Allegato

Agenda digitale dell'Umbria

Regione Umbria

Unione Europea
Fondo Europeo
di Sviluppo Regionale

REPUBBLICA ITALIANA

Regione Umbria

UMBRIA por FESR
Programma Operativo Regionale
Fondo Europeo
di Sviluppo Regionale

Progetto PRJ-___ CUP _____

" ICT Security 2021-2022 "

Documentazione progettuale vigente:

☒Quadro esigenziale (*business case*)

☐Progetto di fattibilità (ove sia necessario)

☐Progetto definitivo (*project brief*)

☐Progetto esecutivo (*PID)*

☑Cronoprogramma

☑Prospetto economico

1. Stato del documento

1.1 Storico revisioni

Versione	Emesso il	Stato rilascio	Contributori	Parti del documento	Variazioni da versione precedente
1.0	__/__/2021	approvato dal dirigente executive __ con atto DD. n.___ del __/__/2021 (trasmesso con nota prot.n. _____) inserito nel PDRT con DGR n.___ del __/__/2021	---------- ---------- F.Azzola G. Cecchetti M. Tosti	Parte I business case	prima stesura del business case
				Allegato: crono-programma	prima stesura
				Allegato:prospetto economico	prima stesura

1.2 Scopo del documento

- Il Quadro esigenziale "*Business Case*" serve a documentare la giustificazione per l'esecuzione di un progetto in base ai costi stimati (non solo per lo sviluppo e l'implementazione, ma anche i costi che dovranno essere sostenuti durante l'esercizio e la manutenzione) rispetto ai benefici previsti, prendendo inoltre in considerazione gli eventuali rischi correlati e le tempistiche necessarie. Il documento individua, sulla base dei dati disponibili, gli obiettivi generali da perseguire attraverso la realizzazione dell'intervento, i fabbisogni della collettività posti a base dello stesso, le specifiche esigenze qualitative e quantitative che devono essere soddisfatte anche in relazione alla specifica tipologia di utenza destinataria;
- Il Progetto definitivo "*Project Brief*" (anche definito "*Charter*") definisce scopo, costo, tempistica e requisiti di prestazione, nonché restrizioni al progetto. Viene creato durante il processo di avvio di un progetto, e viene utilizzato durante il processo di inizio al fine di creare il Progetto esecutivo (PID).
- Il Progetto esecutivo "*PID*" (anche definito "*Piano di progetto*" o "*Handbook*") definisce progressivamente i contenuti del progetto al fine di costituire la base per la sua gestione, la valutazione del suo successo globale e per distribuire le informazioni a tutti gli interessati al progetto. Il PID guida l'esecuzione del progetto e, per ogni fase, costituisce il "contratto" tra il *Project Manager* e il Comitato di Progetto.

1.3 Rimando ad altri documenti da considerare parte integrante

- Linee guida strategiche per lo sviluppo della Società dell'Informazione (LGSI) di cui alla legge regionale n.9/2014 vigente
- DGR n.1778/2014 sul Disciplinare per l'attuazione della legge regionale n.9/2014, pubblicato nel Supplemento ordinario n.3 al B.U.R. n.14 dell'11/03/2014
- DGR n.371/2015 sul Modello operativo per i dataset del patrimonio informativo e gli open data (MOOD)
- DGR n.1572/2015 sul Repository regionale del codice sorgente e delle buone pratiche per il riuso
- DGR n.1560/2016 sul Quadro di riferimento per l'attuazione del PDRT nella Giunta regionale e per il Contratto tra Giunta e Umbria Digitale Scarl
- DGR n.825/2019 su Ufficio per la transizione al digitale e Responsabile per la transizione digitale di cui all'art.17 del d.lgs. n.82/2005
- DGR n.826/2019 rispetto all'Interoperabilità attraverso interfacce API, pubblicata nel BUR n. 34 del 10/07/2019 Serie generale
- DGR n.1085/2019 rispetto a Sicurezza informatica, Abilitazione al *cloud* ed Accesso unico a servizi/dati
- Piano triennale per l'informatica nella PA vigente
- Linee guida strategiche per lo sviluppo della Società dell'Informazione (LGSI) di cui alla legge regionale n.9/2014 (definite con DGR n.155 del 20/02/2017 e successivamente approvate con deliberazione n.213 del 28/11/2017 dell'Assemblea legislativa regionale)
- Disciplinare per l'attuazione della legge regionale n.9/2014 di cui alla DGR n.1778 del 22/12/2014 pubblicato nel Supplemento ordinario n.3 al B.U.R. n.14 dell'11/03/2014
- Schema architetturale della CN-Umbria di cui all'allegato C della DGR n.1637/2015
- Quadro di riferimento per l'attuazione del PDRT nella Giunta regionale e per il Contratto tra Giunta e Umbria Digitale Scarl, di cui alla DGR n.1560 del 19/12/2016
- Legge 28 dicembre 2015, n. 208 (Legge di stabilità 2016) e circolare AGID n. 2 del 24 giugno 2016
- Piano triennale per l'informatica nella PA 2017-2019 di cui al DPCM 31/05/2017
- POR FESR 2014-2020 della Regione Umbria, approvato dalla Commissione EU con Decisione C (2015) 929 del 12/02/2015, e presa d'atto con DGR n.184/2015
- Piano di razionalizzazione dell'Infrastruttura digitale dell'Umbria" (PRID) previsto dall'art.19, comma 2, della l.r. n.9/2014, ed approvato con DGR n.829/2014
-

1.4 Definizioni ed acronimi

- n/a

1.5 Programma

POR FESR 2014-2020 *della Regione Umbria, approvato dalla Commissione EU con Decisione C (2015) 929 del 12/02/2015, e presa d'atto con DGR n.184/2015*

- **Responsabile di Azione** (RdA): dirigente del Servizio Sistema informativo regionale, infrastrutture digitali della Regione Umbria

- **Responsabile di Progetto** (RdP): dirigente del Servizio Sistema informativo regionale, infrastrutture digitali della Regione Umbria
- **Beneficiario EU**: - Umbria Digitale Scarl

1.6 Comitato di progetto

- **Dirigente "executive"** (anche detto "*Project Owner*"): Amministratore unico Umbria Digitale Scarl
- **Dirigenti "utenti senior"** (anche detti "*Business Manager*"):
  per classe utenti A
    - dirigente del Servizio Sistema informativo regionale, infrastrutture digitali della Regione Umbria
- **Fornitori senior** (anche detti "*Solution Provider*"): -

1.7 Nucleo di progetto

- **Project Manager**: da definire
- **Technical Project Manager:** coincidente con il PM indicato sopra
- **Garanzia del progetto**:
  per executive
    - Cognome Nome

  per RdA/RdP
    - Cognome Nome

  per utenti senior
    - Cognome Nome
    - Cognome Nome
- **RUP ove siano presenti approvvigionamenti ai sensi del Codice appalti**: -

Parte I: Business case

2. Mandato progettuale

2.1 Descrizione breve del progetto

Potenziamento/Ampliamento della Infrastruttura ICT Security dell'infrastruttura Regionale (DCRU, ReRU, Sedi Istituzionali), estensione delle features di difesa oggi attive a protezione del DCRU, a salvaguardia delle reti e dei sistemi in esercizio presso la Regione Umbria e le Aziende Sanitarie/Ospedaliere umbre. L'intervento è necessario alla luce dell'incremento qualitativo e quantitativo delle minacce di sicurezza nel recente passato e degli oneri derivanti dal GDPR.

Eventuale titolo amministrativo del progetto e codici identificativi (CUP, CLP, CUI):
n/a

2.2 Tempi e spesa massima stimati per il progetto

Il progetto nel suo complesso dovrà essere concluso e rendicontato entro il 31/12/2022, secondo il cronoprogramma da definire in seguito.

Il budget omni-comprensivo messo a disposizione del progetto è di € 850.000, il prospetto economico e pianificazione finanziaria sono da definire in seguito, l'articolazione del budget, secondo delle macro voci che, in funzione delle analisi di dettaglio che seguiranno l'approvazione del BC, potranno essere:

- acquisizione dotazioni tecnologiche adeguate,
- acquisizione licenze di strumenti SW adeguati,
- attività di Umbria Digitale
- attività di supporto specialistico e formativa mirata

sarà quindi declinato in sede di progettazione esecutiva.

2.3 Ragioni per agire

Nel maggio del 2018 è entrato definitivamente in vigore il Regolamento UE 2016/679 meglio noto come GDPR (General Data Protection Regulation), il fondamento di tale regolamento è quella che viene definita "accountability" ovvero responsabilizzazione.

L'ottica con la quale affrontare i temi legati alla sicurezza informatica è pertanto cambiata, dalla concezione consolidata che si realizzava nell'ottemperare a requisiti specifici (vedi Misure Minime di sicurezza definite da AgID), si è trasforma in un'analisi continua, in logica PDCA (Plan-Do-Check-Act) alla ricerca del livello di sicurezza adeguato alla tipologia/riservatezza dei dati gestiti.

L'adeguatezza di una misura è un concetto in costante evoluzione sia perché la natura dei dati da proteggere può cambiare, ma anche perché le minacce informatiche, e di conseguenza le contromisure tecniche che il mercato rende disponibili, sono esse stesse in continua evoluzione, rendendo potenzialmente obsoleta o comunque non più adeguata, una misura che aveva in precedenza tutti i requisiti necessari.

Inoltre, l'obiettivo di adeguare l'infrastruttura, perché sia capace di garantire la disponibilità delle risorse necessarie per assicurare la disponibilità dei servizi applicativi già pubblicati presso il DCRU, e di accoglierne di nuovi i server è sempre all'ordine del giorno.

Il Data Center Regionale Unitario (DCRU), è stato definito dalla LR n.9/2014 come polo regionale unico presso il quale allocare una infrastruttura ICT pubblica al servizio dell'intera PA dell'Umbria nonché degli istituti della formazione e ricerca e degli operatori privati.

Il DCRU è arrivato ad ospitare oltre 1.400 sistemi virtuali ed eroga oltre 400 servizi applicativi per la PA Umbra. Per consentire la corretta erogazione dei servizi è necessario valutare continuamente l'adeguatezza degli strumenti di difesa disponibili, la loro configurazione e la loro efficacia. Inoltre, a fronte della classificazione AgID che ha visto il DCRU essere riconosciuto come "candidabile PSN", e quindi secondo la nuova articolazione definita nel Piano Triennale 2020-2022, DC di classe A, le richieste di consolidamento/migrazione dei CED della PA Umbra al DCRU si sono incrementate in maniera importante e di conseguenza aumenta il livello di protezione che è necessario assicurare.

Coerentemente, è necessario prevedere un potenziamento delle componenti di ICT Security che possa soddisfare sia le esigenze del DCRU come polo regionale unico, sia quelle degli Enti che gestiscono dati sensibili ed erogano servizi critici, come le Aziende Sanitarie/Ospedaliere Umbre e la Regione Umbria stessa.

È altresì necessario provvedere all'ampliamento delle componenti di sicurezza a protezione delle reti e dei posti di lavoro della Regione Umbria, al fine di salvaguardare i servizi applicativi oggetto di attività di gestione a partire dai posti di lavoro dell'Ente.

La linea d'indirizzo strategica che sta alla base del progetto è quella di rendere disponibili componenti di ICT Security omogenei a livello regionale, capaci di assicurare un adeguato presidio, ai vari livelli di controllo, per le Aziende Sanitarie/Ospedaliere Umbre e la Regione Umbria.

In questo contesto trova la sua giusta collocazione l'istituzione di un Security Operation Center (SOC) regionale che, oltre a fornire il necessario supporto sui temi di ICT Security, fornisca anche una visione d'insieme coordinata e coerente rispetto alle politiche di ICT Security tra tutti i principali Enti della regione; si tratta di un obiettivo sfidante, del quale, in questo intervento progettuale, viene inserita la necessaria ed attenta fase di progettazione, rinviando ad un momento successivo la fase realizzativa.

Questo progetto risponde a quanto previsto nella programmazione strategica regionale, nazionale ed europea, ed in particolare le ragioni per agire sono:

- Operare secondo il principio di "accountability" di cui all'articolo 5 comma 2 del Regolamento Ue 2016/679, noto come "General Data Protection Regulation" (GDPR);
- Linee guida strategiche per lo sviluppo della Società dell'Informazione (LGSI) di cui alla legge regionale n.9/2014 (definite con DGR n.155 del 20/02/2017 e successivamente approvate con deliberazione n.213 del 28/11/2017 dell'Assemblea legislativa regionale) - Missione dell'Agenda digitale dell'Umbria di riferimento: ***Servizi pubblici digitali***
- Piano triennale per l'informatica nella PA 2017-2019 di cui al DPCM 31/05/2017 - in particolare gli adempimenti previsti su cloud service provider (CSP), migrazione al cloud e miglioramento della sicurezza informatica;
- Piano triennale per l'informatica nella PA 2020-2022 di cui al DPCM 17/07/2020;
- POR FESR 2014-2020 della Regione Umbria, approvato dalla Commissione EU con Decisione C (2015) 929 del 12/02/2015, e presa d'atto con DGR n.184/2015 - in particolare questo progetto è in attuazione dell'Asse 2 "Crescita e cittadinanza digitale" del POR FESR 2014-2020 della Regione Umbria ed in particolare dell'Azione 2.3.1 che riguarda soluzioni tecnologiche per la digitalizzazione e l'innovazione dei processi delle PA;
- Piano di razionalizzazione dell'Infrastruttura digitale dell'Umbria" (PRID) previsto dall'art.19, comma 2, della l.r. n.9/2014. ed approvato con DGR n.829/2014 - attuazione del PRID;
- Necessità di **potenziamento delle risorse *ICT Security* del DCRU** per rispettare standard qualitativi dei servizi erogati agli attuali soci di Umbria Digitale utenti dei servizi di infrastruttura e direte.

2.4 Descrizione di massima delle esigenze

Obiettivi:

I dati ed i servizi applicativi gestiti/erogati dal DCRU, ed a maggior ragione quelli gestiti/erogati dalle Aziende Sanitarie/Ospedaliere Umbre e da Regione Umbria, hanno sostanzialmente tutti la caratteristica comune di essere di titolarità della Pubblica Amministrazione Locale (PAL), ovvero di riguardare i singoli cittadini in quelli che sono i rapporti con la PAL e con i servizi erogati dalla PAL.

Si tratta perciò di dati sensibili da proteggere con la massima attenzione.

L'obiettivo progettuale che ci poniamo è pertanto quello di incrementare il livello di protezione dei dati e dei servizi, capitalizzando al massimo le capacità della struttura attuale del DCRU, incrementandone il valore complessivo ed estendendo per quanto possibile l'azione di difesa verso Regione Umbria e le Aziende Sanitarie / Ospedaliere Umbre.

Soluzione progettuale:

La soluzione progettuale prevede 4 fasi.

La *prima fase* sarà rivolta al potenziamento della dotazione di componenti dedicati alle funzioni di ICT Security a protezione dell'infrastruttura tecnologica, ovvero aumento della sicurezza del DCRU e della capacità di risposta.

La *seconda fase* sarà finalizzata all'ampliamento delle componenti di sicurezza a protezione delle reti e dei posti di lavoro della Regione Umbria al fine di salvaguardare i servizi applicativi oggetto di attività di gestione a partire dai posti di lavoro dell'Ente.

La *terza fase* sarà rivolta alle Aziende Sanitarie/Ospedaliere e realizzerà un potenziamento dei componenti strutturali di ICT Security disponibili al DCRU, perché estendano le loro funzioni di protezione verso le loro infrastrutture.

La *quarta fase* avrà l'obiettivo di progettare la realizzazione di un Security Operation Center (SOC) regionale a supporto delle strutture ICT degli Enti Umbri.

Le quattro fasi comprenderanno sia l'acquisizione di componenti tecnologiche specifiche, sia l'acquisizione di competenze professionali a supporto che attività di formazione, finalizzate alla crescita dell'infrastruttura di ICT Security regionale, al fine di sfruttarla al meglio ed incrementare le competenze di cyber security dei tecnici impegnati nella gestione.

Coerenza strategica:

Questo progetto è coerente con il Piano triennale nazionale per l'ICT nella PA e rispetta la strategia complessiva dell'Agenda digitale dell'Umbria riportata nelle vigenti "*Linee guida strategiche per lo sviluppo della Società dell'Informazione*" (LGSI) ex legge regionale n.9/2014.

Missione dell'Agenda digitale dell'Umbria di riferimento: ***Servizi pubblici digitali***

in LGSI:

> ***Consolidare a tutti i livelli architetturali (database, sistemi operativi, ecc)*** *per ricercare economie di scala e potenziare la cybersecurity in tutte le PA (..)*

in LGSI e in PO FESR:

> ***1. potenziare ed adeguare la ICT-Security del Data Center Regionale Unico (DCRU)*** *(l.r. n.9/2014),*

nel PDRT:

> ***RA- 6107 Cybersecurity e protezione dati personali*** *costruire ed ampliare le competenze e gli strumenti per rispondere alle minacce cibernetiche, rafforzando le competenze dei tecnici, le conoscenze degli utenti, rafforzare il livello tecnologico di DCRU e rete regionale ed il livello applicativo relativo ai servizi erogati*

Piano triennale per l'informatica nella PA 2020-2022 di cui al DPCM 17/07/2020:

Macro aree correlate:

- *Infrastrutture fisiche*

    - *Data center e cloud* **- adeguamento DCRU**
    - *Connettività*
- *Infrastrutture immateriali/Piattaforme abilitanti (ANPR, PagoPA, SPID, Fatturazione elettronica PA, e-procurement/ComproPA, Sistema di avvisi e notifiche di cortesia, NoiPA, Sistema di gestione dei procedimenti amministrativi nazionali, SIOPE+, Poli di conservazione)* **– mantenimento dei sistemi/servizi**
- *Dati della Pubblica amministrazione (Basi di dati di interesse nazionale, Open data, Vocabolari controllati)* **– mantenimento dei sistemi/servizi**
- *Modello di interoperabilità (API)* **– mantenimento/ dei sistemi/servizi**
- *Ecosistemi (Sanità, Scuola, Infrastruttura e logistica - Mobilità, Sviluppo e sostenibilità, Beni culturali e turismo, Sicurezza e soccorso - Legalità, Giustizia, Agricoltura, Finanza pubblica,...)* **– mantenimento dei sistemi/servizi**
- *Strumenti per l'accesso ai servizi digitali (accessibilità, linee di design)*
- *Sicurezza (CERT-PA e cyber security)* **- miglioramento della sicurezza**
- *Data & Analitycs Framework (DAF)*
- *Cittadinanza digitale (app io.italia.it)*
- *Competenze digitali*
- *Smart city*
- *Gestione del cambiamento (community, ecc)* **-**

Modalità di attuazione:

Questo progetto è in diretta prosecuzione delle attività già svolte da Umbria Digitale nei precedenti progetti in cui è stata beneficiaria dei fondi FESR. L'investimento accresce il valore delle infrastrutture immateriali a favore di tutti i soci della società in house Umbria Digitale Scarl e rientra nella *mission* della società di cui alla l.r. n.9/2014.

I documenti di progettazione definitiva ed esecutiva individueranno le modalità di attuazione e conterranno la valutazione della congruità tecnico-economica rispetto al mercato in relazione alle prestazioni che possono essere erogate da operatori privati in regime di concorrenza, evidenziando i benefici per la collettività riguardo alla scelta di tale contraente, secondo quanto previsto dal Codice contratti (d.lgs. n.50/2016).

3. Background del progetto

3.1 Relazione tecnico-illustrativa del contesto

Stato dell'arte nei vari domini (capacità org.ve, applicazioni/dati, tecnologie):

Rispetto al Data center regionale unitario (DCRU), da collocare come elemento abilitante nel più ampio alveo del SIRU (Sistema informativo regionale dell'Umbria) la l.r. n.9/2014 stabilisce all'art.5 quanto segue:

> *(..) 2. Il Data center regionale unitario dell'Umbria, di seguito DCRU, è l'infrastruttura digitale abilitante del SIRU.*
>
> ***2.** Sono collocati nel DCRU tutti i sistemi server della Regione, delle agenzie e degli enti strumentali regionali, nonché degli altri organismi comunque denominati controllati dalla Regione medesima, delle aziende sanitarie e degli enti del servizio sanitario regionale.*
> ***3.** Sono, altresì, collocati nel DCRU i sistemi server degli enti locali, e di altri soggetti pubblici, sulla base di specifici accordi attuativi con i soggetti interessati.*

ed il Disciplinare di attuazione della l.r. n.9/2014 specifica inoltre che:

> *"(..) 6.10 Nell'ambito del DCRU, è implementato un Cloud di comunità (Community cloud dell'Umbria) in grado di erogare servizi IaaS, Paas e Saas secondo modalità individuate nell'ambito del Comitato tecnico con il supporto tecnico di Umbria Digitale (..)".*

Negli anni la Regione Umbria ha investito per la razionalizzazione ed il consolidamento dei CED nel DCRU e della connettività di rete. Oggi il data center e la rete regionale sono utilizzati da numerosi enti della CN-Umbria, soci di Umbria Digitale Scarl, perseguendo una logica di economia di scala e di scopo.

Si può fare riferimento alla documentazione dei progetti precedenti per maggiori informazioni di contesto.

Progetti pregressi da considerare:

- Programma #PRID di cui alla DGR n.829/2014
- PRJ-1048 Potenz./Ampliam infrastruttura ICT del DCRU

- PRJ-1286 Potenziamento/ampliamento Infrastr.ICT (PO#1)
- PRJ-0111 Impianto funz. "Community Cloud Umbria" (PO#3)
- PRJ-0112 Potenziamento/ampliamento ICT-Security (PO#2)
- PRJ-1522 "Potenziamento/ampliamento dotazioni tecnologiche del DCRU in sicurezza/capacità"
- PRJ-1293 Prog. impianto e messa eserc. SGSI ISO 27001
- PRJ-1504 Realizzazione della System Continuity
- PRJ-1486 ICT Security delle applicazioni
- PRJ-1493 Consolidamento CED degli EELL nel DCRU e Centro di competenza cloud regionale
- PRJ-1494 Qualificazione del DCRU come Cloud Service Provider (CSP)

Servizi ed asset in esercizio coinvolti:

- vari sistemi da identificare in sede di progettazione esecutiva

3.2 Opzioni di intervento considerate

Sono state considerate le seguenti opzioni:

- **Opzione 1) non fare niente ("opzione zero")**. L'opzione zero non comporta investimenti ma è stata esclusa in quanto, la natura di centro di aggregazione/consolidamento che caratterizza il DCRU, e più in generale i requisiti di sicurezza e disponibilità che debbono soddisfare le infrastrutture della pubblica amministrazione rendono indispensabile che sia il DCRU che le Aziende Sanitarie/Ospedaliere, abbiano una protezione a livello ICT Security in quantità e qualità sufficiente a contrastare le minacce sempre più evolute dal punto di vista Tecnico. Stesso discorso vale per la protezione dei posti di lavoro dell'Ente Regione. Opzione non praticabile.
- **Opzione 2) fare il minimo**. "fare il minimo" non è coerente con il principio di accountability che deve essere alla base degli interventi di questo progetto e di tutti gli interventi in materia di ICT Security più in generale..
- **Opzione 3) fare qualcosa**. L'opzione massimale intende dare risposta alle esigenze che si evidenziano nel progetto, fornendo una risposta adeguata al fine di assicurare la piena operatività in sicurezza di tutti i componenti di ICT Security coinvolti.

L'opzione scelta che garantisce il pieno rispetto delle norme vigenti e una prospettiva temporale maggiore di valorizzazione e consolidamento degli investimenti fatti negli ultimi anni è l'opzione n.3

3.3 Vincoli derivanti dall'architettura enterprise

L'intervento è da realizzare nel rispetto di quanto previsto dalle seguenti DGR regionali in materia ICT: n.371/2015, n.1572/2015, n.1560/2016, n.825/2019, n.826/2019 e n.1085/2019 (vedere descrizione documenti in premessa).
Il progetto dovrà prevedere, ogni qual volta ciò sia fattibile, la rilevazione automatica degli indicatori di *output*, di *outcome* nonché dei dati relativi al funzionamento ed utilizzo dei servizi realizzati, da esporre tramite API.

P3O: Nessuna osservazione.

Programma/Ambito: Nessuna osservazione.

Infrastrutture: Il progetto prevede il potenziamento/ampliamento della componente Infrastrutturale di ICT Security, che deve essere effettuata in coerenza e continuità con gli interventi pregressi.

Sicurezza informatica: Il progetto ha uno specifico indirizzo in tema di sicurezza Informatica che, vedi il corpo del presente documento, si realizza a livello infrastrutturale, sia centralmente presso il DCRU che verso le strutture delle Aziende Sanitarie/Ospedaliere che di Regione Umbria.

DPO: Il progetto non prevede trattamenti diretti di dati personali.

4. Prodotto del progetto, ambito incluso/escluso ed altri aspetti di prestazione

4.1 Descrizione del "Prodotto del progetto"

Il prodotto complessivo che deve realizzare il progetto, in accordo con utenti e fornitori, è stato suddiviso nei seguenti prodotti di primo livello, da dettagliare nel corso della progettazione esecutiva e delle fasi previste:

Prodotto specialistico	Descrizione	Classi di utenti destinatari	Fase
P01 Aumento della sicurezza del DCRU e della capacità di risposta	*Rif.BC: " … adeguare l'infrastruttura, perché sia capace di garantire la disponibilità delle risorse necessarie per assicurare la disponibilità dei servizi applicativi già pubblicati presso il DCRU Garantire la corretta operatività del DCRU ……..."* Il prodotto comprende sostanzialmente il potenziamento dei componenti di sicurezza che sono alla base dell'infrastruttura tecnologica.	**TUTTI**	**1** *(anno 2021/2022)*
P02 Hardening sedi Regionali	Rif.BC: " *……all'ampliamento delle componenti di sicurezza a protezione delle reti dei posti di lavoro della Regione Umbria al fine di salvaguardare i servizi applicativi oggetto di attività di gestione a partire dai posti di lavoro dell'Ente…..* Il prodotto comprende l'adeguamento delle dotazioni di sicurezza per la gestione e l'accesso ai servizi applicativi.	**TUTTI**	**2** *(anno 2021/2022)*
P03 Incremento della sicurezza infrastrutturale per le Aziende Sanitarie/ Ospedaliere	*Rif.BC: " ….. potenziamento della componente di ICT Security che comprenda sia le esigenze del DCRU come "contenitore" di servizi, sia quelle degli Enti che gestiscono dati sensibili ed erogano servizi critici come le Aziende Sanitarie/Ospedaliere Umbre ……"* Il prodotto prevede il potenziamento delle principali componenti di ICT Security già in esercizio perché siano in grado di proteggere anche le sedi delle Aziende Sanitarie/Ospedaliere.	**TUTTI**	**3** *(anno 2021/2022)*
P04 Progetto SOC Regionale	*Rif.BC: " ….. La linea d'indirizzo strategica che sta alla base del progetto è quella di rendere disponibili componenti di ICT Security omogenei a livello regionale, capaci di assicurare un adeguato presidio per i vari livelli di controllo per le Aziende Sanitarie/Ospedaliere Umbre e la Regione Umbria. In questo contesto trova la sue giusta collocazione l'istituzione di un Security Operation Center (SOC) regionale ……"* Il prodotto realizza la progettazione dell'istituzione di un SOC regionale al servizio dei principali Enti Umbri, Regione ed Aziende Sanitarie/Ospedaliere.	**TUTTI**	**4** *(anno 2021/2022)*

4.2 Ambito incluso (*in scope*)

E’ incluso nel progetto:

- fare riferimento a quanto riportato al paragrafo 2.4

Destinatari, estensione e forme di aggregazione:

In questo intervento la Regione opera nel ruolo di "soggetto aggregatore territoriale per il digitale" a favore in primo luogo delle Aziende Sanitarie/Ospedaliere umbre, ma anche di tutti gli enti della CN-Umbria soci della società in house Umbria Digitale (quale intermediario tecnologico e beneficiario dei fondi FESR) e fruitori, assieme ai cittadini umbri, dei servizi oggetto dell’intervento progettuale.

Indicatori di "output" specifici per il progetto:

- *da identificare e stimare in sede di progettazione esecutiva*

Indicatori di "output" dal PO FESR:

- TC44-794 - Unità di beni acquistati - 10

Indicatori "KPI di realizzazione" dalla Strategia Crescita digitale:

- DA STABILIRE

Indicatori di "risultato" dal PO FESR:

- N/A

4.3 Ambito escluso (*out of scope*)

E’ esclusa dal progetto:

- fare riferimento a quanto riportato al paragrafo 2.4

4.4 Congruenza di tempi e costi rispetto al mandato

A livello di valutazione preliminare, e considerato quanto detto sopra rispetto all'ambito incluso/escluso, i limiti di tempo complessivi ed il budget appaiono sufficienti rispetto al mandato progettuale.

La stima dei costi è avvenuta prendendo come riferimento interventi di acquisizione/potenziamento realizzati in precedenti progetti;

5. Analisi dei rischi a livello di progetto

Il progetto individua i seguenti rischi (da approfondire in sede di progettazione esecutiva):

- fare riferimento a quanto riportato al paragrafo 2.4 e al paragrafo 3

Sinteticamente i fattori di rischio al successo dell'intervento sono riepilogati in tabella:

N	Fattori di rischio	Classificazione alto/medio/basso			Azione	Responsabile azione
		A	M	B		
	RISCHI LEGATI ALLA COMPLESSITÀ’ DEL PROGETTO					
	Complessità gestionale					

1	Rilevanza strategica del progetto	X			Rispetto dei tempi, produzione di SAL	Project Manager
2	Eterogeneità degli attori		X		Verifiche in fase realizzativa	Project Manager
3	Eterogeneità delle esigenze		X		Verifiche in fase realizzativa	Project Manager
4	Mancata individuazione di interlocutori con potere decisionale			X		
5	Disponibilità dei referenti dei progetti pre-esistenti a reperire e fornire informazioni e materiali			X		
6	Interdipendenza con altri obiettivi			X		
	Dimensioni del progetto					
7	N. complessivo di mesi/persona previsti		X			
8	Dimensione del sistema		X			
9	Stime inesatte relative a durata e costo			X		
	RISCHI LEGATI ALLA INCERTEZZA					
	Incertezza dei requisiti					
10	Stabilità dell'ambiente, dei processi, del contesto normativo			X		
11	Probabilità di modifiche in corso d'opera		X		Approccio evolutivo e verifiche con i referenti	Project Manager
12	Novità del tema trattato		X			
	Innovazione tecnologica					
13	Novità delle soluzioni SW prescelte			X		
14	Necessità di integrazione di tecnologie eterogenee		X		Verifica puntuale delle caratteristiche tecnologiche degli oggetti che compongono il sistema e possibilità di integrazione	Team Manager
	ALTRI RISCHI					
	nessuno					
=> VALUTAZIONE GLOBALE DEL RISCHIO DEL PROGETTO		**MEDIO**				

6. Analisi costi/benefici

6.1 Classi di utenti, benefici attesi ed eventuali contro-benefici

Le classi di utenti destinatari del progetto sono riportate nella tabella seguente con i relativi benefici e contro-benefici di massima. Partendo da quelli indicati nella tabella, benefici (e relativi indicatori) e contro-benefici saranno ulteriormente dettagliati progressivamente nelle fasi successive del progetto.

Il progetto adegua/potenzia l'infrastruttura tecnologica alla base di oltre 1.300 sistemi virtuali che erogano servizi destinati alla maggiore parte della Pubblica Amministrazione Umbra nonché ai professionisti e cittadini. I benefici/contro-benefici che si possono indicare sono relativi al mantenimento della disponibilità del servizio, alla possibilità di adeguamento dei sistemi ed alla relativa sicurezza. L'unico utente destinatario che può valutare gli eventuali benefici/contro-benefici attesi è chi ha la visione d'insieme del DCRU e cioè il Servizio Sistema informativo regionale, infrastrutture digitali della Regione Umbria.

Classe di utenti destinatari	Utente senior	Benefici attesi e relativi indicatori	Contro-benefici
A. Servizio Sistema informativo regionale, infrastrutture digitali della Regione Umbria B. Direzione salute e Welfare –Servizio Gestione flussi del sistema informativo sanitario e sociale, mobilità sanitaria, Sistema tariffario	Graziano Antonielli Barbara Gamboni	1. Disponibilità del servizio ○ SLA 2. Attività sospette/malevole bloccate ○ numero di eventi	● Mantenimento dell'infrastruttura

6.2 Valutazione ex ante dei criteri di selezione per il PDRT

Nella tabella seguente è riportata la valutazione del progetto per ognuno dei criteri di cui al punto 3.3, lettera e), del disciplinare ex D.G.R. n.1778/2014.

I criteri di selezione ad oggi vigenti sono quelli contenuti nell'allegato E della DGR n.365/2017, confermati anche nei successivi PDRT.

CRITERI DI RILEVANZA STRATEGICA - *indicare (A)lto, (M)edio, (B)asso*			
Il grado di strategicità rispetto a:			
A			*r1. missioni dell'Agenda digitale dell'Umbria*
A			*r2. esigenze esplicite espresse dal confronto col contesto di riferimento*
A			*r3. essere precondizione per la fattibilità degli altri progetti strategici*
	M		*r12. obiettivi del Piano di Semplificazione*
Il grado di coerenza con l'obiettivo di sviluppo di:			
	M		*r4. reti di servizi o filiere produttive*
		B	*r5. reti di conoscenza e competenze digitali attraverso l'openness (open data, open source, open gov)*
		B	*r6. interventi di sussidiarietà "misurabili"*
		B	*r13. API o dati aperti che abilitano applicazioni interattive di terzi (app)*
La modalità dichiarate di coinvolgimento di altri soggetti attori attraverso:			
	M		*r7. co-progettazione (co-design)*
		B	*r8. co-produzione (co-makership)*
		B	*r9. marketing cooperativo (co-marketing)*
Le previsioni di ottimizzazione delle risorse impiegate:			
A			*r10. relativamente a competenze, tecnologie e risorse strumentali, risorse economico-finanziarie*
	M		*r11. con previsione di cumulabilità con altri progetti/servizi in termini di sinergia o amplificazione dei risultati, economie di scala o di scopo*
	M		*r14. secondo il paradigma del cloud computing (IaaS, PaaS, SaaS, BPaaS)*
=> valutazione di rilevanza strategica nel complesso: **ALTA**			

CRITERI DI SOSTENIBILITÀ' O FATTIBILITÀ' TECNICO/GESTIONALE - *indicare (A)lto, (M)edio, (B)asso*			
Fattibilità per:			
A			*f1. spesabilità nel budget dell'anno di riferimento*
A			*f2. condivisione degli obiettivi con altre strutture coinvolte/stakeholder*
Sostenibilità per:			
A			*f3. valore aggiunto generato rispetto alle risorse da impiegare*
A			*f4. tempi attesi di ritorno dell'investimento*
	M		*f5. impostazione organizzativa e gestionale della progettazione e delle realizzazioni*
=> valutazione di sostenibilità e fattibilità nel complesso: **ALTA**			

CRITERI DI TIPOLOGIA/SPESA - *indicare (S)ì o (N)o*			
Requisiti di spesa:			
S			*t1. Investimento complessivo nel progetto superiore ad € 200.000*
S			*t2. Costo di esercizio complessivo del servizio che prevede un aumento*
Requisiti di tipologia:			
S			*t3. acquisizione di hardware, software, connettività e sicurezza riferibili a sistemi server, cloud computing o data center di importo superiore ad € 10.000*
		N	*t4. progetti sull'identità digitale, la fatturazione elettronica, i pagamenti elettronici o altre infrastrutture immateriali nazionali di importo superiore ad € 10.000*
		N	*t5. progetti sulla valorizzazione del patrimonio informativo pubblico e sulla diffusione di dati aperti di importo superiore ad € 10.000*
=> rientra nei criteri di tipologia/spesa nel complesso: **NO**			

6.3 Valutazione *ex ante* dell'impatto di gestione e dei relativi costi di esercizio

La gestione dei I nuovi prodotti, realizzati dal progetto avranno necessità di essere gestiti nello specifico. Non si prevede che l'onere di gestione sia particolarmente significativo, ma costituirà in ogni caso un incremento nelle attività di gestione.

6.4 Valutazione complessiva sull'investimento ad oggi

L'investimento è giustificato in quanto l'infrastruttura tecnologica regionale, e le dotazioni tecnologiche dell'Ente Regione Umbria, sono una realtà sulla quali fanno riferimento numerosi enti della PAL Umbra. Il loro adeguamento in termini di ICT Security, è la risposta alla domanda di digitalizzazione che viene da tutta la comunità della PAL Umbra nel suo complesso.