POR CAMPANIA FESR 2014-2020

ASSE 2 "ICT E AGENDA DIGITALE"

OBIETTIVO SPECIFICO 2.2 "DIGITALIZZAZIONE DEI PROCESSI AMMINISTRATIVI E DIFFUSIONE DI SERVIZI DIGITALI PIENAMENTE INTEROPERABILI"

AZIONE 2.2.1 "SOLUZIONI TECNOLOGICHE PER LA DIGITALIZZAZIONE E L'INNOVAZIONE DEI PROCESSI INTERNI DEI VARI AMBITI DELLA PUBBLICA AMMINISTRAZIONE NEL QUADRO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ"

PROGETTO DEFINITIVO

SOGGETTO PROPONENTE	AZIENDA OSPEDALIERA UNIVERSITARIA FEDERICO II	
CODICE FISCALE	06909360635	
PEC	aou.protocollo@pec.it	
REFERENTE PROGETTO	Dott. Giuseppe Longo	Mail: diraup@unina.it
		Telefono: 0817464921

TITOLO DEL PROGETTO

Incremento delle performance sanitarie e sicurezza informatica del dato sanitario

DESCRIZIONE DEL PROGETTO, CON EVIDENZA DEGLI ELEMENTI DI COERENZA CON LA DGR N. 354 DEL 19/06/2023 E CON L'AZIONE 2.2.1 DEL POR CAMPANIA FESR 2014-2020

(Partendo dall'analisi dei fabbisogni, illustrare, in maniera dettagliata, gli interventi proposti e le spese consequenziali, riportando, in maniera puntuale, le spese relative a:

a) Servizi di digitalizzazione della documentazione sanitaria a supporto degli assistiti e degli operatori sanitari (specificare la tipologia di documenti da digitalizzare ed il numero di documenti per ciascuna tipologia);

b) Attrezzature per la digitalizzazione dei risultati diagnostici (indicare le singole attrezzature ed il relativo numero, nonchè eventuali software di funzionamento);

c) *Sistemi di Cyber Security (specificare componenti hardware, componenti software ed eventuali spese necessarie ai fini dell'installazione).*

Il **progetto**, in linea con quanto richiesto dall' Azione 2.2.1 del POR Campania FESR 2014-2022, consentirà all'Azienda Ospedaliera Universitaria Federico II di intensificare la sicurezza informatica nella gestione dei dati, sensibili e non, e migliorare la performance dell'erogazione delle prestazioni Sanitarie.

Punto a) ***Servizi di digitalizzazione della documentazione sanitaria a supporto degli assistiti e degli operatori sanitari (specificare la tipologia di documenti da digitalizzare ed il numero di documenti per ciascuna tipologia);***

L'AOU Federico II intende procedere con la digitalizzazione del fascicolo del dipendente per gestire in modo informatizzato tutti gli eventi della vita lavorativa del personale quali, ad esempio, gli inquadramenti e i profili professionali, le posizioni giuridiche occupate in relazione agli sviluppi di carriera, le assegnazioni alle varie strutture dell'Amministrazione, decreti e provvedimenti, anzianità utile ai fini pensionistici e della buonuscita o del trattamento di fine rapporto.
I fascicoli del personale sono di fatto ibridi. La sfida, e allo stesso tempo l'opportunità, che questo progetto si pone è complessa e va a toccare diversi punti fondamentali della gestione documentale, analogica e soprattutto digitale:

- garantire un accesso immediato ai documenti ed alle informazioni in essi contenute;
- garantire il valore dei fascicoli (giuridico e probatorio);
- garantire la tutela e riservatezza delle informazioni;
- evitare la replicazione delle informazioni.

Il fascicolo da un punto di vista puramente documentale, è un insieme di documenti, istanze, provvedimenti ed atti giuridici: rappresenta tutto il corpus informativo, che perviene al datore di lavoro, circa il rapporto che si instaura con il dipendente, ne testimonia la carriera e la storia lavorativa, infatti:

- riflette e rappresenta il rapporto fra il lavoratore ed il datore di lavoro;
- documenta e testimonia la correttezza, nel contesto giurisprudenziale di riferimento, del rapport;
- testimonia la carriera del dipendente;
- garantisce i diritti anche futuri del dipendente.

Tale digitalizzazione permetterà pertanto a questa AOU di migliorare la gestione e l'organizzazione del personale sanitario, permettendo una migliore divisione dei compiti con la definizione di responsabilità e mansioni. Inoltre essa permetterà di mettere insieme, integrare, armonizzare il lavoro di uno o più soggetti, appartenenti alla stessa o a diverse unità operative, per evitare duplicazioni, sovrapposizione, lacune e migliorare l'efficacia e l'efficienza delle prestazioni sanitarie erogate, al fine di aumentare la customer satisfaction.

Pertanto, visto il numero di dipendenti attualmente in serivizo presso questa AOU Federico II, si procederà con la digitalizzazione di n. 2163 fascicoli (n.1 fascicolo per ogni dipendente), come da piano dei fabbisogni (all.n.1).

Gli interventi proposti recepiscono pienamente quanto indicato nel POR/FESR 2014-2020 e nella DGR Campania 354 del 19/6/2023, in quanto intevengono su:

a) ***Digitalizzazione di documentazione a supporto degli operatori sanitari per attività di sorveglianza sanitario;***
b) ***Diffusione di servizi digitali pienamente Interoperabili****, garantendo la condivisione delle informazioni raccolte (relativamente Fascicoli dei dipendenti digitalizzati) e trasformate in flussi informativi strutturati e utilizzabili da sistemi informativi esterni per le operazioni di consultazione on line;*
c) ***Potenziamento della domanda di ict di cittadini e imprese in termini di utilizzo dei servizi online*** *mettendo a disposizione degli operatori sanitari le informazioni in formato digitale;*
d) ***Rafforzare le applicazioni delle TIC per l'e-government, l'e-learning, l'e-inclusione, l'e-culture e l'e-health,*** *relativamente ai processi di digitalizzazione dei fascicoli del personale;*
e) ***Digitalizzazione dei processi amministrativi e diffusione di servizi digitali pienamente interoperabili,*** *per le Attività di digitalizzazione dei fascicoli del personale.*

Punto b) Attrezzature per la digitalizzazione dei risultati diagnostici (indicare le singole attrezzature ed il relativo numero, nonchè eventuali software di funzionamento):

L'AOU Federico II ha intenzione di adottare nuove soluzione volte a supportare la diagnosi di precisione per cure sempre più personalizzate, attraverso la combinazione di hardware, software e algoritmi per l'analisi di immagini, integrata nella soluzione software Winsap, di gestione della Anatomia Patologica, di Engineering in esercizio presso l'AOU.

Nello specifico l'AOU intende:

- Acquisire il modulo software di Anatomia Patologica ai fini sopra descritti tramite interoperabilità con gli strumenti diagnostici del laboratorio di Anatomia Patologica (es: scanner di vetrini);
- Acquisire nuovi strumenti diagnostici di ultima generazione per la digital Pathology: n.2 Scanner per vetrini, n.2 Workstation di Refertazione, n.4 stampanti per etichette QRCODE, n.1 stampante per vetrini per l'etichettatura con QR Corde, n.1 Stampante per biocassette, n.1 Server per lo storage dei file scannerizzati; n.1 tissue microarrayer (TMA) semiautomatic. Tali strumenti sono necessari per la digitalizzazione dell'intero processo di anatomia patologica: allestimento del vetrino che deve essere identificato univocamente per tenerne la tracciabilità, attraverso l'utilizzo delle diverse stampanti per le differenti tipologie di campioni; inizio del processo di diagnosi grazie all'accesso ai vetrini digitali e alla consultazione delle immagini archiviate(utilizzo di scanner, TMA, server per lo storage); diagnosi conclusive e refertazione (workstation di refertazione).
- Migliorare il processo di diagnosi in termini di tempo e precision;
- Aumentare l'efficienza e la produttività attraverso un elevato livello di automazione, standardizzazione delle procedure e gestione paperless;
- Aumentare il livello di servizio ai pazienti;
- Facilitare le attività di second opinion e consentire processi diagnostici a distanza;
- Creare gradualmente un archivio digitale dei vetrini che possa essere utilizzato non solo per il processo diagnostico ma anche per scopi di ricerca, educazionali e nuovi algoritmi AI.

Le funzionalità che saranno installare e messe in esercizio nell'ambito del progetto AOU - Digital Pathology sono:

- Integrazione con gli scanner
- Navigazione del vetrino sui 3 assi
- Zoom-in e zoom-out
- Visualizzazione di più vetrini digitali contemporaneamente
- Tracking delle zone già visualizzate
- Misurazioni e Annotazioni
- Regolazioni luminosità e contrasto

- Funzionalità di snap shot esportabili
- Condivisione dei vetrini digitali con sistemi di chat e videochiamata all'interno del servizio di anatomia patologica

Gli interventi proposti recepiscono pienamente quanto indicato nel POR/FESR 2014-2020 e nella DGR Campania 354 del 19/6/2023, in quanto intevengono su:

a) ***Diffusione di servizi digitali pienamente Interoperabili****, garantendo la condivisione di dati sanitari trasformati in flussi informativi strutturati e utilizzabili da sistemi informativi per le operazioni di consultazione on line;*

b) ***Potenziamento della domanda di ict di cittadini e imprese in termini di utilizzo dei servizi online*** *mettendo a disposizione degli operatori sanitari le informazioni in formato digitale;*

c) ***Rafforzare le applicazioni delle TIC per l'e-government, l'e-learning, l'e-inclusione, l'e-culture e l'e-health,*** *relativamente ai processi di digitalizzazione dell'Anatomia Patologica.*

Punto c) Sistemi di Cyber Security (specificare componenti hardware, componenti software ed eventuali spese necessarie ai fini dell'installazione).

L'Azienda Ospedaliera Universitaria Federico II vuole sviluppare il seguente progetto di potenziamento della propria infrastruttura informatica nel rispetto delle misure minime di sicurezza dettate dall'Agid, aderendo così alle raccomandazioni del perimento nazionale di sicurezza e delle principali raccomandazioni internazionali (NIST). Tale progetto include anche la sicurezza dei dispositivi elettromedicali, ai quali è associato il maggiore livello di rischio di cyber security.
L' AOU Federico II è in una fase di profonda evoluzione della propria rete di sicurezza informatica, oramai obsoleta e non idonea a resistere ai moderni attacchi informatici, pertanto è intenzione dell'Amministrazione dotarsi di elementi innovativi per la protezione dei dati sanitari dagli attacchi informatici e nel contempo monitorare il comportamento dei sistemi elettromedicali collegati in rete e aumentarne le performance. Pertanto, l'AOU Federico II vuole dotarsi di un ecosistema di funzionalità necessarie, che inter-operando fra loro sono in grado di segnalare anomalie sui comportamenti attesi dei sistemi informatici, come ad esempio attacchi informatici quali ransomware, ddos, etc.
Questa AOU, per il raggiungimento di questi obiettivi, vuole dotarsi di:

1. Multifactor Authentication
2. Piattaforma per il controllo accessi: Network Access Control (NAC)
3. Endpoint Detection and Response: dall'antivirus alla telemetria degli EndPoint
4. Protezione delle applicazioni e dei Servizi Esposti al WEB: Web Application Firewall
5. Piattaforma di cybersecurity asset & risk management

Nel dettaglio:

1. Utilizzo di Multifactor Authentication

Al fine di aumentare il livello di sicurezza degli accessi da remoto, l'AOU Federico II utilizzerà un sistema di Identity management che implementa funzioni di MultiFactorAuthentication integrandosi con sistemi di autenticazione più diffusi come LDAP, 802.1x, SAML etc etc.
La soluzione con il doppio fattore di autenticazione, consentirà all'AOU Federico II di validare e verificare l'identità di chi tenta di accedere alla network aziendale, sia che i richiedenti si trovino all'interno o all'esterno del perimetro della rete, in sintonia con l'approccio Zero Trust Access.
L'Identificazione dell'identità dell'accedente prevede la verifica delle credenziali tipo MFA (Multifactor Authentication), ossia basata su credenziali login/passaword + ulteriori fattori come ad esempio i token. La MFA è necessaria in quanto il principale e più pericoloso vettore di attacco è quello del furto delle credenziali. Normalmente questa funzione si accompagna al modello di accesso Sigle Sign On, un solo momento di accesso per tutte le risorse disponibili all'utente.
La soluzione è costituita da n.2 software per la gestione di n. 400 utenti.

2. Utilizzo di una piattaforma per il controllo accessi: Network Access Control

L'AOU Federico II vuole predisporre un sistema di controllo degli End-Point (PC, Stampanti ,apparati medicali) che utilizzano l'infrastruttura LAN dei relativi dipartimenti e delle sedi remote, al fine di migliorare la governance dell'accesso degli utenti alle risorse aziendali. Tale sistema di controllo è una infrastruttura virtuale basata su soluzione Network Access Control (da qui in poi NAC)
Il NAC, tecnologicamente, è la funzione che ha lo scopo di governare l'accesso alle risorse di rete sulla base di: identità dell'utente, identità del dispositivo, sua postura di sicurezza del dispositivo e contesto di accesso. Il NAC avrà una profonda integrazione con la rete (switch di accesso) e con i sistemi di autenticazione (Domain Controller) al fine di automatizzare le operazioni di accesso alle risorse.
Tale sistema ha inoltre la capacità di profilare e certificare i dispositivi, verificarne la postura di sicurezza, creare modelli di accesso tipo captive portal/sponsorship, ed inter-operare con la rete ed i firewall al fine di automatizzare l'accesso in rete sulla base delle politiche definite centralmente.
La fornitura prevede n.1 software di network access control come si evince da bozza del piano dei fabbisogni allegato alla presente (cfr. all.2).

3. Endpoint Detection and Response: dall'antivirus alla telemetria degli EndPoint

L'AOU Federico II, ad oggi, è dotata di un solo sistema Antivirus limitando la protezione degli stessi Endpoint, perché le attuali soluzioni antivirus proteggono i file (potenzialmente dannosi) che vengono introdotti nel sistema. Al contrario, una soluzione EDR, si concentra sulla raccolta di dati dall'endpoint e sull'esame degli stessi alla ricerca di modelli dannosi o anomali in tempo reale.
La protezione degli end point attraverso gli antivirus classici basati su firme non è più sufficiente a causa di due fattori: la velocità con la quale vengono generarti nuovi malware, la modalità di attacco sempre più complessa. Alla poca efficacia dei metodi tradizionali, si aggiunge la mancanza di risorse professionali adeguatamente competenti per rispondere agli attacchi. Una nuova generazione di sistemi di protezione nasce per ovviare a queste debolezze: EDR (End Point Detection and Response) e XDR (eXtended EDR).
Questi sistemi si basano su tre elementi fondamentali:

- Analisi comportamentale basata su intelligenza artificiale
- Raccolta e correlazioni delle attività degli End Point
- Risposta automatica agli attacchi

Questi tre pilastri consentono di avere:

- Risposta agli attacchi di nuova generazione molto più efficace rispetto ai tradizionali antivirus;
- Completa visibilità delle azioni degli end point e conseguente capacità di determinare i movimenti degli attacchi;
- Riduzione della necessita di personale qualificato e dei tempi di risposta agli attacchi attraverso l'automazione (Playbook).

Le quattro funzioni principali della piattaforma EDR prevedono

- Indagine e Prevenzione: identificazione dei dispositivi in rete, analisi delle vulnerabilità del sistema e Virtual Patching;
- Prevenzione: analisi in real time dei comportamenti;
- Identificazione e disinnesco: identificazione dei comportamenti malevoli e disinnesco del malware;
- Automazione della risposta: contenimento ed eradicazione della minaccia.

La Fornitura in argomento è costituita da:

- EPP: n.1 software per la gestione di n. 1000 postazioni di lavoro
- SPP: n.1 software per la gestione di n. 300 VM

Come si evince da bozza del piano dei fabbisogni allegato alla presente (cfr. all.2).

4. Protezione delle applicazioni e dei Servizi Esposti al WEB

L'AOU Federico II ha deciso di dotarsi di un sistema a protezione delle applicazioni e delle API HTTP, essendo queste tra le principali cause di attacco, attraverso l'utilizzo della tecnologia WEB Application Firewall (da qui in poi WAF).
La tecnologia WAF sarà utilizzata dall'AOU Federico II per proteggere a livello infrastrutturale le applicazioni HTTP. I sistemi WAF firewall rendono le organizzazioni indipendenti dagli sviluppatori software, che pure devono essere conformi agli standard, per quanto attiene alla protezione degli attacchi. In questo senso le funzioni di Machine Learning sono fondamentali in quanto riducono i falsi positivi e automatizzano la protezione attraverso l'auto apprendimento. In questo modo, gli aggiornamenti di configurazioni del WAF non devono andare di pari passo alle modifiche del software, in quanto il WAF apprende e si adatta. Altro elemento essenziale del WAF è il virtual patching, attraverso di esso, il WAF pone rimedio, ad esempio, alle mancanze di aggiornamento dei sistemi operativi sulle quali le applicazioni si basano.
Si elencano di seguito i principali obiettivi che l'AOU intende perseguire con l'utilizzo del WAF:

- Protezione delle applicazioni HTTP su base censimento OWASP10
- Difesa dagli attacchi BOT come il DOS
- Reportistica ai fini della conformità alle normative
- Protezione del meccanismo di comunicazione API

La fornitura in argomento è costituita da n.2 web application firewall

5. Piattaforma di cybersecurity asset & risk management con l'implementazione automatica di regole di sicurezza

L'AOU Federico II vede collegati alla rete aziendale un elevato numero di device (circa 10.000), di differente natura, di cui il 20% è costituito da apparecchiature elettromedicali.
Tenuto conto che tale percentuale prevede un tasso di crescita pari al 40% per il prossimo bienno, l'Azienda vuole dotarsi di uno strumento di sicurezza agentless capace di monitorare continuamente il comportamento di tutti i dispositivi in rete per identificare anomalie che possano indicare che il device sia stato compromesso.
Tale strumente prevede l'utilizzo di n.1 piattaforma che prevede l'integrazione con i sistemi di vulnerability management, consente la gestione e il controllo dei malware e del traffico anomalo.
Lo scopo è quello di individuare ogni vulnerabilità un full asset enrichment e non soltanto un semplice indirizzo IP ma informazioni specifiche di contesto sul device medicale impattato dalla vulnerabilità
Grazie alla capacità di elaborare tag ed oggetti del protocollo DICOM la piattaforma mette a disposizione dashboard, report e informazioni sui dispositivi elettromedicali tali, per cui è possibile analizzare in maniera estremamente semplice anche l'utilizzo effettivo dei dispositivi elettromedicali.
Sulla piattaforma vengono abilitate policy e signature specifiche per la gestione dei device elettromedicali (oltre alle engine di threat detection, analisi comportamentale e signature generiche per le altre tipologie di apparati), che consentiranno una corretta gestione di tutto ciò che concerne:

- Medical Device Asset Management
- Medical Device Inventory
- Medical Device Threat

Il Sistema individua inoltre tutte le vulnerabilità degli asset presenti nella rete e propone le remediation tramite un asset inventory management.
L'infrastruttura dovrà essere prevedere n.1 piattaforma di gestione ed un numero illimitato di sonde virtuali per assicurare la raccolta puntuale di tutte le informazioni presenti sulla rete e, allo stesso modo, garantire l'adeguata ridondanza in caso di fault.

OBIETTIVI DEL PROGETTO E RISULTATI ATTESI

Il **progetto,** in linea con quanto richiesto dall'Azione 2.2.1, consentirà all'Azienda Ospedaliera Universitaria Federico II di raggiungere i seguiti obiettivi:

1. gestione sicura del dato sanitario attraverso l'analisi, il contenimento e la governance di eventuali attacchi informatici;
2. potenziamento nella gestione delle tecnologie biomediche in rete (asset management, localizzazione dei dispositivi, stato di utilizzo etc);
3. efficientamento della digitalizzazione dei dati relativi alla vita lavorativa del dipendente, permettendo un accesso unico e semplificato alle informazioni anagrafiche, giuridiche e di rileazione presenze e ai documenti digitali;
4. la digitalizzazione dei risultati diagnostici dell'Anatomia patologica per supportare al meglio le competenze e la visione unica del patologo attraverso second opinion più rapide, diagnosi in remoto, maggiore precisione e quantificazione, flusso di lavoro più efficace, al fine di ottenere diagnosi più rapide e cure ottimali.

POR Campania FESR 2014-2020 - AZIONE 2.2.1 "SOLUZIONI TECNOLOGICHE PER LA DIGITALIZZAZIONE E L'INNOVAZIONE DEI PROCESSI INTERNI DEI VARI AMBITI DELLA PUBBLICA AMMINISTRAZIONE NEL QUADRO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ"
D.G.R. 345/2023 - Progetto: ``Incremento delle performance sanitarie e sicurezza informatica del dato sanitario``- CUP C69B23000130006

QUADRO ECONOMICO DEL PROGETTO

VOCI DI SPESA	IMPORTO COMPLESSIVO	IVA	ALIQUOTA IVA
A) Beni oggetto dell'acquisto:			
Servizi di digitalizzazione della documentazione sanitaria a supporto degli assistiti e degli operatori sanitari (specificare la tipologia di documenti da digitalizzare ed il numero di documenti per ciascuna tipologia);	€ 1.372.207,20	€ 247.447,20	22%
Attrezzature per la digitalizzazione dei risultati diagnostici (indicare le singole attrezzature ed il relativo numero, nonchè eventuali software di funzionamento			
N. 2 Scanner per vetrini	€ 570.960,00	€ 102.960,00	22%
N. 3 workstation di refertazione	€ 36.600,00	€ 6.600,00	22%
N. 4 stampanti per etichette QRCODE	€ 4.880,00	€ 880,00	22%
n.1 Stampante per Biocassette + n.1 Stampante per vetrini per l'etichettatura con QRCode	€ 82.960,00	€ 14.960,00	22%
n.1 Server per lo storage dei file scannerizzati	€ 146.400,00	€ 26.400,00	22%
n.1 TMA semiautomatico	€ 79.300,00	€ 14.300,00	22%
N.1 Software di digital Pathology	€ 244.000,00	€ 44.000,00	22%
Sistemi di Cyber Security			
N. 1 Piattaforma di cybersecurity asset & risk management con	€ 260.958,00	€ 47.058,00	22%

l'implementazione automatica di regole di sicurezza			
N. 2 Web Application Firewall	€ 213.500,00	€ 38.500,00	22%
N. 2 MFA	€ 31.872,50	€ 5.747,50	22%
N. 2 Endpoint Detection and Response	€ 56.453,06	€ 10.180,06	22%
N. 2 Network Access Control	€ 162.450,00	€ 29.294,28	22%
b) Altro:			
b1. Spese per la relativa installazione e messa in esercizio			
b2. Lavori connessi alla funzionalità			
b3. Spese di collaudo (lavori e forniture)			
c) IVA su voce a) e b) (se non recuperabile)	€ 588.327,04		
TOTALE PROGETTO	3.262.540,86 €		

DIGITALIZZAZIONE DELLA DOCUMENTAZIONE SANITARIA A SUPPORTO DEGLI ASSISTITI E DEGLI OPERATORI SANITARI				
DESCRIZIONE *(dettagliare i servizi da attivare, indicando, per ciascun servizio, la tipologia di documenti da digitalizzare ed il numero di documenti per ciascuna tipologia; sono escluse le spese relative a manutenzione ordinaria, aggiornamenti, assistenza periodica, formazione del personale)*	**IMPONIBILE**	**IVA**	**IMPORTO COMPLESSIVO (comprensivo di IVA se non recuperabile)**	**MODALITA' DI ACQUISTO**
Servizi di digitalizzazione di n. 2163 fascicoli del personale	€ 1.124.760,00	€ 247.447,20	€ 1.372.207,20	Convenzione PSN
TOTALE	€ 1.124.760,00	€ 247.447,20	€ 1.372.207,20	

ATTREZZATURE PER LA DIGITALIZZAZIONE DEI RISULTATI DIAGNOSTICI				
DESCRIZIONE *(dettagliare le attrezzature ed il relativo numero, nonchè gli eventuali software di funzionamento; sono escluse le spese relative a manutenzione ordinaria, aggiornamenti, assistenza periodica, formazione del personale)*	**IMPONIBILE**	**IVA**	**IMPORTO COMPLESSIVO (comprensivo di IVA se non recuperabile)**	**MODALITA' DI ACQUISTO**

N. 2 Scanner per vetrini	€ 468.000,00	€ 102.960,00	€ 570.960,00	Procedura autonoma
N. 3 workstation di refertazione	€ 30.000,00	€ 6.600,00	€ 36.600,00	Procedura autonoma
N. 4 stampanti per etichette QRCODE	€ 4.000,00	€ 880,00	€ 4.880,00	Procedura autonoma
n.1 Stampante per Biocassette + n.1 Stampante per vetrini per l'etichettatura con QRCode	€ 68.000,00	€ 14.960,00	€ 82.960,00	Procedura autonoma
n.1 Server per lo storage dei file scannerizzati	€ 120.000,00	€ 26.400,00	€ 146.400,00	Procedura autonoma
n.1 TMA semiautomatico	€ 65.000,00	€ 14.300,00	€ 79.300,00	Procedura autonoma
Software di digital Pathology	€ 200.000,00	€ 44.000,00	€ 244.000,00	Procedura autonoma
TOTALE	€ 955.000,00	€ 210.100,00	€ 1.165.100,00	

SISTEMI DI CYBER SECURITY				
DESCRIZIONE *(dettagliare componenti hardware, componenti software ed eventuali spese necessarie per l'installazione; sono escluse le spese relative a manutenzione ordinaria, aggiornamenti, assistenza periodica, formazione del personale)*	**IMPONIBILE**	**IVA**	**IMPORTO COMPLESSIVO (comprensivo di IVA se non recuperabile)**	**MODALITA' DI ACQUISTO**
N. 1 Piattaforma di cybersecurity asset & risk management con l'implementazione automatica di regole di sicurezza	€ 213.900,00	€ 47.058,00	€ 260.958,00	Procedura autonoma
N. 2 Web Application Firewall	€ 175.000,00	€ 38.500,00	€ 213.500,00	Procedura autonoma
N. 2 MFA	€ 26.125,00	€ 5.747,50	€ 31.872,50	Procedura autonoma
N. 2 Endpoint Detection and Response	€ 46.273,00	€ 10.180,06	€ 56.453,06	AQ Consip
N. 2 Network Access Control	€ 133.155,82	€ 29.294,28	€ 162.450,00	AQ Consip
TOTALE	€ 594.453,82	€ 130.779,84	€ 725.233,66	

Cronoprogramma

SOGGETTO ATTUATORE: AOU FEDERICO II. Intervento: "POR Campania FESR 2014-2020 - AZIONE 2.2.1 "SOLUZIONI TECNOLOGICHE PER LA DIGITALIZZAZIONE E L'INNOVAZIONE DEI PROCESSI INTERNI DEI VARI AMBITI DELLA PUBBLICA AMMINISTRAZIONE NEL QUADRO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ" D.G.R. 345/2023 - Progetto: ``Incremento delle performance sanitarie e sicurezza informatica del dato sanitario``- CUP C69B23000130006"

ATTIVITA' (1)	Programmazione annuale (2)	Data avvio		Data conclusione		2022												2023											
		prevista	effettiva	prevista	effettiva	Gen	Feb	Mar	Apr	Mag	Giu	Lug	Ago	Set	Ott	Nov	Dic	Gen	Feb	Mar	Apr	Mag	Giu	Lug	Ago	Set	Ott	Nov	Dic
Atto di approvazione del programma annuale per l'acquisizione di beni e servizi			11.11.2022		11.11.2022																								
Approvazione progetto			14.07.2023		12.09.2023																								
Procedure di gara per l'affidamento della fornitura di beni/servizi		24.07.2023		19.10.2023																									
Aggiudicazione procedura di affidamento		19.10.2023		19.10.2023																									
Stipula del contratto di fornitura		20.10.2023		27.10.2023																									
Esecuzione del contratto		30.10.2023		30.11.2023																									
Regolare esecuzione/Verifica di conformità		01.12.2023		20.12.2023																									
Funzionalità / fruibilità dell'opera		21.12.2023		31.12.2023																									