Scheda di Obiettivo BDSR-003-2022
Cloud Infrastructure and Security

AFFIDAMENTO DI SERVIZI APPLICATIVI DI DATAMANAGEMENT MEDIANTE ORDINATIVO DI FORNITURA NELL'AMBITO DELL'ACCORDO QUADRO PER I SERVIZI APPLICATIVI DI DATA MANAGEMENT PER LE PUBBLICHE AMMINISTRAZIONI STIPULATO DA CONSIP - ID 2212 – LOTTO 1

CIG DERIVATO 9144969B25 – CUP J81F22000000001

Versione: 3.0

Data: 28/10/2022

TABELLA DELLE VERSIONI			
Data	**Versione**	**Descrizione**	**Par. modificati**
28/07/2022	1.0	Prima redazione del documento	Tutti
23/09/2022	2.0	Aggiornamento post revisione congiunta	Tutti
28/10/2022	3.0	Aggiornamento modalità di fatturazione	Tutti

Scheda Intervento

Titolo obiettivo	Cloud Infrastructure and Security		
Valore economico dell'obiettivo	**562.534,61 €**		
Descrizione dell'intervento	A seguire si riportano i temi oggetto di intervento: • **Infrastruttura DM (core)** – progettazione e realizzazione dell'infrastruttura DM all'interno del Public Cloud Provider AWS, comprensiva degli ambienti infrastrutturali Collaudo e Produzione; • **Security** - Attività di Supporto alle fasi di design e sviluppo dell'infrastruttura. • **Competence Center DevOps & Architecture** – definizione processi, linee guida e piattaforma DevOps e avvio del Competence Center di supporto ai gruppi Applicativi e delle Operations, per i servizi applicativi da rilasciare in ambito AWS.		
Responsabile intervento (fornitore)	Michele Del Prete (Accenture)		
Responsabile intervento (MiTur)	Filippo Corsi		
Ciclo di vita	Iterativo		
Data inizio	01/07/2022		
Data fine	21/10/2022		
Servizio Attivato	LA.DW.6 - Supporto Specialistico	LA.DW.1 - Sviluppo e manutenzione evolutiva di software ad hoc	Seleziona
Metrica	Team Ottimale	Consumo GG/PP	Seleziona
Tariffa	226,15 €	248,12 €*	-
Quantità	1.195	1.178	-
Importo	**270.249,25 €**	**292.285,36 €**	**-**

* La tariffa è stata calcolata con media delle tariffe delle singole figure professionali previste da contratto

Descrizione dell'intervento

L'intervento relativo alla presente scheda obiettivo ha come ambito:

- **Infrastruttura Data Management (DM)** – progettazione e realizzazione dell'infrastruttura DM all'interno del Public Cloud Provider AWS, comprensiva degli ambienti infrastrutturali Collaudo e Produzione;
- **Security** - Attività di Supporto alle fasi di design e sviluppo dell'infrastruttura.

Linea di Servizio	Attività
LA.DW6 – Supporto Specialistico	**Realizzazione e messa in linea dell'infrastruttura per il tenant infrastrutturale volto ad ospitare l'ambiente di Collaudo DM** Attività di Analisi e Design per la realizzazione di un'infrastruttura cloud, sulla piattaforma target AWS, che ospiterà la soluzione DM. L'attività prevede: • stesura dei requisiti di rete per definire le mimiche di accesso verso la piattaforma DM, nonché di comunicazione interna tra le componenti applicative ed esterna, verso i servizi componenti la piattaforma DM esterni alla bolla Cloud ospitata all'interno del Public Cloud Provider AWS; • disegno dell'architettura infrastrutturale volta ad ospitare gli ambienti non produttivi (Collaudo); • disegno dell'architettura di provisioning automatico dell'infrastruttura, omnicomprensiva degli strumenti che ne consentono la predisposizione attraverso il paradigma Infrastructure as Code (IaC), nonché delle mimiche di provisioning e aggiornamento delle configurazioni; • aggiornamento del capacity plan con le nuove componenti infrastrutturali previste dall'architettura, omnicomprensivo delle previsioni per l'ambiente di produzione; • stesura dei casi di test di accesso, comunicazione e rilascio applicativo; • predisposizione degli script per il provisioning automatico dei servizi infrastrutturali attraverso il paradigma IaC; • provisioning dell'infrastruttura per l'ambiente di Collaudo attraverso l'esecuzione degli script IaC sviluppati; • esecuzione dei test di accesso e comunicazione; • redazione della manualistica di gestione dell'infrastruttura per i gruppi di Operations. **Realizzazione e messa in linea dell'infrastruttura per il tenant infrastrutturale volto ad ospitare l'ambiente di Produzione DM** Attività di Analisi e Design per la realizzazione di un'infrastruttura cloud, sulla piattaforma target AWS, che ospiterà la soluzione infrastrutturale di Produzione. L'attività prevede: • stesura dei requisiti di rete per definire le mimiche di accesso verso la piattaforma DM, nonché di comunicazione interna tra le componenti applicative ed esterna, verso i servizi componenti la piattaforma DM esterni alla bolla Cloud ospitata all'interno del Public Cloud Provider AWS; • disegno dell'architettura infrastrutturale volta ad ospitare gli ambienti non produttivi (Produzione), in cui occorre tenere conto anche degli aspetti non funzionali di disponibilità e scalabilità, in linea con i volumi attesi e/o di garantire eventuale resilienza infrastrutturale in caso di volumi inattesi; • integrazione dell'infrastruttura con eventuali sistemi terzi di produzione; • aggiornamento del capacity plan con le nuove componenti infrastrutturali previste dall'architettura, omnicomprensivo delle previsioni per l'ambiente di produzione;

- stesura dei casi di test di accesso, comunicazione e rilascio applicativo;
- predisposizione degli script per il provisioning automatico dei servizi infrastrutturali attraverso il paradigma IaC;
- provisioning dell'infrastruttura per l'ambiente di Produzione attraverso l'esecuzione degli script IaC sviluppati;
- esecuzione dei test di accesso e comunicazione;
- redazione della manualistica di gestione dell'infrastruttura per i gruppi di Operations.

Sicurezza dell'infrastruttura DM

L'architettura e lo sviluppo del sistema dovranno avvenire, nel rispetto non solo delle specifiche tecniche ma anche di sicurezza e privacy.

Per la sicurezza del dato e per l'affidabilità della soluzione si adotta il paradigma del "privacy by design" e del "privacy by default", introdotto dal GDPR dove, il concetto di privacy by default intende sottolineare la necessità che le architetture debbano applicare principi legati alla sicurezza del dato "di default", cioè come impostazione predefinita. Il concetto di privacy by design si riferisce alla necessità di tutelare il dato sin dalla progettazione di sistemi informatici che ne prevedano l'utilizzo.

L'intervento previsto è quello di definire, descrivere ed implementare i requisiti di sicurezza infrastrutturali della soluzione proposta tramite l'adozione del Cloud AWS. A seguire si riporta la descrizione delle attività:

- supporto al design dell'infrastruttura sistemistica;
- disegno e configurazione integrazione con Spid;
- supporto alla configurazione degli strumenti di sicurezza negli ambienti AWS del DM per il perimetro infrastrutturale;
- configurazione dei moduli IAM;
- redazione documentazione di sicurezza (Documento di linee guida e requisiti);
- vulnerability assessment infrastrutturale.

Attività di Analisi e Design per la realizzazione dei processi DevOps, per la gestione dei flussi d'automazione per la piattaforma DM all'interno del Public Cloud Provider AWS. Si prevedono le seguenti attività continuative, erogate dal Competence Center "DevOps & Architecture":

- analisi e disegno dei processi del ciclo di vita del software, tra i team di sviluppo applicativo (Dev) e di Operations (Ops), per consentire:
  - la predisposizione degli ambienti applicativi all'interno dell'infrastruttura AWS del DM;
  - gli aggiornamenti delle configurazioni all'interno di ogni singolo ambiente applicativo;
  - il rilascio automatizzato delle applicazioni;
  - la promozione automatica delle applicazioni attraverso la catena di delivery del software;
  - il versioning degli ambienti e delle applicazioni;
- declinazione dell'architettura delle nuove componenti applicative verso il catalogo dei servizi AWS a disposizione del Ministero;
- attività di fine tuning prestazionali

Threat modeling ("Banca Dati Strutture Ricettive")

Attività di analisi della documentazione architetturale, di design, di requisito e della documentazione progettuale, volto a innalzare il livello di sicurezza già in fase di impostazione del progetto e finalizzata a:

- rilevare le risorse da proteggere;
- identificare e classificare le minacce potenziali;
- valutare il rischio delle minacce in termini di livello di impatto e probabilità di accadimento;

	• rilevare le principali criticità, vulnerabilità strutturali o l'assenza, al momento dell'analisi, di misure di sicurezza adeguate; • definire i rimedi potenziali da mettere in campo per L'attività prevede in particolare l'analisi della seguente documentazione tecnica: • design architetturale; • low level design della componente applicativa; • workflow applicativi; • misure di sicurezza eventualmente in essere. **Code review ("Banca Dati Strutture Ricettive")** Attività di analisi statica del codice, finalizzata alla verifica di adeguatezza dello stesso in termini di sicurezza e di qualità. Per quanto riguarda l'analisi di sicurezza, l'attività è rivolta a rilevare le vulnerabilità presenti, secondo quanto previsto dai principali standard internazionali di settore (OWASP, CWE, SANS), proponendo possibili remediation. Con riferimento all'analisi di qualità, l'attività è rivolta a fornire indicazioni sulle modalità volte alla riduzione della complessità del codice, al fine di migliorarne la leggibilità e la manutenibilità. L'attività di Code review prevede in particolare: • l'acquisizione del codice da testare in un ambiente dedicato; • la scansione di tutte le righe di codice dell'applicazione tramite l'ausilio di strumenti automatizzati, messi a punto con un set di regole di sicurezza customizzate; • l'individuazione delle vulnerabilità di sicurezza del codice e degli ambiti di miglioramento qualitativi; • la definizione dei possibili rimedi volti alla risoluzione delle criticità riscontrate. **Security Assessment ("Banca Dati Strutture Ricettive")** L'attività prevede l'esecuzione delle seguenti due categorie di assessment: • Penetration Test infrastrutturali su perimetro interno; • Penetration Test applicativi su perimetro esposto su internet. I Penetration Test simulano un attacco informatico verso un'infrastruttura o un un'applicazione o asset di altro tipo, tramite attività di expoiting manuale e con l'ausilio anche di tool semi-automatici, costantemente monitorati dal team di assessment. Il fine ultimo dell'attività è l'individuazione delle vulnerabilità cui è esposta l'applicazione o l'infrastruttura e l'indicazione delle azioni rivolte alla mitigazione delle stesse. Per l'erogazione del servizio verranno applicati i seguenti standard internazionali: • OWASP; • OSSTTMM; • ISECOM. In particolare, il **Penetration Test infrastrutturale** è rivolto alla verifica del livello di sicurezza degli asset infrastrutturali e degli host che costituiscono un servizio o un'applicazione (sistemi di back-end, web server, application server, database, etc.). Tale tipo di servizio può essere erogato, rispetto all'infrastruttura che si intende testare, sia da segmenti interni che esterni della rete, in modalità black box o gray box. Il **Penetration Test applicativo** consiste nell'analisi delle vulnerabilità di una applicazione web, effettuata tramite tentativi di attacco reali aventi come obiettivo la compromissione dell'applicazione e dei suoi dati. Dato il livello di accesso ottenuto si tenderà infatti a compiere azioni solitamente non ammesse, dimostrando la possibilità di prelevare dati dal database, esfiltrare file o sorgenti dal disco, modificare informazioni e laddove possibile ottenere il pieno controllo della macchina.

Pianificazione, deliverable e stima

Fermo restando quanto riportato nella documentazione contrattuale e all'interno del Piano di Qualità Specifico del presente Contratto Esecutivo, le informazioni riportate di seguito in merito a "pianificazione" e "deliverable" sono da intendersi in deroga rispetto a tale documento per la presente scheda obiettivo.

Pianificazione:

Sprint	Fase	Criterio di Uscita	Data inizio	Data fine
1	Sprint	Approvazione sprint	01/07/2022	31/07/2022
	Validazione dello sprint		29/07/2022	31/07/2022
2	Sprint	Approvazione sprint	01/08/2022	31/08/2022
	Validazione dello sprint		29/08/2022	31/08/2022
3*	Sprint	Approvazione sprint	01/09/2022	14/10/2022
NA	Collaudo finale	Accettazione (verifica di conformità)	17/10/2022	21/10/2022

* In deroga a quanto previsto contrattualmente, lo sprint avrà una durata maggiore di un mese per consentire la corretta esecuzione e coerenza di tutte le attività previste.

Deliverable:

Sprint	Fase	Deliverable	Data fine

1	Sprint	**Realizzazione infrastruttura di collaudo e Produzione per ospitare le componenti applicative Banca Dati Strutture Ricettive**
		• (BDSR-003-2022_01) Documento (PDF) contenente il dettaglio dei setup delle componenti infrastrutturali predisposte, in cui si prevede:
		  ○ una sezione in cui sono riportati gli screenshot relativi alle configurazioni delle componenti per l'ambiente di collaudo;
		  ○ una sezione in cui sono riportati gli screenshot relativi alle configurazioni delle componenti per l'ambiente di produzione
		• (BDSR-003-2022_02) Disegno architetturale (PDF) componenti per l'integrazione con SPID
			29/07/2022

2	Sprint	**Realizzazione infrastruttura di collaudo e Produzione per ospitare le componenti applicative Banca Dati Strutture Ricettive** • (BDSR-003-2022_03) Documento (DOCX) contenente il dettaglio dell'architettura infrastrutturale del tenant di Collaudo di DM • (BDSR-003-2022_04) Documento (DOCX) contenente il dettaglio dell'architettura infrastrutturale del tenant di Produzione di DM	31/08/2022

		Attività di Analisi e Design per la realizzazione dei processi DevOps, per la gestione dei flussi d'automazione per la piattaforma DM all'interno del Public Cloud Provider AWS. • (BDSR-003-2022_05) Documento (DOCX) contenente il report mensile degli interventi effettuati dal gruppo DevOps&Architecture Competence Center **Vulnerability assessment infrastrutturale** • (BDSR-003-2022_06) Report (DOCX) esecuzione vulnerability assessment infrastrutturale	
3	Sprint	**Aggiornamento dell'infrastruttura di Collaudo con nuove estensioni delle applicazioni esistenti ("Banca Dati Strutture Ricettive")** • (BDSR-003-2022_07) Documento (DOCX) contenente il dettaglio dell'architettura infrastrutturale del tenant di Collaudo di DM, in cui si prevede: o una sezione in cui è dettagliata l'analisi e il disegno dell'estensione dei tenant infrastrutturali, ospitanti le applicazioni "Banca Dati Strutture Ricettive"; o script di Infrastructure as Code relative al provisioning automatico dell'infrastruttura implementata. **Aggiornamento dell'infrastruttura di Produzione con nuove estensioni delle applicazioni esistenti ("Banca Dati Strutture Ricettive")** • (BDSR-003-2022_08) Documento (DOCX) contenente il dettaglio dell'architettura infrastrutturale del tenant di Produzione di DM, in cui si prevede: o una sezione in cui è dettagliata l'analisi e il disegno dell'estensione dei tenant infrastrutturali, ospitanti le applicazioni "Banca Dati Strutture Ricettive"; o script di Infrastructure as Code relative al provisioning automatico dell'infrastruttura implementata. **Attività di Analisi e Design per la realizzazione dei processi DevOps, per la gestione dei flussi d'automazione per la piattaforma DM all'interno del Public Cloud Provider AWS.** • (BDSR-003-2022_09) Documento (DOCX) contenente il report mensile degli interventi effettuati dal gruppo DevOps&Architecture Competence Center	30/09/2022
		Threat modeling ("Banca Dati Strutture Ricettive") • (BDSR-003-2022_10) Documento (PDF) strutturato come Report e suddiviso in due sezioni. Nella prima sono rappresentate le potenziali minacce e i problemi di sicurezza riscontrati, per i quali viene fornita una valutazione dei rischi, in relazione alle conseguenze (impatti) e alla probabilità di accadimento dell'evento avverso.	14/10/2022

		Nella seconda sezione sono riportati i potenziali rimedi applicabili per ciascuna delle minacce individuate. **Code review ("Banca Dati Strutture Ricettive")** • (BDSR-003-2022_11) Documento (XLS) strutturato come Report nel quale viene indicato l'esito dell'attività di Code Review. Il report viene strutturato su due livelli: un **executive summary**, orientato al management, contenente informazioni di "alto livello" sui test e un **dettaglio tecnico**, contenente l'analisi di tutte le vulnerabilità, le anomalie individuate e le azioni suggerite per la mitigazione delle stesse. **Security Assessment ("Banca Dati Strutture Ricettive")** (BDSR-003-2022_12) Documento (PDF) strutturato come Report suddiviso in suddiviso in tre sezioni: - Executive summary: sezione del documento prevalentemente orientata al management, contenente una panoramica di alto livello sulle attività eseguite e i risultati ottenuti; - Technical Report: sezione contenente un'analisi di dettaglio di tutte le vulnerabilità riscontrate, orientata ad evidenziare gli step da seguire per riprodurre le stesse; - Remediation Plan: sezione del documento contenente i suggerimenti relativi alle tecniche di mitigazione dei problemi di sicurezza che sono stati riscontrati nel corso dell'intera attività.	

Stima:

Sprint	Metrica	Servizio	Tariffa	Quantità	Data inizio	Data fine	Valore economico
1	Team Ottimale	LA.DW.6	€ 226,15	352	01/07/2022	31/07/2022	€ 79.604,80
1	Consumo GG/PP	LA.DW.1	€ 248,12	576	01/07/2022	31/07/2022	€ 142.917,12
2	Team Ottimale	LA.DW.6	€ 226,15	151	01/08/2022	31/08/2022	€ 34.148,65
2	Consumo GG/PP	LA.DW.1	€ 248,12	302	01/08/2022	31/08/2022	€ 74.932,24
3	Team Ottimale	LA.DW.6	€ 226,15	692	01/09/2022	14/10/2022	€ 156.495,80
3	Consumo GG/PP	LA.DW.1	€ 248,12	300	01/09/2022	14/10/2022	€ 74.436,00

Si riporta di seguito la modalità di fatturazione prevista per la presente scheda:

- ***Quota fissa***
  - *5% dell'importo totale in corrispondenza dell'attivazione della scheda.*
  - *60% dell'importo del singolo sprint in corrispondenza dell'accettazione del medesimo sprint.*

- *35% dell'importo totale in corrispondenza della chiusura complessiva del collaudo della scheda.*

- ***Quota variabile***
  - *In corrispondenza del superamento degli indici di prestazione relativi agli specifici servizi utilizzati.*

Vincoli, assunzioni, punti di attenzione ed eventuali ulteriori note

#	Tipo	Descrizione
1	Assunzione	Le attività di supporto si intendono in orario lavorativo, 5 giorni su 7 dalle ore 9 alle 18. L'ingaggio del team potrà avvenire attraverso sistema di ticketing e/o canale e-mail concordato.
2	Assunzione	Si assume che il perimetro tecnologico per l'intervento è rappresentato dal public cloud provider AWS
3	Assunzione	Gli interventi di setup infrastrutturali sono previsti esclusivamente per gli account AWS di Collaudo e Produzione, non saranno predisposti gli account AWS di Integrazione e Pre-Produzione.
4	Assunzione	Il provisioning dell'environment di Produzione non prende in considerazione analisi e setup del sito di Disaster Recovery.