ARES Sardegna
Azienda Regionale Salute

SERVIZIO SANITARIO DELLA
REGIONE AUTONOMA DELLA SARDEGNA

DELIBERAZIONE DEL DIRETTORE GENERALE N. 333 **DEL** 29/12/2023

Proposta n. 420 del 22/12/2023

STRUTTURA PROPONENTE: DIPARTIMENTO PER LA SANITÀ DIGITALE E L'INNOVAZIONE TECNOLOGICA

Ing. Giancarlo Conti

OGGETTO: Approvazione preliminare del progetto di Cybersicurezza per le Aziende Sanitarie della Sardegna, denominato *Digital Security & Compliance*, da realizzarsi attraverso l'adesione all'Accordo Quadro Consip ID 2296 per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni (lotti 1 e 2).

Con la presente sottoscrizione i soggetti coinvolti nell'attività istruttoria, ciascuno per le attività e le responsabilità di competenza dichiarano che la stessa è corretta, completa nonché conforme alle risultanze degli atti d'ufficio, per l'utilità e l'opportunità degli obiettivi aziendali e per l'interesse pubblico.

Ruolo	Soggetto	Firma Digitale
L'istruttore	Dott. Emiliano Arca	EMILIANO ARCA Firmato digitalmente da EMILIANO ARCA Data: 2023.12.22 10:51:10 +01'00'
Il Responsabile della SSD Acquisti di Tecnologie Informatiche		
Il Responsabile del Procedimento	Ing. Maurizio Medda	ARES Sardegna Firmato digitalmente da MEDDA MAURIZIO Data: 2023.12.22 11:06:58 +01'00'

La presente Deliberazione prevede un impegno di spesa a carico della Azienda Regionale della Salute - ARES

SI [ ] NO [X] DA ASSUMERE CON SUCCESSIVO PROVVEDIMENTO [ ]

La presente Deliberazione è soggetta al controllo preventivo di cui all'art. 41 della L.R. 24/2020

SI [ ] NO [X]

IL DIRETTORE DEL DIPARTIMENTO PER LA SANITÀ DIGITALE E L'INNOVAZIONE TECNOLOGICA

VISTO il decreto legislativo n. 502 del 30 dicembre 1992 "Riordino della disciplina in materia sanitaria" e ss.mm.ii.;

VISTA la legge regionale n. 24/2020 "Riforma del sistema sanitario regionale e riorganizzazione sistematica delle norme in materia. Abrogazione della legge regionale n. 10 del 2006, della legge regionale n. 23 del 2014 e della legge regionale n. 17 del 2016 e di ulteriori norme di settore" e ss.mm.ii.;

VISTA la deliberazione del Direttore Generale n. 30 del 01/02/2023 e le successive modifiche ed integrazioni, con la quale sono state conferite, in via provvisoria e nelle more dello svolgimento delle procedure previste dalla normativa vigente per il conferimento degli incarichi, le funzioni dirigenziali al fine di garantire il funzionamento delle strutture aziendali a seguito dell'entrata in vigore dell'Atto Aziendale di Ares Sardegna;

DATO ATTO che il soggetto che adotta il presente atto non incorre in alcuna delle cause di incompatibilità previste dalla normativa vigente, con particolare riferimento al Codice di Comportamento dei Pubblici Dipendenti e alla Normativa Anticorruzione e che non sussistono, in capo allo stesso, situazioni di conflitto di interesse in relazione all'oggetto dell'atto, ai sensi della Legge 190 del 06/11/2012 e norme collegate;

VERIFICATA la compatibilità e conformità con le norme nazionali, regionali e regolamenti in materia, relaziona al Direttore Generale quanto di seguito riportato:

PREMESSO

- che la mission di ARES, dotata di personalità giuridica di diritto pubblico, di autonomia amministrativa, patrimoniale, organizzativa, tecnica, gestionale e contabile, è quella di supportare le Aziende sanitarie regionali nella produzione di servizi sanitari e sociosanitari;
- che la L.R. 24/2020 assegna ad ARES importanti compiti di programmazione, monitoraggio e trasformazione digitale: in particolare, vengono assegnate ad ARES, tra le altre, le funzioni di gestione delle infrastrutture di tecnologia informatica, connettività, sistemi informativi e flussi dati per tutte le Aziende sanitarie della regione Sardegna, in un'ottica di omogeneizzazione e sviluppo del sistema ICT;

PRESO ATTO

- che negli ultimi anni la minaccia cibernetica è notevolmente cresciuta in quantità e qualità e le tipologie di attacchi con finalità estorsive hanno trovato nuove e più invasive forme; ARES, come ogni Ente di medie-grandi dimensioni, si trova a fronteggiare ogni giorno decine di migliaia di attacchi informatici, per lo più automatici, ma talora anche mirati e preparati con competenza e risorse dedicate;
- che il contesto infrastrutturale e applicativo delle Aziende Sanitarie della Sardegna, richiede una gestione della sicurezza applicata non solo al contesto IT, ma anche a quello delle apparecchiature biomediche al fine di garantire la sicurezza informatica delle Amministrazioni mediante la prevenzione e la gestione delle minacce, ed un governo efficace ed efficiente dei rischi di sicurezza;

DATO ATTO che il Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica, attraverso le proprie strutture, assicura la gestione delle tecnologie biomediche, delle infrastrutture informatiche e dei sistemi di sanità digitale di tutte le Aziende del Servizio Sanitario Regionale in termini di efficienza, efficacia e sicurezza;

EVIDENZIATO che il Dipartimento ha identificato la necessità di realizzare un progetto integrato per l'intero Servizio Sanitario Regionale, al fine di rispondere in maniera organizzata e completa ai bisogni di sicurezza, affidabilità, disponibilità e conformità normativa dei servizi e dell'infrastruttura tecnologica;

CONSIDERATO che solo affrontando in maniera unitaria i suddetti bisogni è possibile avere un impatto uniforme sull'intero sistema regionale, riducendo i rischi di *security*, *data protection* e *safety* e consentendo di conformare alle normative vigenti il complesso dei sistemi e dei servizi di sanità digitale senza generare disparità territoriali;

RITENUTO inoltre opportuno fare in modo che il servizio sanitario regionale possa usufruire di un sistema di gestione dei dispositivi connessi in rete, compresi i dispositivi medici, che consenta la gestione inventariale in tempo reale e garantisca agli utenti una efficace tutela dei propri dati personali riducendo al contempo i rischi di sanzioni per le aziende titolari: gli utenti potranno in tal modo usufruire di servizi di sanità digitale e di diagnosi e cura più affidabili e sicuri e il sistema sanitario regionale, grazie anche al contenimento dei rischi di *security*, *data protection* e *safety* potrà ottenere un significativo aumento dell'efficacia ed efficienza dei servizi erogati riducendo le perdite di dati, i blocchi dei sistemi e le possibili conseguenti sanzioni;

ATTESO che tra le varie iniziative CONSIP, il Piano delle Gare Strategiche ICT si pone tra i suoi obiettivi quello di mettere a disposizione delle PA specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in tale ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza;

VISTO, in particolare, l'Accordo Quadro ID 2296 per l'affidamento di servizi di sicurezza da remoto, di *compliance* e controllo per le pubbliche amministrazioni (lotti 1 e 2), che affiancandosi alle gare strategiche ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese, offre strumenti adeguati a garantire il fabbisogno sopra espresso di realizzare un progetto integrato di protezione cibernetica per le aziende sanitarie della Regione Sardegna, tenuto conto che vengono garantiti:

- l'accesso semplificato a fornitori qualificati e servizi specializzati in sicurezza informatica, semplificando il processo di selezione e acquisizione di servizi specifici per la protezione cibernetica delle aziende sanitarie;
- il rispetto delle normative e degli standard vigenti nel settore sanitario, come l'HIPAA o il GDPR, riducendo così il rischio di non conformità;
- la riduzione dei tempi di approvvigionamento, riducendo i tempi complessivi di attuazione dei progetti di protezione cibernetica per le aziende sanitarie.
- un livello predefinito di qualità e standardizzazione dei servizi offerti dai fornitori selezionati, contribuendo a garantire che le soluzioni adottate siano di alta qualità e affidabili.
- il controllo dei costi, consentendo di negoziare tariffe competitive e di stabilire prezzi fissi per i servizi di sicurezza informatica;
- il supporto continuativo post-vendita e assistenza, assicurando un supporto costante e l'accesso a un aiuto tempestivo in caso di necessità;

CONSIDERATO che il suddetto Accordo Quadro ID 2296 - Servizi di Sicurezza da Remoto, di *Compliance* e Controllo per le Pubbliche amministrazioni, che prevede una modalità di affidamento dei Contratti Esecutivi tramite ordinativo di fornitura a condizioni tutte fissate, previa definizione del "Piano dei fabbisogni" e del successivo "Piano Operativo", si compone di due lotti, di cui uno dedicato ai servizi di sicurezza e l'altro a quello di *compliance* e di controllo:

- l'Accordo Quadro relativo al Lotto 1 (CIG 88846293CA) è dedicato ai Servizi di Sicurezza da Remoto; aggiudicato in via definitiva ed efficace il 24/05/2022, è stato stipulato il 04/08/2022, è attivo dal 26/09/2022 ed ha durata di 24 mesi (i Contratti esecutivi hanno una durata massima di 48 mesi); i fornitori aggiudicatari sono, per le Pubbliche Amministrazioni Locali (PAL), il RTI costituito Accenture S.p.A. - Fincantieri Nextech S.p.A. - Fasteweb S.p.A. - Deas, Difesa e Analisi Sistemi S.p.A.;
- l'Accordo Quadro relativo al Lotto 2 (CIG 8884642E81) è dedicato ai Servizi di compliance e controllo; aggiudicato in via definitiva ed efficace il 16/03/2022, è stato stipulato il 29/04/2022, è attivo dal 27/05/2022 ed ha durata di 24 mesi (i Contratti esecutivi hanno una durata massima di 48 mesi); I fornitori aggiudicatari sono, per le Pubbliche Amministrazioni Locali (PAL), il RTI costituito Deloitte Risk Advisory S.r.l. - EY Advisory S.p.A. - Teleco S.r.l.;

EVIDENZIATO che ARES Sardegna ha predisposto un progetto generale relativo alla Cybersicurezza che prevede un piano di *security/data protection enforcement* e *compliance* attinente alle infrastrutture e servizi "digitali" ricadenti nel perimetro di seguito riportato:

- ARES;
- AREUS;
- n. 8 Aziende Sanitarie Locali;
- Azienda Ospedaliera Universitaria di Cagliari;
- Azienda Ospedaliera Universitaria di Sassari;
- ARNAS Brotzu;

DATO ATTO che la strategia di *Digital Security* che si intende perseguire è declinata secondo 11 obiettivi:

- Asset intelligence sull'intero perimetro dell'infrastruttura sanitaria regionale, tramite l'utilizzo di tecnologie innovative che consentono la visione completa dell'ecosistema digitale;
- Protezione degli asset digitali;
- Monitoraggio continuo dell'efficacia delle misure di sicurezza;
- Rilevazione e risposta tempestiva agli attacchi cyber;
- Protezione dei dati personali degli interessati;
- Rafforzamento della "safety" dei sistemi critici medicali a garanzia dei pazienti e degli operatori;
- Adeguamento delle organizzazioni sanitarie alle normative nazionali ed europee in ambito security e data protection (det.628, NIS2, GDPR);
- Adeguamento di AREUS al PSCN;
- Certificazione ISO 27001, ISO 27017, ISO 27018 di ARES;
- Qualificazione ACN per i servizi SAAS di ARES;
- Continuità operativa e integrità dei servizi di sanità digitale;

PRECISATO che il progetto prevede da una parte l'attivazione di nuove funzionalità di monitoraggio e controllo e dall'altra il potenziamento di alcune già esistenti e pienamente operative; coerentemente, per quanto concerne l'*end-point protection*, attualmente pienamente operativa ed in forma centralizzata, si è valutato, per motivi sia logistici che di interfacciamento con i nuovi sistemi avanzati, di procrastinare la sua eventuale sostituzione/conferma in una seconda fase e comunque a progetto avviato;

VISTI il Piano dei Fabbisogni per i servizi di sicurezza da remoto (Lotto 1) e il Piano dei Fabbisogni per i servizi di compliance e controllo (Lotto 2) predisposti dal Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica, allegati al presente atto per costituirne parte integrante e sostanziale;

DATO ATTO che ARES ha suddiviso e parcellizzato il progetto generale relativo alla Cybersicurezza tenendo conto delle attività e dei servizi disponibili nei due lotti attivi dell'AQ 2296, definendo due distinti sottoprogetti di durata quadriennale per un valore complessivo stimato, allo stato, pari a € 14.086.486,00 (€ 10.743.416,00 per il lotto 1 e € 3.343.070,00 per il lotto 2), IVA esclusa;

RITENUTO opportuno procedere all'approvazione preliminare del progetto di Cybersicurezza per le Aziende Sanitarie della Sardegna, denominato *Digital Security & Compliance*;

EVIDENZIATO che dall'approvazione preliminare di tale progetto non derivano direttamente oneri a carico del Servizio Sanitario Regionale, essendo al momento non impegnativa la presentazione dei Piani dei Fabbisogni ai Fornitori di riferimento ai fini dello sviluppo dei rispettivi Piani Operativi;

TENUTO CONTO in ogni caso che il progetto complessivo troverebbe adeguata copertura nella programmazione finanziaria e nella programmazione delle acquisizioni di beni e servizi tra gli interventi in materia di sicurezza informatica;

PROPONE

1) **DI APPROVARE** in via preliminare il progetto di Cybersicurezza per gli Enti Sanitari della Sardegna, denominato *Digital Security & Compliance*, da realizzarsi attraverso l'adesione all'Accordo Quadro Consip ID 2296 per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni (lotti 1 e 2), come meglio descritto nel Piano dei Fabbisogni per i servizi di

sicurezza da remoto (Lotto 1) e nel Piano dei Fabbisogni per i servizi di *compliance* e controllo (Lotto 2) predisposti dal Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica, allegati al presente atto per costituirne parte integrante e sostanziale;

2) **DI DARE ATTO** che dall'approvazione preliminare del progetto di Cybersicurezza per le Aziende Sanitarie della Sardegna, denominato *Digital Security & Compliance*, non derivano direttamente oneri a carico del Servizio Sanitario Regionale, essendo al momento non impegnativa la presentazione dei Piani dei Fabbisogni ai Fornitori di riferimento ai fini dello sviluppo dei rispettivi Piani Operativi;

3) **DI TRASMETTERE** copia del presente atto all'Ufficio Delibere per la pubblicazione all'Albo Pretorio on-line dell'Azienda regionale della salute – ARES.

IL DIRETTORE DEL DIPARTIMENTO
PER LA SANITÀ DIGITALE E L'INNOVAZIONE TECNOLOGICA
Ing. Giancarlo Conti

Giancarlo Conti
22.12.2023
10:25:37
UTC

IL DIRETTORE GENERALE

Dott.ssa Annamaria Tomasella, nominata con DGR n. 51/34 del 30.12.2021, coadiuvata dal Dott. Attilio Murru - Direttore Amministrativo, nominato con deliberazione n. 131 del 01.07.2022, e dalla Dott.ssa Evelina Gollo, Direttore Sanitario, nominata con deliberazione n° 198 del 29/08/2023;

VISTA la su estesa proposta, che si richiama integralmente;

ACQUISITO i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario;

Direttore Amministrativo
Dott. Attilio Murru

MURRU ATTILIO
Firmato digitalmente da MURRU ATTILIO
Data: 2023.12.28 17:42:12 +01'00'

Direttore Sanitario
Dott.ssa Evelina Gollo

EVELINA GOLLO
Firmato digitalmente da EVELINA GOLLO
Data: 2023.12.28 17:54:05 +01'00'

DELIBERA

1) **DI APPROVARE** il contenuto della proposta di deliberazione sopra richiamata e per l'effetto di darne integrale esecuzione;

IL DIRETTORE GENERALE
Dott.ssa Annamaria Tomasella

Annamaria
Tomasella
29.12.2023
08:42:12
GMT+01:00

ALLEGATI SOGGETTI A PUBBLICAZIONE

ALLEGATI NON SOGGETTI A PUBBLICAZIONE

- Piano dei Fabbisogni per i servizi di sicurezza da remoto (Lotto 1)
- Piano dei Fabbisogni per i servizi di *compliance* e controllo (Lotto 2)

Si attesta che la presente deliberazione viene pubblicata nell'Albo Pretorio on-line dell'Azienda regionale della salute - ARES dal 29/12/2023 al 13/01/2024

Il Dirigente Responsabile per la pubblicazione o suo delegato

LEI GAVINO

Firmato digitalmente da LEI GAVINO
Data: 2023.12.29 11:01:11 +01'00'