

AS SDAPA PER L'ACQUISIZIONE DI SERVIZI CLUOD IAAS E PAAS EROGATI DAL CLOUD PUBBLICO MICROSOFT AZURE PER IL PROGETTO IDEA@PA DI CDC

CAPITOLATO TECNICO



INDICE

1.	GLOSSARIO, ACRONIMI E TERMINOLOGIA	3
2.	PREMESSA	5
3.	INTRODUZIONE	5
4.	DEFINIZIONE DEL FABBISOGNO	5
5.	OGGETTO, DURATA E CONTESTO TECNOLOGICO	6
5.1.	Oggetto	7
5.2.	Durata	14
5.3.	Contesto Tecnologico	15
5.4.	Servizi Cloud Computing IaaS	15
5.4.1.	IaaS: Servizi di Elaborazione (compute instance)	15
5.4.2.	IaaS: Servizi di Archiviazione (storage)	18
5.4.3.	IaaS: Virtual Appliance	20
5.4.4.	IaaS: VPN Gateway	21
5.4.5.	IaaS: Connettività dedicata per VPN	21
5.4.6.	IaaS: IP Pubblici	22
5.4.7.	IaaS: Traffico in Uscita (outbound)	22
5.5.	Servizi Cloud Computing PaaS	22
5.5.1.	Macro categorie del catalogo dei servizi	23
5.5.2.	Servizi di Piattaforma a Supporto Gestione IaaS	24
5.5.3.	Servizi di Piattaforma abilitanti al cloud native	26
6.	EROGAZIONE DEI SERVIZI	29
6.1.	Consegna in gestione	30
6.2.	Requisiti di qualità	30
6.3.	Responsabile della fornitura	30
7.	ESECUZIONE DELLA FORNITURA	31
7.1.	Modalità di esecuzione della fornitura	31
7.1.1.	Modalità di erogazione continuativa	31
7.1.2.	Livelli di servizio	32
7.2.	Pianificazione e Consuntivazione	32
7.3.	Verifica di conformità	32
7.4.	Azioni contrattuali	33
7.5.	Exit strategy e Grace period	33



1. GLOSSARIO, ACRONIMI E TERMINOLOGIA

GLOSSARIO

Amministrazione o Committente	Società Generale d'Informatica S.p.A. o Sogei, Corte dei conti o Cdc.
Consip	La società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato.
Impresa o Fornitore	La società affidataria della presente procedura negoziata
Contratto	Il contratto che verrà stipulato tra la Amministrazione e Documento dove sono enunciate le regole giuridiche alle quali si dovrà conformare la fornitura.
Fornitura	Il complesso dei servizi IaaS e PaaS offerti e le attività descritte nel presente documento tecnico.
Malfunzionamento	Qualsiasi anomalia funzionale del software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso.
Responsabile della Fornitura	La persona individuata dall'Impresa come interlocutore dell'Amministrazione e responsabile di tutte le attività contrattuali.
Giorni e Ore	Nella documentazione per giorno e ora si intendono rispettivamente giorno lavorativo e ora lavorativa; l'orario previsto per la fornitura è dalle 8,00 alle 18,00 dal lunedì al venerdì.

ACRONIMI

Cdc	Corte dei conti
MEF	Ministero Economia e Finanze
MAC	Manutenzione Correttiva
MEV	Manutenzione Evolutiva

TERMINOLOGIA

Accettazione	Validazione dei prodotti finali di fornitura.
Approvazione	Validazione dei prodotti intermedi di fornitura, previa verifica di merito.
Assistenza	Supporto da parte di risorse professionali del fornitore ad attività di gestione dell'esercizio e di assistenza agli utenti.
Attivazione	Comunicazione di nuove esigenze, quindi della partenza di un nuovo task.
Attività	Quota parte di un servizio contrattuale, omogenea per tipologia, alla quale si applica una ben definita modalità di esecuzione.
Autorizzazione	Assenso a procedere con le attività sul singolo task, secondo la stima e la pianificazione proposte dal fornitore.

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



Consegna

Rilascio dei prodotti di fornitura, sia intermedi che finali.

Difetto

Errore presente sull'applicazione, latente finché non rilevato, la cui rimozione è a carico della manutenzione correttiva.

Modalità di esecuzione

Complesso di regole e clausole che regolano la prestazione dei servizi e delle attività oggetto della fornitura.

Task

Una o più attività o interventi volta a soddisfare specifiche esigenze dell'Amministrazione.



2. PREMESSA

Il Fornitore prende atto che, con delibera n. 15/50, del 23 febbraio 2015, la Commissione di garanzia dell'attuazione della legge sullo sciopero, in relazione alla funzione assolta dalla Sogei, definita "infrastruttura critica informatica di interesse nazionale" dal Decreto del Ministero dell'Interno del 9 gennaio 2008, ha stabilito che la stessa "si può inquadrare nella categoria dei soggetti attivi, la cui attività istituzionale è finalizzata allo svolgimento della funzione fiscale. Tale attività presenta un carattere essenziale nell'attuale sistema di fiscalità di massa, in quanto strumentale alla fase dei controlli e dell'istruttoria tributaria, con l'obiettivo di assumere informazioni ed acquisire elementi di prova rispetto al comportamento dei contribuenti. Per tale motivo, l'attività della SOGEI S.p.A. può essere qualificata come servizio strumentale a sostenere l'agire amministrativo per il migliore perseguimento degli obiettivi di efficienza ed efficacia della funzione fiscale. L'eventuale interruzione del servizio da parte della SOGEI S.p.A. potrebbe determinare effetti negativi in relazione all'erogazione di un servizio pubblico (corrispondente alla fase di attuazione delle prestazioni fiscali), con possibili ricadute anche nei confronti dei cittadini".

La Sogei è responsabile del corretto funzionamento dei sistemi informatici utilizzati dalle Amministrazioni per lo svolgimento di tali attività, intervenendo all'occorrenza, in tempo reale, per sanare eventuali interruzioni e/o malfunzionamenti di tali sistemi attraverso la conduzione tecnico-operativa continuata ed una corretta manutenzione degli stessi;

Con Deliberazione n. 18/159 pubblicata, come previsto per legge, sulla Gazzetta Ufficiale della Repubblica Italiana nonché sul sito internet della Commissione di garanzia, adottata nella seduta del 10 maggio 2018 la Commissione ha adottato la Regolamentazione da applicare alle astensioni collettive dalle prestazioni, a fini di protesta o di rivendicazioni di categoria, del personale dipendente della Società Sogei S.p.A. prevedendo le prestazioni indispensabili da garantire in caso di sciopero, nonché le modalità e le procedure di erogazione delle stesse, conformemente a quanto previsto dagli articoli 2, comma 2, e 13, comma 1, lett. a), della legge n. 146 del 1990, e successive modificazioni.

3. INTRODUZIONE

Il presente capitolato è parte integrante della documentazione della presente procedura e definisce le caratteristiche e i requisiti richiesti per l'acquisizione di servizi Cloud IaaS e PaaS erogati dal Cloud pubblico di Microsoft Azure per il progetto IDEA@PA di Cdc.

Le condizioni di cui al presente documento, gli atti e i documenti ivi richiamati, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del Contratto.

Le prescrizioni del presente capitolato rappresentano i requisiti minimi dell'affidamento.

4. DEFINIZIONE DEL FABBISOGNO

La Corte dei conti e gli istituti associati al programma IDEA@PA (CNEL, Avvocatura dello Stato e Team Digitale) dispongono di sottoscrizioni nel Cloud pubblico (Microsoft Azure) utilizzate per erogare servizi

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



IaaS, PaaS e SaaS ad utenti interni ed a quelli di altre Amministrazioni. L'infrastruttura è integrata con i servizi trasversali e applicativi erogati dalla componente "tradizionale" del CED. In particolare, l'accesso da rete esterna e l'autenticazione alle "nuvole" sono garantiti dalle infrastrutture comuni a tutti i servizi.

La componente tradizionale del CED (sistemi on premise) è ad oggi nettamente inferiore, per numero e per importanza dei servizi, rispetto a quella attiva nel cloud pubblico.

Inoltre, la Corte dei conti ha realizzato una soluzione DR dei sistemi on premise su infrastrutture Cloud (Azure) e in alcuni casi (Team Digitale) i servizi Cloud sono utilizzati in modo esclusivo per la realizzazione di specifici servizi (App IO, DAF).

Nell'ambito del piano di trasformazione digitale intrapreso dalla Corte dei conti e dagli Istituti associati, infatti, è stato previsto che tutte le iniziative progettuali utilizzino esclusivamente servizi PaaS e SaaS evitando, ove possibile, altre soluzioni legate al paradigma IaaS, attraverso l'acquisizione di servizi Cloud da utilizzare per la realizzazione di sistemi moderni e per la definitiva dismissione delle componenti IT tradizionali.

In linea con le previsioni AgID si considera di riferimento il Modello Cloud della PA, nel quale è possibile individuare i servizi Cloud e CSP qualificati, consultabili mediante il Cloud Marketplace, suddivisi in IaaS, PaaS e SaaS.

Nella definizione dei servizi Cloud da acquisire, è necessario mantenere un legame con un specifico service provider, nel caso di specie Microsoft Azure, per le forti dipendenze tecnologiche venutesi a creare tra lo sviluppo applicativo custom e le interfacce di alcuni servizi PaaS (Azure Search, Azure API Gateway, MS SQL, Azure Cache, ecc.), il cui adeguamento richiede ingenti investimenti economici e, soprattutto, interventi progettuali della durata di circa 12-18 mesi.

5. OGGETTO, DURATA E CONTESTO TECNOLOGICO

L'iniziativa di acquisizione ha per oggetto servizi Cloud IaaS e PaaS del Cloud pubblico Microsoft Azure volti a soddisfare le seguenti esigenze:

- migrazione dei workload applicativi tradizionali da infrastrutture IT del programma IDEA@PA, eserciti nel Data Center sorgente in via Carucci a Roma, da trasferire su Sito Cloud che assumerà il ruolo di sito Primario per l'erogazione di tali servizi applicativi (nel seguito Sito Cloud Primario), e creazione ambiente disaster recovery su altro Sito Cloud che assumerà ruolo di sito Secondario (nel seguito Sito Cloud Secondario);
- continuità dei workload cloud-native delle applicazioni Mission Critical già realizzate ovvero in corso di realizzazione, attraverso servizi PaaS (Microsoft Azure);
- sviluppo di nuovi workload cloud-native, su Sito Cloud Primario.



5.1. Oggetto

L'oggetto dell'esigenza espressa da Cdc, riguarda l'acquisizione di servizi del Cloud Pubblico Microsoft Azure, elencati nella successiva tabella che dettaglia la composizione di ogni singola unità elementare elaborativa mensile denominata SKU. La denominazione del servizio di riferisce ad una descrizione "commerciale", talvolta tradotta in italiano che potrebbe essere suscettibile di cambiamenti in funzione di strategie commerciali o di aggregazione con altri servizi.

CATEGORIA	SERVIZIO	Tipologia
Analisi		
	Azure Databricks	PaaS
	Piattaforma analitica veloce e collaborativa basata su Apache Spark	
	Analisi di flusso di Azure	PaaS
	Elaborazione dei flussi di dati in tempo reale da milioni di dispositivi IoT	
	SQL Data Warehouse	PaaS
	Data warehouse elastico distribuito come servizio con funzionalità di livello aziendale	
	Data Factory	PaaS
	Integrazione dei dati ibrida semplificata su scala aziendale	
	Data Lake Analytics	PaaS
	Servizio di analisi distribuito che semplifica l'uso di Big Data	
	Hub eventi	PaaS
	Gestione dati di telemetria da milioni di dispositivi	
	Power BI Embedded	PaaS
	Integrazione delle visualizzazioni interattive dei dati	
	Azure Analysis Services	PaaS
	Motore di analisi di livello aziendale come servizio	
	R Server per HDInsight	PaaS
	Analisi predittiva, Machine Learning e modellazione statistica per Big Data	
	Data Catalog	PaaS
	Realizza valore maggiore dalle tue risorse dati aziendali	
	Azure Data Lake Storage	PaaS
	Funzionalità di Data Lake Storage sicura con scalabilità elevatissima basata sull'archiviazione BLOB di Azure	
	Esplora dati di Azure	PaaS
	Servizio veloce e a scalabilità elevata per l'esplorazione dei dati	
	Condivisione dati di Azure	PaaS
	Servizio sicuro per la condivisione di Big Data con organizzazioni esterne	
Archiviazione		
	Account di archiviazione	IaaS
	Archiviazione cloud duratura, a disponibilità elevata ed estremamente scalabile	
	Backup di Azure	PaaS
	Aumenta la sicurezza dei dati e proteggiti dagli attacchi ransomware	
	StorSimple	IaaS
	Soluzione di archiviazione cloud ibrida aziendale	
	Azure Data Lake Storage	PaaS

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Funzionalità di Data Lake Storage sicura con scalabilità elevatissima basata sull'archiviazione BLOB di Azure	
	Archiviazione BLOB	PaaS
	Archiviazione di oggetti basata su REST per dati non strutturati	
	Archiviazione su disco	IaaS
	Opzioni su disco persistenti e sicure che supportano le macchine virtuali	
	Managed Disks	IaaS
	Archiviazione su disco persistente e sicura per le macchine virtuali di Azure	
	Archiviazione code	PaaS
	Scalabilità efficace delle app in base al traffico	
	Archiviazione file	PaaS
	Condivisioni file che usano il protocollo SMB 3.0 standard	
	Data Box	IaaS
	Appliance e soluzioni per il trasferimento dei dati ad Azure ed edge computing	
	Cache HPC di Azure	PaaS
	Memorizzazione nella cache dei file per HPC (High Performance Computing)	
	Spazio di archiviazione	IaaS
	Archiviazione di dati ad accesso sporadico	
	Storage Explorer	PaaS
	Esplorazione delle risorse di Archiviazione di Azure e interazione con esse	
	Azure NetApp Files	PaaS
	Condivisioni file di Azure di livello aziendale con tecnologia NetApp	
	Condivisione dati di Azure	PaaS
	Servizio per la condivisione di Big Data con organizzazioni esterne	
Blockchain		
	Servizio Azure Blockchain	PaaS
	gestione e sviluppo delle reti blockchain per consorzi	
	Azure Blockchain Workbench	PaaS
	Sviluppo prototipi di app blockchain sul cloud	
	App per la logica	PaaS
	Automatizza l'accesso e l'uso dei dati tra cloud senza scrivere codice	
	Azure Cosmos DB	PaaS
	Database multimodello distribuito a livello globale a qualsiasi livello di scalabilità	
Calcolo		
	Macchine virtuali	IaaS
	Provisioning di macchine virtuali Windows e Linux	
	Batch	PaaS
	Pianificazione dei processi e gestione dei calcoli di livello cloud	
	SQL Server nelle macchine virtuali	IaaS
	Esecuzione app SQL Server aziendali nel cloud	
	Servizi cloud	PaaS
	Sviluppo applicazioni cloud e API scalabili a elevata disponibilità	
	Funzioni di Azure	PaaS
	Elabora eventi con codice senza server	
	Set di scalabilità di macchine virtuali	IaaS

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Gestione automatizzata di macchine virtuali Linux e Windows	
	Host dedicato di Azure	IaaS
	Server fisico dedicato per ospitare le tue macchine virtuali di Azure per Windows e Linux	
	Desktop virtuale Windows	IaaS
	La migliore esperienza di desktop virtuale, disponibile in Azure	
Container		
	Servizio Azure Kubernetes	PaaS
	Servizio per la distribuzione, la gestione e le operazioni di Kubernetes	
	Service Fabric	PaaS
	Sviluppo di microservizi e orchestrazione di contenitori in Windows o Linux	
	Istanze di Container	PaaS
	Esecuzione dei contenitori in Azure senza gestire server	
	Funzioni di Azure	PaaS
	Elaborazione eventi con codice senza server	
	Registro Container	PaaS
	Archiviazione e gestione delle immagini dei contenitori in tutti i tipi di distribuzione di Azure	
	App Web per contenitori	PaaS
	Distribuzione ed esecuzione delle App Web in contenitori che si adattano alle dimensioni del business	
	Azure Red Hat OpenShift	PaaS
	Servizio OpenShift completamente gestito, fornito in collaborazione con Red Hat	
Contenuti multimediali		
	Servizi multimediali	PaaS
	Codifica, archiviazione e distribuzione in streaming di audio e video scalabili	
	Codifica	PaaS
	Codifica cloud di livello professionale	
	Streaming live e on demand	PaaS
	Distribuzione contenuti in tutti i dispositivi con la scalabilità necessaria per le tue esigenze aziendali	
	Azure Media Player	PaaS
	Lettore per tutte le esigenze di riproduzione	
	Protezione del contenuto	PaaS
	Distribuzione dei contenuti con AES, PlayReady, Widevine e Fairplay	
	Analisi Servizi multimediali	PaaS
	Analisi approfondite dai file video con i servizi di riconoscimento vocale e visivo	
	Indicizzatore video	PaaS
	Informazioni dettagliate per i video	
Database		
	SQL Server nelle macchine virtuali	IaaS
	SW app SQL Server aziendali nel cloud	
	Database SQL di Azure	PaaS
	SQL gestito intelligente sul cloud	
	Azure Cosmos DB	PaaS

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Database multimodello distribuito a livello globale a qualsiasi livello di scalabilità	
	Cache Redis di Azure	PaaS
	Integrazione per le applicazioni bassa latenza e velocità effettiva elevata	
	Estensione database di SQL Server	PaaS
	Estensione in modo dinamico dei database di SQL Server locali in Azure	
	Archiviazione tabelle	PaaS
	Archivio chiave-valore NoSQL con set di dati semi strutturati	
	Database di Azure per PostgreSQL	PaaS
	Un servizio di database PostgreSQL gestito per gli sviluppatori di app	
	Database di Azure per MySQL	PaaS
	Un servizio di database MySQL gestito per gli sviluppatori di app	
	Azure Database Migration Service	PaaS
	Servizio per semplificare la migrazione dei database locali al cloud	
	Database SQL di Azure Edge	PaaS
	Motore dati con footprint ridotto e ottimizzato per dispositivi perimetrali con intelligenza artificiale integrata	
DevOps		
	Azure DevOps	PaaS
	Servizi per i team per condividere codice, tenere traccia del lavoro e fornire software	
	Azure Pipelines	PaaS
	Distribuzione SW automatizzata in qualsiasi piattaforma e cloud	
	Azure Boards	PaaS
	Pianificazione verifica e analisi del lavoro in diversi team	
	Azure Repos	PaaS
	Ottieni repository Git privati, ospitati sul cloud e senza limitazioni per il tuo progetto	
	Azure Artifacts	PaaS
	Creazione gestione e condivisione di pacchetti nel team	
	Azure Test Plans	PaaS
	Test e distribuzione con un toolkit per testing esplorativo e manuale	
	Azure DevTest Labs	PaaS
	Creazione di ambienti con elementi e modelli riutilizzabili	
	Integrazione con gli strumenti per DevOps	PaaS
	Integrazione degli strumenti DevOps preferiti con Azure	
	Monitoraggio di Azure	PaaS
	Visibilità completa su applicazioni, infrastruttura e rete	
Dispositivi mobili		
	Servizio app	PaaS
	Realizzazione app cloud potenti per il Web e per i dispositivi mobili	
	Hub di notifica	PaaS
	Invio di notifiche push a qualsiasi piattaforma da qualsiasi back-end	
	Gestione API	PaaS
	Pubblicazione API per sviluppatori, partner e dipendenti in modo sicuro e scalabile	
	App per dispositivi mobili di Azure	PaaS
	Strumenti di connessione ad Azure, sempre e ovunque	

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Visual Studio App Center	PaaS
	Esecuzione test, rilascio e monitoraggio delle pp	
	App Web per contenitori	PaaS
	Soluzione per distribuire ed eseguire con app Web in contenitori	
Gestione e governance		
	Backup di Azure	PaaS
	Sicurezza dei dati e protezione dagli attacchi ransomware	
	Azure Site Recovery	PaaS
	Servizio predefinito per il ripristino di emergenza (Disaster Recovery)	
	Azure Advisor	PaaS
	Il tuo motore di raccomandazione di procedure consigliate per Azure personalizzato	
	Utilità di pianificazione	PaaS
	Esecuzione di processi in base a una pianificazione semplice o complessa	
	Automazione	PaaS
	Gestione del cloud grazie all'automazione dei processi	
	Gestione traffico	PaaS
	Instradamento del traffico in arrivo per prestazioni e disponibilità elevate	
	Monitoraggio di Azure	PaaS
	Servizio per la visibilità completa su applicazioni, infrastruttura e rete	
	Network Watcher	PaaS
	Soluzione di monitoraggio e diagnostica delle prestazioni di rete	
	Integrità dei servizi di Azure	PaaS
	Indicazioni personalizzate e supporto tecnico in caso di impatto dei problemi dei servizi di Azure sulle attività	
	Portale di Microsoft Azure	PaaS
	Gestione e monitoraggio di tutti i prodotti Azure in una sola console unificata	
	Azure Resource Manager	PaaS
	Semplifica la gestione delle risorse della tua app	
	Cloud Shell	PaaS
	Amministrazione di Azure con una shell basata sul browser	
	Criteri di Azure	PaaS
	Implementa la governance e gli standard aziendali su larga scala per le risorse di Azure	
	Gestione dei costi	PaaS
	Gestione e ottimizzazione dei costi per il cloud	
	Azure Migrate	PaaS
	Individuazione, valutazione, dimensionamento e migrazione facile delle macchine virtuali locali ad Azure	
	Azure Blueprint	PaaS
	Creazione rapida e ripetibile di ambienti regolamentati	
Identità		
	Azure Active Directory	PaaS
	Servizio per la gestione delle identità degli utenti e gli accessi, strumenti di protezione avanzate tra dispositivi, dati, app infrastruttura di directory locali e abilitazione di Single Sign-On	
	Azure Active Directory Domain Services	PaaS
	Servizi di dominio senza controller di dominio	

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Azure Active Directory B2C	PaaS
	Gestione di identità e accessi degli utenti nel cloud	
Integrazione		
	Griglia di eventi	PaaS
	Gestione eventi affidabile su larga scala	
	App per la logica	PaaS
	Automazione per l'accesso e l'uso dei dati tra cloud senza scrivere codice	
	Gestione API	PaaS
	Pubblicazione API per sviluppatori, partner e dipendenti in modo sicuro e scalabile	
	Service BUS	PaaS
	Connessione tra ambienti cloud privati e pubblici	
Intelligenza artificiale + Machine Learning		
	Servizio Azure Bot	PaaS
	Servizio bot intelligente senza server con scalabilità on demand	
	Azure Databricks	PaaS
	Piattaforma analitica veloce e collaborativa basata su Apache Spark	
	Azure Search	PaaS
	Servizio di ricerca cloud basato su intelligenza artificiale per sviluppo di app per dispositivi mobili e Web	
	Servizi cognitivi	PaaS
	Funzionalità API intelligenti per consentire le interazioni contestuali	
	Servizio di Azure Machine Learning	PaaS
	Piattaforma attendibile, scalabile e completa con gestione di modelli e sperimentazioni machine learning	
	Machine Learning Studio	PaaS
	Sviluppo, distribuzione e gestione delle soluzioni analitiche predittive	
Migrazione		
	Azure Database Migration Service	PaaS
	Servizi per la migrazione dei database locali al cloud	
	Azure Migrate	PaaS
	Individuazione, valutazione, dimensionamento e migrazione delle macchine virtuali locali ad Azure	
	Data Box	IaaS
	Appliance e soluzioni per il trasferimento dei dati ad Azure ed edge computing	
Rete		
	Rete per la distribuzione di contenuti	PaaS
	Distribuzione di contenuti sicura e affidabile con ampia copertura globale	
	DNS di Azure	PaaS
	Configurazione Dominio DNS in Azure	
	Rete virtuale	IaaS
	Provisioning di reti private e connessione facoltativa a data center locali	
	Gestione traffico	PaaS
	Instradamento del traffico in arrivo con prestazioni e disponibilità elevate	
	Bilanciamento del carico	IaaS
	Disponibilità elevata e prestazioni di rete per le applicazioni	

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Gateway VPN	IaaS
	Servizio per la connessione cross-premise sicura	
	Gateway applicazione	IaaS
	Realizzazione front-end Web sicuri, scalabili e a disponibilità elevata in Azure	
	Protezione DDoS di Azure	PaaS
	Protezione per le applicazioni da attacchi Distributed Denial of Service (DDoS)	
	Rete WAN virtuale	PaaS
	Configurazione e automatizzazione della connettività da ramo a ramo tramite Azure	
	Frontdoor di Azure	PaaS
	Punto di distribuzione scalabile e ottimizzato per la sicurezza per applicazioni Web basate su microservizi globali	
	Azure Bastion	PaaS
	Accesso RDP ed SSH privato e completamente gestito alle macchine virtuali	
Sicurezza		
	Key Vault	PaaS
	Protezione delle chiavi e altri dati segreti	
	Centro sicurezza	PaaS
	Centralizza la gestione della sicurezza e abilita la protezione avanzata dalle minacce nei carichi di lavoro cloud ibridi	
	Azure Sentinel	PaaS
	Servizi di analisi della sicurezza intelligenti per l'intera organizzazione	
	Firewall di Azure	PaaS
	Funzionalità di firewall native con disponibilità elevata incorporata, scalabilità cloud senza limiti e nessuna manutenzione	
Strumenti per sviluppatori		
	Visual Studio	PaaS
	Ambiente avanzato e flessibile per lo sviluppo di applicazioni sul cloud	
	Visual Studio Code	PaaS
	Editor di codice leggero e avanzato per lo sviluppo cloud	
	SDK	PaaS
	SDK e strumenti da riga di comando necessari	
	Azure DevOps	PaaS
	Servizi per i team per condividere codice, tenere traccia del lavoro e fornire software	
	Interfacce della riga di comando	PaaS
	Creazione, distribuzione, diagnosi e gestione di app e servizi scalabili multiplatforma	
	Azure Pipelines	PaaS
	Automazione test e distribuzione continua del SW in qualsiasi piattaforma e cloud	
	Azure Lab Services	PaaS
	Configurazione lab per formazione, per prove, sviluppo test e altri scenari	
	Azure DevTest Labs	PaaS
	Creazione ambienti con elementi e modelli riutilizzabili	
	Integrazioni con gli strumenti per sviluppatori	PaaS

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



	Strumenti per lo sviluppo tra cui Eclipse, IntelliJ e Maven, integrati con Azure	
	Configurazione app	PaaS
	Archiviazione di parametri veloce e scalabile per la configurazione di app	
Web		
	App Web	PaaS
	Realizzazione App Web mission critical su vasta scala	
	App per dispositivi mobili	PaaS
	Sviluppa e ospita il back-end per qualsiasi app per dispositivi mobili	
	App per le API	PaaS
	Crea e usa facilmente API cloud	
	Servizio app	PaaS
	Realizzazione app cloud i per il Web e per i dispositivi mobili	

5.2. Durata

La durata contrattuale prevista è disciplinata all'art. 25 dello Schema Speciale di Contratto.

Si precisa che nel corso della durata contrattuale è possibile anticipare durante il primo anno di vigenza, sino al 20% del corrispettivo annuale complessivo dei servizi previsto per l'anno successivo, a causa di eventuali esigenze da parte dell'Amministrazione di maggior potenza elaborativa, imprevedibili all'inizio del contratto stesso.

L'eventuale quota parte economica dei servizi che verrà anticipata nel primo anno di contratto, verrà recuperata alla fine del contratto stesso, sotto forma di ulteriori servizi, mediante l'utilizzo del quinto d'obbligo.

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



5.3. Contesto Tecnologico

In relazione alle esigenze e agli obiettivi sopra descritti, si riportano di seguito alcuni cenni del contesto tecnologico, utili all'inquadramento del contesto di operatività e integrazione nel quale si inseriscono i servizi oggetto della iniziativa.

L'analisi della distribuzione delle tecnologie middleware per applicazione, evidenzia una discreta differenziazione tecnologica, accompagnata ad una sensibile presenza di software Oracle, una presenza importante di Sistemi operativi Linux, quasi totalmente Red Hat Enterprise Linux e un ottimo livello di virtualizzazione degli ambienti.

Queste tecnologie sono completamente integrate con i servizi Cloud, attraverso la definizione di servizi infrastrutturali (IaaS) o mediante l'integrazione con servizi nativi del Cloud Azure (ad es. Azure Active Directory, Security Center, Azure SQL DB, VPN, ecc..). Inoltre, sia i servizi di tipo IaaS che quelli di tipo PaaS sono a loro volta integrati con strumenti di Office365 (ad es. SharePoint online)

5.4. Servizi Cloud Computing IaaS

Tali articoli hanno la finalità di garantire all'Amministrazione un catalogo di servizi in cui le funzionalità cloud offerte sono di tipo infrastrutturale, con la possibilità di disporre di modalità di acquisizione autonome e in modo programmatico di risorse di computing, di storage e networking.

Si assume che i servizi IaaS proposti siano erogati da un unico CSP (Microsoft Azure) per garantire la continuità dei servizi e la possibilità di migrazione di questi workload su altro eco-sistema. Inoltre, è necessario che tali servizi siano fruibili da almeno 2 distinti siti geografici di localizzazione delle risorse, su territorio europeo e con distanza adeguata alla realizzazione di soluzioni di disaster recovery.

Le esigenze sono quindi espresse identificando i fabbisogni per entrambi i siti geografici di localizzazione delle risorse, che saranno nel seguito identificati genericamente come Sito Cloud Primario e Sito Cloud Secondario.

Il dimensionamento massimo stimato per i servizi, riferito all'intera durata contrattuale, è al meglio delle conoscenze attuali. Tale dimensionamento si intende pertanto non vincolante, riservandosi Sogei di:

- non attivare i servizi;
- attivare i servizi in misura maggiore o minore rispetto a quanto di seguito riportato.

5.4.1. IaaS: Servizi di Elaborazione (compute instance)

Per i servizi di elaborazione richiesti si assume il BYOL di tutte le licenze di sistema operativo. Nella definizione del fabbisogno di servizi computazionali si assumono sempre inclusi – quindi non associati ad ulteriori oneri oltre il costo del singolo servizio – servizi di virtual networking e virtual firewalling di base. Sono invece esclusi fabbisogni relativi a licenze o subscription – anche in forma pay-as-you-go – di sistema operativo.

Si ritiene comunque di interesse, in ottica evolutiva dei servizi da attivare in Cloud, l'avere visibilità dell'incremento di costo legato all'attivazione delle istanze con licenze o subscription – anche in forma pay-



as-you-go – di sistema operativo.

Si riportano di seguito:

- le shape e classi di istanze elaborative di interesse;
- i modelli di consumo identificati e le relative dimensioni stimate.

5.4.1.1. Definizione Shape e Classi di Istanze Elaborative

Il fabbisogno di servizi di elaborazione cloud è stato modellato attraverso la definizione di alcune tipologie (shape) di istanze computazionali, la cui nomenclatura si basa sul requisito minimo – in termini di numero di vCPU e Gigabyte vRAM – da soddisfare per poter considerare la tipologia di compute instance definita da Microsoft Azure come assimilabile alla shape:

- e.g. per soddisfare la tipologia di shape C2R4 Microsoft Azure utilizza i profili di VM “Standard A2; Standard F2, ecc. caratterizzati da un numero minimo di 2 vCPU ed una quantità minima di vRAM pari a 4 GB.

Il fabbisogno di istanze compute è stato inoltre ipotizzato sulla base del modello di consumo:

- onDemand: istanze con modello di consumo pay-as-you-go, tariffate sull’utilizzo effettivo;
- Reserved: istanze considerate sempre accese, e per le quali è possibile ottimizzazione costi mediante eventuale tariffazione di maggior favore legata ad un impegno plurimensile/pluriennale.

Per semplicità, le tipologie di istanza possono inoltre essere aggregate in 3 macro-classi sulla base dei requisiti minimi richiesti:

- HighMem: (ratio vRAM/vCPU ≥ 6);
- S-M (small e medium) (ratio vRAM/vCPU < 6) e (vCPU ≤ 4);
- L-XL (large e extraLarge) (ratio vRAM/vCPU < 6) e (vCPU > 4).

Sono identificate le istanze per le quali si assume come requisito la scalabilità verticale delle risorse elaborative. Tale scalabilità dovrà essere assicurata con la possibilità di definire regole di scaling pianificato e/o basato su specifiche metriche.

La tabella seguente mostra i profili Azure utilizzati attualmente e le relative corrispondenze di *shape* con i requisiti minimi:

Size	cpu core	ram	SSD temp	dischi	QUANTITA' VM
Basic_A2 =C2R4	2	3,5	60		2
Basic_A3 =C2R4	4	7	120		1
Standard_A1 =C1R2	1	1,75	70		1
Standard_A1_v2 =C1R2	1	1,75	70		1
Standard_A2 =C2R4	2	3,5	135		25

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell’art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l’informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l’acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



Standard_A3 =C4R8	4	7	285		22
Standard_A4 =C8R16	8	14	240		14
Standard_A4m_v2 =C8R16	8	14	240		1
Standard_A5 =C2R16	2	14	135		7
Standard_A6 =C4R32	4	28	285		11
Standard_B2ms =C2R32	2	8	16		2
Standard_B4ms =C4R16	4	16	32		2
Standard_D1 =C1R4	1	3,5	50		1
Standard_D1_v2 =C1R4	1	3,5	50	4	5
Standard_D11 C2R16	2	14	100		1
Standard_D11_v2 =C2R16	2	14	100		5
Standard_D12_v2 =C2R32	2	28	200		1
Standard_D2 =C2R8	2	7	100	4	2
Standard_D2_v2 =C2R8	2	7	100	4	50
Standard_D2s_v3 =C2R8	2	8	16	4	10
Standard_D3_v2 =C4R16	4	14	200	16	4
Standard_D4_v3 =C4R32	8	28	400		1
Standard_D4s_v3 =C4R16	4	16	100	8	20
Standard_D8_v3 =C8R32	8	32	200	16	2
Standard_D8s_v3 =C8R32	8	32	64	16	5
Standard_DS12_v2_Promo =C4R32	4	28	200		1
Standard_DS14_V2 =C32R128	16	112	800		1
Standard_DS2 =C2R8	2	7	14	4	1
Standard_DS2_v2 =C2R8	2	7	14	8	4
Standard_DS2_v2_Promo =C238	2	7	14	8	1
Standard_DS3 =C4R16	4	14	28	8	5
Standard_DS3_v2 =C4R16	4	14	28	8	3
Standard_F2 =C2R4	2	4		4	18
Standard_F2s =C2R4	2	4		4	2
Standard_F4 =C4R8	4	8		8	8
Standard_F4s_v2 =C4R8	4	8		8	5
Standard_F8 =C8R16	8	16		16	5

Per tutte le tipologie di istanze descritte, si assume capacità di gestire traffico di rete fino ad 1 Gbps.

5.4.1.2. Istanze Reserved

L'attivazione delle istanze reserved seguirà una progressione nel corso del periodo di fornitura

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



dipendente dalla capacità di trasferimento questi workload su altri Cloud Provider. A titolo esemplificativo, la tabella seguente mostra il numero indicativo di istanze che si prevede di tenere attive contemporaneamente:

Shape	Sito Cloud Primario [istanze]			Sito Cloud Secondario [istanze]		
	Anno1	Anno2	Anno3	Anno1	Anno2	Anno3
c1r2	5	0	0	5	0	0
c1r4	5	0	0	5	0	0
c2r4	10	0	0	10	0	0
c2r8	20	0	0	20	0	0
c4r8	20	0	0	20	0	0
c2r16	20	0	0	20	0	0
c4r16	20	0	0	20	0	0
c4r32	20	0	0	20	0	0
c8r16	30	0	0	30	0	0
c8r32	30	0	0	30	0	0
c8r64	25	0	0	25	0	0
c16r32	10	0	0	10	0	0
c16r64	10	0	0	10	0	0
c32r64	5	0	0	5	0	0
c32r128	5	0	0	5	0	0
c32r256	5	0	0	5	0	0
c64r512	5	0	0	5	0	0
c64r1024	5	0	0	2	0	0
Totale	250	0	0	250	0	0

In relazione al tipo di sistema operativo, la tabella sotto riportata esemplifica la distribuzione indicativa censita alla data:

Sistema Operativo	Distrib. S.O. (% mesi reserved)
Red Hat Enterprise Linux 5.x	5,00%
Red Hat Enterprise Linux 6.x	15,00%
Red Hat Enterprise Linux 7.x	15,00%
Altre distribuzioni Linux	5,00%
Windows Server 2008 R2	5,00%
Windows Server 2012 R2	55,00%
Grand Total	100,00%

5.4.1.3. Istanze OnDemand

L'attivazione delle istanze onDemand seguirà una progressione nel corso del periodo di fornitura in dipendenza delle esigenze estemporanee di attivazione di nuovi workload.

5.4.2. IaaS: Servizi di Archiviazione (storage)

Tra i fabbisogni IaaS censiti rientrano i servizi di archiviazione, organizzati nelle tipologie seguenti:

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



- block storage, a supporto delle istanze compute attivate in modalità reserved e onDemand;
- Storage di file, per le applicazioni che devono poter accedere a file condivisi e richiedono un file system;
- Cold storage, a supporto della conservazione dei dati di back up o comunque di dati con requisiti di conservazione a lungo termine e bassa frequenza di accesso.

5.4.2.1. Block Storage (standard)

La tipologia di classificazione identificata con “*standard*” raccoglie le esigenze per spazio di archiviazione da associare a compute per le quali non sussiste l’esigenza di garantire prestazioni elevate a workload ed applicativi *demanding* o più sensibili alle latenze.

Per la continuità degli attuali servizi e per la capacità di trasferimento dei workload su altri Cloud provider, si stima che l’ammontare di storage a blocchi “*standard*” utilizzato sia pari a circa 200 TB sul sito Cloud primario e 100 TB sul sito secondario.

In aggiunta ai fabbisogni sopradescritti, sul solo sito cloud secondario è previsto l’utilizzo di block storage “*standard*” anche per periodi non continuativi (es. fase di test dei meccanismi di DR). In particolare, per un totale di circa 10 TB è previsto un consumo “ad ore”; il numero di ore di utilizzo durante ciascun anno solare è riportato nella tabella che segue.

Sito Cloud Secondario [ore]				
Unità	Anno1	Anno2	Anno3	Quantità [TB]
ore/anno	1.440	720	720	10

5.4.2.2. Block Storage Premium

Per alcune delle istanze compute si rileva invece l’esigenza di garantire prestazioni elevate a workload ed applicativi *demanding* o più sensibili alle latenze. Per tali istanze si assume l’utilizzo di storage ad alte prestazioni, tipologia identificata con la classificazione “*premium*”. Per il primo anno si prevede che l’ammontare di storage a blocchi “*premium*” utilizzato sia pari a circa 50 TB sul sito primario e circa 50 TB sul sito secondario.

5.4.2.3. Cold Storage

Con tale tipologia sono state raccolte le esigenze di storage per l’archiviazione di dati e backup con obiettivi di conservazione a lungo termine, ma ai quali si accede con scarsa frequenza.

Sono dati considerati “inattivi” e quindi non usati di frequente (es. dati di archivio, backup di sistemi e dati).

Per la continuità degli attuali servizi e per la capacità di archiviazione dei dati, si stima che l’ammontare di *cold storage* utilizzato sia pari a circa 100 TB sul sito Cloud primario e 100 TB sul sito secondario.



5.4.2.4. Filesystem Condiviso

Per alcune istanze compute, in ragione delle soluzioni applicative da attivare, si stima l'esigenza di spazio di archiviazione in modalità filesystem condiviso secondo il seguente fabbisogno: 500 GB/mese.

5.4.3. IaaS: Virtual Appliance

La strategia di adozione di un modello di erogazione dei servizi in modalità ibrida (servizi on Premise + servizi in Cloud), prevede, almeno nella prima fase di attuazione, la conservazione delle attuali caratteristiche di security e networking del data center on premise.

L'immagine sottostante mostra una vista di alto livello dell'attuale organizzazione/segmentazione del network degli ambienti operativi presenti, in totale 5 (Produzione, Collaudo, Sviluppo, Manutenzione e Pre-Esercizio), i quali presentano un layout logico speculare.

Ogni ambiente è organizzato in zone logiche protette da istanze virtuali su firewall fisici.

Tutte le zone che erogano servizi – sia verso l'utenza, che servizi infrastrutturali – prevedono Load Balancer fisici, organizzati in istanze virtuali.

I servizi di firewalling e load balancing sono attualmente basati, rispettivamente, su appliance Fortigate e NetScaler VPX.

Per facilitare modalità e tempistiche di migrazione su cloud di servizi, agevolare le prime fasi di gestione delle operation in un ecosistema ibrido, in attesa di andare a regime con un nuovo modello operativo specifico e trasformare l'organizzazione preesistente, la strategia definita prevede l'utilizzo di istanze virtuali NetScaler VPX e Fortigate in linea con l'assetto on premise.

I fabbisogni identificati sono riportati nei paragrafi seguenti, da assumere a titolo di stima indicativa e fatto salvo che in una successiva fase di esercizio dei servizi in Cloud il modello di erogazione dei servizi potrà evolvere verso soluzioni cloud based.

5.4.3.1. Citrix ADC/NetScaler VPX Enterprise

Nelle tabelle di seguito si riportano le stime di attivazione di istanze elaborative NON inclusive del software Citrix VPX Enterprise che sarà installato attraverso licenze di proprietà dell'Amministrazione (BYOL).

Tali fabbisogni tengono conto delle esigenze censite per estensione/migrazione delle configurazioni in essere sul DC on-Premise, di rete (e.g., bilanciamento L4-L7) e di sicurezza (e.g., policy e configurazioni specifiche per ciascun applicativo).

Le istanze dovranno essere configurabili in termini di interfacciamento network (e.g., possibilità di interfacce di indirizzi di rete multipli e/o interfacce di rete multiple).



Shape	Licenza SW	Mesi
#vpx-ha-3Gbps	3000 Mbps	36
#vpx-single-1000Mbps	1000 Mbps	36
#vpx-single-200Mbps	200 Mbps	36

5.4.3.2. Fortigate IaaS

Nel seguito si riportano le stime di attivazione di istanze elaborative NON inclusive del software Fortigate che sarà installato attraverso licenze di proprietà della Amministrazione (BYOL)

Tali fabbisogni tengono conto delle esigenze censite per estensione/migrazione di policy e configurazioni di sicurezza in essere sul DC on-Premise (e.g., firewall e prevenzione attacchi, segmentazione, protezione workload applicativi).

Le istanze dovranno essere configurabili in termini di interfacciamento network (e.g., possibilità di interfacce di indirizzi di rete multipli e/o interfacce di rete multiple).

Per consentire opportuno dimensionamento, la tabella seguente include throughput di riferimento; in particolare, per il sito cloud primario si consideri riferimento di 3 Gbps, mentre per il sito cloud secondario l'indicazione di throughput stimato è di 200 Mbps.

Shape	Throughput	Mesi
#Fortigate 1500D	3000 Mbps	36
#Fortigate 900D	200 Mbps	36

5.4.4. IaaS: VPN Gateway

Per assolvere alla necessità di stabilire – attraverso la rete Internet pubblica – connessioni IPsec sicure e crittografate verso reti cloud virtuali, e verso altre reti nella disponibilità dell'Amministrazione (on premise, ovvero altre reti in cloud) sono stati stimati i seguenti fabbisogni:

- n.10 gateway sul sito cloud primario;
- n.5 gateway sul sito cloud secondario;

ciascuno attivo per l'intera durata della fornitura.

5.4.5. IaaS: Connettività dedicata per VPN

In una prima fase di attivazione dei servizi Cloud si assume di realizzare connessioni IPsec sicure su rete Internet.

Al fine di disporre della possibilità di attivare anche soluzioni di connettività dedicata tra il sito on premise e i siti Cloud, qualora le esigenze di trasporto e prestazioni ne evidenzino l'esigenza, si richiede di avere una proposta di soluzioni di connettività punto-punto attivabili dal sito cloud primario e dal sito cloud secondario verso punti di accesso al backbone di trasporto su territorio italiano.

Per il dimensionamento si consideri di riferimento quello riportato al precedente paragrafo.

Le soluzioni proposte dovranno essere descritte nelle caratteristiche tecniche e opzioni disponibili.



Aspetti di particolare interesse sono ridondanza, latenza e potenzialità di switching tra siti (es. da primario a secondario in caso di DR, configurazioni in business continuity).

5.4.6. IaaS: IP Pubblici

Per consentire la comunicazione in ingresso verso specifiche risorse Cloud (o la comunicazione in uscita mediante specifico IP) è stato formulato il fabbisogno di servizi di indirizzamento IP pubblico IPv4. Ciascun indirizzo pubblico potrà essere associato dall'Amministrazione ad interfaccia di rete di istanza computazionale, ad un servizio di bilanciamento di carico di rete o applicativo con connessione Internet, ad un gateway VPN, o ad altra risorsa eleggibile per tale associazione.

5.4.7. IaaS: Traffico in Uscita (outbound)

Il fabbisogno in termini di trasferimento dati in uscita, dal sito cloud primario, è stato quantificato nella misura di un massimo di 10 TB/mese per l'intera durata del contratto

In considerazione del carattere di stima del fabbisogno, si rappresenta l'esigenza di avere evidenza delle soluzioni di scalabilità disponibili in offerta.

Il traffico in ingresso ed il traffico cross-region si assumono inclusi nei corrispettivi dei servizi IaaS di cui ai precedenti requisiti e senza ulteriori oneri oltre i corrispettivi previsti per i servizi richiesti.

5.5. Servizi Cloud Computing PaaS

Il catalogo individuato per i fabbisogni espressi al precedente paragrafo 4.3 prevede articoli per la copertura delle esigenze infrastrutturali di base, quali istanze compute, servizi storage, appliance di bilanciamento e sicurezza, ed elementi base legati alla connettività.

Tali articoli sono volti ad assicurare la continuità dei servizi cloud di parte dei servizi applicativi del programma IDEA@PA ospitati attualmente nel cloud pubblico Microsoft Azure ed il consolidamento di una soluzione di DR per tutti i servizi della Corte dei conti e degli istituti associati al programma IDEA@PA.

L'Amministrazione intende proseguire il percorso evolutivo del proprio contesto IT con la progressiva revisione in ottica cloud based dei workload applicativi attraverso soluzioni in modalità nativa cloud.

Per disporre degli strumenti utili a tale ulteriore scenario di intervento, parte della iniziativa di fornitura ha l'obiettivo di definire un catalogo di servizi nel seguito identificati genericamente come PaaS (sebbene per taluni sia applicabile anche la classificazione IaaS) e al quale si farà riferimento sulla base dell'effettivo percorso di attuazione definito.

I servizi possono essere raccolti in un catalogo di macro categorie, distinguibili in due sottoinsiemi:

- Servizi a supporto, ovvero servizi per la gestione dello strato cloud IaaS e delle applicazioni sopra implementate;
- Servizi avanzati, che risultano abilitanti alle evoluzioni applicative in ottica cloud native.

Il dimensionamento delle esigenze espresse per singolo servizio è stato stimato ipotizzando uno scenario di massima di utilizzo e individuando componenti specifici del Cloud Microsoft Azure.

Tale dimensionamento si intende pertanto vincolante, riservandosi Sogei di:

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



- non attivare in tutto o in parte i servizi elencati nel seguito;
- attivare i servizi in misura maggiore o minore rispetto a quanto di seguito riportato;
- attivare i servizi utilizzando gli effettivi parametri dimensionali degli articoli offerti a copertura delle esigenze indicate;
- attivare i servizi disponibili nelle macro categorie, indipendentemente dalle modifiche al catalogo dei servizi Azure, dovute all'introduzione di nuovi servizi o alle modifiche tecniche e/o commerciali di quelli esistenti.

nel rispetto comunque del massimale contrattuale previsto per il totale dei servizi oggetto del presente paragrafo.

Per ciascun servizio, la modalità di remunerazione (canone, pay as you go) potrà essere definita all'atto della attivazione del servizio stesso e sulla base dell'effettivo consumo atteso

5.5.1. Macro categorie del catalogo dei servizi

Il fabbisogno del programma [IDEA@PA](#) riguarda le seguenti macro categorie di servizi PaaS, che dovranno essere completamente disponibili indipendentemente dalle declinazioni specifiche che seguono nei successivi paragrafi:

- Analisi – Raccolta, archiviazione, analisi di qualsiasi tipo di dati;
- Archiviazione – Soluzione di archiviazione dei dati sicura e scalabile;
- Blockchain – Creazione e gestione applicazioni con strumenti integrati per Blockchain;
- Calcolo – capacità di calcolo per specifiche esigenze;
- Container - creazione e gestione integrata dei container;
- Contenuti Multimediali – distribuzione di contenuti Video/audio di alta qualità su qualunque dispositivo;
- Database – Servizi di Database completamente gestiti;
- Desktop Virtuale Windows – Servizi di desktop virtuale;
- Dispositivi Mobili – creazione e gestione di App per dispositivi mobili.
- Gestione e Governance – Monitoraggio delle risorse, Gestione dei costi, definizione delle Politiche, Disaster Recovery;
- Gestione Identità – gestione delle identità per l'accesso ai servizi e strumenti di controllo e di sicurezza;
- Ibrido – Strumenti e servizi per la migrazione o trasferimento dei dati, tra sistemi del Data Center e sistemi del Cloud, Disaster Recovery, archiviazione dei dati remota;
- Integrazione – Servizi di ricerca avanzati, intelligenza artificiale, machine learning, servizi cognitivi, riconoscimento vocale, analisi linguistica, ecc.;
- IoT – Servizi di gestione dei dispositivi, strumenti per il controllo dei dispositivi in un contesto geo spaziale, strumenti per lo sviluppo di App per dispositivi di qualsiasi tipo;
- Rete – Servizi per la definizione di reti locali nel cloud e di interconnessione con il Data Center o con altri Cloud provider, Gateway VPN, Monitoraggio;

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



- Sicurezza – Servizi di gestione centralizzata della sicurezza per tutti i workload;
- Strumenti per lo sviluppo – strumenti per la produzione e la gestione del ciclo di vita del SW, DevOps, analisi e debug;
- Web – Creazione e gestione di servizi per le applicazioni web.

5.5.2. Servizi di Piattaforma a Supporto Gestione IaaS

Gli articoli elencati in questo paragrafo raccolgono i fabbisogni di servizi Cloud che potranno essere attivati a supporto di una gestione nativa di risorse IaaS e dei workload ospitati.

5.5.2.1. VPN – GW Service (Azure VPN Gateway)

Tale fabbisogno è volto ad assicurare esigenze superiori a quelle considerate nella sezione IaaS.

Utilizzo atteso: servizio attivo continuativamente per 18 mesi.

5.5.2.2. Load Balancing Service (Azure Load Balancer)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- bilanciamento del carico altamente affidabile;
- possibilità di definire diverse modalità di bilanciamento;
- utilizzo di SSL off-loading;
- supporto autoscaling automatico;
- supporto definizione metriche/eventi che determinano scale-out o scale-in automatico.

Utilizzo atteso: servizio attivo continuativamente per 18 mesi.

5.5.2.3. Security Monitoring Service (Azure Security Center, Azure Log Analytics)

Il servizio dovrà garantire la disponibilità di funzionalità avanzate di monitoring ed analisi di eventi di sicurezza legati a tentativi di accesso ai sistemi sia infrastrutturali che applicativi al fine di rilevare potenziali minacce di sicurezza.

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- possibilità di raccogliere dati di monitoraggio del sistema operativo guest (e.g., utilizzo cpu, ram, disco, rete);
- monitoraggio risorse definite nel contesto dello stesso CSP;
- monitoraggio sottoscrizioni ed info relative all'integrità e al funzionamento dei servizi offerti dal CSP, anche a livello di singolo tenant;
- Possibilità di definire eventi e metriche personalizzate e dashboard personalizzate.

Fabbisogno stimato alla data: protezione avanzata per 600 server e 50 applicazioni; per ciascun server si stimano 500 MB di traffico giornaliero.

Utilizzo atteso: servizio attivo continuativamente per 36 mesi.



5.5.2.4. Application Monitoring Service (Azure Monitoring, Application Insight)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- possibilità di raccogliere dati di monitoraggio dell'applicazione relativi alle prestazioni ed alle funzionalità del codice (e.g., numero di utenti/sessioni, response time, frequenza richieste, richieste fallite, eccezioni), indipendentemente dalla piattaforma;
- possibilità di definire eventi e metriche personalizzate e dashboard personalizzate. Fabbisogno stimato alla data: tracciamento di circa 2,5 milioni di operazioni/ora; 100 interrogazioni al giorno, con recupero di almeno 5000 tracce per ciascuna interrogazione.

Utilizzo atteso: servizio attivo continuativamente per 36 mesi.

5.5.2.5. Auditing Service (Azure Log Analytics, Azure Sentinel, Azure Advisor, Azure Security Center)

Il servizio dovrà assicurare le funzionalità a supporto della governance, compliance e gestione del rischio nell'utilizzo del proprio account sul/i CSP. Il servizio dovrà permettere di monitorare in maniera continuativa le attività eseguite nell'ambito dei vari servizi e fornire uno storico di tutte le azioni che sono state intraprese. Lo storico sarà ad uso di analisi di sicurezza, troubleshooting e change tracking e dovrà quindi assicurare adeguati contenuti informativi a tal fine.

Fabbisogno stimato alla data: tracking di 1.000.000 di eventi di gestione (memorizzati in duplice copia); 10 milioni di eventi sui dati.

Utilizzo atteso: servizio attivo continuativamente per 36 mesi.

5.5.2.6. Application log service (Azure Log Service)

Il servizio è volto a garantire la possibilità di raccogliere e centralizzare i log applicativi e di sistema. E' inoltre richiesta la possibilità di integrare il collettore con SIEM di terza parte. Fabbisogno stimato alla data: si stima di raccogliere 1 TB/mese di log applicativi custom, in aggiunta ad 1 TB/mese di log relativi a servizi di piattaforma.

Utilizzo atteso: servizio attivo continuativamente per 36 mesi.

5.5.2.7. Security service (Azure Security Center)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- rilevamento delle minacce (e.g. DoS, DDoS);
- disponibilità di Intrusion & Prevention Systems;
- disponibilità di antivirus.

Fabbisogno stimato alla data: copertura dell'intera infrastruttura IaaS oggetto di fornitura.

Utilizzo atteso: servizio attivo continuativamente per 18 mesi.

5.5.2.8. Backup Service (Azure Backup)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- possibilità di definire le policy di backup in maniera personalizzata e anche specificatamente per singolo componenti infrastrutturale;

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



- possibilità di definire policy di retention dei dati in maniera personalizzata e anche specificatamente per tipologia di dati trattati.

Fabbisogno stimato alla data: copertura di almeno 100 istanze.

Utilizzo atteso: servizio attivo continuativamente per 36 mesi.

5.5.2.9. DR Automation Service (Azure Site Recovery)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- replica dischi, abilitante ripristino su altro sito geografico che ospita servizi cloud secondario;
- funzionalità di supporto per la migrazione dati e servizi da sito on-premise a sito cloud secondario;
- funzionalità di replica geografica orchestrata e distribuzione dei processi di replica.

Fabbisogno stimato alla data: copertura di almeno 100 istanze.

Utilizzo atteso: servizio attivo continuativamente per 36 mesi.

5.5.2.10. Strumenti per lo sviluppo (Azure Visual Studio, Azure DevOps, Azure SDK, Azure DevTest Lab, Azure Pipelines)

Strumenti di sviluppo per qualsiasi piattaforma o linguaggio, per la distribuzione di applicazioni cloud. Il servizio offre ambienti di sviluppo integrati con funzionalità complete e di debug avanzato.

5.5.3. Servizi di Piattaforma abilitanti al cloud native

Il catalogo di servizi di seguito riportato, raccoglie le esigenze per strumenti abilitanti alla revisione in ottica cloud dei servizi migrati dal sito on premise e per la realizzazione di nuove soluzioni in linea con i paradigmi del cloud.

5.5.3.1. Web Application (Azure App Web Service)

Il servizio permette la creazione e la gestione di applicazioni utilizzando framework più diffusi, tra cui .NET, .NET Core, Java, Node.js, Python, PHP e Ruby. Distribuzione delle app in contenitori o come codice, in esecuzione in Linux o Windows.

5.5.3.2. Dispositivi Mobili (Azure App per dispositivi Mobili, API Mgmt, App Service)

Il servizio permette la realizzazione dei APP multi piattaforma per qualsiasi ti di dispositivo.

5.5.3.3. Relational Database as a service (Azure SQL Service, Azure MySQL)

Il servizio dovrà garantire la continuità delle istanze gestite per database relazionali. Sono richieste funzionalità di crittografia dati sia in transito che a riposo (TDE).

Il fabbisogno è definito per la continuità degli attuali DB PaaS delle istanze DB Microsoft SQL dell'Amministrazione, attivate su IaaS in una prima fase di erogazione dei servizi su Cloud (post migrazione servizi da sito on premise).

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



5.5.3.4. No SQL Service (Azure Cosmos DB)

Il servizio dovrà garantire la disponibilità di istanze gestite per database non relazionali. Sono richieste funzionalità di crittografia dati sia in transito che a riposo.

5.5.3.5. In memory data archive service (Azure Cache for Redis)

Il servizio dovrà garantire la disponibilità di risorse di archiviazione rapida (in memory) ad uso delle applicazioni (memorizzazione dati su memoria distribuita, per ottenere prestazioni elevate). È prevista la possibilità di accedere alle risorse di archiviazione anche tramite client esterni alle infrastrutture cloud ospitanti. Sono richieste funzionalità di crittografia dati sia in transito che a riposo.

5.5.3.6. Shared Filesystem service (Azure File Service)

Il servizio dovrà garantire la disponibilità di share NFS condivise e la possibilità di gestire quote dello spazio isolate per applicazione/tenant.

5.5.3.7. Large object service (Azure BLOB Storage Service)

Il servizio dovrà garantire la disponibilità di risorse di archiviazione scalabili per dati non strutturali. È di interesse la visibilità dei diversi modelli di servizio/prestazioni disponibili.

5.5.3.8. Datalake Storage Service (Azure Datalake Storage – Azure Datalake Analytics)

Il servizio dovrà garantire la possibilità di usare storage Data Lake altamente scalabile e sicuro per analisi Big Data (dati non strutturati, semi strutturati e strutturati; senza limiti dimensionali).

5.5.3.9. Analisi dei dati (Azure Power BI Embedded)

Dashboard e analisi prodotte in modo semplice e immediato, personalizzate in base esigenze di sviluppo per le automazioni di monitoraggio con funzionalità di analisi intelligente dei dati.

5.5.3.10. WAF Service (Azure Application Gateway)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- protezione app web da attacchi esterni;
- possibilità di proteggere più app con un unico waf;
- aggiornamento automatico per protezione da nuove vulnerabilità;
- supporto ssl offloading;
- supporto end-2-end ssl;
- Disponibilità log di diagnostica;
- Servizi di Filtering (e.g. IP, URL, malicious web traffic).

5.5.3.11. IDM Service (Azure Active Directory)

Il servizio dovrà garantire la continuità delle caratteristiche funzionali minime di seguito elencate:

Classificazione del documento: Consip Public

AS SDAPA ai sensi dell'art. 55 del D.Lgs. n. 50/2016, per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni (procedura indetta ex artt. 55 e 61 del D.Lgs. 50/2016, per l'acquisizione di servizi Cloud IaaS e PaaS Microsoft Azure per il progetto IDEA@PA di Cdc – ID 2234 – Capitolato Tecnico



- gestione identità per accesso sicuro a servizi/applicazioni/risorse su cloud;
- supporto integrazione con i servizi nativi web-app;
- compatibilità con soluzione SSO in uso presso sito on premise.

5.5.3.12. Key Management Service (Azure Key Vault)

Il servizio dovrà garantire le caratteristiche funzionali minime di seguito elencate:

- archiviazione credenziali e certificati delle applicazioni;
- funzionalità di generazione chiavi;
- possibilità di importare chiavi generate autonomamente.

5.5.3.13. API Management Service (Azure Api Gateway)

Il servizio dovrà garantire la continuità delle funzioni minime di seguito elencate:

- creazione, pubblicazione, manutenzione, monitoraggio e protezione di API;
- possibilità di accettare e inoltrare chiamate tra layer con differenti livelli di sicurezza (tipicamente da front end verso back end);
- verifica chiavi, token, certificati ed altre credenziali;
- raccolta log chiamate;
- prevenzione attacchi DOS;
- possibilità di attivare canali di comunicazioni protetti tra gateway API e layer contattati (tipicamente verso back end).

5.5.3.14. Container Registry Service (Azure Container Registry)

Il servizio dovrà garantire la disponibilità di un registro di immagini container, completamente gestito, per la conservazione e distribuzione in modo affidabile. È richiesta l'integrazione con il sistema di Identity management, per la configurazione delle policy di controllo accesso al repository ed alle risorse.

5.5.3.15. Container service (Azure Kubernetes Service)

Il servizio è finalizzato a rendere disponibile all'Amministrazione la possibilità di eseguire su cloud applicazioni realizzate ne rispetto di un'architettura a microservizi.

Il servizio è finalizzato a rendere disponibili all'Amministrazione funzionalità a supporto del deploy di applicazioni web, senza necessità di configurare le risorse computazionali sulle quali l'applicazione sarà eseguita.

Le caratteristiche minime richieste sono di seguito elencate:

- supporto dei linguaggi più comuni;
- scalabilità automatica e bilanciamento del carico integrati;
- disponibilità di piani dimensionali con tagli differenti di risorse computazionali.

5.5.3.16. Serverless computings (Azure Service Fabric)

L'esigenza è quella di rendere disponibile all'Amministrazione, anche per sperimentazione e test,



soluzioni di elaborazione serverless end to end che consentano una totale astrazione da attività di configurazione e gestione infrastrutturale.

Si assumono come caratteristiche funzionali minime:

- Provisioning infrastruttura totalmente gestito;
- scalabilità e prestazioni by design;
- esecuzione automatica del codice attivabile da diversi tipi di eventi (es. richieste http, azioni su oggetti storage).

5.5.3.17. Messaging queue service (Azure Message Bus)

L'esigenza è quella di garantire la continuità del servizio per la gestione di code di messaggi, nell'ambito di comunicazioni asincrone tra servizi (es. a supporto di architetture applicative basate su microservizi).

Caratteristiche funzionali minime richieste sono:

- affidabilità dei meccanismi di trasmissione dei messaggi;
- scalabilità delle risorse;
- supporto protezione crittografica dei messaggi scambiati.

5.5.3.18. Search service (Azure Search Service)

L'esigenza è quella di garantire la continuità del servizio gestito con il quale configurare e gestire soluzioni di ricerca "chiavi in mano" per un sito Web o un'applicazione senza intervenire per la configurazione della infrastruttura ed avere specifiche competenze tematiche:

Caratteristiche funzionali minime richieste sono:

- possibilità di definire indici;
- estrapolazione risultati maggiormente rilevanti;
- supporto multi-language;
- supporto suggerimenti di completamento automatico;
- alta scalabilità;
- prestazioni risposte in near real time.

5.5.3.19. Cognitive Service (Azure Cognitive Service)

Il servizio dovrà permettere l'utilizzo di algoritmi intelligenti nelle App e nei siti Web per vedere, ascoltare, parlare, comprendere le esigenze degli utenti tramite metodi di comunicazioni naturali.

6. EROGAZIONE DEI SERVIZI

L'erogazione dei servizi IaaS e PaaS oggetto di acquisizione dovrà essere effettuata, improrogabilmente, **entro 5 (cinque) giorni** a decorrere dalla data di stipula del contratto oppure entro il diverso termine stabilito tra le parti.

Contestualmente all'erogazione dei servizi IaaS e PaaS, l'Impresa dovrà, altresì, consegnare un "Piano



operativo/di collaudo”, contenente la proposta relativa alle operazioni e funzionalità che saranno oggetto di verifica di conformità dei prodotti oggetto della fornitura. Tale Piano Operativo dovrà essere approvato dalla Committente entro 5 (cinque) giorni dall’avvenuta consegna dello stesso.

La disponibilità dei nuovi servizi dovrà essere assicurata senza soluzione di continuità e senza alcuna operazione di migrazione. I servizi attualmente configurati all’interno di ciascuna sottoscrizione, dovranno essere mantenuti attivi e trasferiti “amministrativamente” all’interno del nuovo contesto contrattuale.

L’intervento si intende chiuso solo quando le attività di predisposizione e verifica si sono concluse con esito positivo.

6.1. Consegna in gestione

È compresa nella fornitura la consegna in gestione dei servizi IaaS e PaaS erogati, al fine di assicurare un appropriato passaggio di consegne ai team dedicati ai servizi di gestione; l’attività deve essere formalizzata nel suddetto *Piano Operativo/di collaudo* che dovrà essere consegnato alla Committente entro 5 (cinque) giorni solari dalla stipula del Contratto; in particolare dovranno essere previste almeno le seguenti attività:

- illustrazione della documentazione prodotta nell’ambito del rilascio dei servizi;
- passaggio di conoscenza funzionale e tecnica.

Il Fornitore è tenuto, preliminarmente al passaggio dei servizi in gestione, a fornire il proprio supporto a Sogei nell’esecuzione dei test di qualità e della certificazione dei servizi stessi.

6.2. Requisiti di qualità

Il Fornitore deve assicurare la qualità dei servizi erogati, attraverso la presenza al suo interno di specifiche funzioni di verifica, validazione, riesame, assicurazione qualità sui prodotti e sui processi.

Su richiesta della Committente, il Fornitore dovrà predisporre delle rappresentazioni dell’andamento della fornitura basandosi sui dati riportati nei rapporti sugli indicatori di qualità della fornitura, anche al fine di effettuare analisi a vari livelli di dettaglio delle informazioni.

6.3. Responsabile della fornitura

Entro **5 (cinque) giorni** lavorativi dalla stipula del contratto, l’Impresa dovrà comunicare all’Amministrazione il nominativo del proprio rappresentante designato quale **Responsabile della fornitura** (o Responsabile della Società per le attività contrattuali). In particolare, tale responsabile sarà, per gli aspetti amministrativi e contrattuali, l’interlocutore unico di Sogei.

Sarà cura del Responsabile della fornitura verificare il rispetto di tutti gli adempimenti contrattuali.

Tale referente non dovrà comportare alcun onere aggiuntivo per la Committente.

Il Responsabile della fornitura dovrà essere reperibile telefonicamente e partecipare alle riunioni su richiesta della Committente con un preavviso massimo di **3 giorni lavorativi**.

Il Responsabile della fornitura non farà parte di alcuno dei gruppi di lavoro relativi ai servizi oggetto della fornitura.



Il Responsabile della fornitura dovrà in particolare:

- predisporre ed aggiornare il piano operativo;
- monitorare i livelli di servizio sulle attività oggetto della fornitura ed intraprendere eventuali azioni correttive a fronte del mancato rispetto delle soglie previste;
- farsi carico della soluzione dei problemi tecnici e/o di eventuale non disponibilità dei servizi Cloud che dovessero verificarsi nel corso della durata contrattuale.

7. ESECUZIONE DELLA FORNITURA

Al Fornitore è richiesto in tutte le attività della fornitura il rispetto dei processi, degli standard e delle linee guida adottate dalla Committente; il Fornitore deve farsi carico di conoscere e diffondere al proprio interno tali conoscenze, di applicarle proattivamente, e di recepirne tempestivamente eventuali variazioni.

La tipologia delle attività da svolgere e la delicatezza della materia trattata richiedono che tutte le attività dell'Impresa siano improntate a un'assoluta attenzione alla riservatezza. È inoltre fatto divieto all'Impresa di utilizzare il presente affidamento quale riferimento per altri incarichi, salvo esplicita autorizzazione da parte dell'Amministrazione.

Il corrispettivo complessivo offerto dall'Impresa si intende comprensivo di tutte le attività richieste e necessarie per l'esecuzione della fornitura. Tale corrispettivo non potrà subire aumenti neanche al variare della pianificazione effettiva rispetto a quanto inizialmente previsto.

Tutte le attività dovranno essere svolte in collaborazione con i referenti dell'Amministrazione, secondo modalità che saranno opportunamente concordate in fase di avvio.

L'amministrazione si riserva di modificare le modalità di esecuzione descritte e di introdurre nuove modalità, anche in corso d'opera, dandone congruo preavviso all'Impresa. In aggiunta, tali modalità di esecuzione potranno essere congiuntamente riviste, su proposta dell'Impresa, e potranno essere concordate opportune semplificazioni o variazioni in funzione delle specificità dei singoli interventi.

Sogei si riserva di avvalersi di terzi per il supporto allo svolgimento di attività di propria competenza, ferma restando la responsabilità globale di Sogei nello svolgimento di tali attività.

7.1. Modalità di esecuzione della fornitura

La fornitura dei servizi cloud IaaS e PaaS erogati dal Cloud pubblico Microsoft Azure dovrà essere espletata attraverso piattaforma elettronica messa a disposizione a cura del Fornitore.

Le attività correlate alla erogazione dei servizi cloud avranno luogo presso la sede della Corte dei conti.

7.1.1. Modalità di erogazione continuativa

Il servizio Cloud da erogare è in modalità continuativa.



L'attivazione è prevista a partire dalla data di avvio delle attività e l'erogazione è senza soluzione di continuità fino alla data di fine delle attività, salva ed impregiudicata la facoltà della Committente di sospendere, ridurre e/o interrompere il servizio.

Dal momento in cui una richiesta per malfunzionamento è registrata nel sistema della Committente, o nel sistema del Fornitore in assenza dello stesso, decorrono i tempi relativi ai livelli di servizio definiti nel presente capitolato tecnico.

Il Fornitore ha la responsabilità della esecuzione dell'attività di risoluzione del malfunzionamento ed è tenuto ad aggiornare le informazioni di propria competenza sul sistema fino alla soluzione del malfunzionamento stesso motivato con la opportuna e dettagliata diagnosi.

7.1.2. Livelli di servizio

Le modalità di erogazione del servizio (Livelli di servizio e penali) sono regolate in dettaglio nell'Allegato 13 - Classificazione CSP (Documento AGID).

Qualora nell'erogazione dei servizi Cloud di cui al paragrafo 4.1, si verificassero dei problemi tecnici o una non disponibilità degli stessi, la Committente contatterà il Fornitore, per la soluzione di tali problematiche, contattando il Responsabile della fornitura a un numero telefonico o a un indirizzo di posta elettronica o un numero di fax all'uopo preposti.

7.2. Pianificazione e Consuntivazione

Il Fornitore si impegna a ottenere dalla Committente il rilascio della regolare esecuzione sulle forniture prima di emettere la relativa fattura (che sarà associata alla regolare esecuzione attraverso appositi codici identificativi, da concordare).

7.3. Verifica di conformità

Entro il termine di 10 giorni decorrente dalla data di sottoscrizione del contratto e nel corso di efficacia del contratto stesso l'Amministrazione effettuerà le verifiche di conformità delle prestazioni, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

Il Fornitore dovrà consegnare un "Piano Operativo/di collaudo", contenente la proposta relativa alle operazioni e funzionalità che saranno oggetto di Verifica di conformità dei prodotti oggetto della fornitura.

Delle operazioni di verifica di conformità verrà redatto apposito verbale. La Verifica di conformità si intende positivamente superata solo nel caso in cui le prestazioni risultino eseguite a regola d'arte, sotto il profilo tecnico-funzionale, ed in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente documento.

L'Impresa è tenuta a prestare all'Amministrazione, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Amministrazione le attrezzature eventualmente occorrenti alle operazioni di verifica di conformità.

La verifica di conformità della fornitura di servizi Cloud IaaS e PaaS del Cloud pubblico Microsoft Azure, di



cui al precedente paragrafo 4.1, verrà conclusa la prima volta, entro 20 giorni dalla data di sottoscrizione del contratto, successivamente con cadenza trimestrale entro il mese successivo al trimestre di riferimento.

Nel caso di esito positivo della verifica di conformità la data del verbale verrà considerata quale **“Data di accettazione del Servizio”**.

La conformità sarà accertata attraverso il controllo della disponibilità dei servizi acquisiti attraverso il portale Azure.

In caso di esito negativo della verifica di conformità, l’Impresa dovrà provvedere, a propria cura e spese, ad eliminare i vizi accertati entro il termine massimo che le verrà comunicato dalla Amministrazione. In tale ipotesi, la verifica di conformità verrà ripetuta, con le modalità precedentemente descritte.

Nel caso in cui anche la seconda verifica di conformità dia esito negativo, l’Amministrazione, ferma l’applicazione delle penali, avrà facoltà di risolvere il contratto e di fare eseguire in tutto o in parte le prestazioni a terzi in danno dell’Impresa.

Tutti gli oneri derivanti dalla verifica di conformità si intendono a carico dell’Impresa.

Le verifiche saranno ripetute in corso di esecuzione del contratto per le prestazioni continuative.

7.4. Azioni contrattuali

Ogni inadempimento contrattuale darà origine ad un’azione commisurata alla criticità della violazione.

Pertanto, il mancato rispetto dei requisiti minimi richiesti e/o come migliorati dal Fornitore in Offerta tecnica determina azioni contrattuali conseguenti che possono consistere in una o più delle seguenti azioni:

- coinvolgimento di un livello più elevato di interlocutori, sia del Fornitore che della Committente, allo scopo di prendere le decisioni necessarie al ripristino delle situazioni fuori soglia o fuori controllo (attivazione di una procedura di escalation);
- ripetizione da parte del Fornitore dell’erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto (chiusura di una non conformità);
- azione di intervento sui processi produttivi del Fornitore per evitare il ripetersi di sistematiche non conformità (esecuzione di una azione correttiva);
- azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.

7.5. Exit strategy e Grace period

Il Fornitore si obbliga a fornire supporto alla Committente nell’attività di Exit strategy che avverrà entro 30 (trenta) giorni dalla scadenza naturale del contratto, ovvero, se prima della scadenza naturale, l’Exit strategy dovrà essere comunicata al Fornitore con 30 (trenta) giorni di preavviso (cd. Grace period), e consisterà in un supporto all’individuazione dei dati oggetto di migrazione.



Il Fornitore, inoltre si obbliga a fornire tutte le idonee garanzie a dimostrazione della eliminazione dei dati sul cloud al termine della fase di Exit strategy, nonché la disponibilità a far eseguire verifiche in tal proposito da parte della Committente o di soggetti terzi da questa designati.

Preliminarmente alla fase di Exit strategy, il Fornitore si obbliga a esportare i dati in un formato che andrà stabilito in accordo con la Committente e, comunque, idoneo a consentire il ricaricamento dei dati su infrastrutture individuate da Sogei.

Al momento della scadenza naturale del contratto, il Fornitore non avrà più titolo per emettere fatture, in quanto deve intendersi attivato il Grace period, per un periodo massimo di 30 giorni, durante il quale la Committente si riserva di procedere al rinnovo del contratto, anche con altro service provider di cloud ovvero alla migrazione dei servizi (Exit strategy) senza alcun onere aggiuntivo per la Committente, che dovrà avvenire entro il Grace period.