

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

PROGETTO dei FABBISOGNI

**per la fornitura di “Servizi di Cloud Computing”
SPC CLOUD LOTTO1**

**REGIONE ABRUZZO
Servizio Programmazione
Innovazione e Competitività
(DPH001)**

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

| | | |
|---|------------------|--|
| REDATTO da: (Autore) | B.S/C.PSD | Michele La Monaca |
| APPROVATO da: (Proprietario) | B.S/C.PSD | Michele La Monaca |
| LISTA DI DISTRIBUZIONE: | | Ufficio Speciale per la Ricostruzione dell'Aquila |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

SOMMARIO

| | | |
|------------|---|-----------|
| 1 | SOMMARIO | 5 |
| 2 | AMBITO | 5 |
| 3 | DEFINIZIONE ED ACRONIMI | 6 |
| 4 | RIFERIMENTI | 7 |
| 4.1 | Documenti contrattuali | 7 |
| 4.2 | Documenti di riferimento | 7 |
| 5 | PROGETTO DI ATTUAZIONE DEL SERVIZIO BAAS e PAAS | 8 |
| 5.1 | Descrizione | 8 |
| 5.2 | Dettagli servizio contrattualizzato (ID servizio, quantità costi) | 9 |
| 5.3 | Configurazioni da realizzare | 10 |
| 5.4 | Specifiche di Collaudo | 12 |
| 6 | DESCRIZIONE CENTRO SERVIZI | 14 |
| 7 | MODALITÀ DI PRESENTAZIONE E APPROVAZIONE STATI AVANZAMENTO MENSILI | 17 |
| 8 | PIANO DI ATTUAZIONE DEL SERVIZIO | 18 |
| 8.1 | Piano di Lavoro Servizio SaaS – Conservazione Digitale | 18 |
| 8.2 | Documento Programmatico di Gestione della Sicurezza dell'Amministrazione | 18 |
| 9 | TABELLA RIEPILOGATIVA FINALE SERVIZI | 18 |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

| DESCRIZIONE MODIFICA | REVISIONE | DATA |
|----------------------|-----------|------------|
| Prima Emissione | 1 | 10/04/2017 |
| | | |
| | | |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

1 SOMMARIO

Il presente documento descrive il Progetto dei Fabbisogni del RTI Telecom Italia, HP Enterprise Service, Postel e Telecom Italia Trust Technologies, relativamente alla richiesta di fornitura dei servizi di Cloud Computing (IAAS/PAAS/SAAS) nell'ambito del sistema pubblico di connettività e cooperazione (SPC) per l'Amministrazione.

Quanto descritto, è stato redatto in conformità alle richieste dell'Amministrazione e sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e sulla base delle informazioni contenute nel Piano dei Fabbisogni.

2 AMBITO

Il contratto per la fornitura di "Servizi di Cloud Computing, di Sicurezza, di Soluzioni di Portali di Servizi online e di Cooperazione Applicativa" Lotto 1, per le Pubbliche Amministrazioni ed il Raggruppamento Temporaneo di Impresa (RTI) costituito da:

- **Telecom Italia S.p.A.** (mandataria)
- **Telecom Italia Trust Technologies S.r.l.**
- **HP Enterprise Service Italia**
- **Poste Italiane**
- **Postecom**
- **Postel**

prevedono la fornitura dei seguenti servizi Cloud nell'ambito del Sistema Pubblico di Connettività e Cooperazione (SPC):

- Servizi IAAS
- Servizi PAAS
- Servizi SAAS

tutto secondo quanto stabilito nel Capitolato Tecnico e nell'Offerta Tecnica, nella misura richiesta dalle amministrazioni Contraenti con i Contratti di Fornitura.

Telecom Italia, in qualità di mandataria, avrà in carico tutte le attività propedeutiche all'attivazione dei servizi contrattualizzati dall'Amministrazione Contraente relative, sia alla ricezione dei Piani dei Fabbisogni ed al conseguente invio dei relativi Progetti di Fabbisogni, sia all'accettazione dei Contratti di Fornitura

In particolare la procedura per l'affidamento dei predetti servizi è articolata attraverso la stipula da parte di Consip S.p.A. di un Contratto Quadro con l'Aggiudicatario della procedura medesima, che si impegna a stipulare, con le singole Amministrazioni Contraenti, Contratti di Fornitura aventi ad oggetto i predetti servizi alle condizioni stabilite nel Contratto Quadro.

La durata del Contratto Quadro è fissata in 36 mesi prorogabili, su comunicazione di Consip, sino ad un massimo di ulteriori 24 mesi;

I singoli Contratti Esecutivi di Fornitura di ciascun Lotto avranno una durata decorrente dalla data di stipula del Contratto Esecutivo medesimo e sino al massimo della scadenza ultima, eventualmente prorogata (Lotto 1) del Contratto Quadro

Le singole Amministrazioni contraenti potranno richiedere una proroga temporale dei singoli Contratti Esecutivi di Fornitura al solo fine di consentire la migrazione dei servizi ad un nuovo Fornitore al termine del Contratto Quadro, qualora la selezione dell'Operatore Economico subentrante non sia intervenuta entro i 3 mesi antecedenti la scadenza del presente Contratto Quadro.

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

3 DEFINIZIONE ED ACRONIMI

La seguente tabella riporta le descrizioni o i significati degli acronimi e delle abbreviazioni presenti nel documento.

| Acronimi | Descrizione |
|---------------|--|
| AgID | Agenzia per Italia Digitale |
| API | Application Programming Interface |
| BI | Business Intelligence |
| CAD | Codice dell'Amministrazione Digitale |
| CONSIP | Consip S.p.A. |
| F/OSS | Free and Open Source Software |
| IaaS | Infrastructure as a Service |
| ICT | Information and Communication Technology |
| IE | Internet Explorer |
| IT | Information Technology |
| KPI | Key Performance Indicator |
| PA | Pubblica Amministrazione |
| PAC | Pubblica Amministrazione Centrale |
| PAL | Pubblica Amministrazione Locale |
| PaaS | Platform as a Service |
| SaaS | SaaS: Software as a Service |
| SPCoop | Sistema Pubblico di Connettività e Cooperazione |
| HTTP | Hyper Text Transport Protocol |
| HTTPS | Hyper Text Transport Protocol Secure |
| SAL | Stato Avanzamento Lavori |
| SAN | Storage Area Network |
| SGSI | Sistema di Gestione della Sicurezza delle Informazioni |
| SPC | Sistema Pubblico di Connettività |
| VDC | Virtual Data Center |
| VLB | Virtual Load Balancer |
| VM | Virtual Machine |
| VN | Virtual Network |
| VF | Virtual Firewall |
| VTS | Virtual Traffic Shaper |
| VPN | Virtual Private Network |

Tabella – Glossario

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

4 RIFERIMENTI

4.1 Documenti contrattuali

| Rif. | Documento |
|------|--|
| #1 | PIANO dei Fabbisogni SERVIZIO del 28/02/2017 |

Tabella dei documenti di contrattuali

4.2 Documenti di riferimento

La seguente tabella riporta i documenti che costituiscono il riferimento a quanto esposto nel seguito del presente documento.

| Rif. | Documento |
|------|--|
| #1 | BANDO DI GARA D'APPALTO – CONSIP S.p.A. |
| #2 | LOTTO 1 - Relazione Tecnica "Procedura ristretta suddivisa in 4 lotti per l'affidamento di Servizi di Cloud Computing, di Sicurezza, di Soluzioni di Portali di Servizi online e di Cooperazione Applicativa per le Pubbliche Amministrazioni" (ID SIGEF 1403)" |
| #3 | CAPITOLATO TECNICO – PARTE GENERALE – "Procedura ristretta suddivisa in 4 lotti per l'affidamento di Servizi di Cloud Computing, di Sicurezza, di Soluzioni di Portali di Servizi online e di Cooperazione Applicativa per le Pubbliche Amministrazioni" (ID SIGEF 1403)" |
| #4 | Piano di Sicurezza dei Centri Servizi e Centri Servizi Ausiliari Cod. BU1600003 |
| #5 | Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di test (Test Bed) |
| #6 | Piano di Qualità CONSIP |

Tabella dei documenti di riferimento

| | | | | |
|--|-----------|--|--|---------------------------------|
|  | | | Tipo documento: Progetto dei Fabbisogni | |
| Titolo documento: Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001 | | | | |
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO BAAS e PAAS

5.1 Descrizione

Il servizio “BaaS – Backup as a Service” permette alle Amministrazioni di acquistare e gestire in completa autonomia un servizio base di backup, per effettuare il salvataggio di dati presenti su server fisici di proprietà delle singole Amministrazioni o virtuali, compresi i dati di PC desktop o portatili del personale delle Amministrazioni stesse. Il servizio è fatturato a scaglioni sul consumo per mese per gigabyte archiviato.

I servizi di tipo Platform as a Service (PaaS) prevedono l'erogazione alle Amministrazioni di servizi middleware per lo sviluppo, collaudo, manutenzione ed esercizio di applicazioni. Ciascun PaaS poggia su infrastruttura hardware sottostante di tipo IaaS, del tutto trasparente all'Amministrazione.

Tali servizi PaaS sono resi disponibili dal Fornitore attraverso piattaforme e/o ambienti remoti utilizzati per ospitare ed erogare servizi applicativi sviluppati direttamente dalle Amministrazioni. I PaaS offerti dal Fornitore sono identificati attraverso una o più architetture software complete e non scindibili singolarmente (template di Solution Stack).

Il costo di acquisto del servizio PaaS è comprensivo delle risorse elaborative hardware minime necessarie al funzionamento del servizio.

L'Amministrazione ha comunque sempre facoltà di installare del software proprietario nel rispetto dei requisiti di compatibilità hardware e software e di capacità elaborativa. Eventuali risorse elaborative aggiuntive necessarie al corretto funzionamento del servizio possono essere acquistate dall'Amministrazione mediante l'utilizzo dei servizi IaaS.

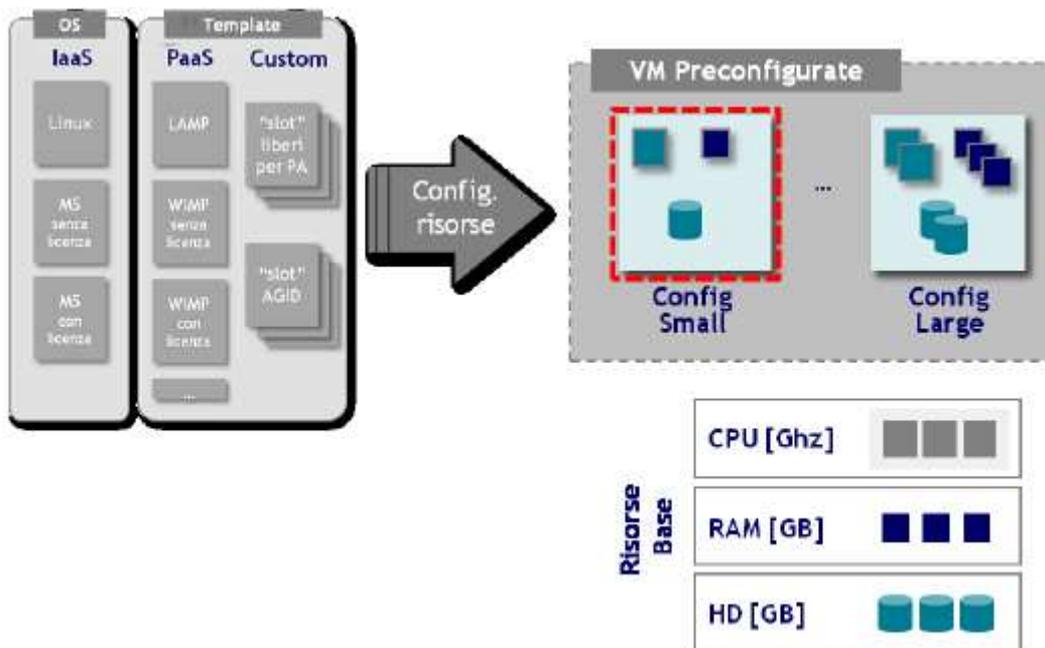
Le tipologie di template di Solution Stack si diversificano in funzione del servizio applicativo che viene erogato; la lista dei principali Solution Stack di tipo PaaS previsti includono le seguenti categorie:

- Application Server;
- Web Server;
- DBMS;
- Monitoring

come meglio specificato nella figura successiva che riporta il dettaglio delle architetture software previste. In figura inoltre è rappresentato il flusso attraverso il quale ciascuna Amministrazione può usufruire dei suddetti servizi PaaS.

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|



Nel servizio è inoltre inclusa la disponibilità di funzionalità e strumenti (console e/o pannelli) web-based che abilitano la fruizione di tali servizi e supportano funzionalità di acquisto, gestione e configurazione delle suddette risorse tramite workflow predefiniti.

La modalità di remunerazione del servizio "PaaS - Servizio Base" è "a canone" (risorse su base mensile).

5.2 Dettagli servizio contrattualizzato (ID servizio, quantità costi)

| Servizio | Elementi | Profilo | Quant | Durata mesi \ ore | | Importi Euro | Totale Euro |
|---------------------|------------------------------|---|-------|-------------------|-----------------------------|--------------|-------------|
| Backup as a Service | Medium - Consumo | da 6 a 50 GB di spazio di archiviazione | 6 | 24 | Elimina Backup as a Service | 24,8160 | 24,8160 |
| Elementi Opzionali | Virtual Network - Canone | vNetwork base - IP | - | | | | |
| Servizio PaaS | Monitoring - Pandora FMS CPU | 1 vCPU 2 GB RAM 10 GB HD | 1 | 24 | Elimina PaaS | 294,6240 | 294,6240 |
| Servizio PaaS | Web Server - LAMP | 1 vCPU 2 GB RAM 10 GB HD Linux, Apache, MySql, PHP | 1 | 24 | Elimina PaaS | 293,1120 | 884,9520 |
| Servizio PaaS | DBMS - Mysql | 1 vCPU 8 GB RAM 20 GB HD | 1 | 24 | Elimina PaaS | 410,1840 | 410,1840 |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

5.3 Configurazioni da realizzare

| | | |
|--|---|----------|
|  Web Server - LAMP | 1 vCPU 2 GB RAM 10 GB HD Linux, Apache, MySql, PHP | 1 |
| Risorse aggiuntive CPU - Canone | 1 GHz | 3 |
| Risorse aggiuntive RAM - Canone | 1 GB | 2 |
| Risorse aggiuntive Storage - Canone | 10 GB | 5 |
| Storage prestazionale - Canone | Dischi di tipo SAS o FC da almeno 15k rpm | - |
| Protezione Avanzata - Canone | Tempo di ripristino e Uptime migliorativi | - |
| Virtual Network -Canone | vNetwork base - IP | - |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

| | | |
|--|--|----------|
|  DBMS - Mysql | 1 vCPU 8 GB RAM 20 GB HD | 1 |
| Incremento per vCPU aggiuntive | 2 vCPU aggiuntive fino ad un massimo di 16 | - |
| Risorse aggiuntive RAM - Canone | 1 GB | - |
| Risorse aggiuntive Storage - Canone | 10 GB | - |
| Storage prestazionale - Canone | Dischi di tipo SAS o FC da almeno 15k rpm | - |
| Protezione Avanzata - Canone | Tempo di ripristino e Uptime migliorativi | - |
| Virtual Network -Canone | vNetwork base - IP | - |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

| | | |
|---|--|----------|
|  Monitoring - Pandora FMS CPU | 1 vCPU 2 GB RAM 10 GB HD | 1 |
| Incremento per vCPU aggiuntive | 2 vCPU aggiuntive fino ad un massimo di 16 | - |
| Risorse aggiuntive RAM - Canone | 1 GB | - |
| Risorse aggiuntive Storage - Canone | 10 GB | - |
| Storage prestazionale - Canone | Dischi di tipo SAS o FC da almeno 15k rpm | - |
| Protezione Avanzata - Canone | Tempo di ripristino e Uptime migliorativi | - |
| Virtual Network -Canone | vNetwork base - IP | - |

| | | | |
|---------------------|---|---|----------|
| Backup as a Service |  Medium - Consumo | da 6 a 50 GB di spazio di archiviazione | 6 |
| Elementi Opzionali | Virtual Network -Canone | vNetwork base - IP | - |

5.4 Specifiche di Collaudo

I test di collaudo saranno eseguiti presso la sede del Cliente.

Le seguenti linee guida descrivono lo svolgimento delle prove di collaudo atte a verificare la conformità delle configurazioni particolari richieste dall'Amministrazione per il servizio in oggetto e descritte nel relativo paragrafo del presente documento.

Le modalità di esecuzione ed i relativi documenti di output saranno conformi a quanto già previsto per il collaudo Consip.

I test saranno eseguiti secondo il seguente processo:

- 1) configurazione del servizio, degli apparati e degli strumenti in base a quanto specificato nella scheda di test;

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

- 2) esecuzione del test secondo quanto descritto nella relativa scheda;
- 3) se l'esito del test è positivo si ritorna al punto 1) procedendo con il test successivo;
- 4) se l'esito è negativo viene registrata l'anomalia, a cui è associato un livello di gravità (bloccante, grave, accettabile);
- 5) se l'anomalia è di tipo bloccante si sospende il test in corso proseguendo eventualmente con il test successivo tornando al punto 1).

Le anomalie saranno gestite con le seguenti modalità:

- **Classificazione:** ogniqualvolta sia rilevata una anomalia essa sarà registrata dall'operatore che esegue il test con la classificazione "grave". Sarà poi cura del team di verifica riclassificare, se necessario, l'anomalia in occasione dei controlli periodici di avanzamento della verifica.
- **Notifica di rilevamento:** la scheda anomalia compilata dall'operatore ed eventualmente quella con la riclassificazione operata dal team di verifica saranno inviate alle strutture di competenza.
- **Notifica di risoluzione:** le modalità di risoluzione delle anomalie saranno esaminate dal team di verifica in occasione dei controlli periodici di avanzamento delle verifiche in collaborazione con le strutture di competenza. Sarà quindi ripianificato il processo di verifica per effettuare i nuovi test a valle della risoluzione dell'anomalia.

Nel corso delle attività di verifica saranno condotti opportuni controlli di avanzamento con l'obiettivo di:

1. verificare l'avanzamento della pianificazione temporale;
2. analizzare le anomalie rilevate;
3. analizzare le modalità di risoluzione delle anomalie;
4. progettare i test di regressione per chiusura anomalie;
5. ripianificare le sessioni di test ed aggiornare la pianificazione temporale.

Il Piano di Test è articolato in schede, divise nelle seguenti sezioni:

| Campo | Significato |
|--------------------------------|--|
| Requisito | Identificativo del requisito oggetto del test |
| Scopo | Riassume l'obiettivo del test |
| Modalità di esecuzione | Indica la modalità di esecuzione del test, ad esempio per accesso diretto alla piattaforma, iniziando dall'accesso all'ambiente. |
| Scenario di riferimento | Descrive lo 'scenario utente' nel quale avviene il test e le condizioni che caratterizzano lo scenario |
| Macro azioni | Sono i passi operativi che si compiono durante la rappresentazione del test. |
| Risultato atteso | E' lo scenario utente atteso, a seguito dell'esecuzione del test. |

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

| | |
|-----------------------|---|
| Esito del test | E' l'esito del test, positivo se lo scenario ottenuto a seguito del test coincide con lo scenario atteso, negativo in caso contrario. |
|-----------------------|---|

6 DESCRIZIONE CENTRO SERVIZI

I Centri Servizi per la fornitura di tutti i Servizi Cloud previsti in convenzione, mettono a disposizione della Pubblica Amministrazione italiana le migliori caratteristiche di **affidabilità**, **solidità** e **sicurezza** disponibili sul mercato.

Il modello prevede:

- una zona riservata (anche detta "region") dedicata alla Pubblica Amministrazione italiana all'interno di ciascuno dei Centri Servizi primari (Rozzano e Inverno), per l'esercizio dei servizi;
- due region dedicate alla Pubblica Amministrazione italiana all'interno del centro di Disaster Recovery (Roma), in grado di subentrare ad una o ad entrambe le region di esercizio;
- una serie di centri che forniscono funzioni di controllo: Security Operation Center (SOC), Network Operation Center (NOC), Control Room.

La presenza di una doppia infrastruttura di esercizio è intesa ad assicurare maggiore **flessibilità** nella distribuzione del carico computazionale, il che garantisce maggiore **solidità** e **continuità operativa** all'intera fornitura. La soluzione è in linea con i dettami del "Community Cloud" e garantisce tempi di RTO e RPO migliorativi rispetto ai requisiti minimi di gara.

Rispetto al modello precedente, il servizio SaaS di Conservazione Digitale utilizzerà infrastrutture, già accreditate presso AgID o in fase di accreditamento, attestate presso il centro di Pomezia (primario) e i centri di Torino e Roma (Disaster Recovery).

I siti sono connessi fra loro attraverso la VDCN di Telecom (Virtual Data Center Network), rete di trasmissione dati ad altissima velocità attraverso la quale un Centro Servizi ad essa afferente può erogare i servizi IT verso le reti pubbliche e generare traffico di allineamento dati con gli altri centri del Raggruppamento. Più specificamente, la VDCN è una rete IP/MPLS costituita da un anello ottico realizzato attraverso collegamenti in tecnologia DWDM a multipli di 10Gbps e ricavato sul backbone trasmissivo della Rete di Trasporto Nazionale di Telecom Italia, la dorsale della più grande infrastruttura di connettività disponibile nel nostro paese. L'elevata capacità di forwarding di questa rete, la sua affidabilità e la sua rapida scalabilità le consentono di garantire una totale continuità del servizio. Ciò permette di considerare tutto il modello architetturale come un unico grande centro di erogazione dei servizi.

I Centri Servizi sono collegati sia ad Internet sia alla rete SPC, il che consentirà alle Amministrazioni contraenti di **usufruire dei servizi senza soluzione di continuità**

Il Centro Servizi Telecom di Roma fungerà da Sito di Disaster Recovery. La distanza del sito dai Centri Servizi primari garantisce la continuità operativa a fronte di qualsiasi scenario possibile di indisponibilità:

- infrastruttura hardware fuori uso;
- perdita dei dati elaborati tramite l'infrastruttura;
- evento disastroso che renda il Centro Servizi inagibile e non più funzionante;
- evento disastroso che interessi una area geografica ampia.

La protezione da questi eventi è garantita da un insieme di misure:

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|------------|--|--------------|---------------------------------|
| Emesso da: | B.S./C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|------------|--|--------------|---------------------------------|

- impianti di sicurezza dei Centri Servizi (sistemi anti-incendio, anti-allagamento, anti-intrusione, continuità elettrica);
- tecniche di ridondanza delle infrastrutture IT (connettività, sistemi elaborativi e sistemi di storage duplicati con tecniche di clusterizzazione, mirroring, virtualizzazione, ecc.) che garantiscono un alto --grado di resilienza all'insorgere di guasti;
- backup dei dati delle Amministrazioni sia su infrastrutture di storage poste in ambienti separati dei Centri Servizi con garanzia di elevata protezione fisica, sia su copie di sicurezza trasferite in caveau esterni;
- trasferimento dei dati dai siti di produzione al sito di Disaster Recovery attraverso le funzionalità dei -sistemi di storage, con indici RTO ≤ 4 ore e RPO ≤ 1 ora (vedi anche §5.1);
- trasferimento dei dati dai siti di produzione al sito di Disaster Recovery, con meccanismi tali da -assicurare valori RTO e RPO uguali o inferiori a quattro ore e un'ora rispettivamente

Ogni Centro Servizi ha il suo Piano di Disaster Recovery. Nel momento in cui si verifica un problema e/o un disservizio all'interno del Centro Servizi, viene attivato il **processo di escalation** che include una procedura operativa che ha lo scopo di informare istantaneamente il management di eventi particolarmente significativi.

Mezzi preferenziali per attivare il "team di crisi" sono la chiamata in voce o l'SMS, con modalità che tutelano la tracciabilità di tutte le comunicazioni avvenute. Le informazioni pervenute sono analizzate al fine di stabilire se il livello di criticità raggiunto è tale da richiedere il coinvolgimento dei livelli superiori: in tal caso, si attiva l'escalation di 2° livello che prevede il coinvolgimento del Responsabile dei Centri Servizi, che ha il compito di attivare il Comitato di Crisi se il problema viene classificato come "disastro"

Il Comitato di Crisi è composto dal Responsabile del Contratto Quadro, dal Responsabile dei Centri Servizi e dai Coordinatori di tutti i siti.

Il comitato ha il compito di:

- analizzare velocemente il problema in corso e dichiarare lo stato di emergenza;
- attivare il Piano di Disaster Recovery;
- reperire personale o apparati di supporto alle attività;
- gestire la comunicazione interna ed esterna;
- seguire l'evolversi della situazione e l'avanzamento delle attività di ripristino e di rientro;
- al termine dell'emergenza, compilare una relazione sulle attività svolte e avviare eventuali iniziative di miglioramento intese ad evitare l'insorgere di eventi analoghi in futuro.

Il modello di servizio viene completato dai *Centri Servizi ausiliari*. Si tratta di unità operative dislocate sul territorio italiano e focalizzate sulla gestione dell'infrastruttura tecnologica, con particolare riferimento alle architetture tecniche, alle piattaforme (storage, server, network) e ai servizi infrastrutturali (backup, monitoraggio, asset management, disaster recovery, ecc.).

La scelta di separare fisicamente i Centri Servizi ausiliari dai Centri Servizi propriamente detti è in primo luogo funzionale alla necessità di **garantire la continuità operativa**.

Infatti:

- in caso di disastro in uno dei Centri Servizi primari gli operatori dei centri ausiliari possono continuare a svolgere le loro attività senza necessità di trasferimenti;
- al tempo stesso, l'attività dei centri ausiliari non richiede particolari infrastrutture in loco (gli operatori accedono ai sistemi attraverso le reti aziendali, con credenziali d'accesso specifiche e riservate): in caso di problemi tecnici nella sede di un centro ausiliario, gli operatori possono spostarsi in una diversa sede aziendale e proseguire la loro attività.

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

Vediamo quali sono i Centri Servizi ausiliari.

SOC (Security Operation Center) – Si occupano di tutte le attività volte ad assicurare la sicurezza dei sistemi e delle operazioni che rientrano nel perimetro della fornitura, secondo una logica di interoperabilità ed integrità. Le attività del SOC si riconducono a questi macro-blocchi:

- Security Risk Management: tutte le iniziative per la definizione e la gestione del rischio informatico declinato in funzione delle esigenze operative;
- Security Intelligence & Incident Response: attività che hanno come fine ultimo l'evoluzione delle discipline di gestione, di risposta e di analisi degli eventi di sicurezza, da attività manuali a processi automatizzati, che sfruttano la conoscenza del contesto (intelligence) per attivare risposte automatiche agli attacchi informatici;
- Threat & Vulnerability Management: iniziative intese ad individuare il livello di minaccia e identificare/gestire la soluzione nell'ambito delle vulnerabilità di sistema, infrastrutturali e applicative;
- Data Protection & Privacy: individuazione, e gestione del livello di sensibilità delle informazioni in uso, in transito e archiviate, in conformità alle normative vigenti (es., D.Lgs. 196/2003 e s.m.i.);
- Secure Identity & Access: gestione del ciclo di vita delle identità, in termini di riconducibilità a persona fisica degli account di sistema canonici e/o privilegiati, di accesso standard e/o federato alle risorse informatiche, di strong authentication;
- Application Security: supporto all'individuazione, all'analisi e alla gestione delle vulnerabilità del codice applicativo;
- Security Architecture: revisione periodica delle architetture di sicurezza, per colmare le non conformità individuate in sede di valutazione del rischio e le vulnerabilità in genere;
- Digital Investigation & Forensic: analisi delle motivazioni, raccolta delle evidenze di attacco ai fini legali, eventuale stima del danno e raccomandazioni da adottare a valle di un attacco informatico;
- Governance & Compliance: definizione di processi, procedure e politiche per la corretta gestione delle informazioni di sicurezza e l'analisi delle eventuali non conformità verso le best practice, definite dagli standard di mercato (ISO27001, ISAE2434002, PCI DSS, ecc.) e dalle normative di legge.

NOC (Network Operation Center) – Sono le strutture deputate al monitoraggio, alla gestione e alla configurazione dell'infrastruttura di rete del Centro Servizi (LAN di Data Center e delle postazioni di lavoro). Le attività svolte includono la supervisione proattiva/reattiva della rete, la ricezione di reclami e/o richieste di supporto su tematiche di rete, diagnosi di primo livello e di secondo livello, correlazione di allarmi, intervento da remoto, inoltro delle segnalazioni verso altri enti in funzione delle competenze, monitoraggio/supporto fino alla chiusura dell'anomalia.

Control Room – Si occupano di monitorare e gestire le infrastrutture ospitate nei Centri Servizi. Sono costituite da team di specialisti, in possesso delle competenze metodologiche e tecniche necessarie per coprire tutte le attività di analisi e gestione sistemistica delle risorse IT (sistemi operativi, database, middleware). In particolare, al personale delle Control Room sono affidate attività di Capacity Planning, attività di valutazione di impatto (impact analysis) che precedono il change management, attività di monitoraggio e gestione incident, software distribution (es. inserimento di patch di aggiornamento software) – includendo in quest'ultima categoria anche le eventuali attività di test in ambiente di pre-produzione, per la verifica preventiva dei potenziali impatti sul servizio.

I Centri Servizi ausiliari sono ubicati come segue:

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

- per Telecom: il SOC, il NOC e la Control Room sono attestati a Roma (su sedi distinte);
- per HP: il SOC è attestato a Pomezia, il NOC a Cernusco sul Naviglio; le Control Room sono due, una dedicata alle attività di monitoraggio e attestata a Bari, l'altra alle attività più propriamente di gestione e attestata a Cernusco sul Naviglio;
- per Postel: il NOC e la Control Room sono attestate a Pomezia, il SOC a Roma.
- Nel caso di indisponibilità di uno di questi centri, l'operatività viene spostata rispettivamente su:
 - SOC Telecom di Napoli;
 - NOC Telecom di Roma (sede diversa da quella del NOC primario);
 - Control Room Telecom di Milano;
 - SOC/NOC HP di Roma;
 - Control Room HP di Cernusco sul Naviglio o di Bari (il sito rimasto attivo eroga tutta l'attività);
 - SOC/NOC/Control Room Postel di Genova.
- Per effetto del modello, restano presso i Centri Servizi le sole funzioni responsabili dei servizi di facility (spazi, condizionamento, alimentazione, cablaggio) e dei servizi di prossimità.

7 MODALITÀ DI PRESENTAZIONE E APPROVAZIONE STATI AVANZAMENTO MENSILI

Al fine di verificare l'andamento del servizio, sino al superamento del collaudo, lo RTI produrrà dei SAL (Stato Avanzamento Lavori) mensili contenenti le seguenti informazioni:

- avanzamento delle attività relative al piano di realizzazione dell'infrastruttura dedicata al sito;
- evidenze di eventuali scostamenti rispetto al piano temporale di realizzazione;
- eventuali proposte per la nuova pianificazione delle attività;
- evidenze di attività correttive intraprese per la gestione delle criticità rilevate;
- esito di eventuali collaudi parziali e del collaudo finale effettuati;
- varianti e modifiche emerse nel periodo.

I SAL saranno prodotti con cadenza mensile a partire dalla data di approvazione del Progetto stesso ed entro il 15 del mese successivo a quello di riferimento del SAL.

Tutti i SAL saranno soggetti ad approvazione da parte dell'Amministrazione.

Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1: Regione Abruzzo - DPH001**

| | | | | |
|------------|-----------|--|--------------|---------------------------------|
| Emesso da: | B.S/C.PSD | Codice documento: 178000317 0661002Pdf | Versione 1.0 | Data di emissione 10/04/2017 |
|------------|-----------|--|--------------|---------------------------------|

8 PIANO DI ATTUAZIONE DEL SERVIZIO

8.1 Piano di Lavoro Servizio SaaS – Conservazione Digitale

La piattaforma sarà resa disponibile all'Amministrazione entro i termini e le modalità stabilite nel Capitolato Tecnico e relative Appendici. Le modalità e le tempistiche di rilascio saranno comunque concordate con l'Amministrazione.

8.2 Documento Programmatico di Gestione della Sicurezza dell'Amministrazione

Il Documento programmatico di gestione della Sicurezza verrà consegnato entro 20 gg dalla data in cui l'Amministrazione Contraente ne farà richiesta.

9 TABELLA RIEPILOGATIVA FINALE SERVIZI

| Famiglia di Servizi | Durata | Canone Annuo | Totale |
|------------------------------|---------|--------------|-------------------|
| PaaS – Platform As A Service | 24 mesi | 794,88€ | 1589,76€ |
| BaaS – Backup As A Service | 24 mesi | 12,408€ | 24,816 |
| TOTALE | | | 1.614,576€ |