e database.*
- ***Fornire opzioni** per la gestione flessibile delle chiavi, tali da consentire al cliente di scegliere se affidare al CISP la gestione delle chiavi di crittografia o assumere direttamente il controllo completo delle proprie chiavi.*
- ***Fornire API** che consentano ai clienti di integrare la crittografia e la protezione dei dati con eventuali servizi sviluppati o implementati in un ambiente CISP.*

- ***Fornire** gli **strumenti** di implementazione che consentano di gestire la creazione e la disattivazione delle risorse del CISP in base agli standard dell'ente.*
- ***Fornire strumenti** di gestione della configurazione e dell'inventario per individuare le risorse del CISP e, successivamente, monitorare e gestire le eventuali modifiche a tali risorse nel corso del tempo.*
- ***Fornire strumenti e funzionalità** che consentano ai clienti di vedere con esattezza cosa accade nel proprio ambiente CISP.*
- ***Supportare** la **visibilità** avanzata delle chiamate API, inclusi i dati su autore, tipo di chiamata, data, ora e origine.*
- ***Fornire opzioni** di aggregazione dei registri per razionalizzare le indagini e il reporting di conformità.*
- *Fornire le funzionalità per configurare le notifiche di avviso al verificarsi di determinati eventi o in caso di superamento di determinate soglie.*
- ***Fornire le funzionalità** per definire, applicare e gestire le policy di accesso utente nell'ambito dei servizi del CISP.*
- ***Fornire** le **funzionalità** per definire i singoli account utente con autorizzazioni nell'ambito delle risorse del CISP.*
- ***Fornire** le **funzionalità** per l'integrazione e la federazione con le directory aziendali, al fine di ridurre i costi di gestione e migliorare l'esperienza dell'utente finale.*

Molti dei suddetti requisiti sono descritti nell'*Appendice A - Requisiti tecnici per il confronto tra* offerenti.

È possibile utilizzare le funzionalità superiori allo standard minimo di sicurezza per svolgere un'analisi più approfondita delle "opzioni a valore aggiunto" o del "miglior rapporto qualità-prezzo" in una RDO. In tema di sicurezza, maggiore è l'integrazione e l'automazione delle funzionalità, meglio è. Quanto ai requisiti per il confronto tra gli offerenti, vedere ancora l'*Appendice A - Requisiti tecnici per il confronto tra* offerenti.

Gli enti pubblici devono prestare attenzione alle certificazioni e alle valutazioni riguardanti l'accreditamento del cloud, per accertare la presenza concreta dei controlli di sicurezza del CISP. Consideriamo, ad esempio, un CISP che ha ottenuto la convalida e la certificazione da parte di un revisore indipendente che attesta la conformità allo standard di certificazione ISO 27001. Nell'Annesso A, dominio 14, dello standard ISO 27001 vengono approfonditi i controlli specifici ai quali aderisce un CISP in conformità ai requisiti ISO riguardanti acquisizione, sviluppo e manutenzione del sistema. È probabile che questi controlli coprano gran parte o tutti i controlli in materia di acquisizione, sviluppo e manutenzione del sistema che normalmente vengono richiesti da un ente in una RDO di risorse IT. Ha dunque senso che l'ente chieda semplicemente la certificazione ISO 27001 del CISP, anziché duplicare l'elenco dei requisiti di controllo riguardanti acquisizione, sviluppo e manutenzione del sistema in una RDO di servizi cloud.

Questo metodo, che sfrutta le certificazioni di conformità rilasciate da terze parti, può essere applicato alla maggior parte dei controlli di sicurezza e conformità, ad esempio: codice di condotta CISPE sulla protezione dei dati (GDPR), ISO, SOC ecc.

Testo di esempio di una RDO: sicurezza

*Il CISP deve rivelare all'**<ENTE>** i propri processi di sicurezza non proprietari e le proprie limitazioni tecniche, in modo da consentire che vengano raggiunti livelli soddisfacenti di protezione e flessibilità tra l'**<ENTE>** e il fornitore di servizi.*

Il CISP deve dichiarare i ruoli e le responsabilità che gli competono in materia di sicurezza e conformità:

- *Nella proposta è necessario descrivere i ruoli e le responsabilità sia del CISP sia dell'**<ENTE>** in materia di sicurezza. È necessario dichiarare con precisione le responsabilità e descrivere i servizi del CISP che possono aiutare l'**<ENTE>** a costruire e automatizzare le funzioni di sicurezza nell'ambiente cloud di quest'ultimo.*
- *Occorre rispondere alle specifiche tecniche riportate nell'**APPENDICE A** riguardo ai requisiti di sicurezza dell'**<ENTE>**.*

PROPRIETÀ E CONTROLLO DEI CONTENUTI DELL'<ENTE>

*Descrivere in che modo le funzionalità del CISP possono proteggere la privacy dei dati dell'**<ENTE>**. Includere i controlli posti in essere per la protezione dei contenuti dell'**<ENTE>**. Il CISP deve fornire un solido isolamento regionale, cosicché gli oggetti archiviati in una regione non escano mai da quella regione, tranne quando l'**<ENTE>** esplicitamente li trasferisce altrove.*

- *L'**<ENTE>** gestirà l'accesso ai propri contenuti, servizi e risorse. Il CISP deve fornire una serie di funzionalità avanzate per accesso, crittografia e registrazione, in modo da aiutare l'**<ENTE>** a realizzare efficacemente tale operazione. Il CISP non dovrà accedere ai contenuti dell'**<ENTE>** o utilizzarli per alcuna finalità, tranne nei casi previsti dalla legge e nella misura in cui ciò sia necessario per la gestione dei servizi del CISP e per l'erogazione degli stessi all'**<ENTE>** e ai rispettivi utenti finali.*
- *L'**<ENTE>** potrà scegliere la regione (o le regioni) in cui archiviare i propri contenuti. Il CISP non potrà trasferire o replicare i contenuti dell'**<ENTE>** al di fuori della regione o delle regioni scelte, tranne nei casi previsti dalla legge e nella misura in cui ciò sia necessario per la gestione dei servizi del CISP e per l'erogazione degli stessi all'**<ENTE>** e ai rispettivi utenti finali.*
- *L'**<ENTE>** sceglierà come rendere sicuri i propri contenuti. Il CISP deve mettere a disposizione una crittografia solida per i contenuti dell'**<ENTE>**, sia in transito sia a riposo, concedendo all'**<ENTE>** la possibilità di gestire le proprie chiavi di crittografia.*
- *Il CISP è tenuto ad avere un programma di controlli di sicurezza fondato su best practice universalmente riconosciute in materia di privacy e protezione dei dati, per consentire all'**<ENTE>** di definire, gestire e sfruttare al meglio l'ambiente di controllo della sicurezza del CISP. Tali procedure di controllo e protezione della sicurezza devono essere convalidate in modo indipendente tramite valutazioni condotte da terze parti.*

Per gli enti pubblici, le certificazioni e le valutazioni di accreditamento del cloud rappresentano la garanzia che i CISP abbiano predisposto controlli di sicurezza fisica e logica efficaci. Grazie all'apporto di questi accreditamenti nelle RDO, è possibile semplificare le procedure di appalto ed evitare attività ripetitive e gravose, o processi di approvazione non strettamente necessari in un ambiente cloud.

Le RDO in ambito cloud devono conferire ai CISP la possibilità di dimostrare l'adeguamento ai sistemi di accreditamento e alle valutazioni della conformità. Come accennato in precedenza, vi è una notevole sovrapposizione degli scenari di rischio e delle pratiche di gestione dei rischi tra i diversi sistemi di accreditamento esistenti. Poiché i controlli e i requisiti formano un tutt'uno in questi accreditamenti, per risolvere la questione della conformità in una RDO la soluzione più rapida consiste nel richiedere ai CISP di dichiarare la propria conformità agli accreditamenti, anziché raddoppiare gli sforzi attraverso l'elencazione dei singoli controlli (molti dei quali potrebbero essere

ricavati da una RDO precedente per i data center on-premise e, in quanto tali, potrebbero non essere pertinenti al cloud computing).

NOTA: inoltre, è molto importante comprendere come consultare i report elencati di seguito. Ad esempio, i report SOC 1 e SOC 2 sono generalmente documenti sensibili. Occorre capire quali accordi sono necessari ai fini della consultazione (ad esempio, gli accordi di non divulgazione o NDA), anziché richiedere semplicemente che detti documenti siano allegati alla risposta a una RDO (si tratta di documenti che potrebbero essere resi pubblici attraverso atti giuridici o legislativi, con il rischio di compromettere la sicurezza del cloud).

Testo di esempio di una RDO: conformità

L'uso di standard di sicurezza, conformità e operatività consolidati e derivanti dalle best practice nelle attività dei servizi cloud (tra cui gestione dei dati, sicurezza dei dati, riservatezza, disponibilità ecc.) semplifica l'approvvigionamento delle tecnologie cloud.

L'<ENTE> dovrà valutare le singole offerte in rapporto agli standard di sicurezza, conformità e operatività accettati, come spiegato più avanti e nell'Appendice A. Affidandosi alla certificazione di conformità dichiarata dal fornitore per ciascuno standard, l'<ENTE> può utilizzare la conformità minima rispetto allo standard come criterio di valutazione dell'offerta.

Chiedendo al CISP di garantire che la conformità allo standard minimo sia mantenuta per l'intera durata del contratto, si otterrà, come vantaggio, un servizio sempre conforme.

Il CISP che presenta l'offerta (direttamente o per il tramite di un suo rivenditore) deve dimostrare di essere in possesso dei seguenti attestati, report e certificazioni rilasciati da soggetti terzi indipendenti (nota: qualora sussistano delle limitazioni alla divulgazione di alcuni di questi attestati, report e certificazioni per motivi di sicurezza, l'<ENTE> si impegna a collaborare con il CISP per ottenere l'accesso tramite azioni concordate):

Certificazioni/attestati	*Leggi, normative e privacy*	*Allineamenti/Framework*
☐ C5 [Germania]		*☐ CDSA*
☐ Codice di condotta CISPE sulla protezione dei dati (GDPR)		
☐ CNDCP (Climate Neutral Data Centre Pact, Patto per la neutralità climatica dei data center)		
☐ DIACAP	*☐ Direttiva dell'UE sulla protezione dei dati*	*☐ CIS*
☐ DoD SRG – Livelli 2 e 4	*☐ Clausole modello dell'UE (EU Model Clauses)*	*☐ Criminal Justice Info. Service (CJIS, servizi di informazione sulla giustizia penale)*
☐ HDS (Francia, Sanità)		
☐ FedRAMP	*☐ FERPA*	*☐ CSA*
☐ FIPS 140-2	*☐ GDPR*	*☐ Scudo UE-USA per la privacy*
☐ ISO 9001	*☐ GLBA*	*☐ Approdo sicuro (Safe harbor) UE*

☐ *ISO 27001*	☐ *HIPAA*	☐ *FISC*
☐ *ISO 27017*	☐ *HITECH*	☐ *FISMA*
☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [Regno Unito]*
☐ *IRAP [Australia]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 Part 11)*
☐ *MTCS Tier 3 [Singapore]*	☐ *PDPA – 2010 [Malesia]*	☐ *ICREA*
☐ *PCI DSS livello 1*	☐ *PDPA – 2012 [Singapore]*	☐ *IT Grundschutz [Germania]*
☐ *Rule 17-a-4(f) della SEC*	☐ *PIPEDA [Canada]*	☐ *MARS – E*
☐ *SecNumCloud (Francia)*		
☐ *SOC1/ISAE 3402*	☐ *Privacy Act [Australia]*	☐ *MITA 3.0*
☐ *SOC2/SOC3*	☐ *Privacy Act [Nuova Zelanda]*	☐ *MPAA*
☐ *Codice SWIPO IaaS*		
	☐ *Autorizzazione DPA (Spagna)*	☐ *NIST*
	☐ *U.K. DPA – 1988*	☐ *Livelli di certificazione Uptime Institute*
	☐ *VPAT/Sezione 508*	☐ *UK Cloud Security Principles*

L'elenco di cui sopra viene fornito a puro scopo illustrativo e non pretende di essere esaustivo per quanto concerne le certificazioni e gli standard applicabili ai servizi cloud.

2.3.1.1 Protezione dei dati

Quando si utilizzano i servizi cloud, un aspetto fondamentale riguarda il trattamento dei dati personali in conformità alla normativa UE applicabile sulla protezione dei dati, compreso il Regolamento generale sulla protezione dei dati (GDPR). Il GDPR è un regolamento fondato su principi e, pertanto, non fornisce indicazioni specifiche di settore a garanzia della conformità. Tuttavia, il GDPR incoraggia l'adozione di strumenti di conformità, come i codici di condotta, per fornire tali indicazioni. Il CISPE, in collaborazione con l'Autorità francese per la protezione dei dati (CNIL) ha sviluppato un codice di condotta per la protezione dei dati (Codice CISPE[6]) approvato dal Comitato europeo per la protezione dei dati, applicabile in Europa a livello generale. Lo scopo del Codice è aiutare i CISP a rispettare il GDPR e guidare i clienti nella valutazione circa l'idoneità dei CISP al trattamento dei dati personali che il cliente desidera effettuare.

- Il Codice si concentra esclusivamente sul settore IaaS e illustra i ruoli e le responsabilità specifici dei fornitori IaaS.
- Contribuisce a chiarire gli aspetti riguardanti il trattamento equo e trasparente, nonché le misure di sicurezza adeguate nel contesto dei servizi di infrastrutture cloud (GDPR, articolo 40 [2]).

[6] https://cispe.cloud/code-of-conduct/

- Aiuta i clienti a capire come mantenere la sovranità sui propri dati, garantendo che questi ultimi rimangano all'interno dell'UE.
- Promuove le best practice in materia di protezione dei dati a sostegno dell'iniziativa GAIA-X dell'UE per lo sviluppo di servizi di dati cloud europei.

La conformità del CISP ai codici di condotta sulla protezione dei dati, come il Codice CISPE, garantisce che i dati personali saranno trattati nel pieno rispetto del GDPR.

Testo di esempio di una RDO: protezione dei dati

Il CISP che presenta l'offerta (direttamente o per il tramite di un suo rivenditore) dovrebbe dimostrare la propria capacità di rispettare un codice di condotta sulla protezione dei dati come il Codice CISPE. Il codice sulla protezione dei dati deve essere conforme ai requisiti indicati dal framework GDPR. Il codice dovrebbe includere almeno: (1) una definizione chiara dei ruoli e delle responsabilità del CISP; (2) il requisito in base al quale il CISP non utilizza i dati dei clienti per scopi di marketing o pubblicitari e (3) la possibilità per i clienti di selezionare i servizi CISP che consentono il trattamento dei dati interamente all'interno dello Spazio economico europeo. La conformità al codice deve essere verificata da organi di controllo esterni (organi di vigilanza) accreditati da revisori esterni indipendenti, a loro volta accreditati dall'Autorità europea per la protezione dei dati personali.

2.3.1.2 Cambio di fornitori di servizi cloud e portabilità dei dati

I clienti dovrebbero avere la libertà di scegliere i servizi cloud che desiderano utilizzare e non essere "bloccati" dai vincoli contrattuali di un CISP o fornitore di servizi PaaS/SaaS.

I servizi cloud forniti dal CISP sono standardizzati e progettati per funzionare secondo il modello "uno a molti", pertanto la configurazione, il provisioning e il controllo dei servizi sono a carico del cliente. Un vantaggio del cloud computing consiste nel fatto che i clienti possono scegliere i servizi standardizzati di cui hanno bisogno per sviluppare le proprie applicazioni e soluzioni specifiche. Tale vantaggio comporta la possibilità di passare, in qualsiasi momento, a servizi nuovi o diversi, che soddisfano al meglio le rispettive esigenze.

Come nel caso della protezione dei dati, i codici di condotta conferiscono ai clienti sicurezza e fiducia quando si tratta di passare dall'infrastruttura on-premise al cloud oppure da un CISP all'altro. Insieme a EuroCIO (l'Associazione europea dei CIO), il CISPE ha co-presieduto lo sviluppo del codice di condotta per la portabilità dei dati e il passaggio dei clienti dai servizi cloud ai servizi cloud IaaS (Codice SWIPO IaaS[7] [8]). La prima versione del codice è stata sviluppata in conformità al Regolamento UE sulla libera circolazione dei dati, consegnata alla Commissione europea a novembre 2019 sotto la presidenza finlandese dell'UE e pubblicata dall'associazione SWIPO AISBL a maggio 2020. Ad aprile 2021 SWIPO AISBL ha dichiarato la conformità al codice dei primi servizi; a maggio 2021 è stata riconosciuta l'adesione al codice dei primi servizi forniti dagli associati CISPE.

Testo di esempio di una RDO: cambio di fornitori di servizi cloud e portabilità dei dati

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security
[8] https://swipo.eu/

Il CISP che presenta l'offerta (direttamente o per il tramite di un suo rivenditore) dovrebbe dimostrare la propria capacità di rispettare un codice di condotta in materia di "cambio di fornitori di servizi cloud e portabilità dei dati" come il Codice SWIPO IaaS. Il codice deve indicare la modalità in cui il CISP offre ai clienti il trasferimento sicuro dei dati aziendali, qualora essi decidano di affidarsi ad un altro CISP.

2.3.2 Confronto tra fornitori

Come spiegato nei paragrafi precedenti con riferimento ai criteri tecnici, in una RDO di servizi cloud, oltre ai requisiti di sicurezza minimi, è importante indicare anche i criteri in base ai quali le funzionalità e i servizi in materia di sicurezza offerti dal CISP saranno messi a confronto in caso di valutazione competitiva.

Per un esempio dei requisiti minimi di sicurezza di un CISP, vedere l'*Appendice A - Requisiti tecnici per il confronto tra* offerenti. Si consiglia vivamente agli enti pubblici di svolgere una valutazione dei CISP tenendo conto delle funzionalità di sicurezza elencate di seguito:

Testo di esempio di una RDO: considerazioni importanti in materia di sicurezza

- *Conoscenza del modello di responsabilità condivisa e della relativa documentazione da parte del CISP; ciò aiuta i clienti a comprendere come si delineano le responsabilità, in tema di sicurezza, relative alle funzionalità e ai servizi del CISP (ad esempio, nel contesto del regolamento GDPR).*
- *Comprovata sicurezza dell'infrastruttura del CISP, mediante documenti non proprietari e di pubblico dominio che attestano la posizione di sicurezza e i controlli fisici/logici posti in essere dal CISP.*
- *Supporto specifico del CISP alla sicurezza del cloud.*
- *Servizi che consentono ai clienti di formalizzare la progettazione degli account, automatizzare i controlli di sicurezza e governance del cloud, semplificare il controllo.*
- *Funzionalità per creare, fornire e gestire un insieme di risorse sotto forma di modello (inclusi i modelli di sicurezza "gold-standard" dei CISP o dei loro partner).*
- *Funzionalità per definire azioni di controllo affidabili e ripetibili.*
- *Funzionalità per svolgere controlli continui e in tempo reale.*
- *Funzionalità per la redazione tecnica delle policy di governance del cloud.*
- *Funzionalità per creare funzioni obbliganti (forcing functions), che non possono essere annullate dagli utenti senza le autorizzazioni necessarie per la modifica.*
- *Capacità di implementare in modo affidabile quanto precedentemente redatto nelle policy, negli standard e nelle norme, nonché di creare procedure applicabili di sicurezza e conformità; tutto ciò, di rimando, crea un modello di governance del cloud funzionale e affidabile per gli ambienti IT.*
- *Servizi per la protezione dagli attacchi DDoS più comuni e frequenti nei confronti della rete e del livello di trasporto, con la capacità di scrivere regole personalizzate per attenuare gli attacchi sofisticati al livello delle applicazioni.*
- *Servizio gestito di rilevamento delle minacce.*

2.3.3 Appalto

Come accennato in precedenza, i termini e le condizioni del CISP devono riflettere il modello di funzionamento dei servizi cloud (non si tratta di acquistare risorse materiali; inoltre, i CISP operano su grande scala, fornendo servizi standardizzati). Di conseguenza, è essenziale che i termini e le condizioni del CISP siano incorporati e applicati nella misura più ampia possibile. Per ulteriori informazioni su termini e condizioni, e sull'appalto, vedere il paragrafo *2.5*.

Quando si tratta di sicurezza, è importante che i CISP possano aggiornare costantemente le proprie offerte; in alternativa, si dovrebbe dare la possibilità ai fornitori di aggiungere dei prodotti dopo la scadenza del termine per la presentazione dell'offerta, purché i prodotti siano conformi ai parametri originali della RDO. In questo modo si tiene conto del fatto che le funzionalità e i servizi correlati alla sicurezza si evolvono rapidamente; i CISP rilasciano spesso servizi orientati alla sicurezza che, in molti casi, sono gratuiti. È importante stabilire un livello di sicurezza minimo di riferimento (vedere i requisiti minimi descritti in precedenza), per garantire che le modifiche alle offerte in materia di sicurezza non siano peggiorative.

Il modello di responsabilità condivisa è, ovviamente, al centro della sicurezza in una RDO di servizi cloud. Ciascuna parte deve avere la nozione esatta delle proprie responsabilità in materia di sicurezza; i CISP dovrebbero essere tenuti a documentare le proprie responsabilità e quelle del cliente in materia di sicurezza rispetto alle tecnologie cloud fornite dal CISP, nonché a fornire la documentazione necessaria per aiutare i clienti a integrare e automatizzare le best practice in materia di sicurezza.

Un Accordo quadro per il cloud deve offrire la flessibilità necessaria per poter rimuovere un fornitore qualora quest'ultimo non soddisfi più i requisiti minimi di sicurezza e conformità previsti nella RDO di servizi cloud.

2.4 Prezzi

Per affidare un contratto di fornitura di tecnologie cloud che tenga conto della fluttuazione della domanda, gli enti pubblici necessitano di un contratto che consenta loro di pagare i servizi in base al consumo effettivo (con la governance del cloud e la visibilità richieste in materia di utilizzo e di spesa).

È importante che le RDO di servizi cloud tengano in considerazione il valore e il costo totale di proprietà (TCO), anziché fare semplicemente un confronto diretto dei prezzi unitari, articolo per articolo. Il criterio del prezzo unitario più basso non è compatibile con il modello cloud e, pertanto, non necessariamente l'appalto viene aggiudicato all'offerta economicamente più vantaggiosa o al prezzo complessivamente più basso.

Per agevolare la valutazione del prezzo del CISP, è utile provvedere alla pre-qualificazione o alla selezione dei CISP mediante i ***requisiti minimi correlati ai prezzi****, in modo da permettere ai CISP con funzionalità simili di qualificarsi per l'Accordo quadro. Nella procedura di valutazione degli ordini a chiamata e delle mini-gare, è possibile consultare una gamma di architetture cloud tipiche e gli* ***scenari di prezzo*** *che riflettono i carichi di lavoro dell'ente pubblico, chiedendo ai CISP di proporre dei prezzi per tali voci. Anche i test dimostrativi (Live Test Demos) sono utili per mettere a confronto le prestazioni e l'elasticità dei servizi delle tecnologie cloud fornite dai CISP. Per esaminare un test dimostrativo di esempio delle tecnologie cloud, vedere l'Appendice B.*

2.4.1 Requisiti minimi

Il capitolo dei prezzi in una RDO di servizi cloud è composto da quattro elementi chiave:

1. Prezzo a consumo: i clienti dei servizi cloud stanno assimilando il modello di pagamento in base al consumo, secondo il quale, alla fine del mese, si paga solo ciò che si è utilizzato effettivamente. Questo metodo è ottimale per conoscere i parametri di utilizzo e delle risorse.
2. Prezzi trasparenti: i prezzi del CISP devono essere pubblici e trasparenti.
3. Prezzi dinamici: comporta la flessibilità necessaria per consentire la fluttuazione dei prezzi del cloud in base ai prezzi di mercato. Questo approccio sfrutta il dinamismo e la competitività dei prezzi del cloud, stimolando l'innovazione e la riduzione dei prezzi.
4. Spesa controllata: i CISP devono offrire strumenti per il reporting, il monitoraggio e le previsioni affinché i clienti possano (1) monitorare l'utilizzo e la spesa sia a livelli granulari che di riepilogo, (2) ricevere avvisi quando l'utilizzo e la spesa superano le soglie personalizzate e (3) stimare l'utilizzo e la spesa per pianificare i futuri budget destinati al cloud.

Testo di esempio di una RDO: prezzi

L'<ENTE> chiede ai CISP candidati di indicare, nella loro proposta, il metodo e il modello di determinazione dei prezzi per la fornitura di ciascuno dei servizi offerti agli utenti finali sotto forma di funzionalità cloud commerciale.

Il CISP deve fornire:

- *Un documento contenente le definizioni dei servizi o i link alle definizioni dei servizi*
- *Un documento contenente i termini e le condizioni*
- *Un documento contenente i prezzi (i link ai prezzi al pubblico sono ammessi a condizione che, su richiesta, sia disponibile un documento/listino prezzi completo)*

Il prezzo corrisponderà al costo della configurazione più comune del servizio. I CISP devono offrire delle opzioni di sconto in base al volume e strumenti di calcolo adeguati per determinare il prezzo effettivo di ciò che viene acquistato, più il valore complessivo a vantaggio dell'acquirente (ad esempio, servizi di ottimizzazione con conseguente abbattimento dei costi).

Nell'ambito dell'Accordo quadro, gli acquirenti possono interagire con i fornitori per chiedere chiarimenti circa la descrizione di un servizio, i termini e le condizioni applicati, i prezzi o il modello/documento che definisce il servizio. È necessario mantenere traccia di tutte le interazioni con i fornitori.

Ulteriori requisiti riguardanti i prezzi

- *Le tecnologie cloud devono essere fornite con un modello dinamico di determinazione dei prezzi, che assicuri la massima flessibilità commerciale e supporti scalabilità e crescita.*
- *Gli attributi dei prezzi devono includere quanto segue:*
  - *I prezzi forniti riguardano un servizio on demand, in base all'utilità, con pagamento in base al consumo? Spiegare il modello utilizzato per la determinazione dei prezzi.*
  - *È possibile ottenere ulteriori sconti in caso di impegno ad utilizzare/acquistare grandi volumi? Fornire spiegazioni in forma dettagliata.*
  - *I prezzi sono di dominio pubblico e trasparenti? Includere i link dei prezzi al pubblico.*
  - *I prezzi sono dinamici e si adattano in modo rapido ed efficiente alla concorrenza sul mercato?*
  - *Vengono fornite best practice e risorse per monitorare la spesa?*
  - *Vengono fornite best practice e risorse per ottimizzare i costi?*

Trasparenza dei prezzi
*Data la costante tendenza al ribasso dei prezzi delle tecnologie cloud, trainata dall'innovazione e dalla concorrenza, il costo unitario a consumo del servizio del CISP che viene sostenuto dall'**<ENTE>** nell'ambito dell'Accordo quadro non potrà mai essere superiore al prezzo unitario pubblicato sul sito Web del fornitore del servizio cloud, che è valido nel momento in cui il servizio viene utilizzato dal cliente.*

Avvisi/report per budget e fatturazione
*Per dimostrare la fornitura e l'utilizzo delle tecnologie cloud, i CISP devono fornire all'**<ENTE>** gli strumenti per generare report di fatturazione con il dettaglio dei costi per ora, giorno o mese, per ogni account dell'ente, per prodotto o risorsa del prodotto, o per tag definiti dal cliente. L'**<ENTE>** riconosce che, nell'ambito del modello di responsabilità condivisa del cloud, l'**<ENTE>** sarà responsabile dell'uso di funzionalità e strumenti per il budget e la fatturazione forniti dal CISP al fine di soddisfare specifici requisiti di previsione e reporting.*

- *Fornire indicazioni sul modo in cui l'**<ENTE>** può visualizzare i dati sulla fatturazione a livello dettagliato o sintetico, che evidenziano i modelli di spesa per le risorse del CISP nel tempo e forniscono, inoltre, una previsione di spesa futura.*
- *Fornire indicazioni su come l'**<ENTE>** può filtrare i dati di utilizzo e fatturazione in base al servizio, all'account collegato o ai tag personalizzati applicati alle risorse e creare avvisi di fatturazione per ricevere notifiche quando l'utilizzo dei servizi si avvicina o supera il budget/le soglie impostati dall'<**ENTE**>.*
- *Fornire indicazioni su come l'**<ENTE>** può prevedere la quantità di servizi cloud da utilizzare in un determinato periodo di tempo, in base all'utilizzo precedente. Il CISP deve fornire una **stima** di quanto fatturerà all'**<ENTE>** e consentire all'**<ENTE>** di utilizzare allarmi e budget relativi alle quantità che quest'ultimo prevede di utilizzare ai fini di una maggiore governance sui costi e sulla spesa.*

2.4.2 Confronto tra fornitori

Gli enti pubblici spesso sollecitano la competizione tra gli offerenti applicando dei criteri di valutazione, ad esempio il miglior rapporto qualità-prezzo, l'offerta economicamente più vantaggiosa (MEAT, Most Economically Advantageous Tender) o il prezzo più basso. Quando si definiscono i prezzi degli ordini a chiamata o delle mini-gare nell'ambito di un accordo quadro, è consigliabile utilizzare un approccio che tenga conto delle caratteristiche uniche del cloud. Ad esempio, è importante comprendere che un semplice confronto tra le voci elencate nelle proposte dei fornitori di servizi cloud (come calcolo o archiviazione) non costituisce un metodo efficace per confrontare le offerte. Tale metodo, infatti, non tiene conto di caratteristiche importanti come le prestazioni, l'ottimizzazione dei costi tramite l'uso di servizi nativi per il cloud e degli strumenti di monitoraggio del CISP, o la differenziazione dei servizi che i CISP potrebbero offrire gratuitamente. Inoltre, il prezzo di catalogo di un CISP può comprendere decine di migliaia di voci/articoli e i modelli dei prezzi possono variare da un servizio all'altro e da un fornitore all'altro.

Analisi del costo totale di proprietà

È consigliabile concentrarsi sul costo totale di proprietà dei casi d'uso definiti, che tengono conto di tutti gli aspetti di una soluzione cloud (compresi i servizi dei partner, gli sconti standardizzati del CISP, le caratteristiche tecniche in grado di aumentare le performance, ridurre/ottimizzare i costi ecc.).

Confronto in base allo scenario

Il processo di valutazione può anche contemplare gli scenari tipici che corrispondono a sistemi o applicazioni comuni. Tali scenari (come il Web hosting o l'implementazione di un sistema di risorse

umane con un numero x di utenti ecc.) possono includere variabili come la velocità e la scalabilità delle risorse, le prestazioni dell'applicazione o della soluzione, i tempi di accesso all'archiviazione, dati complessi a basso volume rispetto a semplici attività di elaborazione ad alto volume e così via. Inoltre, gli scenari tipici delle applicazioni o dei sistemi possono comprendere l'elaborazione di volumi elevati in concomitanza con le dichiarazioni dei redditi e gli avvisi di emergenza, quali l'allerta alluvioni. Gli scenari dovranno essere esaustivi, in modo da comprendere tutte le tecnologie e i servizi che il cliente potrebbe utilizzare durante il progetto. In questo modo il cliente riuscirà a confrontare il costo complessivo stimato del progetto.

Confronto finanziario e tecnico tra scenari

Quando si confrontano i prezzi delle offerte dei CISP, è altrettanto importante tenere conto dei vantaggi tecnici. Ad esempio, un CISP può permettere ai clienti di realizzare una topologia di ripristino di emergenza (Disaster Recovery, DR) in modalità attivo/attivo grazie al suo modello che prevede la presenza di cluster di data center all'interno di una regione geografica. Un CISP che non dispone di questo tipo di ridondanza e di configurazione dei data center potrebbe costare un x% in più, a causa dei costi imputabili al ripristino di emergenza. Per capire l'importanza di un approccio olistico ai prezzi, che include caratteristiche tecniche aggiuntive, ai fini della valutazione dei CISP, consideriamo il seguente esempio di confronto diretto, articolo per articolo.

Esempio: un cliente vuole confrontare il prezzo del servizio di archiviazione di oggetti offerto dai CISP qualificati nell'ambito di un Accordo quadro. Il CISP 1 propone un prezzo di 0,023 EUR/GB per la voce "unità" di archiviazione. Il CISP 2 propone un prezzo di 0,01 EUR/GB per la stessa voce. Se si facesse un semplice confronto tra unità, il cliente non farebbe domande essenziali come:

1. Quante copie ridondanti dell'oggetto sono disponibili in caso di guasto? Nell'esempio precedente, il CISP 1 è progettato per sostenere la perdita simultanea di dati in due strutture diverse e conserva copie multiple dei dati. Nel caso del CISP 2, non vengono create copie ridondanti.
2. Qual è il livello di sostenibilità degli oggetti archiviati? Per il CISP 1 è del 99,999999999%; per il CISP 2 è del 99%.
3. Bisogna considerare il costo dell'intero ciclo di vita della proprietà del progetto o del carico di lavoro totale; bisogna, altresì, considerare in quale misura le funzionalità di ottimizzazione dei costi possono ridurre i costi dal punto di vista dell'archiviazione e dell'utilizzo dei dati (ad esempio, aumentando l'uso delle funzioni serverless di un CISP, è possibile ridurre i costi di un x%).

Queste sono solo alcune delle tante considerazioni tecniche che incidono sui prezzi, in particolare per quanto riguarda la sicurezza e la conformità.

Punti da considerare nell'ambito degli scenari per la determinazione dei prezzi

Tariffe base: in pratica, i prezzi pubblici dei CISP. I CISP devono rendere pubblici questi prezzi. Tuttavia, come indicato in precedenza, per confrontare in modo efficace i CISP tra di loro, i clienti

La valutazione delle capacità complessive di un CISP è un requisito indispensabile per i clienti di servizi cloud che puntano al miglior rapporto qualità-prezzo. Ad esempio, alcuni CISP potrebbero offrire una serie di servizi gratuiti, o praticamente gratuiti: una valutazione dei prezzi dovrebbe tenere conto di tale aspetto. Di contro, altri CISP potrebbero addebitare un costo per funzionalità analoghe.

possono chiedere a tutti i fornitori di stabilire i prezzi in base a 3-5 scenari specifici (o qualsiasi altro numero ritenuto opportuno dal cliente). Gli scenari dovranno essere esaustivi, così da comprendere l'intero ventaglio di tecnologie e servizi che il cliente potrebbe utilizzare durante il progetto. In questo modo, il cliente potrà confrontare il costo complessivo stimato del progetto. I confronti effettuati a livello di singole voci/SKU tendono ad essere più problematici che utili per clienti e fornitori. I clienti dovrebbero confrontare decine di migliaia di voci di tutti i CISP; dal canto loro, i fornitori dovrebbero fornire questo livello di dettaglio e gestirlo, qualora il prezzo effettivo sia determinato solo dal consumo del servizio.

I criteri di valutazione possono essere redatti in modo tale da permettere ai CISP di indicare le funzionalità "incluse di default" e quanto tali servizi incidono sul costo complessivo. I criteri di valutazione possono anche prendere in considerazione i prezzi del CISP a volume/a scaglioni e gli sconti commerciali disponibili, come le istanze riservate/le istanze Spot. Ad esempio:

- x% di risparmio se i clienti acquistano capacità di calcolo riservata (1 anno, 3 anni ecc.)
- x% di sconto sui prezzi a volume/a scaglioni
- x% di risparmio in base a verifiche dell'architettura e a ottimizzazioni dell'infrastruttura, ad esempio il passaggio all'opzione di calcolo più adeguata
- Come osservato in precedenza, occorre considerare il costo dell'intero ciclo di vita e le modalità con cui le funzioni di ottimizzazione possono ridurre i costi.

SCENARIO PER LA DETERMINAZIONE DEI PREZZI
Gli offerenti devono indicare i prezzi relativamente al seguente scenario solo per le finalità di valutazione. Il prezzo effettivo si baserà sul consumo dei servizi secondo un modello di pagamento in base all'uso.

I requisiti riportati sotto sono solo indicativi ai fini della determinazione dei prezzi e vengono forniti con l'esplicita consapevolezza che, durante la durata dell'appalto, tali requisiti nominali cambieranno. Indicare sia i prezzi on demand per 12 e 36 mesi, sia i prezzi per capacità riservata per 12 e 36 mesi.

Indicare:

- *Nome delle soluzioni proposte:*
- *Miglior prezzo dell'offerente:*
- *Ore di servizio: 24x7x365*
- *Disponibilità del servizio: 99,95%*

Gli scenari per la determinazione dei prezzi possono anche includere esempi di clienti esistenti con carichi di lavoro simili, che hanno ottimizzato la loro spesa in 1/2/3 anni, utilizzando strumenti di monitoraggio e ottimizzazione del CISP, adottando soluzioni native ottimizzate per il cloud e attraverso riduzioni dei prezzi da parte del CISP.

2.5 Schema/Termini e condizioni per l'esecuzione dell'appalto

Le tecnologie e le operazioni cloud fornite dal CISP sono standardizzate in base a un progetto predefinito (by-design), pertanto anche le condizioni contrattuali sono standardizzate. Tuttavia, vi è la possibilità di modificare marginalmente questi contratti per adeguarli ai contesti legislativi e normativi locali.

Spesso le tradizionali procedure di appalto del settore IT prevedono regole rigorose che impongono ai candidati di rispettare molti o tutti i requisiti dell'appalto per non essere esclusi. In alternativa, prevedono un sottoinsieme vincolante di requisiti obbligatori. Quando si utilizza questo metodo di approvvigionamento per le tecnologie cloud – che sono, in realtà, un insieme di componenti e strumenti standardizzati per la progettazione di una soluzione personalizzata – tendenzialmente gli appalti non vanno a buon fine.

2.5.1 Termini e condizioni

Quando si negoziano le condizioni di un appalto nell'ambito di una RDO di servizi cloud, il primo passaggio consiste nell'esaminare e comprendere i termini commerciali in essere del CISP che, in molti casi, sono pubblicati nel sito Web del CISP in questione. Gli enti pubblici sono sempre più orientati ad accettare i termini commerciali dei CISP. L'incontro con i CISP e con i loro partner, per approfondire i rispettivi orientamenti, rientra tra gli sforzi volti a comprendere i termini commerciali. La domanda chiave da porre è "perché" i CISP operano con termini specifici. Alcuni di questi termini possono sembrare diversi dai termini classici del settore IT; tuttavia, sussistono ragioni molto precise per cui tali termini vengono inseriti in un appalto per la fornitura di servizi cloud. Qualora i termini pubblicamente disponibili non siano accettabili, i CISP spesso offrono accordi leggermente modificabili per i clienti aziendali, che sono suscettibili di analisi.

Oltre a esaminare i termini e le condizioni del CISP, è importante comprendere anche le policy, le normative e/o le leggi esistenti (ad esempio, in materia di tecnologie, classificazione dei dati, privacy, risorse umane ecc.). Spesso esistono policy, normative e leggi che sono concepite per l'acquisto e l'utilizzo delle offerte IT classiche; tuttavia, esse possono essere in contrasto con il modello del CISP. Eccone un esempio: consentire solo l'utilizzo delle tecnologie cloud incluse nell'Accordo quadro originale tramite la RDO di servizi cloud. I CISP aggiungono costantemente nuovi servizi e funzionalità. Impedire l'accesso a questi nuovi servizi semplicemente per seguire un approccio tradizionale di aggiornamento dei prodotti IT non ha alcun senso per il cliente finale. In tale eventualità, è importante svolgere dei colloqui approfonditi con i CISP, con una seria riflessione su tali policy, normative e/o leggi.

Vantaggi dei colloqui preliminari alla RDO

Come detto in precedenza, prima di redigere una RDO è necessario dedicare del tempo agli incontri con i CISP e con i rispettivi fornitori, per comprenderne i termini e le condizioni, e per sensibilizzarli circa l'approccio dell'ente, le policy, le normative e le leggi vigenti. L'aspetto principale di questi colloqui è assicurare che entrambe le parti comprendano il "motivo" alla base del funzionamento dei termini rilevanti. Ad esempio, i termini e le condizioni dei servizi cloud differiscono dai termini applicati ai tradizionali data center, servizi gestiti, hardware, software pacchettizzati e sistemi integrati. Poiché si tratta di modelli unici, che comportano un'innovazione costante, i rispettivi modelli aziendali richiedono una procedura della RDO sufficientemente flessibile da consentire trattative o colloqui di chiarimento.

Grazie alla possibilità di chiarire i termini e le condizioni nel corso di colloqui o trattative, gli enti pubblici acquisiscono una maggiore conoscenza dei modelli cloud ed evitano il problema di escludere fornitori che, di fatto, potrebbero essere in grado di soddisfare le loro esigenze. Un modo di procedere tipico dell'ente è quello di individuare in anticipo determinati termini che l'ente

medesimo è disposto a discutere e negoziare prima dell'aggiudicazione. Negoziando in anticipo con gli offerenti, l'ente avrà la certezza di ottenere i termini di aggiudicazione più idonei e potrà risolvere le eventuali difformità che, altrimenti, potrebbero portare all'esclusione di una proposta valida. Inoltre, gli enti pubblici possono rivedere le proprie policy, normative e leggi, ed entrambe le parti possono comprendere come l'uso del cloud si adatterà a tali modelli. Spesso si trova il modo di lavorare con le clausole esistenti. Se, tuttavia, emerge un'area particolarmente problematica, i due team possono collaborare per trovare una soluzione (è consigliabile svolgere questi colloqui molto prima di qualsiasi RDO o negoziazione contrattuale successiva).

Flessibilità nelle trattative

Per poter firmare i contratti in conformità alla legislazione locale, pur basandosi sulle condizioni contrattuali standard del CISP, è consigliabile (1) richiedere ai candidati il loro contratto standard, (2) non applicare condizioni contrattuali inadeguate al momento della redazione dell'Accordo quadro per la RDO di servizi cloud e (3) prevedere un'opzione di negoziazione su tutte le disposizioni della procedura di consultazione e sulle proposte che daranno luogo all'Accordo quadro (ad eccezione, ovviamente, delle clausole obbligatorie previste dalla legge).

Nota: l'ambito della responsabilità condivisa è insito nel modello cloud e deve riflettersi nei termini del contratto. Ad esempio, il CISP conferma che i clienti sono proprietari dei loro dati e che esercitano pieno controllo sul luogo in cui gli stessi risiedono; il CISP mette a disposizione gli strumenti per garantire che la scelta delle ubicazioni dei dati sia limitata. TUTTAVIA, l'uso di tali strumenti è responsabilità del cliente o del partner.

È importante che vi siano delle ***serie distinte di termini e condizioni*** *del contratto per ognuno dei LOTTI indicati in un Accordo quadro per il cloud. L'adozione di un unico approccio indifferenziato per appaltare tutti i LOTTI potrebbe infatti causare problemi di fattibilità e compatibilità tecnica.*

Come già osservato, le RDO che contemplano termini vincolanti non negoziabili costituiscono essenzialmente una proposta "prendere o lasciare" per i fornitori, che può determinare l'esclusione di una proposta altrimenti accettabile. Gli enti pubblici devono considerare attentamente le conseguenze derivanti dall'uso di termini vincolanti, tranne quando si tratta di un obbligo di legge. Gli enti devono essere certi della reale necessità di applicare un requisito o un termine vincolante, dal momento che le trattative future saranno inibite da tale natura vincolante. L'uso di requisiti o termini vincolanti deve essere ridotto al minimo, affinché l'ente possa godere della flessibilità necessaria per acquisire la tecnologia migliore e la soluzione più idonea.

Le tecnologie cloud del CISP sono, peraltro, completamente standardizzate e vengono fornite in modo completamente automatizzato. Il CISP non è dunque in grado di apportare alcuna modifica ai termini e alle condizioni, qualora questa imponga una personalizzazione del servizio sottostante. Inoltre, i prezzi dei servizi sono generalmente pubblici e standardizzati per tutti gli utenti; di conseguenza, il CISP non è in condizione di adeguarli per poter assorbire il maggiore rischio per conto di un particolare cliente.

Acquisti indiretti

Un'alternativa all'acquisto delle tecnologie cloud direttamente dal CISP consiste nell'acquisto tramite un rivenditore del CISP. Per ulteriori informazioni sui rivenditori del CISP, vedere il paragrafo ***2.1.3*** precedente.

Testo di esempio di una RDO: termini e condizioni

I CISP o i rivenditori autorizzati devono indicare i termini e le condizioni applicate al pubblico e devono fornire un feedback sui termini e sulle condizioni applicate in generale dall'<ENTE>.

L'<ENTE> intende stipulare un contratto scritto con l'aggiudicatario in base ai termini contrattuali di quest'ultimo. L'offerente deve sottoporre alla valutazione dell'<ENTE> una serie di termini contrattuali, che rappresentano la migliore offerta sotto il profilo commerciale e legale. Gli offerenti e l'<ENTE> possono discutere entrambe le proposte (termini e condizioni) durante la fase di <DISCUSSIONE/TRATTATIVA>.

- *I termini principali dell'Accordo quadro a livello generale dovrebbero consistere, al massimo, nei seguenti elementi:*
  - *Durata dell'Accordo quadro*
  - *Governance dell'Accordo quadro*
  - *Prestazioni dell'Accordo quadro*
  - *Risoluzione (termination) dell'Accordo quadro*
  - *Ambito di applicazione dell'Accordo quadro*
  - *Procedura di ordinazione*
  - *Disposizioni riguardanti la riservatezza*
  - *IP e informazioni specifiche per categoria*
  - *Requisiti tecnici minimi che i CISP devono soddisfare, ad esempio standard di qualità, accreditamento, sicurezza e protezione dei dati.*
- *I termini saranno diversi per ciascun lotto dell'Accordo quadro*
- *Le specifiche dei servizi del CISP possono essere prese in considerazione e saranno esaminate al momento dell'ordine a chiamata.*
- *Consentire modifiche contrattuali: i termini non devono costringere i clienti e i fornitori a concordare modifiche contrattuali per aggiungere nuovi servizi o miglioramenti. I servizi cloud si evolvono così rapidamente che i miglioramenti ai servizi avvengono in forma costante, con vantaggi per l'efficienza dei clienti.*
- *Gli Accordi sul Livello di Servizio (SLA) non dovrebbero essere definiti dal cliente. I termini del cliente non dovrebbero definire accordi SLA specifici e personalizzati, che differiscono dai modelli standard di fornitura dei servizi del CISP. Grazie agli accordi SLA standard dei CISP, questi ultimi potranno mantenere bassi i costi, trasferirli ai clienti e, al tempo stesso, rassicurarli sul fatto che i CISP potranno onorare l'accordo SLA.*
- *I massimali di responsabilità devono essere proporzionati. La responsabilità deve essere proporzionata ai servizi acquistati e i massimali di responsabilità non devono essere eccessivamente elevati. Un massimale eccessivamente elevato costituirebbe un disincentivo per i CISP ad accettare progetti di valore modesto. Questi progetti sono spesso utili per avviare una collaborazione e rappresentano una sorta di "test" con cui i clienti valutano se determinate soluzioni cloud sono valide per il proprio ente.*
- *I clienti devono essere proprietari dei loro dati. I clienti devono controllare e possedere i propri dati e avere la possibilità di decidere il luogo geografico in cui gli stessi saranno conservati. In questo modo, i clienti potranno evitare il "vendor lock-in" e potranno trasferire liberamente i dati a nuovi fornitori.*

2.5.2 Termini e condizioni del software

Sebbene il presente manuale si concentri sull'acquisto di tecnologie cloud IaaS e PaaS fornite da un CISP, è importante evidenziare i termini e le condizioni del software che gli enti pubblici possono prendere in considerazione quando acquistano software dai fornitori. Fare riferimento alla Figura 1 (Pagina 5) per esaminare le modalità di acquisto del software nell'ambito di una RDO di servizi cloud ben strutturata.

Il software svolge un ruolo fondamentale in quasi tutte le aziende, compreso il settore pubblico. L'introduzione di obblighi, quali i termini e le condizioni di licenza del software in una RDO di servizi cloud, aiuta a garantire che gli enti pubblici ottengano il valore migliore e abbiano la libertà di scegliere i fornitori al momento dell'acquisto di software.

Per ulteriori informazioni, consultare i Dieci Principi per una gestione delle licenze software equa e corretta per gli utenti del cloud[9]. I Principi sono stati sviluppati da Cigref[10], un'associazione di grandi aziende ed enti pubblici francesi che rappresentano gli utenti della tecnologia digitale, in collaborazione con il CISPE e con il supporto di altre associazioni di categoria europee di CIO e fornitori, al fine di affrontare pratiche che entrambe le associazioni considerano dannose per la trasformazione digitale delle organizzazioni di tutte le dimensioni nel rispettivo percorso verso il cloud.

Testo di esempio di una RDO: software

*L'<**ENTE**> intende stipulare un contratto scritto con l'aggiudicatario in base ai termini contrattuali di quest'ultimo. L'offerente deve sottoporre alla valutazione dell'<**ENTE**> una serie di termini contrattuali, che rappresentano la migliore offerta sotto il profilo commerciale e legale. I fornitori di software e l'<ENTE> possono discutere entrambe le proposte (termini e condizioni) durante la fase di <DISCUSSIONE/TRATTATIVA>.*

***Requisito 1.0.** I fornitori di software devono fornire termini di licenza chiari, inclusa una ripartizione dei costi sia a livello granulare sia di riepilogo.* ***Requisito 1.1.** Tutti gli addebiti relativi all'eventuale mancato rispetto dei termini di licenza devono essere forniti sia a livello granulare sia di riepilogo.*
***Requisito 2.0.** Le licenze software devono fornire all'<Ente> la possibilità di migrare il software con licenza dall'ambiente on-premise al cloud di propria scelta, senza l'obbligo di acquistare licenze duplicate separate per lo stesso software.* ***Requisito 2.1.** Le licenze software non devono prevedere restrizioni delle condizioni di licenza e costi maggiori che limitino la capacità dell'<Ente> di eseguire il software ricevuto in licenza nel cloud di propria scelta.*
***Requisito 3.0.** Le licenze software devono consentire all'<Ente> di eseguire il software con licenza sul proprio hardware (in genere denominato software "on-premise") e sul cloud di propria scelta.*
***Requisito 4.0.** Le licenze software non devono imporre che il software con licenza venga eseguito solo su hardware dedicato esclusivamente all'<Ente>.*

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Requisito 5.0. *I fornitori di software non devono penalizzare l'<Ente> se il software con licenza dei fornitori viene utilizzato su un'offerta cloud di un altro fornitore, ad esempio includendo il diritto di intraprendere controlli software maggiori o intrusivi o di imporre tariffe di licenza software più elevate.*
Requisito 6.0. *Il software di directory deve supportare standard aperti per la sincronizzazione e l'autenticazione delle identità degli utenti, in modo non discriminatorio verso altri servizi di identificazione.*
Requisito 7.0. *I fornitori di software non devono addebitare prezzi diversi per lo stesso software in base esclusivamente a chi possiede l'hardware su cui detto software è installato.* ***Requisito 7.1.*** *I prezzi del software non devono fare differenze tra il software installato nel data center dell'<Ente>, in un data center gestito da una terza parte, su computer noleggiati da terzi o nell'infrastruttura del fornitore di servizi cloud scelto dall'<Ente>.*
Requisito 8.0. *Durante il periodo di validità del contratto, i fornitori di software non devono apportare modifiche sostanziali ai termini di licenza che limitano gli usi consentiti all'<Ente> in precedenza, tranne laddove richiesto dalla legge o per motivi di sicurezza.*
Requisito 9.0. *I fornitori di software non devono fuorviare l'<Ente> dichiarando che le licenze software copriranno l'utilizzo previsto del software da parte dell'<Ente>, come indicato dai <Requisiti dell'ente>, qualora la copertura di tale utilizzo richieda l'acquisto di licenze aggiuntive.*
Requisito 10.0. *Laddove l'<Ente> ha il diritto di rivendere e trasferire licenze software, i fornitori di software devono continuare a offrire supporto e patch a condizioni eque all'<Ente> che ha legalmente acquisito una licenza rivenduta.*

2.5.3 Come scegliere l'assegnatario migliore in base a un progetto

Gli enti pubblici che sono parte dell'accordo quadro possono ricorrere a un "ordine a chiamata" per i servizi di cui hanno bisogno, al momento opportuno. Inserendo un ordine a chiamata nell'ambito dell'Accordo quadro, gli acquirenti possono correggere o aggiungere dei requisiti tecnici relativi all'ordine a chiamata specifico, senza rinunciare ai vantaggi offerti dall'Accordo quadro.

Se necessario, è possibile indire una mini-gara per individuare il fornitore migliore per un determinato carico di lavoro o progetto. Si parla di mini-gara quando un cliente aumenta il livello della concorrenza nell'ambito dell'Accordo quadro, invitando tutti i fornitori di un determinato lotto a rispondere a una serie di requisiti. Il cliente invita tutti i fornitori qualificati del lotto a presentare un'offerta. Per tale ragione, è importante che gli aggiudicatari di una RDO di servizi cloud siano in possesso dei requisiti minimi: ciò garantisce uno standard elevato di opzioni nell'ambito di ciascun lotto.

Come già detto, è importante che vi siano serie distinte di termini e condizioni del contratto per ciascuna categoria di lotto in base al tipo di offerta (ad esempio, soluzione IaaS/PaaS pubblica, comunitaria o privata), in quanto l'adozione di un unico approccio indifferenziato per appaltare tutti i lotti potrebbe causare problemi di fattibilità e compatibilità tecnica.

Per quanto riguarda la selezione degli aggiudicatari, vedere il testo di esempio di una RDO nel paragrafo ***2.1.4***.

2.5.4 Onboarding e offboarding

Una considerazione da tenere presente quando si predispone un Accordo quadro per il cloud è la possibilità di adottare un sistema dinamico di acquisto (Dynamic Purchasing System, DPS). In un modello DPS tutti i fornitori che soddisfano i requisiti minimi dell'Accordo quadro saranno ammessi all'Accordo quadro. Non c'è un limite specifico al numero di fornitori che possono aderire all'Accordo quadro e, a differenza del modello tradizionale di accordo quadro, i fornitori possono anche chiedere di aderire all'Accordo quadro DPS in qualsiasi fase del suo ciclo di vita.

Suggeriamo vivamente agli enti pubblici di fissare standard elevati per assicurarsi la qualità e la garanzia del servizio da parte di fornitori qualificati, ma di non utilizzare termini troppo specifici che potrebbero escludere eventuali CISP senza consentire un'equa concorrenza In ultima analisi, l'obiettivo è quello di evitare di saturare l'utente finale con un numero eccessivo di opzioni, contestualmente mantenendo alto lo standard delle tecnologie cloud offerte.

3.0 Best Practice/Lezioni apprese

Di seguito si riportano alcune lezioni apprese circa la realizzazione di un Accordo quadro per il cloud efficace mediante una RDO di servizi cloud ben strutturata.

3.1 Governance del cloud

La governance del cloud è una responsabilità condivisa. I CISP forniscono funzionalità e servizi per l'integrazione della governance del cloud in ogni aspetto di un ambiente cloud; i clienti portano i propri standard di governance esistenti e apprendono il modo in cui il cloud favorisce la governance del cloud.

Nel cloud i clienti hanno la possibilità di creare l'ambiente IT desiderato, anziché limitarsi alla gestione dell'ambiente esistente. Il cloud permette ai clienti di: (1) iniziare con un inventario completo di tutte le risorse IT; (2) gestire tutte queste risorse centralmente e (3) predisporre un meccanismo di avvisi su utilizzo/fatturazione/sicurezza, ecc. Tutti questi essenziali vantaggi del cloud permettono ai clienti di godere di un'architettura ottimizzata e quanto più automatizzata possibile, senza la necessità di acquistare e installare continuamente nuovo hardware. Ciò è reso possibile dal CISP, che consente ai clienti di spostare l'attenzione da una gestione indifferenziata dell'infrastruttura al livello operativo di tipo mission-critical.

Il cloud del CISP può essere considerato, a tutti gli effetti, come un'API di dimensioni molto grandi. Che si tratti di lanciare un nuovo server o modificare un'impostazione di sicurezza, all'atto pratico l'utente effettua delle chiamate API. Ogni modifica all'ambiente viene registrata, ovvero vengono registrati il "chi", "cosa", "dove" e "quando" di ogni modifica. Si ottengono così la governance, il controllo e la visibilità del cloud che solo un ambiente cloud può offrire. Ciò consente ai clienti di ripensare ai propri modelli di governance IT esistenti e di decidere come migliorarli o snellirli sfruttando i vantaggi offerti dal cloud.

Governance del cloud significa anche comunicare e incorporare i cambiamenti positivi nei processi e le nuove competenze derivanti dal cloud. Ad esempio, i project manager sono abituati ad attendere mesi per la realizzazione di un ambiente IT. Pertanto, potrebbero essere indotti a sovrastimare i tempi necessari per realizzare un ambiente di sviluppo o di test nel cloud (operazione che nel cloud richiede letteralmente pochi minuti). L'adattamento a questa ritrovata agilità è un

percorso progressivo che si concretizza attraverso una serie di programmi. È importante condividere le lezioni apprese per favorire l'evoluzione costante dell'Accordo quadro per il cloud, facendo sì che i requisiti siano in linea con i nuovi processi e con livelli più elevati di agilità.

3.2 Budget per il cloud

Quando si tratta di strutturare i prezzi dei servizi cloud in base al consumo e di adattarli ai requisiti di acquisto e budget del settore pubblico, ci siamo resi conto che è utile raggruppare i servizi del CISP sotto un'unica voce (calcolo, archiviazione, reti, database, IoT ecc.), tutti all'interno della voce Tecnologie cloud. Questo approccio assicura la flessibilità necessaria per proporre in tempo reale agli utenti tutte le tecnologie dei CISP nuove ed esistenti; tale approccio assicura agli utenti l'accesso rapido alle risorse necessarie quando ne hanno bisogno. Inoltre, risponde alle fluttuazioni della domanda assicurando un utilizzo ottimizzato e costi bassi.

Gli enti pubblici possono aggiungere eventuali voci aggiuntive di altri lotti agli ordini in un Accordo quadro per il cloud, qualora abbiano bisogno di servizi gestiti o servizi di consulenza/professionali, software da un marketplace, servizi di supporto cloud e formazione sulle offerte del CISP.

È possibile offrire ulteriore flessibilità contrattuale inserendo voci opzionali nel contratto, all'interno delle categorie di risorse appropriate, per incentivare un'eventuale crescita futura. In alternativa, se un ente volesse raggruppare le tecnologie cloud con i servizi gestiti/di consulenza/professionali sotto un'unica voce, potrebbe farlo aggiungendo una voce e chiamandola, ad esempio, "Tecnologie cloud e servizi ancillari".

Di seguito si riporta un esempio di tale approccio. Nell'esempio che segue, ogni unità nella voce n° 1001 - Tecnologie cloud corrisponde a 1,00 EUR di "Tecnologie cloud" utilizzate. Ogni mese è possibile finanziare gli incrementi degli ordini sulla base delle proiezioni di utilizzo correnti e previste.

Tabella 3. Esempio di struttura dei prezzi a voci singole.

N° VOCE	FORNITURE/SERVIZI	QUANTITÀ	UNITÀ	PREZZO UNITARIO	IMPORTO
1001	Tecnologie cloud	1.000	Cad.	1,00 EUR	1.000 EUR
1002	Servizi di consulenza	1	A settimana	3.000 EUR	3.000 EUR
1003	Supporto cloud	1	Al mese	1.000 EUR	1.000 EUR
1004	Formazione sul cloud	1	Al giorno	3,00 EUR	3.000 EUR
1005	Marketplace per cloud	10	Cad.	10 EUR	100 EUR

Ecco un esempio di come funziona questa struttura: un ente pubblico consulta un CISP per ottenere una stima della quantità di servizi di tecnologia cloud che l'ente utilizzerà. L'ente concorda con il fornitore dei termini per un totale di 10 milioni di EUR per 5 anni, ovvero 2 milioni di EUR all'anno. L'ente stanzia l'importo annuale iniziale di 2 milioni di EUR. Ogni mese viene emessa una fattura e il denaro viene prelevato dal fondo per effettuare il pagamento. Viene eseguito un prelievo da quel conto. Il tasso di consumo della liquidità (burn rate) dei fondi rimanenti viene tenuto sotto controllo tramite gli strumenti di monitoraggio e previsione del CISP. Se il livello dei fondi rimanenti cala troppo, l'ente richiede un ulteriore finanziamento al CFO, che può assumersi l'impegno a garantire i servizi.

Testo di esempio di una RDO: determinazione del prezzo - appalti

TERMINI DI PAGAMENTO
*I termini di pagamento devono essere strutturati in modo tale per cui l'**<ENTE>** paga solo le risorse effettivamente utilizzate, come illustrato di seguito:*

1. *Pagamento mensile basato sull'effettivo uso/consumo dei servizi e secondo i prezzi al pubblico dei CISP.*

GARANZIA MINIMA E SPESA MASSIMA
*Poiché l'**<ENTE>** non può stabilire esattamente il volume di risorse di uno specifico fornitore di servizi cloud che sarà consumato in un dato periodo di tempo, gli ordini dovranno indicare le quantità unitarie a prezzo fisso per una singola voce denominata "Tecnologie cloud".*

*Ciascuna unità della voce ordinata equivarrà a **<1,00 EUR>** di Tecnologie cloud ordinate. Gli ordini incrementali saranno inseriti periodicamente tramite una modifica al suddetto ordine in svariate quantità, così da offrire all'**<ENTE>** la flessibilità di pre-ordinare svariati "importi in euro" di Tecnologie cloud del CISP sulla base dell'utilizzo stimato per fabbisogni di diversa durata. L'**<ENTE>** effettuerà pre-ordini periodici delle quantità per importi sufficienti a coprire il costo stimato delle Tecnologie cloud che saranno utilizzate per soddisfare una varietà di fabbisogni.*

N° voce	Descrizione	Quantità	Unità	Prezzo
01	Tecnologie cloud del CISP	1.000	Singola (unità)	1.000,00 EUR

ORDINE MINIMO/ORDINE INCREMENTALE
*Gli ordini di svariate quantità di <10.000> unità per voce saranno inviati periodicamente in base all'utilizzo stimato delle Tecnologie cloud da parte dell'**<ENTE>**. Tale accordo offrirà all'**<ENTE>** la flessibilità di effettuare pre-ordini di **<10.000>** unità di "Tecnologie cloud", secondo necessità, per supportare le operazioni e per attenersi alle pratiche commerciali del cloud computing basate sul pagamento a consumo.*

*Un incremento iniziale di **<100.000>** unità al costo di **<100.000 EUR>** verrà commissionato al momento dell'ordine a chiamata. **<x>** è il numero minimo di unità totali di voci che possono essere inserite in un singolo ordine incrementale comprendente una o più voci. Il numero massimo di unità che possono essere ordinate nell'ambito dell'ordine di consegna non può essere superiore a **<x>** ; tuttavia, tale numero non può mai superare il valore dell'ordine a chiamata sommato a tutte le unità ordinate in precedenza. L'**<ENTE>** ha la responsabilità di assicurare che tutti gli ordini rientrino nei limiti specificati nel presente paragrafo.*

ORDINE MASSIMO
*Il valore massimo totale dell'ordine è **<x>**, pari a **<x>** unità di una singola voce al prezzo di **<x>** per unità. Il valore si basa su una stima del fabbisogno dell'**<ENTE>** nel periodo della fornitura; tuttavia, esso non è garantito.*

3.3 Comprendere il modello di business dei partner

Gli enti pubblici dovrebbero cercare di comprendere i modelli sulla base dei quali i CISP erogano le proprie offerte. Dovrebbero, altresì, riconoscere il ruolo fondamentale svolto dai partner che forniscono consulenza, servizi gestiti, rivendita e molto altro. Molti clienti necessitano di un fornitore di servizi cloud per la propria infrastruttura ed esternalizzano le attività concrete ("hands on keyboard") di pianificazione, migrazione e gestione a un integratore di sistemi (SI) o a un

fornitore di servizi gestiti (MSP). Data la varietà di servizi offerti, alcuni requisiti potrebbero non essere applicabili ai fornitori di servizi cloud, ad esempio le clausole "a cascata" (flow-down clauses) per i subappaltatori.

Queste clausole "a cascata" sono esemplificative per illustrare quanto sia importante capire il modo in cui i partner e i rivenditori operano rispetto ai CISP. In alcuni tipologie di appalto, infatti, sono previste delle clausole che impongono al primo contraente di predisporre a cascata determinate clausole vincolanti per tutti i suoi partner o subappaltatori. Di norma, i CISP non proporranno partner subappaltatori formali, né si proporranno in qualità di partner subappaltatori formali. Infatti, i CISP offrono un servizio standardizzato su vasta scala che non è concepito per soddisfare le esigenze specifiche di un particolare cliente finale (inclusi i clienti del settore pubblico ai sensi di un contratto pubblico). In un modello di appalto indiretto (acquisizione di servizi cloud tramite un rivenditore del CISP), il CISP potrebbe rifiutare tali clausole del suo rivenditore, in quanto non applicabili a un fornitore di servizi commerciali di "2° livello". In questo caso, l'attività oggetto del contratto non viene svolta in prima persona dal CISP, ma, piuttosto, da un partner che utilizza l'infrastruttura CISP a tale scopo. Il CISP è quindi un fornitore commerciale (non un subappaltatore) rispetto alle attività di un partner. In un modello di appalto diretto (acquisto di servizi di cloud direttamente dal CISP), il CISP di norma rifiuterebbe queste clausole "vincolanti" che sono appropriate nel caso di un tipico subappaltatore di beni, a causa della natura commerciale dei servizi oggetto dell'appalto e del fatto che la maggior parte dei CISP non si avvale di subappaltatori per fornire i propri servizi commerciali.

3.4 Cloud broker

Il concetto di cloud broker come strumento per ridurre la possibilità di "vendor lock-in" può essere problematico. Sebbene, in teoria, un cloud broker possa sembrare un'idea valida, nella pratica probabilmente creerebbe più complessità e confusione che valore effettivo.

Il tentativo di strutturare applicazioni che funzionano in più servizi cloud contemporaneamente o in modo intercambiabile provoca – inevitabilmente – dei compromessi sul piano della capacità (**non esiste la bacchetta magica per il cloud**). In ultima analisi, un approccio simile può aggiungere un inutile livello di complessità tra i clienti del settore pubblico e i rispettivi servizi cloud, tale da compromettere l'efficienza e i benefici perseguiti sul piano della sicurezza, con la conseguente perdita di scalabilità e agilità, l'aumento dei costi e il rallentamento dell'innovazione.

3.5 Approvvigionamento/ricerca di mercato antecedente la RDO

Quando un ente pubblico pianifica una RDO di servizi cloud, dovrebbe cercare di coinvolgere tutti i soggetti interessati all'interno dell'ente (dirigenti, parti interessate aziendali, area tecnologica, finanziaria, appalti, ufficio legale e contratti) fin dall'inizio del processo. In questo modo, tutte le parti interessate possono farsi un'idea del modello cloud e, di conseguenza, assumere un approccio consapevole nel rivedere i tradizionali metodi di gestione degli acquisti IT.

Per quanto riguarda il dialogo con gli operatori del settore, raccomandiamo vivamente agli enti pubblici di prendersi il tempo necessario per fissare colloqui approfonditi e raccogliere feedback da CISP, partner dei CISP, fornitori di marketplace PaaS/SaaS ed esperti del settore. Un esempio di tali dialoghi potrebbero essere gli incontri di settore o i seminari sulla sicurezza e sugli appalti. Un altro modo efficace per comprendere approfonditamente gli appalti cloud consiste nel pubblicare una

richiesta di informazioni (RFI) o, idealmente, una bozza della richiesta di offerta (RDO). Spesso questi documenti contengono potenziali problemi che possono essere identificati, discussi e corretti prima della pubblicazione della RDO di servizi cloud definitiva.

3.6 Sostenibilità

La sostenibilità è inerente al cloud computing: il passaggio al cloud produce un aumento dell'efficienza energetica rispetto ai server on-premise o ai data center aziendali. L'individuazione di un CISP che dà priorità alla sostenibilità e che si è impegnato pubblicamente a raggiungere tali obiettivi rappresenta un'ulteriore garanzia della sostenibilità del cloud. I CISP e i gestori europei di data center (con il supporto della Commissione europea) hanno creato il Patto per la neutralità climatica dei data center[11]. Si tratta di un'iniziativa di autoregolamentazione volta a stabilire criteri di sostenibilità chiari, semplici e di vasta portata per il settore dei data center; l'iniziativa intende, altresì, garantire che i gestori di data center e i fornitori di servizi cloud siano neutri dal punto di vista climatico entro il 2030. L'iniziativa di autoregolamentazione include obiettivi chiari, riguardanti l'efficienza energetica dei data center, il risparmio idrico, il riutilizzo e la riparazione dei server e l'uso di energia priva di emissioni di carbonio per alimentare i data center. I CISP che aderiscono all'iniziativa di autoregolamentazione si impegnano a raggiungere tali obiettivi e a rispettare i criteri validi per la certificazione di gestore neutro dal punto di vista climatico.

Una RDO di servizi cloud dovrebbe chiedere ai CISP se si sono impegnati a rispettare tali criteri, chiedendo, in particolare, se hanno sottoscritto l'autoregolamentazione e quando hanno assunto tale impegno.

Testo di esempio di una RDO: sostenibilità

Il CISP si è impegnato a gestire data center neutri dal punto di vista climatico aderendo all'Iniziativa di autoregolamentazione per la neutralità climatica dei data center? In caso affermativo, quando ha sottoscritto tale iniziativa di autoregolamentazione?

È possibile certificare la propria adesione in qualità di firmatario del Patto per la neutralità climatica dei data center?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

Appendice A - Requisiti tecnici per il confronto tra offerenti

Di seguito sono elencati alcuni requisiti generici della tecnologia cloud che potrebbero essere utilizzati per confrontare i CISP in occasione degli ordini a chiamata o delle mini-gare nell'ambito di un Accordo quadro per il cloud.

1. Profilo del fornitore di servizi cloud

	Requisito
1.	*ESPERIENZA SUL MERCATO:* *Da quanti anni il fornitore di servizi cloud opera nel segmento di mercato dei servizi cloud?*
2.	*DIVULGAZIONE E PROTEZIONE DEI DATI:* *Il fornitore di servizi cloud aderisce ai codici di condotta del settore riguardanti la protezione dei dati o la reversibilità? Il fornitore di servizi cloud aderisce ai principi di sviluppo open source e open API?*

2. Infrastruttura globale

	Requisito
1.	*PORTATA GLOBALE:* *Il fornitore di servizi cloud offre un'infrastruttura globale per fornire agli utenti bassa latenza e velocità effettiva elevata?*
2.	*REGIONI:* *Il fornitore di servizi cloud è presente nelle regioni delle aree geografiche richieste?*
3.	*DOMINI/ZONE:* *Il fornitore di servizi cloud adotta il principio di domini o zone, in base al quale più data center sono raggruppati attraverso una rete a bassa latenza per fornire un livello maggiore di disponibilità elevata e tolleranza ai guasti?* • *Se sì, elencare il numero di domini o zone e il numero di data center all'interno delle aree geografiche richieste*
4.	*DISTANZA DOMINI/ZONE:* *Il fornitore di servizi cloud crea i suoi domini o zone con data center fisicamente distanti per supportare ridondanza, disponibilità elevata e latenza ridotta?*
5.	*DATA CENTER CREATI:* *Il fornitore di servizi cloud offre data center progettati in modo che siano isolati dai guasti che si verificano in altri data center, con alimentazione, raffreddamento e reti ridondanti?*
6.	*REPLICA DEI DATA CENTER:* *Il fornitore di servizi cloud fornisce repliche dei dati nei data center all'interno di un dominio o di una zona con failover automatico?*
7.	*REPLICA DI DOMINIO/ZONA:* *Il fornitore di servizi cloud offre repliche dei dati nei domini o nelle zone all'interno di una regione?*

3. Infrastruttura

3.1 Calcolo

	Requisito
1.	*CALCOLO - ISTANZA ORDINARIA - SCOPO GENERICO:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *A scopo generico: ottimizzata per applicazioni generiche, con un giusto equilibrio tra capacità di calcolo, memoria e risorse di rete.* o *Se sì, qual è l'istanza di maggiori dimensioni?*
2.	*CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER LA MEMORIA:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Con ottimizzazione per la memoria: ottimizzata per le applicazioni a uso intensivo della memoria.* o *Se sì, qual è l'istanza di maggiori dimensioni?*
3.	*CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER IL CALCOLO:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Con ottimizzazione per il calcolo: ottimizzata per le applicazioni a calcolo intensivo.* o *Se sì, qual è l'istanza di maggiori dimensioni?*
4.	*CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER L'ARCHIVIAZIONE:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Con ottimizzazione per l'archiviazione: offre un'elevata quantità di capacità di archiviazione locale.* o *Se sì, qual è la capacità di archiviazione massima (ovvero 5, 10, 20, 50 TB) e il numero massimo di dischi (HDD/SSD) di cui è possibile effettuare il provisioning e che possono essere aggiunti a un'istanza?*
5.	*CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER LA GRAFICA:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Grafica a basso costo: offre accelerazione grafica a basso costo per le istanze di calcolo.* o *Se sì, qual è l'istanza di maggiori dimensioni?*
6.	*CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER GPU:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *GPU: offre delle GPU (Graphics Processing Unit) hardware per le applicazioni che fanno uso intensivo di grafica.* o *Se sì, quali modelli e quante GPU il fornitore di servizi cloud è in grado di offrire per istanza?*
7.	*CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER FPGA:* *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *FPGA: fornisce dei Field Programmable Gate Array (FPGA) per lo sviluppo e l'implementazione dell'accelerazione hardware personalizzata per le applicazioni.* o *Se sì, quanti FPGA il fornitore di servizi cloud è in grado di offrire per ciascuna istanza?*
8.	*CALCOLO - ISTANZE ESPANDIBILI:*

	Il fornitore di servizi cloud offre istanze espandibili in grado di fornire un livello base di prestazioni dell'unità di elaborazione centrale (CPU) con la possibilità di espandersi oltre tale livello base? • *Se sì, qual è l'istanza ottimizzabile di maggiori dimensioni?*
9.	*CALCOLO - ISTANZE A USO INTENSIVO DI IO:* *Il fornitore di servizi cloud offre istanze che utilizzano unità a stato solido (SSD) di Non-Volatile Memory Express (NVMe) ottimizzate per latenza ridotta, prestazioni I/O casuali molto elevate e velocità effettiva di lettura sequenziale elevata?* • *Se sì, qual è la capacità massima di operazioni di input/output al secondo (IOPS) dell'istanza di maggiori dimensioni?*
10.	*CALCOLO - ARCHIVIAZIONE LOCALE TEMPORANEA:* *Il fornitore di servizi cloud supporta l'archiviazione locale per le istanze di calcolo da utilizzare per l'archiviazione temporanea delle informazioni modificate di frequente?*
11.	*CALCOLO - SUPPORTO DI PIÙ NIC:* *Il fornitore di servizi cloud supporta più schede di interfaccia di rete (NIC), principali e aggiuntive, da allocare per un'istanza specifica?* • *Se sì, qual è il numero massimo di NIC per istanza?*
12.	*CALCOLO - AFFINITÀ ISTANZA:* *Il fornitore di servizi cloud offre agli utenti la possibilità di raggruppare in maniera logica le istanze all'interno dello stesso data center?*
13.	*CALCOLO - ANTI-AFFINITÀ DELLE ISTANZE:* *Il fornitore di servizi cloud offre agli utenti la possibilità di raggruppare in maniera logica le istanze e collocarle in data center diversi all'interno di una regione?*
14.	*CALCOLO - PROVISIONING SELF-SERVICE:* *Il fornitore di servizi cloud offre il provisioning self-service di più istanze contemporaneamente tramite un'interfaccia programmatica, una console di gestione o un portale Web?*
15.	*CALCOLO - PERSONALIZZAZIONE:* *Il fornitore di servizi cloud offre delle istanze personalizzabili, ovvero la possibilità di modificare le impostazioni di configurazione, quali le unità centrali di elaborazione virtuali (vCPU) e la memoria RAM?*
16.	*CALCOLO - LOCAZIONE:* *Il fornitore di servizi cloud offre istanze a tenant singolo in esecuzione su hardware dedicato a un unico utente?* *• Se sì, qual è l'istanza a tenant singolo più grande disponibile?*
17.	*CALCOLO - AFFINITÀ HOST:* *Il fornitore di servizi cloud offre la possibilità di avviare un'istanza e specificare che venga sempre riavviata sullo stesso host fisico?*
18.	*CALCOLO - ANTI-AFFINITÀ HOST:* *Il fornitore di servizi cloud offre la possibilità di suddividere e ospitare specifiche istanze su diversi host fisici?*
19.	*CALCOLO - SCALABILITÀ AUTOMATICA:* *Il fornitore di servizi cloud offre la possibilità di aumentare automaticamente il numero di istanze durante i picchi di domanda per mantenere le prestazioni (ovvero la "scalabilità orizzontale")?*
20.	*CALCOLO - MECCANISMO DI IMPORTAZIONE DELLE IMMAGINI:*

	Il fornitore di servizi cloud offre agli utenti la possibilità di importare le proprie immagini esistenti e salvarle come immagini nuove e disponibili privatamente, utilizzabili per effettuare il provisioning delle istanze in futuro? • *Se sì, quali sono i formati supportati?*
21.	*CALCOLO - MECCANISMO DI ESPORTAZIONE DELLE IMMAGINI:* *Il fornitore di servizi cloud dà la possibilità di prendere un'istanza esistente in esecuzione o una copia di un'istanza e di esportarla in un formato di macchina virtuale?* • *Se sì, quali sono i formati supportati?*
22.	*CALCOLO - INTERRUZIONE DEL SERVIZIO:* *Il fornitore di servizi cloud offre meccanismi per evitare interruzioni di istanze o tempi di inattività durante le attività di manutenzione dell'hardware o del servizio a livello di host?*
23.	*CALCOLO - RIAVVIO DI ISTANZE:* *Il fornitore di servizi cloud offre meccanismi per riavviare automaticamente le istanze su un host integro se l'host fisico originale smette di funzionare?*
24.	*CALCOLO - NOTIFICHE:* *Qualora dovesse verificarsi un evento capace di condizionare la disponibilità continua delle risorse di calcolo, il fornitore di servizi cloud ha la capacità di notificare tale evento all'utente e l'utente può scegliere di ricevere o meno tale notifica tramite un'opzione self-service?*
25.	*CALCOLO - PIANIFICAZIONE DI EVENTI:* *Il fornitore di servizi cloud offre la capacità di pianificare eventi per le istanze dell'utente, come riavvio, interruzione, avvio o ritiro dell'istanza?*
26.	*CALCOLO - MECCANISMO DI BACKUP E RIPRISTINO:* *Il fornitore di servizi cloud offre un meccanismo di backup e ripristino integrato?*
27.	*CALCOLO - MECCANISMO DI SNAPSHOT:* *Il fornitore di servizi cloud offre un meccanismo di snapshot on demand manuale?*
28.	*CALCOLO - METADATI:* *Il fornitore di servizi cloud offre un servizio per i metadati dell'istanza che consente agli utenti di impostare coppie chiave-valore arbitrarie per l'istanza?*
29.	*CALCOLO - CHIAMATA DEI METADATI:* *Il fornitore di servizi cloud offre un servizio per i metadati dell'istanza che fornisce un'interfaccia del programma dell'applicazione (API) utilizzabile dall'istanza per avere informazioni su sé stessa?*
30.	*CALCOLO - MECCANISMO DI OFFERTA:* *Il fornitore di servizi cloud offre un meccanismo di offerta che permette di formulare un'offerta per le istanze più economiche che possono essere avviate immediatamente per ospitare carichi di lavoro non mission critical?*
31.	*CALCOLO - MECCANISMO DI PIANIFICAZIONE:* *Il fornitore di servizi cloud offre una modalità per pianificare e prenotare capacità di calcolo aggiuntive su base periodica, ovvero piano giornaliero, settimanale, mensile?*
32.	*CALCOLO - MECCANISMO DI PRENOTAZIONE:* *Il fornitore di servizi cloud offre una modalità per prenotare capacità di calcolo aggiuntive per il futuro (ad esempio, 1 anno, 2 anni, 3 anni e così via)?*

33.	*CALCOLO - SISTEMA OPERATIVO LINUX:* *Il fornitore di servizi cloud supporta le ultime due versioni supportate a lungo termine di almeno una distribuzione Linux aziendale (come Red Hat, SUSE) e una distribuzione gratuita e ampiamente diffusa di Linux (come Ubuntu, CentOS e Debian)?*
34.	*CALCOLO - SISTEMA OPERATIVO WINDOWS:* *Il fornitore di servizi cloud supporta le ultime due versioni principali di Windows Server (Windows Server 2017 e Windows Server 2016)?*
35.	*CALCOLO - PORTABILITÀ DELLE LICENZE* *Il fornitore di servizi cloud offre e supporta la portabilità delle licenze?* • *Se sì, indicare il fornitore del software e i nomi delle applicazioni software con edizioni e versioni.*
36.	*CALCOLO - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione calcolo di cui sopra?* *Esempio:* *Numero massimo di istanze per account* *Numero massimo di host dedicati per account* *Numero massimo di indirizzi IP riservati*

3.2 Reti

	Requisito
1.	*RETI - RETI VIRTUALI:* *Il fornitore di servizi cloud offre la possibilità di creare una rete virtuale logica isolata che rappresenta la rete specifica dell'azienda nel cloud?*
2.	*RETI - CONNETTIVITÀ NELLA STESSA REGIONE:* *Il fornitore di servizi cloud supporta la connessione di due reti virtuali all'interno della stessa regione per instradare il traffico tra di esse utilizzando indirizzi IP privati?*
3.	*RETI - CONNETTIVITÀ IN REGIONI DIVERSE:* *Il fornitore di servizi cloud supporta la connessione di due reti virtuali in regioni diverse per instradare il traffico tra di esse utilizzando indirizzi IP privati?*
4.	*RETI - SOTTORETE PRIVATA:* *Il fornitore di servizi cloud offre la capacità di creare reti e sottoreti virtuali (private) completamente isolate in cui è possibile effettuare il provisioning di istanze senza un indirizzo IP pubblico o routing a Internet?*
5.	*RETI - INTERVALLO DI INDIRIZZI PER LE RETI VIRTUALI:* *Il fornitore di servizi cloud supporta gli intervalli di indirizzi IP specificati nella RFC 1918, nonché i blocchi Classless Inter-Domain Routing (CIDR) instradabili pubblicamente?*
6.	*RETI - PIÙ PROTOCOLLI:* *Il fornitore di servizi cloud supporta più protocolli, tra cui TCP (Transmission Control Protocol), UDP (User Datagram Protocol) e ICMP (Internet control message Protocol)?*
7.	*RETI - ASSEGNAZIONE AUTOMATICA DEGLI INDIRIZZI IP:*

	Il fornitore di servizi cloud supporta la funzionalità di assegnazione automatica di indirizzi IP pubblici alle istanze?
8.	*RETI - INDIRIZZI IP STATICI PRENOTATI:* *Il fornitore di servizi cloud supporta gli indirizzi IP associati a un account utente, non a un'istanza specifica? L'indirizzo IP dovrebbe rimanere associato all'account fino a quando non viene rilasciato esplicitamente.*
9.	*RETI - SUPPORTO DI IPV6:* *Il fornitore di servizi cloud supporta il protocollo IP versione 6 (IPv6) a livello di gateway o di istanza e mostra questa funzionalità agli utenti?*
10.	*RETI - PIÙ INDIRIZZI IP PER CIASCUNA NIC:* *Il fornitore di servizi cloud offre la possibilità di assegnare un indirizzo IP primario e un indirizzo IP secondario a una scheda di interfaccia di rete (NIC) associata a un'istanza specifica?*
11.	*RETI - PIÙ NIC:* *Il fornitore di servizi cloud supporta la capacità di assegnare più schede di interfaccia di rete (NIC) a un'istanza specifica?*
12.	*RETI - MOBILITÀ IP E NIC:* *Il fornitore di servizi cloud supporta la capacità di spostare sia le schede di interfaccia di rete (NIC) sia gli indirizzi IP tra le istanze?*
13.	*RETI - SUPPORTO PER SR-IOV:* *Il fornitore di servizi cloud supporta funzionalità come Single Root Input/Output Virtualization (SR-IOV) per prestazioni più elevate (come pacchetti al secondo - PPS), latenza e jitter ridotti?*
14.	*RETI - FILTRO DI INGRESSO:* *Il fornitore di servizi cloud supporta l'aggiunta o l'eliminazione di regole applicabili al traffico in ingresso verso le istanze?*
15.	*RETI - FILTRO DI USCITA:* *Il fornitore di servizi cloud supporta l'aggiunta o l'eliminazione di regole applicabili al traffico in uscita dalle istanze?*
16.	*RETI - ACL:* *Il fornitore di servizi cloud fornisce liste di controllo degli accessi (ACL) per controllare il traffico in entrata e in uscita dalle sottoreti?*
17.	*RETI - SUPPORTO PER FLUSSO DI LOG:* *Il fornitore di servizi cloud offre la funzionalità di acquisizione di flussi di log di traffico della rete?*
18.	*RETI - NAT:* *Il fornitore di servizi cloud offre un servizio gestito per il gateway NAT (Network Address Translation) per abilitare le istanze di una rete privata alla connessione a Internet o ad altri servizi cloud, ma impedisce che Internet avvii una connessione a tali istanze?*
19.	*RETI - CONTROLLO DELL'ORIGINE/DELLA DESTINAZIONE:* *Il fornitore di servizi cloud è in grado di disabilitare il controllo dell'origine/della destinazione sulle schede di interfaccia di rete (NIC)?*
20.	*RETI — SUPPORTO DI VPN:* *Il fornitore di servizi cloud supporta la connettività di rete privata virtuale (VPN) tra il fornitore di servizi cloud e il data center dell'utente?*
21.	*RETI - TUNNEL VPN:*

	Il fornitore di servizi cloud supporta più connessioni di rete privata virtuale (VPN) per rete virtuale?
22.	*RETI - SUPPORTO PER VPN IPSEC:* *Il fornitore di servizi cloud consente agli utenti di accedere ai servizi cloud tramite un tunnel VPN IPsec (Internet protocol security) o un tunnel VPN SSL (Secure Sockets Layer) sulla rete Internet pubblica?*
23.	*RETI - SUPPORTO DI BGP:* *Il fornitore di servizi cloud adotta il protocollo BGP (Border Gateway Protocol) per migliorare il failover su tunnel VPN (Virtual Private Network) IPsec (Internet Protocol Security)?*
24.	*RETI - CONNETTIVITÀ DEDICATA PRIVATA:* *Il fornitore di servizi cloud offre un servizio di connettività privata e diretta tra le proprie sedi e il data center, l'ufficio o l'ambiente di co-locazione di un utente per il trasferimento di dati rapido e di volumi elevati?*
25.	*RETI - BILANCIATORE DEL CARICO FRONT-END:* *Il fornitore di servizi cloud offre un servizio di sistema di bilanciamento del carico front-end (connesso a Internet) che riceve le richieste dai client su Internet e le distribuisce tra istanze registrate con il bilanciatore del carico?*
26.	*RETI - BILANCIATORE DEL CARICO BACK-END:* *Il fornitore di servizi cloud offre un servizio di bilanciamento del carico back-end (privato) che instrada il traffico alle istanze ospitate in sottoreti private?*
27.	*RETI - BILANCIATORE DEL CARICO DI LIVELLO 7:* *Il fornitore di servizi cloud offre un servizio sistema di bilanciamento del carico di livello 7 (Hypertext Transfer Protocol – HTTP) in grado di effettuare il bilanciamento del carico del traffico di rete tra più istanze?*
28.	*RETI - BILANCIATORE DEL CARICO DI LIVELLO 4:* *Il fornitore di servizi cloud offre un servizio sistema di bilanciamento del carico di livello 4 (Transmission Control Protocol - TCP) in grado di effettuare il bilanciamento del carico del traffico di rete tra più istanze?*
29.	*RETI - AFFINITÀ DI SESSIONE PER I BILANCIATORI DEL CARICO:* *Il fornitore di servizi cloud offre un servizio di bilanciamento del carico che supporta l'affinità di sessione?*
30.	*RETI - BILANCIAMENTO DEL CARICO BASATO SU DNS:* *Il fornitore di servizi cloud offre un servizio di bilanciamento del carico in grado di effettuare il bilanciamento del traffico verso le istanze ospitate in più host che appartengono a un singolo dominio?*
31.	*RETI - REGISTRI DEL BILANCIATORE DEL CARICO:* *Il fornitore di servizi cloud offre registri che acquisiscono informazioni dettagliate su tutte le richieste inviate a un bilanciatore del carico?*
32.	*RETI - DNS:* *Il fornitore di servizi cloud offre un servizio di sistema dei nomi di dominio (DNS) altamente disponibile e scalabile?*
33.	*RETI - ROUTING DNS BASATO SULLA LATENZA:* *Il fornitore di servizi cloud offre un servizio di sistema dei nomi di dominio (DNS) che supporta il routing basato sulla latenza (ossia, il servizio DNS risponde a query DNS con le risorse che forniscono la migliore latenza)?*
34.	*RETI - ROUTING DNS BASATO SU AREE GEOGRAFICHE:* *Il fornitore di servizi cloud offre un servizio di sistema dei nomi di dominio (DNS) che supporta il routing basato su aree geografiche (ovvero il servizio DNS risponde alle query DNS in base alla posizione geografica degli utenti)?*
35.	*RETI - ROUTING DNS BASATO SU FAILOVER:*

	Il fornitore di servizi cloud offre un servizio di sistema dei nomi di dominio (DNS) che supporta il routing basato su failover (ovvero il servizio DNS instrada le query DNS a una risorsa attualmente attiva, mentre una seconda risorsa attende e diventa attiva solo in caso di problemi con la risorsa principale)?
36.	*RETI - SERVIZIO DI REGISTRAZIONE DEI DOMINI:* *Il fornitore di servizi cloud offre servizi di registrazione dei nomi dei domini (ovvero gli utenti possono cercare e registrare i nomi di dominio disponibili)?*
37.	*RETI - CONTROLLI DELL'INTEGRITÀ DNS:* *Il fornitore di servizi cloud offre un servizio di sistema dei nomi di dominio (DNS) che utilizza i controlli dell'integrità per monitorare l'integrità e le prestazioni delle risorse?*
38.	*RETI - INTEGRAZIONE DI DNS E BILANCIATORI DEL CARICO:* *Il fornitore di servizi cloud offre un servizio di sistema dei nomi di dominio (DNS) che si integra con il bilanciatore del carico del fornitore stesso?*
39.	*RETI - VISUAL EDITOR:* *Il fornitore di servizi cloud offre uno strumento che consente agli utenti di creare policy per la gestione del traffico?*
40.	*RETE DI DISTRIBUZIONE DI CONTENUTI (CDN):* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) per distribuire contenuti a bassa latenza ed elevate velocità di trasferimento dei dati?*
41.	*RETI - SCADENZA DELLA CACHE CDN:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che consente di rimuovere un oggetto dalle edge cache prima della scadenza e che include caratteristiche come l'invalidazione degli oggetti e il controllo delle versioni degli oggetti?*
42.	*RETI - ORIGINI CDN ESTERNE:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta un'origine personalizzata, ovvero un server HTTP (Hypertext Transfer Protocol)?*
43.	*RETI - OTTIMIZZAZIONE CDN:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) con controllo granulare per la configurazione di più server di origine e proprietà di caching per URL diversi?*
44.	*RETI - CDN CON LIMITAZIONE GEOGRAFICA:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta la limitazione geografica, ovvero evita che gli utenti in specifiche aree geografiche accedano ai contenuti?*
45.	*RETI - TOKEN CDN:* *Il fornitore di servizi cloud fornisce un servizio di rete di distribuzione di contenuti (CDN) che supporta gli URL firmati, i quali solitamente includono informazioni aggiuntive come l'ora/la data di scadenza per offrire agli utenti un maggiore controllo sull'accesso ai propri contenuti?*
46.	*RETI - CERTIFICATI CDN:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta i certificati Secure Sockets Layer (SSL) personalizzati per la distribuzione sicura dei contenuti su HTTPS (Hypertext Transfer Protocol Secure) dalle edge location?*
47.	*RETI - CACHE MULTILIVELLO CDN:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che adotta un approccio cache multilivello con l'uso di edge cache regionali per ridurre la latenza?*

48.	*RETI - COMPRESSIONE CDN:* *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta la compressione dei file?*
49.	*RETI - CARICAMENTI CRITTOGRAFATI CDN:* *Il fornitore di servizi cloud offre una rete di distribuzione di contenuti (CDN) che consente agli utenti di caricare in modo sicuro i propri dati sensibili in modo che tali informazioni possano essere visualizzate solo da componenti e servizi specifici nell'infrastruttura di origine dell'utente?*
50.	*RETI - ENDPOINT:* *Il servizio di rete del fornitore di servizi cloud offre agli utenti degli endpoint in grado di instradare il traffico tramite la connettività di rete interna del fornitore (ovvero tramite connettività privata) per ridurre i costi di comunicazione e migliorare la sicurezza del traffico?*
51.	*RETI - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione reti precedente?* *Esempio:* *Numero massimo di reti virtuali per account* *Dimensione massima di una rete virtuale* *Numero massimo di sottoreti per account* *Numero massimo di bilanciatori del carico per account* *Numero massimo di voci della lista di controllo degli accessi (ACL)* *Numero massimo di tunnel VPN (rete privata virtuale)* *Numero massimo di origini per distribuzione* *Numero massimo di certificati per bilanciatore del carico*

3.3 Archiviazione

	Requisito
1.	*SERVIZIO DI ARCHIVIAZIONE A BLOCCHI:* *Il fornitore di servizi cloud offre volumi di archiviazione a livello di blocchi da utilizzare per le istanze di calcolo?*
2.	*ARCHIVIAZIONE A BLOCCHI - IOPS:* *Il fornitore di servizi cloud offre la possibilità di acquistare un target di prestazioni o un livello di prestazioni esplicito su volumi di archiviazione a blocchi, ad esempio un determinato numero di operazioni di input/output al secondo (IOPS) o megabyte per secondo (MB/S) di velocità effettiva?*
3.	*ARCHIVIAZIONE A BLOCCHI - UNITÀ A STATO SOLIDO:* *Il fornitore di servizi cloud supporta dispositivi di archiviazione basati su unità a stato solido (SSD) che offrono latenze di millisecondi a una cifra?* • *Se sì, qual è il numero massimo di SSD che è possibile allegare per istanza?*
4.	*ARCHIVIAZIONE A BLOCCHI - DIMENSIONAMENTO:* *Il fornitore di servizi cloud offre agli utenti la possibilità di aumentare le dimensioni di un volume di archiviazione a blocchi esistente, senza la necessità di effettuare il provisioning di un nuovo volume e senza la necessità copiare/spostare i dati?*

5.	*ARCHIVIAZIONE A BLOCCHI - SNAPSHOT:* *Il fornitore di servizi cloud dispone di funzionalità di snapshot per il proprio servizio di archiviazione a blocchi?*
6.	*ARCHIVIAZIONE A BLOCCHI - ELIMINAZIONE DATI:* *Il fornitore di servizi cloud supporta l'eliminazione completa dei dati in modo che gli stessi non siano più leggibili o accessibili da utenti e/o terze parti non autorizzati?*
7.	*ARCHIVIAZIONE A BLOCCHI - CRITTOGRAFIA DEI DATI A RIPOSO:* *Il fornitore di servizi cloud offre la crittografia lato server dei dati a riposo per i dati archiviati su volumi e per i relativi snapshot?* • *Se sì, qual è l'algoritmo di crittografia utilizzato?*
8.	*SERVIZIO DI ARCHIVIAZIONE DI OGGETTI:* *Il fornitore di servizi cloud offre l'archiviazione di oggetti protetta, duratura e altamente scalabile per l'archiviazione e il recupero di qualsiasi quantità di dati dal Web?*
9.	*ARCHIVIAZIONE DI OGGETTI - ACCESSO NON FREQUENTE:* *Il fornitore di servizi cloud offre un livello di servizio di archiviazione a costi inferiori per l'archiviazione di oggetti e file ai quali si accede meno frequentemente?*
10.	*ARCHIVIAZIONE DI OGGETTI - DURABILITÀ INFERIORE* *Il fornitore di servizi cloud offre un livello di ridondanza ridotta, in cui un utente può archiviare oggetti non essenziali e facilmente riproducibili?*
11.	*ARCHIVIAZIONE DI OGGETTI - ACCESSO MENO FREQUENTE:* *Il fornitore di servizi cloud offre un livello per i dati a cui si accede meno frequentemente, ma che richiedono accesso rapido?*
12.	*ARCHIVIAZIONE DI OGGETTI - SUDDIVISIONE DEGLI OGGETTI IN LIVELLI:* *Il fornitore di servizi cloud offre una funzionalità di suddivisione in livelli per l'archiviazione di oggetti, ossia la possibilità di suggerire lo spostamento di un oggetto tra classi o livelli di archiviazione di oggetti in base alla relativa frequenza di accesso?*
13.	*ARCHIVIAZIONE DI OGGETTI - GESTIONE DEL CICLO DI VITA:* *Il fornitore di servizi cloud supporta la gestione del ciclo di vita degli oggetti utilizzando una configurazione del ciclo di vita che definisce il modo in cui gli oggetti vengono gestiti durante la loro vita, dalla creazione all'eliminazione?*
14.	*ARCHIVIAZIONE DI OGGETTI - GESTIONE BASATA SU POLICY:* *Il fornitore di servizi cloud offre la possibilità di creare e utilizzare policy per gestire i dati archiviati, i relativi cicli di vita e le impostazioni di suddivisione in livelli?*
15.	*ARCHIVIAZIONE DI OGGETTI - POLICY BASATE SU POSIZIONE E ORA:* *Il fornitore di servizi cloud offre agli utenti la possibilità di creare policy per limitare l'accesso ai dati in base alla posizione dell'utente e all'ora della richiesta?*
16.	*ARCHIVIAZIONE DI OGGETTI - HOSTING DI SITI WEB:* *Il fornitore di servizi cloud supporta l'hosting di siti Web statici oltre al servizio di archiviazione degli oggetti?*
17.	*ARCHIVIAZIONE DI OGGETTI - CRITTOGRAFIA DEI DATI A RIPOSO:* *Il fornitore di servizi cloud supporta la crittografia lato server (SSE) dei dati a riposo in cui il fornitore stesso gestisce le chiavi di crittografia?* • *Se sì, qual è l'algoritmo di crittografia utilizzato?*
18.	*ARCHIVIAZIONE DI OGGETTI - CRITTOGRAFIA CON CHIAVI UTENTE:*

	Il fornitore di servizi cloud offre funzionalità di crittografia lato server (SSE) utilizzando chiavi crittografiche fornite dal cliente?
19.	*ARCHIVIAZIONE DI OGGETTI - SERVIZIO GESTITO DELLE CHIAVI:* *Il fornitore di servizi cloud supporta la crittografia lato server (SSE) utilizzando un servizio di gestione delle chiavi che crea le chiavi di crittografia, definisce le policy che controllano le modalità di utilizzo consentito delle chiavi e controlla l'utilizzo delle chiavi per verificarne il corretto utilizzo?*
20.	*ARCHIVIAZIONE DI OGGETTI - CHIAVE MASTER LATO CLIENT:* *Il fornitore di servizi cloud offre agli utenti la possibilità di mantenere il controllo delle chiavi di crittografia e completare la crittografia/decrittografia di oggetti lato client?*
21.	*ARCHIVIAZIONE DI OGGETTI - COERENZA ASSOLUTA:* *Il fornitore di servizi cloud supporta la coerenza lettura dopo scrittura per le operazioni PUT dei nuovi oggetti?*
22.	*ARCHIVIAZIONE DI OGGETTI - UBICAZIONE DEI DATI:* *Il fornitore di servizi cloud offre un solido isolamento regionale affinché gli oggetti archiviati in una regione non lascino mai la medesima regione tranne quando l'utente li trasferisce esplicitamente in un'altra regione?*
23.	*ARCHIVIAZIONE DI OGGETTI - REPLICA:* *Il fornitore di servizi cloud offre una funzionalità di replica tra regioni che consente di replicare automaticamente gli oggetti tra regioni selezionate dall'utente?*
24.	*ARCHIVIAZIONE DI OGGETTI - CONTROLLO DELLE VERSIONI:* *Il fornitore di servizi cloud supporta il controllo delle versioni, ossia la capacità di archiviare e mantenere più versioni di un oggetto?*
25.	*ARCHIVIAZIONE DI OGGETTI - EVIDENZIATORE DI NON ELIMINABILITÀ:* *Il fornitore di servizi cloud consente a un utente la possibilità di contrassegnare una voce come non eliminabile?*
26.	*ARCHIVIAZIONE DI OGGETTI - ELIMINAZIONE CON MFA:* *Il fornitore di servizi cloud supporta l'autenticazione a più fattori (MFA) per le operazioni di eliminazione quale opzione di sicurezza aggiuntiva?*
27.	*ARCHIVIAZIONE DI OGGETTI - CARICAMENTO IN PIÙ PARTI:* *Il fornitore di servizi cloud consente il caricamento di un oggetto come un insieme di parti, in cui ciascuna parte è una porzione adiacente dei dati dell'oggetto e tali parti degli oggetti possono essere caricate singolarmente e in qualsiasi ordine?*
28.	*ARCHIVIAZIONE DI OGGETTI - TAG:* *Il fornitore di servizi cloud offre la possibilità di creare e associare tag modificabili e dinamici a livello di oggetto?*
29.	*ARCHIVIAZIONE DI OGGETTI - NOTIFICHE:* *Il fornitore di servizi cloud offre la possibilità di inviare notifiche in occasione di determinati eventi a livello di oggetto (ovvero operazioni di aggiunta/eliminazione)?*
30.	*ARCHIVIAZIONE DI OGGETTI - REGISTRI:* *Il fornitore di servizi cloud offre la possibilità di generare registri di controllo che includono dettagli su una singola richiesta di accesso, come il richiedente, l'ora della richiesta, l'operazione della richiesta, lo stato della risposta e il codice di errore?*

31.	*ARCHIVIAZIONE DI OGGETTI - INVENTARIO PER OGGETTI:* *Il fornitore di servizi cloud offre funzionalità di inventario degli oggetti che permette agli utenti di visualizzare rapidamente gli oggetti e il relativo stato, consentendo loro di individuare velocemente gli oggetti con accesso pubblico?*
32.	*ARCHIVIAZIONE DI OGGETTI - INVENTARIO PER METADATI:* *Il fornitore di servizi cloud offre funzionalità di inventario degli oggetti che permette agli utenti di visualizzare rapidamente i metadati degli oggetti?*
33.	*ARCHIVIAZIONE DI OGGETTI - OTTIMIZZAZIONE DEI CARICAMENTI:* *Il fornitore di servizi cloud ha la possibilità di instradare i dati dalle posizioni edge al servizio di archiviazione utilizzando un percorso di rete ottimizzato?*
34.	*ARCHIVIAZIONE DI OGGETTI - FUNZIONALITÀ DI QUERY:* *Il fornitore di servizi cloud offre agli utenti la possibilità di eseguire query sul servizio di archiviazione degli oggetti utilizzando istruzioni SQL?*
35.	*ARCHIVIAZIONE DI OGGETTI - RECUPERO DI SOTTOINSIEMI:* *Il fornitore di servizi cloud offre agli utenti la possibilità di recuperare solo un sottoinsieme di dati da un oggetto utilizzando semplici espressioni SQL?*
36.	*SERVIZIO DI ARCHIVIAZIONE DI FILE:* *Il fornitore di servizi cloud offre un servizio di archiviazione di file semplice e scalabile da utilizzare con istanze di calcolo nel cloud?*
37.	*ARCHIVIAZIONE DI FILE - RIDONDANZA:* *Il fornitore di servizi cloud archivia gli oggetti del file system (ovvero directory, file e link) in modo ridondante in più data center o strutture per ottenere livelli di disponibilità e durabilità più elevati?*
38.	*ARCHIVIAZIONE DI FILE - ELIMINAZIONE DATI:* *Il fornitore di servizi cloud supporta l'eliminazione completa dei dati di archiviazione dei file in modo che gli stessi non siano più leggibili o accessibili da utenti o terze parti non autorizzati?*
39.	*ARCHIVIAZIONE DI FILE - DISPONIBILITÀ ELEVATA:* *Il file system gestito del fornitore di servizi cloud fornisce un alto livello di disponibilità elevata?*
40.	*ARCHIVIAZIONE DI FILE - NFS:* *Il fornitore di servizi cloud supporta il protocollo NFS (Network File System)?*
41.	*ARCHIVIAZIONE DI FILE - SMB:* *Il fornitore di servizi cloud supporta il protocollo SMB (Server Message Block)?*
42.	*ARCHIVIAZIONE DI FILE - CRITTOGRAFIA DEI DATI A RIPOSO:* *Il servizio di archiviazione di file del fornitore di servizi cloud supporta la crittografia dei dati a riposo?*
43.	*ARCHIVIAZIONE DI FILE - CRITTOGRAFIA DEI DATI IN TRANSITO:* *Il servizio di archiviazione di file del fornitore di servizi cloud supporta la crittografia dei dati in transito?*
44.	*ARCHIVIAZIONE DI FILE - STRUMENTO DI MIGRAZIONE DEI DATI:* *Il fornitore di servizi cloud offre uno strumento di migrazione dei dati per consentire agli utenti di spostare dati da sistemi on-premise nel file system basato sul cloud?*
45.	*SERVIZIO DI ARCHIVIAZIONE IN ARCHIVI:*

	Il fornitore di servizi cloud offre un servizio di archiviazione a costi estremamente bassi per l'archiviazione di file e oggetti pressoché immutabili e ai quali si accede con meno frequenza?
46.	*ARCHIVIAZIONE IN ARCHIVI - TOLLERANZA AI GUASTI:* *L'architettura del fornitore di servizi cloud offre tolleranza ai guasti per il proprio servizio di archiviazione in archivi?*
47.	*ARCHIVIAZIONE IN ARCHIVI - IMMUTABILITÀ:* *Il fornitore di servizi cloud supporta l'immutabilità di oggetti e file archiviati?*
48.	*ARCHIVIAZIONE IN ARCHIVI - WORM:* *Il fornitore di servizi cloud offre funzionalità WORM (Write Once Read Many)?*
49.	*ARCHIVIAZIONE IN ARCHIVI - RECUPERO DI SOTTOINSIEMI:* *Il fornitore di servizi cloud offre agli utenti la possibilità di recuperare solo un sottoinsieme di dati da un oggetto archiviato utilizzando semplici espressioni SQL?*
50.	*ARCHIVIAZIONE IN ARCHIVI - RECUPERO CON VELOCITÀ DIVERSE:* *Il fornitore di servizi cloud offre agli utenti più opzioni di recupero dei dati a costi e con tempi di recupero diversi?*
51.	*ARCHIVIAZIONE IN ARCHIVI - CRITTOGRAFIA DEI DATI A RIPOSO:* *Il servizio di archiviazione in archivi del fornitore di servizi cloud supporta la crittografia di dati a riposo?*
52.	*ARCHIVIAZIONE - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione precedente sull'archiviazione?* *Esempio:* *Dimensione massima di volume* *Numero massimo di unità allegate a un'istanza* *Numero massimo di operazioni di input/output al secondo (IOPS)* *Dimensione massima dell'oggetto* *Numero massimo di oggetti per account di archiviazione* *Numero massimo di snapshot*

4. Amministrazione

	Requisito
1.	*AMMINISTRAZIONE - UTENTI E GRUPPI:* *Il fornitore di servizi cloud offre un servizio per creare e gestire utenti e gruppi di utenti della sua infrastruttura e delle sue risorse?*
2.	*AMMINISTRAZIONE - REIMPOSTAZIONE PASSWORD:* *Il fornitore di servizi cloud consente agli utenti di reimpostare la password in modo autonomo?*
3.	*AMMINISTRAZIONE - AUTORIZZAZIONI:* *Il fornitore di servizi cloud offre la possibilità di aggiungere autorizzazioni a utenti e gruppi a livello di risorsa?*
4.	*AMMINISTRAZIONE - AUTORIZZAZIONI TEMPORANEE:*

	Il fornitore di servizi cloud offre la possibilità di creare autorizzazioni valide per un intervallo di tempo specifico?
5.	*AMMINISTRAZIONE - CREDENZIALI TEMPORANEE:* *Il fornitore di servizi cloud offre agli utenti la possibilità di creare e fornire credenziali di sicurezza temporanee a utenti affidabili, configurate per durare indistintamente da pochi minuti a diverse ore?*
6.	*AMMINISTRAZIONE - CONTROLLO ACCESSI:* *Il fornitore di servizi cloud offre controlli di accesso granulare alle proprie risorse infrastrutturali?* • *Se sì, quali condizioni possono essere utilizzate da tali controlli (ovvero ora del giorno, indirizzo IP di origine e così via)?*
7.	*AMMINISTRAZIONE - POLICY INTEGRATE:* *L'infrastruttura del fornitore di servizi cloud contiene policy di controllo degli accessi integrate che possono essere collegate a utenti e gruppi?*
8.	*AMMINISTRAZIONE - POLICY PERSONALIZZATE:* *L'infrastruttura del fornitore di servizi cloud consente la creazione e la personalizzazione di policy di controllo degli accessi che possono essere collegate a utenti e gruppi?*
9.	*AMMINISTRAZIONE - SIMULATORE POLICY:* *Il fornitore di servizi cloud offre un meccanismo per testare gli effetti delle policy di controllo degli accessi prima di utilizzare tali policy nell'ambiente di produzione?*
10.	*AMMINISTRAZIONE - MFA NEL CLOUD:* *Il fornitore di servizi cloud supporta l'utilizzo dell'autenticazione a più fattori (MFA) come ulteriore livello di controllo degli accessi e di autenticazione alla propria infrastruttura?*
11.	*AMMINISTRAZIONE - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione amministrazione precedente?* *Esempio:* *Numero massimo di utenti* *Numero massimo di gruppi* *Numero massimo di policy gestite*

5. Sicurezza

	Requisito
1.	*SICUREZZA - CONTROLLI DEI PRECEDENTI PENALI (BACKGROUND CHECK):* *Tutto il personale del fornitore di servizi cloud che dispone dell'accesso all'infrastruttura del servizio (sia fisico che non fisico) è soggetto ai controlli dei precedenti penali?*
2.	*SICUREZZA - ACCESSO FISICO:* *Il fornitore di servizi cloud limita l'accesso del personale all'infrastruttura del servizio tranne in caso di specifiche richieste di assistenza, richieste di modifica o analoghe autorizzazioni formali?*
3.	*SICUREZZA - REGISTRI DI ACCESSO:* *Il fornitore di servizi cloud registra l'accesso del personale all'infrastruttura in uso, registrando sempre l'accesso e conservando i registri per un minimo di 90 giorni?*

4.	*SICUREZZA - ACCESSI ALL'HOST:* *Il fornitore di servizi cloud limita l'accesso del personale a agli host di calcolo, automatizzando invece tutte le attività eseguite su tali host, registrando i contenuti dei processi automatizzati e conservando i registri per un minimo di 90 giorni?*
5.	*SICUREZZA - CHIAVI CRITTOGRAFICHE:* *Il fornitore di servizi cloud offre un servizio per creare e controllare le chiavi crittografiche utilizzate per crittografare i dati degli utenti?*
6.	*SICUREZZA - GESTIONE DELLE CHIAVI DI ACCESSO:* *Il fornitore di servizi cloud offre la possibilità di individuare l'ultimo utilizzo di una chiave di accesso, ruotare le vecchie chiavi e rimuovere gli utenti inattivi?*
7.	*SICUREZZA - CHIAVI FORNITE DAL CLIENTE:* *Il fornitore di servizi cloud consente agli utenti di importare chiavi dalla propria infrastruttura di gestione chiavi nel servizio di gestione chiavi del fornitore di servizi?*
8.	*SICUREZZA - INTEGRAZIONE DEL SERVIZIO CHIAVI CRITTOGRAFICHE:* *Il servizio di gestione chiavi del fornitore di servizi cloud si integra con altri servizi cloud per fornire funzionalità di crittografia dei dati a riposo?*
9.	*SICUREZZA - HSM:* *Il fornitore di servizi cloud offre moduli di sicurezza hardware (HSM) dedicati, ad esempio dispositivi hardware, che forniscono operazioni protette di crittografia e archiviazione delle chiavi in un modulo hardware antimanomissione?*
10.	*SICUREZZA - DURABILITÀ CHIAVI CRITTOGRAFICHE:* *Il fornitore di servizi cloud supporta la durabilità delle chiavi, ad esempio l'archiviazione di più copie, cosicché le chiavi siano disponibili quando necessario?*
11.	*SICUREZZA - SSO:* *Il fornitore di servizi cloud offre un servizio Single Sign-On (SSO) gestito che consente agli utenti di gestire centralmente l'accesso a più account e applicazioni aziendali?*
12.	*SICUREZZA – CERTIFICATI:* *Il fornitore di servizi cloud offre un servizio gestito per effettuare il provisioning dei certificati Secure Sockets Layer (SSL)/Transport Layer Security (TLS), per gestirli e implementarli?*
13.	*SICUREZZA - RINNOVO CERTIFICATI:* *Il servizio di gestione dei certificati del fornitore di servizi cloud semplifica il rinnovo dei certificati?*
14.	*SICUREZZA - CERTIFICATI JOLLY:* *Il servizio di gestione dei certificati del fornitore di servizi cloud supporta l'uso di certificati jolly?*
15.	*SICUREZZA - AUTORITÀ DI CERTIFICAZIONE:* *Il servizio di gestione dei certificati del fornitore di servizi cloud agisce anche in qualità di autorità di certificazione (CA)?*
16.	*SICUREZZA - ACTIVE DIRECTORY:* *Il fornitore di servizi cloud offre un servizio Microsoft Active Directory (AD) gestito nel cloud?*
17.	*SICUREZZA - ACTIVE DIRECTORY ON-PREMISE:* *Il servizio Microsoft Active Directory (AD) gestito del fornitore di servizi cloud supporta l'integrazione con i servizi Microsoft Active Directory (AD) on-premise?*

18.	***SICUREZZA - LDAP:*** *Il servizio Microsoft Active Directory (AD) gestito del fornitore di servizi cloud supporta il protocollo LDAP (Lightweight Directory Access Protocol)?*
19.	***SICUREZZA - ACTIVE DIRECTORY:*** *Il servizio Microsoft Active Directory (AD) gestito del fornitore di servizi cloud supporta il linguaggio SAML (Security Assertion Markup Language)?*
20.	***SICUREZZA - GESTIONE DELLE CREDENZIALI:*** *Il fornitore di servizi cloud offre un servizio gestito che consente agli utenti di ruotare, gestire e recuperare facilmente le credenziali, ad esempio le chiavi API, le credenziali di database e altre informazioni riservate?*
21.	***SICUREZZA - WAF:*** *Il fornitore di servizi cloud offre un firewall per applicazioni Web (WAF) che consente di proteggere le applicazioni Web da exploit comuni, potenzialmente in grado di influire sulla disponibilità delle applicazioni, compromettere la sicurezza o utilizzare un numero eccessivo di risorse?*
22.	***SICUREZZA - DDOS:*** *Il fornitore di servizi cloud offre un servizio per la protezione dagli attacchi DDoS più comuni e frequenti verso la rete e il livello di trasporto, con la possibilità di scrivere regole personalizzate per ridurre attacchi sofisticati a livello delle applicazioni?*
23.	***SICUREZZA - SUGGERIMENTI IN MATERIA DI SICUREZZA:*** *Il fornitore di servizi cloud offre un servizio per valutare automaticamente potenziali vulnerabilità nelle applicazioni e nelle risorse?*
24.	***SICUREZZA - RILEVAMENTO DELLE MINACCE:*** *Il fornitore di servizi cloud offre un servizio gestito di rilevamento delle minacce?*
25.	***SICUREZZA - LIMITI DEL SERVIZIO:*** *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione precedente sulla sicurezza?* *Esempio:* *Numero massimo di chiavi master del cliente* *Numero massimo di moduli di sicurezza hardware (HSM)*

6. Conformità

L'elenco che segue è fornito a puro scopo illustrativo e non deve essere considerato esaustivo rispetto alle certificazioni e agli standard potenzialmente applicabili ai servizi cloud.

Indicare i set di standard di conformità internazionali e specifici del settore rispettati dal fornitore di servizi cloud:

Certificazioni/attestati	*Leggi, normative e privacy*	*Allineamenti/Framework*
☐ C5 [Germania]	*☐ Direttiva dell'UE sulla protezione dei dati*	*☐ CDSA*
☐ Codice di condotta CISPE in materia di protezione dei dati	*☐ Clausole modello dell'UE (EU Model Clauses)*	

☐ *CNDCP (Climate Neutral Data Centre Pact, Patto per la neutralità climatica dei data center)*		
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG – Livelli 2 e 4*	☐ *GDPR*	☐ *Criminal Justice Info. Service (CJIS, servizi di informazione sulla giustizia penale)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Scudo UE-USA per la privacy*
☐ *HDS (Francia, Sanità)*	☐ *HITECH*	☐ *Approdo sicuro (Safe harbor) UE*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malesia]*	☐ *G-Cloud [Regno Unito]*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapore]*	☐ *GxP (FDA CFR 21 Part 11)*
☐ *IRAP [Australia]*	☐ *PIPEDA [Canada]*	☐ *ICREA*
☐ *MTCS Tier 3 [Singapore]*	☐ *Privacy Act [Australia]*	☐ *IT Grundschutz [Germania]*
☐ *PCI DSS livello 1*	☐ *Privacy Act [Nuova Zelanda]*	☐ *MARS – E*
☐ *Rule 17-a-4(f) della SEC*	☐ *Autorizzazione DPA (Spagna)*	☐ *MITA 3.0*
☐ *SOC1/ISAE 3402*	☐ *U.K. DPA – 1988*	☐ *MPAA*
☐ *SOC2/SOC3*	☐ *VPAT/Sezione 508*	☐ *NIST*
☐ *Codice SWIPO IaaS*		
		☐ *Livelli di certificazione Uptime Institute*
		☐ *UK Cloud Security Principles*

Sulla scorta dei report di conformità di cui sopra, gli enti pubblici possono valutare le singole offerte rispetto agli standard accettati di sicurezza, di conformità e di natura operativa. Tali report evidenziano che il CISP, grazie alla conformità dichiarata, soddisfa i controlli operativi dei data center indicati sotto, obbligatori per i fornitori di servizi cloud pubblici. Mediante il requisito della conformità ai report, gli enti pubblici hanno la certezza che i controlli riportati di seguito siano stati effettuati.

- *Accesso verificato: il CISP deve limitare l'accesso fisico ai soli soggetti che hanno la necessità di recarsi in un luogo per giustificati motivi di lavoro. In caso di concessione dell'accesso, lo stesso dovrà essere revocato non appena il lavoro verrà completato.*

- *Ingresso controllato e monitorato: l'accesso al perimetro del Livello Data Center deve essere controllato. Il CISP deve collocare degli agenti di sicurezza presso i cancelli d'ingresso del personale e assumere supervisori che controllino gli agenti e i visitatori tramite telecamere di sicurezza. Alle persone autorizzate presenti nel sito verrà consegnato un badge con autenticazione a più fattori, che limita l'accesso alle sole aree preventivamente approvate.*

- *Addetti ai data center del CISP: i dipendenti del CISP che devono accedere regolarmente a un data center dovranno essere ammessi nelle aree pertinenti dell'edificio a seconda della mansione che svolgono; il loro accesso dovrà essere controllato in modo sistematico. Gli elenchi del personale devono essere controllati regolarmente da un responsabile degli accessi all'area, per verificare che l'autorizzazione di ciascun dipendente sia ancora necessaria. Se un dipendente non ha l'esigenza di accedere a un data center regolarmente per motivi di lavoro, sarà sottoposto alla stessa procedura per i visitatori.*

- *Monitoraggio degli accessi non autorizzati: i CISP devono monitorare costantemente gli accessi non autorizzati all'edificio in cui è situato il data center tramite sistemi di videosorveglianza, rilevamento delle intrusioni e monitoraggio dei registri degli accessi. Gli ingressi devono essere protetti con dispositivi che emettono allarmi acustici se una porta viene forzata o tenuta aperta.*

- *Monitoraggio della sicurezza globale da parte dei centri operativi per la sicurezza del CISP: i centri operativi per la sicurezza del CISP devono essere dislocati in tutto il mondo; sono responsabili del monitoraggio, della selezione e dell'esecuzione dei programmi di sicurezza per i data center del CISP. Devono vigilare sulla gestione degli accessi fisici e sulla risposta al rilevamento delle intrusioni; contestualmente, devono offrire un supporto globale 24 ore su 24, 7 giorni su 7 giorni ai team di sicurezza locali dei data center, svolgere attività di monitoraggio continuo (ad esempio, controllo delle attività di accesso, revoca dei permessi di accesso) ed essere disponibili a intervenire e analizzare eventuali incidenti riguardanti la sicurezza.*

- *Analisi degli accessi livello per livello: l'accesso al Livello Infrastruttura deve essere limitato in base alle esigenze aziendali. Con l'implementazione di un'analisi degli accessi livello per livello, il diritto di accedere a ogni livello non è automaticamente garantito. L'ingresso a un livello specifico deve essere consentito solo in presenza di una necessità effettiva di accedere a tale livello.*

- *Manutenzione dei dispositivi nell'ambito delle operazioni di routine: i team del CISP devono eseguire test diagnostici su macchine, reti e dispositivi di backup, per garantirne il pieno funzionamento sia in circostanze ordinarie sia in caso di emergenza. I controlli di manutenzione ordinaria dei dispositivi e dei servizi del data center dovrebbero rientrare nelle operazioni di routine del data center del CISP.*

- *Dispositivi di backup pronti per le emergenze: gli impianti per l'erogazione di acqua, energia elettrica, telecomunicazioni e connettività Internet devono essere progettati in modo ridondante, affinché il CISP possa garantire la continuità delle operazioni in situazioni di emergenza. Gli impianti di alimentazione elettrica devono essere progettati in modo completamente ridondante: in caso di interruzione dell'alimentazione, dovranno essere attivati i gruppi di continuità per specifiche funzioni; contestualmente, i generatori forniranno energia di emergenza all'intera struttura. Sia le persone sia i sistemi devono monitorare e controllare la temperatura e l'umidità per prevenire il surriscaldamento e ridurre ulteriormente le possibili interruzioni del servizio.*

- *Collaborazione tra tecnologia e persone per una maggiore sicurezza: è necessario approntare delle procedure obbligatorie per ottenere l'autorizzazione ad entrare nel Livello Dati. Ciò comporta la verifica e l'approvazione della richiesta di accesso di una persona da parte dei soggetti autorizzati. Parallelamente, i sistemi di rilevamento delle minacce e delle intrusioni elettroniche devono monitorare e attivare automaticamente gli allarmi in caso di minacce rilevate o di attività sospette. Qualora, ad esempio, venga forzata o tenuta aperta una porta, scatterà un allarme. Il CISP deve dislocare le telecamere di sicurezza e conservare i filmati nel rispetto del requisiti normativi e di conformità.*

- *Prevenzione delle intrusioni fisiche e tecnologiche: i punti di accesso alle sale server devono essere rafforzati con dispositivi elettronici di controllo che richiedono un'autorizzazione a più fattori. Il CISP deve anche essere pronto a impedire le intrusioni tecnologiche. I server del CISP devono essere in grado di avvertire i dipendenti riguardo a eventuali tentativi di rimozione dei dati. Nel caso improbabile di una violazione, il server deve essere automaticamente disabilitato.*

- *Massima attenzione a server e supporti multimediali: i supporti multimediali utilizzati per archiviare i dati dei clienti devono essere classificati dal CISP come "essenziali" e trattati di conseguenza, in quanto ad alto impatto, per tutto il relativo ciclo di vita. Il CISP deve adottare standard rigorosi per l'installazione, il funzionamento e la distruzione*

finale dei dispositivi quando gli stessi non sono più utili. Quando un supporto di archiviazione raggiunge la fine della sua vita utile, il CISP deve dismetterlo utilizzando le tecniche descritte nel documento NIST 800-88. I supporti su cui sono archiviati i dati dei clienti non sono esclusi dal controllo del CISP fino a quando non vengono dismessi in modo sicuro.

- *Verifica delle procedure e dei sistemi del CISP da parte di revisori di terze parti: il CISP deve essere sottoposto a verifiche da parte di revisori esterni incaricati di ispezionare i data center e di condurre indagini approfondite. Tali verifiche sono finalizzate a confermare il rispetto, da parte del CISP, delle regole consolidate, necessarie per ottenere le pertinenti certificazioni di sicurezza. A seconda del programma di conformità e dei requisiti da esso previsti, i revisori esterni possono porre domande ai dipendenti del CISP sulla gestione e sullo smaltimento dei supporti. I revisori possono anche guardare i filmati delle telecamere di sicurezza e ispezionare gli ingressi e i corridoi di un data center. Inoltre, possono esaminare le apparecchiature, ad esempio i dispositivi elettronici per il controllo degli accessi e le telecamere di sicurezza del CISP.*

- *Preparativi in caso di imprevisti: il CISP deve prepararsi anticipatamente per affrontare potenziali minacce ambientali, come catastrofi naturali e incendi. L'installazione di sensori automatici e di apparecchiature sensibili costituiscono due modi in cui il CISP può proteggere i data center. È necessario installare dei dispositivi di rilevamento dell'acqua per avvertire i dipendenti in caso di problemi, quando le pompe automatiche sono in funzione per rimuovere il liquido e prevenire i danni. Allo stesso modo, le attrezzature per rilevare e spegnere automaticamente gli incendi riducono i rischi e, in caso di problemi, possono allertare i dipendenti del CISP e i vigili del fuoco.*

- *Disponibilità elevata grazie a più zone di disponibilità: il CISP deve prevedere più zone di disponibilità per garantire una maggiore tolleranza ai guasti. Ciascuna zona di disponibilità deve essere costituita da uno o più data center; deve essere fisicamente separata dalle altre e deve disporre di alimentazione elettrica e rete ridondanti. Le zone di disponibilità devono essere collegate tra loro da una rete privata veloce in fibra ottica per realizzare applicazioni in grado di eseguire automaticamente il fail-over tra le varie zone di disponibilità, senza interruzioni.*

- *Simulazione delle interruzioni e misurazione della nostra risposta: il CISP deve dotarsi di un piano di continuità aziendale che agisca da guida al processo operativo. Tale piano stabilisce le modalità per evitare e ridurre le interruzioni dovute a catastrofi naturali, con misure dettagliate da adottare prima, durante e dopo un evento. Per attutire le conseguenze e prepararsi all'imprevisto, il CISP deve testare regolarmente il piano di continuità aziendale mediante esercitazioni che simulano diversi scenari. Il CISP deve documentare le prestazioni del personale e dei processi. Successivamente, deve riferire le lezioni apprese e le eventuali azioni correttive, necessarie per migliorare il tasso di risposta. Il personale del CISP deve essere formato e pronto a ripristinare le attività rapidamente dopo le interruzioni, con un processo di recupero metodico che riduca al minimo ulteriori tempi di inattività dovuti a errori.*

- *Aiuto finalizzato al conseguimento degli obiettivi di efficienza: oltre a occuparsi dei rischi ambientali, il CISP dovrebbe anche integrare il concetto di sostenibilità nella progettazione dei data center. Il CISP deve documentare il proprio impegno a favorire l'uso delle energie rinnovabili nei propri data center. Inoltre, il CISP deve spiegare come i clienti stessi del CISP possono ridurre le emissioni di carbonio rispetto ai propri data center.*

- *Selezione della sede: prima di scegliere una sede, il CISP deve condurre una prima valutazione di impatto ambientale e geografico. Le ubicazioni dei data center devono essere selezionate con cura per mitigare i rischi ambientali, come inondazioni, condizioni meteorologiche estreme e attività sismica. Le zone di disponibilità del CISP devono essere costruite in modo tale da risultare indipendenti e fisicamente separate l'una dall'altra.*

- *Ridondanza: i data center devono essere progettati in modo da anticipare e tollerare i guasti, mantenendo, contestualmente, livelli di servizio adeguati. In caso di guasti, i processi automatizzati devono spostare il traffico dati dall'area interessata. Le applicazioni strategiche devono essere implementate secondo uno standard N+1: in questo modo, in caso di problemi al data center, viene garantita la capacità sufficiente per consentire la distribuzione bilanciata del traffico sui siti rimanenti.*

- *Disponibilità: il CISP deve individuare i componenti essenziali del sistema, necessari per assicurare la disponibilità del sistema e ripristinare il servizio in caso di interruzione. I componenti essenziali del sistema devono essere sottoposti a backup in più siti isolati. Ogni sito o zona di disponibilità deve essere progettato per funzionare in modo indipendente e con un'elevata affidabilità. Le zone di disponibilità dovrebbero essere connesse per permettere alle applicazioni di eseguire automaticamente il fail-over senza interruzioni. L'estrema resilienza del sistema – e, conseguentemente, la disponibilità del servizio – dovrebbe essere una caratteristica della progettazione del sistema*

Una progettazione dei data center che prevede zone di disponibilità e replica dei dati dovrà consentire ai clienti del CISP di raggiungere obiettivi del punto di ripristino e del tempo di ripristino estremamente ridotti, nonché livelli più elevati di disponibilità del servizio.

- ***Pianificazione della capacità**: il CISP deve monitorare costantemente l'utilizzo dei servizi per implementare le infrastrutture a sostegno degli impegni e dei requisiti di disponibilità. Il CISP deve mantenere un modello di pianificazione della capacità che valuta l'uso e la domanda di infrastruttura del CISP almeno con cadenza mensile. Tale modello deve supportare la pianificazione della domanda futura e includere considerazioni quali l'elaborazione delle informazioni, le telecomunicazioni e l'archiviazione dei registri di controllo.*

CONTINUITÀ AZIENDALE e RIPRISTINO DI EMERGENZA

- ***Piano di continuità aziendale**: il piano di continuità aziendale del CISP deve descrivere le misure per evitare e ridurre le interferenze ambientali. Deve includere i dettagli operativi sulle misure da adottare prima, durante e dopo un evento. Il piano di continuità aziendale deve essere suffragato da test che includono le simulazioni dei diversi scenari. Durante e dopo i test, il CISP deve documentare le prestazioni di persone e processi, le azioni correttive e le lezioni apprese con l'obiettivo del miglioramento continuo.*

- ***Risposta alle pandemie**: il CISP deve integrare policy e procedure di risposta alle pandemie nella propria pianificazione di ripristino di emergenza, per reagire rapidamente alle minacce di insorgenza di malattie infettive. Le strategie di mitigazione includono modelli alternativi di gestione del personale. In questo modo, è possibile trasferire i processi essenziali a risorse situate al di fuori della regione e attivare un piano di gestione delle crisi a supporto delle operazioni aziendali essenziali. I piani per le pandemie devono menzionare gli enti e i regolamenti sanitari internazionali, compresi i punti di contatto con gli organismi internazionali.*

MONITORAGGIO e REGISTRAZIONE

- ***Revisione dell'accesso al data center:** è opportuno procedere a una revisione periodica degli accessi ai data center. L'accesso viene revocato automaticamente quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane del CISP. Inoltre, quando l'accesso di un dipendente o collaboratore scade in base alla durata della richiesta approvata, è necessario revocarne l'accesso anche se la persona continua a lavorare per il CISP.*

- ***Registri degli accessi al data center:** l'accesso fisico ai data center del CISP deve essere registrato, monitorato e documentato. Il CISP deve mettere in correlazione le informazioni che riceve dai sistemi di monitoraggio logico e fisico, per migliorare la sicurezza in funzione delle esigenze.*

- ***Monitoraggio dell'accesso al data center**: il CISP deve monitorare i data center utilizzando i centri operativi globali per la sicurezza, che si occupano del monitoraggio, della selezione e dell'attuazione dei programmi di sicurezza. Devono fornire supporto globale 24 ore su 24, 7 giorni su 7, gestendo e monitorando le attività di accesso ai data center, mettendo i team locali e gli altri team di supporto nelle condizioni di intervenire in caso di incidenti riguardanti la sicurezza attraverso le procedure di selezione, la consulenza, l'analisi e l'invio di risposte.*

SORVEGLIANZA e RILEVAMENTO

- ***TELECAMERE A CIRCUITO CHIUSO**: i punti di accesso fisico alle sale server devono essere videosorvegliati con telecamere a circuito chiuso (CCTV). Le immagini devono essere conservate in ottemperanza ai requisiti normativi e di conformità.*

- ***Punti di ingresso al data center**: l'accesso fisico presso i punti di ingresso dell'edificio deve essere sorvegliato da personale di sicurezza esperto mediante sistemi di videosorveglianza, sistemi anti-intrusione e altri dispositivi elettronici. Il personale autorizzato deve utilizzare meccanismi di autenticazione a più fattori per accedere ai data center. Gli ingressi alle sale server devono essere protetti con dispositivi che emettono allarmi acustici per innescare la risposta a un incidente se una porta viene forzata o tenuta aperta.*

- ***Rilevamento delle intrusioni:** è necessario che all'interno del Livello Dati siano installati sistemi elettronici anti-intrusione per monitorare, rilevare e avvisare automaticamente il personale preposto agli incidenti di sicurezza. I punti di ingresso e di uscita delle sale server devono essere dotati di dispositivi di protezione che impongono l'autenticazione a più fattori a chiunque debba entrare o uscire. Tali dispositivi emettono allarmi sonori in caso di apertura forzata*

della porta senza autenticazione o in caso di porta tenuta aperta. I dispositivi di allarme delle porte devono, inoltre, essere configurati in modo da rilevare i casi in cui qualcuno esce o entra in un Livello Dati senza fornire un'autenticazione a più fattori. Gli allarmi devono essere inoltrati tempestivamente ai centri operativi di sicurezza del CISP (attivi 24 ore su 24, 7 giorni su 7) per garantire la registrazione, l'analisi e la risposta immediata.

GESTIONE DEI DISPOSITIVI

- *Gestione delle risorse: le risorse del CISP devono essere gestite in modo centralizzato, mediante un sistema di gestione dell'inventario che consenta di memorizzare e tenere traccia di titolare, ubicazione, stato, manutenzione e altre informazioni descrittive delle risorse di proprietà del CISP. Dopo la fase di approvvigionamento, le risorse devono essere scansionate e monitorate, mentre le risorse in fase di manutenzione devono essere controllate e monitorate per quanto riguarda la titolarità, lo stato e la risoluzione.*

- *Distruzione dei supporti multimediali: i supporti multimediali utilizzati per l'archiviazione dei dati dei clienti devono essere classificati dal CISP come "essenziali" e trattati di conseguenza, in quanto ad alto impatto, per tutto il loro ciclo di vita. Il CISP deve adottare standard rigorosi per l'installazione, la manutenzione e la distruzione finale dei supporti quando gli stessi non sono più utili. Quando un supporto di archiviazione raggiunge la fine della sua vita utile, il CISP deve dismetterlo utilizzando le tecniche descritte nel documento NIST 800-88. I supporti su cui sono archiviati i dati dei clienti non sono esclusi dal controllo del CISP fino a quando non vengono dismessi in modo sicuro.*

SISTEMI DI SUPPORTO OPERATIVO

- *Energia elettrica: gli impianti elettrici dei data center del CISP devono essere completamente ridondanti e la loro manutenzione deve poter essere eseguita senza alcun impatto sull'operatività, 24 ore al giorno. Il CISP deve garantire che i data center siano dotati di alimentazione di emergenza, per assicurare la disponibilità di energia e mantenere l'operatività in caso di guasti elettrici che interessano i carichi importanti ed essenziali della struttura.*

- *Clima e temperatura: i data center del CISP devono utilizzare dei meccanismi di controllo della climatizzazione e mantenere una temperatura operativa adeguata per i server e gli altri componenti hardware, al fine di prevenire il surriscaldamento e ridurre la possibilità di interruzioni del servizio. Il personale e i sistemi devono monitorare e verificare che umidità e temperatura rimangano entro i limiti stabiliti.*

- *Rilevamento ed estinzione degli incendi: i data center del CISP devono essere dotati di apparecchiature automatiche per rilevare ed estinguere gli incendi. I sistemi di rilevamento degli incendi devono utilizzare sensori per rilevare il fumo negli spazi meccanici, infrastrutturali e di rete. Tali aree devono essere protette anche da sistemi di estinzione degli incendi.*

- *Rilevamento delle perdite: per rilevare eventuali perdite d'acqua, il CISP deve dotare i propri data center di sistemi in grado di rilevare la presenza di acqua. In caso di rilevamento di acqua, devono essere predisposti i meccanismi necessari per rimuoverla ed evitare danni ulteriori.*

MANUTENZIONE DELL'INFRASTRUTTURA

- *Manutenzione delle apparecchiature: il CISP deve monitorare ed eseguire la manutenzione preventiva delle apparecchiature elettriche e meccaniche, per garantire il funzionamento ininterrotto dei sistemi all'interno dei propri data center. Le procedure di manutenzione delle apparecchiature devono essere eseguite da personale qualificato e completate secondo un piano di manutenzione documentato.*

- *Gestione dell'ambiente: il CISP deve monitorare i sistemi e le apparecchiature elettriche e meccaniche per consentire il rilevamento immediato di eventuali problemi. A tal fine, è necessario utilizzare gli strumenti di controllo continuo e le informazioni fornite dai sistemi di gestione degli edifici e di monitoraggio elettrico del CISP. La manutenzione preventiva viene eseguita per garantire il funzionamento ininterrotto delle apparecchiature.*

GOVERNANCE e RISCHIO

- *Gestione continua dei rischi connessi ai data center: il centro operativo per la sicurezza del CISP deve effettuare valutazioni periodiche delle minacce e delle vulnerabilità dei data center. La valutazione continua e la mitigazione delle possibili vulnerabilità devono essere svolte attraverso attività di valutazione dei rischi connessi ai data center.*

Tale valutazione va ad aggiungersi al processo di valutazione dei rischi a livello aziendale, utilizzato per identificare e gestire i rischi che riguardano l'impresa nel suo complesso. Il processo deve tenere conto anche dei rischi normativi e ambientali a livello regionale.

- ***Attestato di sicurezza rilasciato da terze parti**: i test effettuati da soggetti terzi sui data center del CISP, come documentato nei rispettivi report, devono garantire che il CISP abbia attuato misure di sicurezza adeguate, in sintonia con le disposizioni necessarie per ottenere le certificazioni di sicurezza. A seconda del programma di conformità e dei relativi requisiti, i revisori esterni possono eseguire dei test sullo smaltimento dei supporti, esaminare i filmati di videosorveglianza, controllare gli ingressi e i corridoi del data center, collaudare i dispositivi elettronici di controllo degli accessi e analizzare le apparecchiature del data center.*

7. Migrazioni

	Requisito
1.	***SERVIZIO MIGRAZIONI:*** *Quanti e quali servizi di migrazione dei dati sono offerti dal fornitore di servizi cloud?*
2.	***MIGRAZIONI - MONITORAGGIO CENTRALIZZATO:*** *Il fornitore di servizi cloud offre un servizio centralizzato (ad esempio una singola interfaccia), per consentire agli enti di tenere traccia e monitorare lo stato delle migrazioni delle applicazioni e dei server utilizzati?*
3.	***MIGRAZIONI - PANNELLO DI CONTROLLO:*** *Lo strumento di migrazione del fornitore di servizi cloud offre un pannello di controllo per visualizzare in modo rapido lo stato delle migrazioni, i parametri correlati e la cronologia delle migrazioni?*
4.	***MIGRAZIONI - STRUMENTI DEL FORNITORE DI SERVIZI CLOUD:*** *Lo strumento di migrazione del fornitore di servizi cloud si integra con altri strumenti di migrazione del fornitore stesso, che possono eseguire la migrazione di applicazioni e server?*
5.	***MIGRAZIONI - STRUMENTI DI TERZE PARTI:*** *Lo strumento di migrazione del fornitore di servizi cloud consente l'integrazione di strumenti di migrazione di terze parti?* • *Se sì, quali sono gli strumenti di migrazione di terze parti supportati?*
6.	***MIGRAZIONI - MIGRAZIONI TRA PIÙ REGIONI:*** *Lo strumento di migrazione del fornitore di servizi cloud offre funzionalità di tracciamento e di monitoraggio delle migrazioni di applicazioni e server che si verificano in regioni diverse?*
7.	***MIGRAZIONI - MIGRAZIONE DEI SERVER:*** *Lo strumento di migrazione del fornitore di servizi cloud prevede la possibilità di eseguire la migrazione di server virtualizzati on-premise nel cloud?* • *Se sì, quali ambienti virtualizzati sono attualmente supportati?*
8.	***MIGRAZIONI - INDIVIDUAZIONE DEI SERVER:*** *Lo strumento di migrazione del fornitore di servizi cloud offre una funzionalità di individuazione per il rilevamento automatico dei server virtuali locali da migrare nel cloud?*
9.	***MIGRAZIONI - DATI SULLE PRESTAZIONI DEI SERVER:*** *Lo strumento di migrazione del fornitore di servizi cloud dispone della funzionalità di raccolta e visualizzazione delle prestazioni relative a server e/o macchine virtuali, come ad esempio l'utilizzo della CPU e della memoria RAM?*
10.	***MIGRAZIONI - DATABASE DI INDIVIDUAZIONE***

	Lo strumento di migrazione del fornitore di servizi cloud offre la possibilità di archiviare tutti i dati raccolti in un database centralizzato? • *Se sì, gli enti hanno la possibilità di esportare i dati? In quali formati?*
11.	*MIGRAZIONI - CRITTOGRAFIA DEI DATI A RIPOSO:* *Il fornitore di servizi cloud offre un servizio di crittografia dei dati a riposo per tutte le informazioni raccolte e memorizzate nel database di individuazione?*
12.	*MIGRAZIONI - REPLICA INCREMENTALE DEI SERVER:* *Lo strumento di migrazione del fornitore di servizi cloud offre la replica incrementale automatizzata dei server attivi durante la migrazione di server o macchine virtuali per garantire che tutte le modifiche apportate a essi siano incluse nell'immagine migrata finale?* • *Se sì, qual è il tempo di esecuzione consentito per il servizio?*
13.	*MIGRAZIONI - VMWARE:* *Lo strumento di migrazione del fornitore di servizi cloud supporta migrazioni di macchine virtuali VMWare da server on-premise nel cloud?*
14.	*MIGRAZIONI - HYPER-V:* *Lo strumento di migrazione del fornitore di servizi cloud supporta migrazioni di macchine virtuali Hyper-V da server on-premise nel cloud?*
15.	*MIGRAZIONI - INDIVIDUAZIONE DELLE APPLICAZIONI:* *Lo strumento di migrazione del fornitore di servizi cloud consente l'individuazione e il raggruppamento delle applicazioni prima della migrazione?*
16.	*MIGRAZIONI - MAPPATURA DELLE DIPENDENZE:* *Lo strumento di migrazione del fornitore di servizi cloud consente l'individuazione delle dipendenze tra i server e le applicazioni prima della migrazione?*
17.	*MIGRAZIONI - MIGRAZIONE DEI DATABASE:* *Lo strumento di migrazione del fornitore di servizi cloud offre funzionalità di migrazione dei database on-premise nel cloud?*
18.	*MIGRAZIONI - TEMPI DI INATTIVITÀ DURANTE LA MIGRAZIONE DEI DATABASE:* *Lo strumento di migrazione del fornitore di servizi cloud offre funzionalità di migrazione dei database nel cloud che garantiscono tempi di inattività minimi, ossia consentono al database di origine di rimanere completamente operativo durante il processo di migrazione?*
19.	*MIGRAZIONI - DATABASE DI ORIGINE:* *Lo strumento di migrazione del fornitore di servizi cloud supporta la migrazione di diverse origini di database, ad esempio Oracle, SQL Server e così via?* • *Se sì, elencare tutti i database di origine supportati che è possibile migrare nel cloud.*
20.	*MIGRAZIONI - MIGRAZIONI ETEROGENEE:* *Lo strumento di migrazione del fornitore di servizi cloud consente di eseguire migrazioni eterogenee dei database, ossia da un database di origine a un database di destinazione diverso, ad esempio da Oracle a SQL Server?* • *Se sì, elencare tutte le possibili combinazioni di migrazioni eterogenee dei database.*
21.	*MIGRAZIONI - MIGRAZIONE DEI DATI NELL'ORDINE DI PETABYTE:* *Il fornitore di servizi cloud offre una soluzione di trasporto dati fino a diversi petabyte che utilizza dispositivi sicuri per trasferire grandi quantità di dati da e verso il cloud?*

22.	*MIGRAZIONI - MIGRAZIONE DEI DATI NELL'ORDINE DI EXABYTE:* *Il fornitore di servizi cloud offre una soluzione di trasporto dati fino a diversi exabyte per trasferire grandi quantità di dati nel cloud?*
23.	*MIGRAZIONI - BACKUP AZIENDALI:* *Il fornitore di servizi cloud offre un servizio che consente una perfetta integrazione del data center del cliente con i servizi di archiviazione nel cloud, consentendo il trasferimento e l'archiviazione dei dati nel servizio di archiviazione del fornitore di servizi cloud?*
24.	*MIGRAZIONI - BACKUP AZIENDALI - ARCHIVIAZIONE DI OGGETTI:* *Il servizio di backup aziendale del fornitore di servizi cloud offre l'integrazione con il servizio di archiviazione di oggetti nel cloud del fornitore?*
25.	*MIGRAZIONI - BACKUP AZIENDALI - ACCESSO AI FILE:* *Il servizio di backup aziendale del fornitore di servizi cloud consente agli utenti di archiviare e recuperare oggetti utilizzando protocolli di file come il protocollo NFS (Network File System)?*
26.	*MIGRAZIONI - BACKUP AZIENDALI - ACCESSO AI BLOCCHI:* *Il servizio di backup aziendale del fornitore di servizi cloud consente agli utenti di archiviare e recuperare oggetti utilizzando protocolli di blocco come il protocollo iSCSI (Internet Small Computer Systems Interface)?*
27.	*MIGRAZIONI - BACKUP AZIENDALI - ACCESSO AI NASTRI:* *Il servizio di backup aziendale del fornitore di servizi cloud consente agli utenti di eseguire il backup dei dati tramite una libreria di nastri virtuali e archiviare questi backup di nastri nel cloud del fornitore?*
28.	*MIGRAZIONI - BACKUP AZIENDALI - CRITTOGRAFIA:* *Il servizio di backup aziendale del fornitore di servizi cloud offre la crittografia dei dati a riposo e in transito?*
29.	*MIGRAZIONI - BACKUP AZIENDALI - INTEGRAZIONE SOFTWARE DI TERZE PARTI:* *Il servizio di backup aziendale del fornitore di servizi cloud si integra con il software di backup di terze parti di uso comune?*
30.	*MIGRAZIONI - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione migrazioni di cui sopra?* *Esempio:* *Numero massimo di migrazioni simultanee di macchine virtuali* *Numero massimo ordinabile di soluzioni di trasporto dei dati*

8. Fatturazione

	Requisito
1.	*FATTURAZIONE - TRACCIAMENTO E CREAZIONE DI REPORT:* *Il fornitore di servizi cloud offre un servizio di fatturazione con tracciamento e creazione di report per consentire agli utenti di gestire e monitorare l'utilizzo delle offerte cloud attive?*
2.	*FATTURAZIONE - ALLARMI E NOTIFICHE:* *Il fornitore di servizi cloud offre agli utenti un meccanismo per impostare degli allarmi con notifiche per avvisare gli utenti in caso di superamento di una soglia specifica di spesa?*
3.	*FATTURAZIONE - GESTIONE DEI COSTI:*

	Il fornitore di servizi cloud offre un meccanismo per creare e visualizzare un grafico riepilogativo dei costi e delle spese?
4.	*FATTURAZIONE - BUDGET:* *Il fornitore di servizi cloud offre un meccanismo per visualizzare e gestire i budget, e per formulare le previsioni dei costi stimati?*
5.	*FATTURAZIONE - VISUALIZZAZIONE CONSOLIDATA:* *Il fornitore di servizi cloud offre un meccanismo per consolidare la fatturazione di più account in un unico account di pagamento principale?*
6.	*FATTURAZIONE - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla precedente sezione sulla fatturazione?* *Esempio:* *Numero massimo di account che è possibile raggruppare* *Numero massimo di allarmi che è possibile creare* *Numero massimo di budget che è possibile gestire*

9. Attrezzature

	Requisito
1.	*GESTIONE – SERVIZIO DI MONITORAGGIO:* *Il fornitore di servizi cloud offre un servizio di monitoraggio per la gestione delle applicazioni e delle risorse cloud, che svolge attività di raccolta, monitoraggio e creazione di report mediante parametri predefiniti?*
2.	*GESTIONE - ALLARMI:* *Il servizio di monitoraggio del fornitore di servizi cloud consente agli utenti di impostare allarmi?*
3.	*GESTIONE - PARAMETRI PERSONALIZZATI:* *Il servizio di monitoraggio del fornitore di servizi cloud consente agli utenti di creare e monitorare i parametri personalizzati?*
4.	*GESTIONE - GRANULARITÀ DEL MONITORAGGIO:* *Il servizio di monitoraggio del fornitore di servizi cloud fornisce diversi livelli di granularità del monitoraggio, fino al livello di granularità di 1 minuto?*
5.	*GESTIONE - SERVIZIO DI TRACCIAMENTO DELL'API:* *Il fornitore di servizi cloud offre un servizio di registrazione, monitoraggio e archiviazione delle attività in rapporto alle risorse cloud, a livello di console e di interfaccia del programma dell'applicazione (API), per una maggiore visibilità?* • *Se sì, quali sono i servizi offerti dal fornitore di servizi cloud che si integrano con tale servizio di tracciamento?*
6.	*GESTIONE - NOTIFICA:* *Il fornitore di servizi cloud offre la funzionalità di invio delle notifiche sulla base dei livelli di attività delle API?*
7.	*GESTIONE - COMPRESSIONE:*

	Il fornitore di servizi cloud offre un meccanismo di compressione dei registri generati dal sistema di tracciamento dell'interfaccia del programma dell'applicazione (API) per consentire agli utenti di ridurre i costi di archiviazione associati al servizio?
8.	*GESTIONE - AGGREGAZIONE DELLE REGIONI:* *Il fornitore di servizi cloud consente di registrare l'attività dell'API dell'account in tutte le regioni e di distribuire le relative informazioni in maniera aggregata per un utilizzo più semplice?*
9.	*GESTIONE - INVENTARIO DELLE RISORSE:* *Il fornitore di servizi cloud offre un servizio per valutare, controllare e verificare le configurazioni delle risorse implementate da un utente?*
10.	*GESTIONE - MODIFICHE ALLA CONFIGURAZIONE:* *Il fornitore di servizi cloud registra in modo automatico le modifiche alla configurazione delle risorse quando le stesse vengono effettuate?*
11.	*GESTIONE - CRONOLOGIA DELLA CONFIGURAZIONE:* *Il fornitore di servizi cloud offre la possibilità di esaminare la configurazione delle risorse in qualsiasi fase temporale precedente?*
12.	*GESTIONE - REGOLE DI CONFIGURAZIONE:* *Il fornitore di servizi cloud offre linee guida e suggerimenti per il provisioning, la configurazione e il monitoraggio continuo della conformità?*
13.	*GESTIONE - MODELLI DI RISORSE:* *Il fornitore di servizi cloud offre agli utenti le funzionalità di creazione, provisioning e gestione di un gruppo di risorse sulla base di un modello?*
14.	*GESTIONE - REPLICA DEI MODELLI DI RISORSE:* *Il fornitore di servizi cloud offre la possibilità di replicare rapidamente tali modelli di risorse in regioni diverse per il potenziale utilizzo delle stesse nel contesto del ripristino di emergenza?*
15.	*GESTIONE - STRUMENTO DI PROGETTAZIONE DEI MODELLI:* *Il fornitore di servizi cloud offre uno strumento grafico semplice da usare, dotato di funzionalità di trascinamento della selezione per accelerare il processo di creazione di tali modelli di risorse?*
16.	*GESTIONE - CATALOGO DEI SERVIZI:* *Il fornitore di servizi cloud offre un servizio per la creazione e la gestione di un catalogo dei servizi, ovvero server, macchine virtuali, software, database e così via?*
17.	*GESTIONE - ACCESSO ALLA CONSOLE:* *Il fornitore di servizi cloud offre un'interfaccia utente basata sul Web per facilitare la gestione e il monitoraggio dei servizi cloud?*
18.	*GESTIONE - ACCESSO TRAMITE CLI:* *Il fornitore di servizi cloud offre uno strumento unificato per gestire e configurare più servizi cloud dall'interfaccia a riga di comando (CLI), nonché per automatizzare le attività di gestione mediante l'uso di script?*
19.	*GESTIONE - ACCESSO DAI DISPOSITIVI MOBILI:* *Il fornitore di servizi cloud offre un'applicazione per smartphone che gli utenti possono utilizzare per connettersi al servizio cloud e gestire le proprie risorse?* • *Se sì, questa applicazione è disponibile sia per iOS sia per Android?*
20.	*GESTIONE - BEST PRACTICE:*

	Il fornitore di servizi cloud offre un servizio che consente agli utenti di valutare il proprio utilizzo del cloud rispetto alle best practice?
21.	*GESTIONE - LIMITI DEL SERVIZIO:* *Il fornitore di servizi cloud applica delle restrizioni (ovvero limiti del servizio) relativamente alla sezione precedente sulla gestione?* *Esempio:* *Numero massimo di regole di configurazione per account* *Numero massimo di allarmi che è possibile creare* *Numero massimo di registri che è possibile archiviare*

10. Supporto

	Requisito
1.	*SUPPORTO - ASSISTENZA:* *Il fornitore di servizi cloud offre supporto continuativo, 24 ore al giorno, 7 giorni a settimana, 365 giorni all'anno via e-mail, telefono e chat?*
2.	*SUPPORTO - LIVELLI DI SUPPORTO:* *Il fornitore di servizi cloud offre diversi livelli di supporto?*
3.	*SUPPORTO - ALLOCAZIONE DEI LIVELLI:* *Il fornitore di servizi cloud consente agli utenti di assegnare in autonomia le risorse/i servizi utilizzati a diversi livelli di supporto in funzione di una classificazione granulare, senza costringerli a gestire account cloud separati per usufruire di livelli diversi di supporto?*
4.	*SUPPORTO - FORUM:* *Il fornitore di servizi cloud offre ai clienti dei forum di supporto pubblici dove discutere dei problemi?*
5.	*SUPPORTO - PANNELLO DI CONTROLLO SULL'INTEGRITÀ DEI SERVIZI:* *Il fornitore di servizi cloud offre un pannello di controllo sull'integrità dei servizi con le informazioni più aggiornate riguardanti la disponibilità del servizio in più regioni?*
6.	*SUPPORTO - PANNELLO DI CONTROLLO PERSONALIZZATO:* *Il fornitore di servizi cloud offre un pannello di controllo che consente di visualizzare in modalità personalizzata la situazione delle prestazioni e la disponibilità dei servizi sottostanti alle risorse specifiche dell'utente?*
7.	*SUPPORTO - CRONOLOGIA DEL PANNELLO DI CONTROLLO:* *Il fornitore di servizi cloud offre una cronologia di 365 giorni relativa al pannello di controllo sull'integrità dei servizi?*
8.	*SUPPORTO - CONSULENTE CLOUD:* *Il fornitore di servizi cloud offre un servizio che svolge le funzioni di un esperto di cloud personalizzato e aiuta a valutare l'utilizzo delle risorse rispetto alle best practice?*
9.	*SUPPORTO - TAM:* *Il fornitore di servizi cloud offre un Technical Account Manager (TAM) che fornisce consulenza tecnica per l'intera gamma dei servizi cloud?*
10.	*SUPPORTO - SUPPORTO PER APPLICAZIONI DI TERZE PARTI:*

	Il fornitore di servizi cloud offre supporto per i sistemi operativi più diffusi e per i componenti della pila di applicazioni più diffusi?
11.	*SUPPORTO - API PUBBLICA:* *Il fornitore di servizi cloud offre un'API pubblica per l'interazione programmatica con i casi di supporto al fine di creare, modificare e chiudere tali casi?*
12.	*SUPPORTO - DOCUMENTAZIONE DEI SERVIZI:* *Il fornitore di servizi cloud offre documentazioni tecniche di buona qualità, consultabili pubblicamente, per tutti i suoi servizi, comprese, a titolo illustrativo ma non esaustivo, guide per l'utente, tutorial, domande frequenti e note di rilascio?*
13.	*SUPPORTO - DOCUMENTAZIONE CLI:* *Il fornitore di servizi cloud offre documentazioni tecniche di buona qualità, consultabili pubblicamente, per l'interfaccia a riga di comando (CLI)?*
14.	*SUPPORTO - ARCHITETTURE DI RIFERIMENTO:* *Il fornitore di servizi cloud offre una raccolta online gratuita di documenti sull'architettura di riferimento, che siano utili ai clienti per costruire soluzioni specifiche in grado di coniugare molti dei servizi cloud offerti dal fornitore?*
15.	*SUPPORTO - IMPLEMENTAZIONI DI RIFERIMENTO:* *Il fornitore di servizi cloud offre una raccolta online gratuita di documenti contenenti procedure guidate dettagliate, testate e convalidate, comprensive di best practice, per l'implementazione di soluzioni comuni (ovvero DevOps, Big Data, data warehouse, carichi di lavoro Microsoft, carichi di lavoro SAP e così via) nelle sue offerte cloud?*

Appendice B – Valutazione tecnica in tempo reale

Quando si seleziona un CISP, è importante valutare le capacità della piattaforma cloud "in tempo reale", utilizzando i servizi e l'infrastruttura del CISP che sono pubblicamente disponibili. Si consiglia di dedicare almeno 1 giornata intera a ciascun CISP selezionato ai fini della valutazione tecnica. In fase di valutazione è possibile: 1) condurre una valutazione approfondita per stabilire se le capacità dimostrate sono in linea con i requisiti della RDO e con le risposte fornite per iscritto dal CISP; 2) fornire ai propri esperti una piattaforma dedicata alla verifica dettagliata delle competenze del CISP al fine di accertare l'idoneità e l'allineamento delle stesse alle esigenze tecniche e organizzative specifiche dell'ente e 3) acquisire fiducia nei servizi del CISP e nella sua capacità di dimensionare, operare in modo sicuro e resiliente e continuare a innovare per soddisfare le esigenze future.

Quando i CISP rispondono a una RDO di servizi cloud, potrebbero dichiarare la propria conformità sulla base di un'interpretazione generale dei requisiti, che non tiene conto del contesto completo delle esigenze dell'ambiente operativo/delle applicazioni dell'ente. Consigliamo di creare un pannello per la valutazione tecnica in tempo reale composto da esperti di spicco in ambito tecnico, operativo, di sicurezza e delle applicazioni. I valutatori dovrebbero mettere alla prova i CISP durante la valutazione e, a titolo di best practice, dovrebbero assegnare loro un punteggio in modo indipendente, valutando gli scenari su una scala prestabilita, ad esempio da 0 a 4 (0=Inaccettabile, 1=Marginale, 2=Accettabile, 3=Buono , 4=Eccezionale). Successivamente, i punteggi della demo possono essere consolidati, sommando il punteggio medio per ogni scenario di valutazione alla valutazione complessiva del CISP. Gli scenari che registrano un'elevata deviazione dallo standard dovrebbero essere discussi all'interno del team di valutazione prima della finalizzazione della valutazione. Una volta consolidati i punteggi, è possibile applicare una ponderazione basata sulla criticità degli scenari.

In ambito dimostrativo, consigliamo di acquisire una visione integrata della piattaforma del CISP, per poi analizzarla in dettaglio e valutare i carichi di lavoro specifici in esecuzione su di essa. Di seguito è riportato l'esempio di una piattaforma e di una valutazione del carico di lavoro. Gli enti possono partire da questo scenario di riferimento o personalizzarlo per garantire che il CISP selezionato soddisfi i loro specifici requisiti, funzionali e non funzionali. Come best practice, i fornitori a cui è stato fornito l'elenco degli scenari e dei requisiti possono essere autorizzati a proporre un'agenda per la valutazione in tempo reale, che sfrutti al massimo la copertura e dedichi il 20% del tempo a domande e risposte.

Valutazione della piattaforma: diversi CISP hanno adottato il termine "Well Architected", ovvero "ben architettato", per riferirsi a un approccio al cloud che offre un valore ottimale e riduce al minimo i rischi. Gli scenari ben architettati nell'ambito di una dimostrazione tecnica dal vivo possono includere:

1. Sicurezza: identità, governance centralizzata, rilevamento automatico delle minacce, protezione dei dati, preparazione agli eventi
2. Efficienza delle prestazioni: ridimensionamento corretto, scalabilità/elasticità, serverless
3. Affidabilità: disponibilità elevata (resilienza ai guasti), riduzione del rischio associato alle modifiche, ripristino di emergenza, backup
4. Gestione dei costi: operazioni finanziarie, ottimizzazione dei processi aziendali, budget e allocazione dei costi
5. Eccellenza operativa: automazione, monitoraggio, supporto, gestione e capacità necessarie per migrare e operare all'interno del cloud

Valutazione del carico di lavoro: un insieme comune di tipologie di applicazioni dimostrabili comprende:

- Applicazione Web: hosting pubblico di un sito Web dinamico, inclusi database back-end e archiviazione di oggetti statici.

- **Analisi dei dati:** un'architettura data lake o lake house che consente il consolidamento di dati provenienti da diversi fornitori di dati e la capacità di gestire livelli elevati in termini di volume (TB/PB di dati), varietà (dati strutturati, non strutturati, in formati diversi, ecc.) e velocità (tasso di generazione dei dati, modifica e modelli di query).
- **Piattaforma di data science:** una piattaforma che consente lo sviluppo, l'implementazione e l'uso di funzionalità basate su IA/ML all'interno dell'ente.
- **Applicazione IoT:** una piattaforma/capacità IoT che copre il cloud, una funzionalità di rete e i dispositivi.

Per ogni carico di lavoro rappresentativo importante per l'ente, è possibile definire gli scenari che devono essere illustrati dal CISP. Gli scenari dovrebbero dimostrare le capacità complessive che consentono l'implementazione del carico di lavoro in una modalità ben architettata. Le pagine seguenti includono un esempio di criteri di valutazione tecnica in tempo reale riguardanti: 1) la piattaforma del CISP e 2) un carico di lavoro esemplificativo di un'applicazione Web.

Piattaforma – Valutazione tecnica in tempo reale

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Piattaforma Sezione 1	Federazione delle identità	4	Dimostrare la capacità di eseguire la federazione da un archivio identità esistente al servizio cloud.	• Supporto per protocolli standard come SAML. • Supporto per la replica dell'identità basata su SCIM (System for Cross-Domain Identity Management). • La capacità di definire diversi livelli di accesso all'interno dell'archivio identità aziendale e di applicarli all'interno del fornitore di servizi cloud. • La capacità di limitare l'accesso di team/individui specifici solo a determinati account/progetti/carichi di lavoro. • Capacità di supportare il controllo dell'accesso basato sugli attributi (ABAC) e di utilizzare tali attributi all'interno del sistema IAM (Identity and Access Management) del fornitore di servizi cloud per controllare l'accesso alle risorse cloud.
Piattaforma Sezione 2	Governance centrale	4	Dimostrare la capacità di definire policy e requisiti a livello centrale, a livello organizzativo (policy globali), nonché a livello di unità aziendale e progetto.	• La policy dovrebbe includere la possibilità di abilitare/disabilitare i servizi e applicare restrizioni geografiche (limitare le regioni). • Le policy dovrebbero inoltre impedire agli utenti, inclusi gli amministratori, di disabilitare qualsiasi controllo di auditing/governance.
Piattaforma Sezione 3	Limitazione delle autorizzazioni utente	3	Dimostrare l'utilizzo di suggerimenti automatici per il rafforzamento delle autorizzazioni utente.	• Possibilità di confrontare le autorizzazioni attuali con le autorizzazioni richieste. • Generazione automatica di policy per promuovere il privilegio minimo.
Piattaforma Sezione 4	Registrazione di controllo	4	Dimostrare la registrazione del controllo dell'attività cloud, incluse le azioni consentite e non consentite.	• Registri centralizzati per l'intero ente. • Registri specifici dell'account/del progetto per supportare il monitoraggio e la responsabilità di basso livello. • Strumenti per abilitare l'interrogazione dei registri.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
				• Strumenti che consentono l'attivazione di azioni in base a eventi/voci di registro specifici. • Possibilità di visualizzare le attività di supporto del fornitore. • Possibilità di impedire la cancellazione dei registri, anche da parte degli amministratori.
Piattaforma Sezione 5	Isolamento della rete	4	Dimostrare ed evidenziare, ove possibile, l'isolamento di diversi tenant all'interno del cloud. Dimostrare la configurazione di sottoreti isolate (senza connettività), private (senza Internet) e pubbliche (con accesso a Internet).	• Separazione dei tenant, anche su VPN e servizi di connessione incrociata. • Capacità di controllare il flusso di traffico dall'esterno dell'infrastruttura cloud (on-premise), al suo interno e verso Internet. • Modalità di applicazione della separazione quando si utilizzano servizi condivisi come l'hosting di container o la funzione come servizio.
Piattaforma Sezione 6	Crittografia dei dati a riposo	4	Dimostrare la capacità di crittografare i dati a riposo, comprese le opzioni per BYOK e la crittografia lato client.	• Possibilità di richiedere la crittografia dei dati sensibili. • Possibilità di utilizzare chiavi gestite dal fornitore o chiavi gestite dal cliente. • Rispetto dello standard FIPS 140-2. • Possibilità di segnalare e registrare il mancato rispetto dei requisiti di crittografia. • Impatto sui costi aggiuntivi. • Impatto sulle prestazioni. • Supporto per algoritmi quantistici e dimensioni delle chiavi.
Piattaforma Sezione 7	Crittografia dei dati in transito	4	Dimostrare la capacità di crittografare i dati in transito.	• Crittografia di default per le API di servizio. • Possibilità di abilitare la crittografia dei dati in transito (TLS) su bilanciatori del carico e API gestite. • Supporto per l'autenticazione reciproca (client e server).

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Piattaforma Sezione 8	Gestione delle chiavi	4	Dimostrare la capacità di gestione delle chiavi. Includere l'intero ciclo di vita della chiave. Includere l'integrazione con i servizi cloud.	• Creazione di registri, utilizzo, rotazione e distruzione delle chiavi.
Piattaforma Sezione 9	Gestione della configurazione	3	Dimostrare le capacità di gestione della configurazione della piattaforma cloud.	• Mantenimento di un accurato database di gestione della configurazione (CMDB). • Verifica della conformità. • Attivazione automatica di azioni in base alla non conformità. • Capacità di valutare le modifiche alla configurazione rispetto a best practice o regole personalizzate.
Piattaforma Sezione 10	Sicurezza della rete	3	Dimostrare le funzionalità di Firewall per applicazioni Web e Firewall, inclusa l'integrazione con set di regole/firewall di terze parti e protezione dagli attacchi volumetrici.	• Funzionalità WAF (Firewall per applicazioni Web): scalabilità. • Supporto per reti private e pubbliche. • Possibilità di iscriversi a feed di settore/fornitore per set di regole. • Attivazione automatica di azioni all'interno dell'infrastruttura sulla base di eventi dal WAF. • Funzionalità firewall, scalabilità. • Firewall basati su host e firewall basati sulla rete. • Capacità di fare riferimento a gruppi od oggetti logici oltre alla possibilità di specificare i blocchi IP CIDR. • Numero di regole supportate a ogni livello/componente. • Capacità di supportare un modello operativo distribuito (team di rete più team di sviluppo) tramite policy e configurazione di rete.
Piattaforma Sezione 11	Connettività di rete	3	Dimostrare la capacità di connettersi a reti on-premise e dimostrare la capacità	• Connettività privata (larghezza di banda elevata > 10 GB). • Capacità di controllare le policy di routing e firewall in tutto l'ente.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
			degli endpoint/client di connettersi a reti private all'interno del cloud.	• Connettività VPN (da sito a sito e basata su client). • Supporto IPV6.
Piattaforma Sezione 12	Gestione delle istanze	3	Dimostrare le capacità di gestione delle istanze.	• Capacità di monitorare e gestire lo stato delle patch di un grande volume di istanze. • Supporto per la gestione delle patch dei sistemi operativi Linux e Windows. • Capacità di eseguire comandi su una flotta di server senza la necessità di SSH. • Possibilità di verificare e controllare l'accesso remoto alle macchine virtuali in modo centralizzato. • Possibilità di modificare la dimensione di un'istanza, allegare volumi aggiuntivi, modificare la configurazione di rete ecc. tramite console, CLI e API.
Piattaforma Sezione 13	Applicazione delle policy	3	Dimostrare la capacità di configurare i servizi per impedire l'accesso da Internet pubblico.	• Possibilità di isolare il traffico verso la rete privata per i servizi che potrebbero contenere dati essenziali/riservati. • Possibilità di definire policy che controllano l'accesso ai dati in base alla rete di origine. • Applicazione di tali restrizioni di accesso a tutti gli utenti, compresi gli utenti con credenziali di livello elevato.
Piattaforma Sezione 14	Scansione delle vulnerabilità	2	Dimostrare la capacità di eseguire la scansione delle immagini (di container e macchine virtuali) per individuare le vulnerabilità.	• Capacità di eseguire automaticamente la scansione dei container in un registro. • Capacità di eseguire la scansione delle macchine virtuali alla ricerca di vulnerabilità note. • Capacità di eseguire la scansione di rete.
Piattaforma Sezione 15	Ispezione della rete	2	Dimostrare la capacità di acquisire/realizzare una copia speculare (mirroring) del traffico di	• Capacità di realizzare una copia speculare di parte/tutto il traffico all'interno dell'infrastruttura del fornitore di servizi cloud (secondo la prospettiva

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
			rete (NetFlow e pacchetto completo) dall'interno dell'ambiente del cliente.	di tenant del cliente), inclusa l'acquisizione completa dei pacchetti. • Capacità di selezionare semplicemente il traffico che si desidera acquisire. • Possibilità di dimensionamento per supportare volumi di traffico molto elevati (>50 GB/s).
Piattaforma Sezione 16	Rilevamento delle minacce	3	Dimostrare la capacità di rilevamento delle intrusioni nella piattaforma, ad esempio le minacce provenienti da una rete, l'utilizzo delle credenziali e l'analisi dei modelli di utilizzo.	• Capacità di rilevare attività sospette come il "mining". • Capacità di rilevare attacchi di forza bruta all'autenticazione, come gli accessi SSH. • Capacità di rilevare la perdita o l'uso illecito delle credenziali. • Applicazione del machine learning, analisi di un grande numero di eventi e visualizzazione di eventi prioritari. • Impegno nell'abilitare/configurare le risorse (la semplicità è la soluzione migliore). • Capacità di integrarsi con servizi esterni e attivare notifiche. • Capacità di configurare il sistema di rilevamento delle intrusioni (Intrusion Detection System, IDS) a livello globale per tutti i progetti/gli account.
Prestazioni della piattaforma 1	Ottimizzazione del calcolo	2	Dimostrare l'utilizzo di suggerimenti automatici per l'ottimizzazione dei costi della macchina virtuale e della funzione come servizio (FaaS).	• Suggerimenti basati sull'utilizzo effettivo e sui modelli di carico di lavoro. • I suggerimenti includono risparmi stimati e informazioni dettagliate sul livello di carico previsto/le implicazioni tecniche. • Le ottimizzazioni dovrebbero includere sia i risparmi che il "rischio di prestazioni scadenti" laddove le macchine virtuali potrebbero, ad esempio, essere sottodimensionate.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Prestazioni della piattaforma 2	Ottimizzazione dell'ambiente	2	Dimostrare l'utilizzo di suggerimenti automatici per altri componenti cloud, ad esempio bilanciatori del carico, reti, database, archiviazione, ecc.	• I suggerimenti individuano i risparmi e le potenziali opportunità di efficientamento delle prestazioni in altri componenti oltre al calcolo di base.
Prestazioni della piattaforma 3	Scalabilità automatica della capacità di calcolo	4	Dimostrare le capacità di scalabilità automatica di un'applicazione implementata alla base di un bilanciatore del carico in un ambiente di calcolo virtuale. Dimostrare le diverse opzioni/i diversi approcci disponibili e la capacità di attivare altre azioni (facoltative) prima/dopo le operazioni di dimensionamento, ad esempio una notifica.	• Diverse opzioni di approcci relativi al dimensionamento, basati sull'attivazione di altre azioni, pianificati, manuali o più intelligenti che applicano il machine learning per prevedere la capacità richiesta. • Dimensionamento completamente automatizzato, inclusa la registrazione con un bilanciatore del carico e controlli di integrità. • La possibilità di eseguire una parte di codice arbitraria in punti specifici del ciclo di vita del dimensionamento.
Prestazioni della piattaforma 4	Dimensionamento online per l'archiviazione	3	Dimostrare la capacità di dimensionare sia la capacità che la velocità effettiva dell'archiviazione a blocchi senza interruzioni del carico di lavoro.	• Capacità di trasferire l'archiviazione a blocchi tra diversi tipi di archiviazione senza la necessità di ricostruire completamente i servizi. • Capacità di aumentare le dimensioni dei volumi presentati alle macchine virtuali.
Prestazioni della piattaforma 5	Scalabilità automatica per i servizi gestiti	3	Dimostrare la capacità dell'archivio oggetti, del gateway API, della piattaforma FaaS e del database NoSQL di dimensionarsi per supportare da pochi (10) a molti (1000) utenti simultanei.	• Scalabilità automatica senza interruzioni, idealmente senza l'intervento dell'amministratore. • Prestazioni costanti durante un periodo di dimensionamento verso l'alto graduale in linea con i requisiti di dimensionamento della produzione. • Per alcuni componenti, come FaaS, esaminare anche le opzioni per il preriscaldamento e la gestione simultanea dei limiti di esecuzione, se necessario.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Prestazioni della piattaforma 6	Carichi di lavoro basati su container	3	Dimostrare la capacità di ospitare carichi di lavoro basati su container.	• Opzioni per piattaforme di hosting di container. • Integrazione con altri componenti IaaS come i bilanciatori del carico. • Disponibilità di una soluzione di mesh di servizi. • Opzioni non proprietarie per l'hosting di container, come Kubernetes. • Supporto nativo per la disponibilità elevata all'interno del piano di controllo del container. • Capacità di gestire host di container on-premise.
Affidabilità della piattaforma 1	Resilienza regionale	4	Dimostrare il failover automatico di un'istanza di database relazionale all'interno di una regione in caso di simulazione di un guasto localizzato geograficamente (ad esempio un'interruzione di corrente).	• Failover automatico. • Aree di errore isolate all'interno di una regione cloud. • Chiaramente delimitate e semplici da progettare per garantire la disponibilità elevata.
Affidabilità della piattaforma 2	Ripristino automatico dell'istanza	2	Dimostrare la capacità di ripristino automatico di un'istanza/insieme di istanze a seguito di un controllo di integrità non riuscito.	• Controlli di integrità configurabili. • Ripristino/nuovo provisioning dell'istanza completamente automatizzato.
Affidabilità della piattaforma 3	Consapevolezza dell'integrità tramite il bilanciatore del carico	3	Dimostrare come un bilanciatore del carico rileva automaticamente un'istanza difettosa e instrada nuovamente il traffico ad altri host integri.	• Controlli di integrità configurabili. • Routing automatico del traffico verso host integri.
Affidabilità della piattaforma 4	Failover regionale	3	Dimostrare la disponibilità di un'architettura su più regioni, incluso lo spostamento automatico del traffico verso una regione secondaria.	• Controlli di integrità a livello globale. • Opzioni di routing automatizzate: latenza, pesata e failover.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
				• Supporto per carichi di lavoro di macchine virtuali e servizi gestiti come un archivio oggetti/servizio di database NoSQL.
Affidabilità della piattaforma 5	Backup e ripristino	4	Dimostrare le opzioni di backup e ripristino per macchine virtuali, database, servizi gestiti.	• Livello di automazione. • Possibilità di eseguire il ripristino nella stessa/in un'altra regione cloud. • Possibilità di copiare i backup in un'altra regione cloud.
Costi della piattaforma 1	Budget	3	Dimostrare la capacità di gestione del budget; ciò comprende la capacità di strutturarlo per account secondari e progetti.	• Considerare la possibilità di applicare controlli e monitoraggio del budget ai diversi livelli del proprio ente. • Verificare la flessibilità, ad esempio per quanto riguarda la possibilità di raggruppare i componenti (tramite l'assegnazione di tag), impostare budget per servizi cloud specifici e configurare soglie per ricevere avvisi o per scopi di monitoraggio.
Costi della piattaforma 2	Allocazione del budget	1	Dimostrare il provisioning di un nuovo ambiente di progetto (account), compreso il processo di assegnazione del budget per il progetto. Il provisioning dovrebbe includere dei passaggi di approvazione manuale per 1) la Revisione tecnica/IT e 2) la Revisione economico-finanziaria.	• Capacità di provisioning automatico, con le dovute approvazioni. • Configurazione automatizzata dell'impostazione del budget, delle notifiche o dei criteri di budget appropriati per il proprio ente.
Costi della piattaforma 3	Creazione di report sul budget	2	Dimostrare la capacità di creare report sui budget dell'intero ente. Creazione di report indirizzati a un dipartimento specifico anziché all'intero ente (limitatamente alle necessità di conoscenza) I report dovrebbero includere sia i valori di spesa "effettivi" sia i valori di spesa previsti/stimati.	• Capacità di fornire visibilità a diversi livelli dell'ente, creando consapevolezza e trasparenza, fornendo, tuttavia, le informazioni in base alla necessità. • Le previsioni dovrebbero basarsi sulle tendenze di consumo attuali e passate, fornendo un avviso tempestivo in caso di potenziali sforamenti di budget.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Costi della piattaforma 4	Controlli del budget	1	Dimostrare la capacità di intraprendere azioni al raggiungimento di una soglia di budget. Le azioni potrebbero includere l'invio di notifiche, l'applicazione di vincoli o un intervento attivo per prevenire il superamento del budget.	• Capacità di definire azioni in modo semplice per diversi progetti. • Possibilità di variare le azioni da un progetto all'altro, ad esempio, tenendo conto delle implicazioni per lo sviluppo e per la produzione. • Capacità di definire più azioni e soglie per lo stesso budget/progetto. • Possibilità di definire azioni personalizzate oltre alle funzionalità standard.
Costi della piattaforma 5	Periodicità del budget	1	Dimostrare la capacità di applicare budget per diversi periodi di tempo, ad esempio giornalieri/mensili/annuali, ecc. In merito ai budget annuali, dimostrare la capacità di applicare una distribuzione variabile della spesa prevista nel corso dell'anno.	• Capacità di definire budget per diversi periodi di tempo. • Possibilità di configurare una distribuzione della spesa nell'arco dell'anno per i budget annuali: un fattore particolarmente importante per i carichi di lavoro stagionali o altamente elastici, come ad esempio la dichiarazione dei redditi annuale.
Costi della piattaforma 6	Marketplace di terze parti	3	Dimostrare la capacità di acquistare e implementare prodotti di terze parti. Dimostrare la capacità di impostare un budget per una serie di prodotti di terze parti disponibili tramite un marketplace, nonché la capacità di limitare i prodotti disponibili.	• Capacità di impostare un budget per un prodotto specifico, un budget globale e un budget per una serie di progetti/account. • Possibilità di presentare agli utenti cloud solo un sottoinsieme del marketplace più ampio.
Costi della piattaforma 7	Modelli di determinazione del prezzo delle risorse di calcolo	3	Dimostrare i diversi modelli di prezzo/commerciali applicabili alle macchine virtuali.	• Le funzionalità dovrebbero includere prezzi on demand, senza impegno a lungo termine, e granulari (al minuto/all'ora). • Impegni a lungo termine facoltativi in cambio di uno sconto. • Possibilità di acquistare istanze, con la disponibilità ad accettarne l'interruzione in cambio di uno sconto.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
				• In particolare, bisognerebbe dare l'opportunità di combinare tali modelli all'interno dello stesso progetto/account e condividere i vantaggi tra account diversi.
Costi della piattaforma 8	Suggerimenti per l'ottimizzazione dei processi aziendali	3	Dimostrare la capacità di ricevere suggerimenti riguardanti l'ottimizzazione dei processi aziendali al fine di ottimizzare la spesa (senza la necessità di apportare modifiche tecniche).	• Suggerimenti integrati per più servizi, tra cui, ad esempio, macchine virtuali e database gestiti. • Capacità di attuare suggerimenti in modo semplice e comprendere i risparmi/benefici attesi.
Costi della piattaforma 9	Host dedicati	4	Dimostrare la capacità di eseguire il provisioning di un host dedicato per consentire l'uso di licenze on-premise associate a un host specifico.	• Provisioning facile. • Capacità di gestire l'utilizzo dell'host. • La possibilità di condividere l'host tra diversi progetti/diverse locazioni.
Operazioni della piattaforma 1	Migrazione di macchine virtuali	3	Dimostrare l'importazione di una macchina virtuale da on-premise a un servizio di macchina virtuale basato sul cloud.	• Possibilità di importare sistemi operativi basati sia su Windows sia su Linux. • Possibilità di importare più macchine contemporaneamente. • Possibilità di mantenere una sessione di replica per abilitare il "failover" rapido nel cloud.
Operazioni della piattaforma 2	Funzionalità DevOps e di automazione	4	Dimostrare le funzionalità DevOps e di automazione, compresi il modo in cui gli ambienti sono definiti in termini di codice, il supporto da implementazioni completamente automatizzate, i test automatizzati e il ripristino dello stato precedente.	• Capacità di definire tutti i componenti del sistema come codice, inclusi rete, macchine virtuali, archiviazione e database. • Possibilità di creare una pipeline. • Possibilità di creare un repository di codice. • Possibilità di automatizzare le build. • Capacità di eseguire implementazioni blu/verdi. • Possibilità di creare più ambienti e disporre di più fasi per le implementazioni. • Ripristino automatico dello stato precedente per le implementazioni non riuscite

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Operazioni della piattaforma 3	Hosting di applicazioni	2	Dimostrare l'hosting di una semplice applicazione a 2 livelli in un servizio/piattaforma a uso limitato di codice (low-code). Compresi un database relazionale e la scalabilità automatica per il livello dell'applicazione/livello Web.	• Configurazione semplice tramite l'interfaccia utente. • Inclusione di controlli di integrità, dimensionamento, disponibilità elevata. Supporto piattaforma, Windows e Linux.
Operazioni della piattaforma 4	Integrazione della sicurezza	2	Dimostrare le capacità di integrazione della piattaforma dal punto di vista della gestione degli incidenti e degli eventi di sicurezza.	• Capacità di integrare e utilizzare facilmente i registri relativi alla sicurezza del fornitore di servizi cloud e le API per l'integrazione.
Operazioni della piattaforma 5	Integrazione della gestione dei servizi IT	3	Dimostrare le capacità di integrazione della piattaforma dal punto di vista della gestione dei servizi IT (IT Service Management, ITSM).	• Capacità di creare, monitorare e aggiornare un caso di supporto tramite un'API. • Capacità di fornire servizi o set di servizi come "prodotti" tramite un'API.
Operazioni della piattaforma 6	Supporto	4	Dimostrare la propria offerta di assistenza.	• Diversi livelli di assistenza per diversi tipi di carichi di lavoro. • Capacità di offrire assistenza anche per il sistema operativo/motore del database ecc., a seconda dei casi per un determinato servizio. • Capacità di offrire un livello di servizio impeccabile, con responsabili di supporto assegnati ai carichi di lavoro essenziali. • Capacità di offrire un processo strutturato di preparazione agli eventi e di revisione dell'architettura. • Informazioni dettagliate sulla roadmap del fornitore.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Operazioni della piattaforma 7	Possibilità di effettuare verifiche	4	Dimostrare gli strumenti disponibili per supportare le verifiche di conformità.	• Possibilità di ottenere i dettagli delle verifiche di conformità tramite la console. • Capacità di gestire e automatizzare le verifiche degli ambienti.
Operazioni della piattaforma 8	Da macchina virtuale a container	1	Dimostrare la capacità di convertire un'applicazione su una macchina virtuale in un container e di gestirla utilizzando la piattaforma container del fornitore di servizi cloud.	• Facilità d'uso della conversione. • Tempo di conversione. • Supporto piattaforma, .Net e Java.

Carico di lavoro: applicazione Web – Esempio di valutazione tecnica in tempo reale

La sezione seguente fornisce una scheda di valutazione illustrativa di uno specifico carico di lavoro di "Applicazione Web". Quando si sviluppa una scheda di valutazione per una determinata applicazione, si consiglia vivamente di coinvolgere gli utenti, gli sviluppatori e gli amministratori dell'applicazione poiché si tratta delle figure che meglio comprendono i requisiti, le sfide e i vincoli attuali.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Sezione Web 1	Sicurezza: protezione dell'applicazione	3	Dimostrare la capacità di bloccare i tentativi dannosi e di impedire l'utilizzo dell'applicazione tramite SQL injection, attacchi di scripting XSS e altri attacchi.	• Funzionalità pronte all'uso per la protezione dagli attacchi comuni mediante regole/capacità standard. • Capacità di creare regole/funzioni/controlli personalizzati.
Sezione Web 2	Sicurezza: protezione	3	Dimostrare la capacità di bloccare/proteggere da attacchi che comportano tassi di richiesta elevati o volumi di dati diretti a un'applicazione.	• Possibilità di configurare limiti e limitare i tassi di richiesta da un determinato indirizzo IP o elenco di indirizzi.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
	basata sul tasso di richieste			
Sezione Web 3	Sicurezza: protezione basata sulla fonte	3	Dimostrare la capacità di limitare l'accesso in base alla rete o alla provenienza geografica.	• Possibilità di limitare l'accesso tramite blocco di rete o un elenco di blocchi di rete. • Possibilità di limitare l'accesso in base al Paese di origine (senza la necessità di gestire elenchi di indirizzi IP).
Sezione Web 4	Sicurezza: segmentazione della rete	4	Dimostrare la capacità di proteggere o isolare i componenti (server Web, server app/server DB) per proteggerli dalla propagazione nord-sud ed est-ovest attraverso l'infrastruttura.	• Possibilità di posizionare i componenti in diverse sottoreti e di controllare il flusso di traffico tra diverse sottoreti. • Capacità di controllare il flusso di traffico a livello di interfaccia di rete. • Capacità di fare riferimento a gruppi logici e blocchi CIDR.
Sezione Web 5	Sicurezza: supporto TLS e gestione dei certificati	4	Dimostrare la capacità di fornire un endpoint protetto con TLS e gestire automaticamente i componenti di supporto per fornire lo stesso, compresa, ad esempio, la rotazione automatica dei certificati.	• Supporto per i protocolli TLS più recenti e possibilità di disabilitare le versioni legacy, se necessario. • Generazione, gestione e rotazione dei certificati in modo semplice (e, idealmente, in modo completamente automatizzato).
Prestazioni Web 1	Prestazioni: scalabilità	4	Dimostrare la capacità di dimensionare in un range compreso tra 10 e 100.000 utenti simultanei dell'applicazione Web, attraverso la scalabilità automatica dinamica.	• Capacità di definire regole di dimensionamento pianificate e basate sull'attivazione di altre azioni. • Dimensionamento senza interruzioni per l'utente finale e l'amministratore. Dimensionamento orizzontale automatico quando il carico aumenta e dimensionamento verticale quando il carico diminuisce. • Assicurarsi che vi sia la scalabilità a ogni livello dell'applicazione Web (bilanciatore del carico, livello Web, livello dati ecc.).

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
				• La disponibilità dei servizi di memorizzazione nella cache a diversi livelli dell'applicazione, a seconda delle esigenze.
Prestazioni Web 2	Prestazioni: distribuzione globale	3	Dimostrare la capacità della CDN, inclusa la dimostrazione della latenza da diversi punti in tutto il mondo, tra cui: Australia, Asia, Africa, Medio Oriente, Nord America, Sud America ed Europa.	• Possibilità di creare e configurare una CDN attraverso la console o le API del CISP. • Regole di distribuzione configurabili per diverse aree geografiche. • Caching configurabile per diversi casi d'uso/applicazioni.
Affidabilità del Web 1	Affidabilità: resilienza in un'unica regione	4	Dimostrare la capacità di tollerare un evento localizzato, come una perdita di connettività di rete al data center del CISP.	• Failover automatico e disponibilità elevata all'interno di una regione cloud (Città).
Affidabilità del Web 2	Affidabilità: implementazione in più regioni	3	Dimostrare l'implementazione di un'applicazione Web in più regioni, incluso un database replicato a livello globale.	• Possibilità di implementare un'applicazione in più regioni in forma programmatica. • Replica tra le regioni per l'archivio dati. • Routing automatico degli utenti alla loro regione ottimale.
Affidabilità del Web 3	Affidabilità: failover in più regioni	3	Dimostrare la capacità di failover automatico di un'applicazione Web in caso di problemi di servizio con impatto regionale.	• Failover automatico e disponibilità elevata su più regioni cloud.
Costo del Web 1	Costo: visibilità	2	Dimostrare la capacità di monitorare il costo per applicazione	• Possibilità di visualizzare la cronologia dei costi rispetto a un'applicazione specifica, anche con l'aumento e la diminuzione delle risorse.
Costo del Web 2	Costo: budget	2	Dimostrare la capacità di predisporre budget e avvisi correlati per applicazione.	• Budget configurati per applicazione e possibilità di attivare azioni/avvisi sulla base di soglie configurate.

ID scenario	Nome scenario	Criticità (1=Livello basso, 4=Livello critico)	Requisiti dimostrativi	Considerazioni per l'assegnazione del punteggio
Operazioni Web 1	Operazioni: finestre di manutenzione	3	Dimostrare la capacità di configurare delle finestre di manutenzione allineate ai requisiti aziendali, specialmente nei casi in cui la manutenzione può influire sulla disponibilità delle applicazioni.	• Finestre di manutenzione configurabili per componenti quali un servizio di database relazionale.
Operazioni Web 2	Operazioni: registrazione	3	Dimostrare la capacità di centralizzare la registrazione di un'applicazione con più componenti, inclusa la persistenza dei registri in caso di chiusura o guasto delle macchine virtuali.	• Possibilità di configurare un servizio di registrazione centralizzato in grado di adattarsi ai requisiti dell'applicazione. • Possibilità di definire regole/filtri per attivare avvisi o azioni in base a registri eventi specifici.
Operazioni Web 3	Operazioni: monitoraggio	3	Dimostrare la capacità di monitorare l'applicazione, comprese le prestazioni, la disponibilità, i tempi di risposta, il conteggio degli errori, ecc. e la funzionalità per intraprendere azioni e attivare notifiche in base a diverse soglie di parametri.	• Una raccolta di parametri standard disponibili come I/O su disco, CPU, parametri del database, rete, bilanciatore del carico ecc. • Possibilità di definire parametri e soglie personalizzate. • Possibilità di creare un pannello di controllo personalizzato per rappresentare i parametri più importanti e condividere tali pannelli di controllo con gli utenti pertinenti.