REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFARIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

02-01-00 - Direzione Generale dell'Innovazione e Sicurezza It

ARES Sardegna

Direzione generale

CONVENZIONE TRA LA REGIONE AUTONOMA DELLA SARDEGNA E ARES SARDEGNA PER REGOLARE LE ATTIVITA' CONNESSE AL PIANO DI ATTUAZIONE E GESTIONE DELLA CYBERSICUREZZA DELLA MISURA #55 DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

STRATEGIA NAZIONALE DELLA CYBERSICUREZZA 2022-2026
Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR
MISURA #55

FINANZIAMENTO AUTORIZZATO CON DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 8 luglio 2024 relativo al fondo per l'attuazione della strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza.

CONVENZIONE APPROVATA CON

DGR N° 65/30 DEL 12 DICEMBRE 2025

TRA

la Regione Autonoma della Sardegna – Assessorato degli affari generali, personale e riforma della regione, Direzione generale dell'innovazione e sicurezza IT, domiciliata in viale Trento 69 Cagliari, C.F. 80002870923, nella persona Ing. Marco Melis, in qualità di Direttore generale dell'innovazione e sicurezza IT, nel seguito denominato "Regione",

E

l'Azienda Regionale della Salute della Sardegna (ARES), con sede legale in via Piero della Francesca, n.1 Selargius, C.F. 03990570925, nella persona del Dott. Giuseppe Pintor, in qualità di Direttore generale, nel seguito denominata "Beneficiario" o "Azienda".

(la Regione e il Beneficiario saranno anche denominati, nella presente Convenzione, "le Parti")

VISTO lo Statuto Regionale L. Cost. 26 febbraio 1948, n.3

VISTA la Legge Regionale 7 gennaio 1977, n.1

VISTA la legge 7 agosto 1990, n. 241 e successive modifiche ed integrazioni recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso agli atti amministrativi;

VISTO l'articolo 15, comma 1 della legge 7 agosto 1990, n. 241, e s.m.i. ai sensi del quale le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse e comma 2-bis recante l'obbligo della sottoscrizione degli accordi mediante utilizzo di firma digitale;

VISTI gli articoli 9, 33 e 34 della Costituzione relativi alla ricerca scientifica e tecnica e all'istruzione, in coerenza con le attribuzioni di cui all'articolo 117 della stessa Costituzione

VISTA il decreto legislativo 23 giugno 2011, n. 118 recante disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi;

VISTA la legge regionale n. 12 del 08/05/2025 - Legge di Stabilità 2025;

VISTA la legge Regionale n. 13 del 08/05/2025 - Bilancio di previsione 2025-2027;

VISTA la Delibera del 14 maggio 2025, n. 26/17 - Ripartizione delle tipologie e dei programmi in categorie e macroaggregati ed elenchi dei capitoli di entrata e spesa, conseguenti all'approvazione della legge regionale 8 maggio 2025, n. 13 (Bilancio di previsione 2025-2027);

VISTA la L. 7 agosto 1990, n. 241, recante "Norme in materia di procedimento amministrativo e di accesso ai documenti amministrativi" e s.m.i, e la L.R. 20 ottobre 2016, n. 24, recante "Norme sulla qualità della regolazione e di semplificazione dei procedimenti amministrativi

VISTO Il Piano di implementazione della Strategia Nazionale Di Cybersicurezza 2022 – 2026 approvato dall'Agenzia Nazionale per la Cybersicurezza;

CONSIDERATO che suddetto piano ha approvato la Misura #55 al fine di "Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR";

DATO ATTO CHE l'Agenzia per la Cybersicurezza Nazionale (ACN) ha avviato una rilevazione dei fabbisogni finanziari necessari all'attuazione della Misura #55 – "Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR" – nell'ambito del Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 con l'obiettivo di sostenere la transizione digitale e l'innalzamento dei livelli di cybersicurezza nella PA, attraverso la pianificazione e il finanziamento di interventi specifici con scadenza 15/02/2024 ore 18:00 con destinatari tutte le Amministrazioni ed Enti pubblici a livello centrale, le Regioni e le Province autonome che intendano attuare la Misura;

DATO ATTO CHE per la realizzazione degli interventi sono stati istituiti, presso il Ministero dell'Economia e delle Finanze (ai sensi dell'art. 1, comma 899, Legge 197/2022):

- il Fondo per l'attuazione della Strategia nazionale di cybersicurezza (per investimenti e autonomia tecnologica digitale);

- il Fondo per la gestione della cybersicurezza (per la copertura delle attività operative).

CONSIDERATO CHE la Direzione generale dell'innovazione e sicurezza IT ha partecipato all'avviso della Misura #55 (rif. nota prot. n.1202 del 15/02/2024) presentando due interventi strategici riferibili ai sistemi informativi interni della Regione Autonoma della Sardegna, e uno in ambito sanitario che individua come attuatore responsabile l'ARES Sardegna:

- Consolidamento della strategia di cybersecurity – Attuatore responsabile ARES Sardegna

VISTO il Decreto del Presidente del Consiglio dei Ministri dell' 8 luglio 2024, avente ad oggetto "Ripartizione del Fondo per l'attuazione della strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza", prevede l'assegnazione alla Regione Autonoma della Sardegna - Azienda regionale della salute (ARES) di un finanziamento totale pari a Euro 9.735.260, così suddivisi:

- € 4.477.090 per l'attuazione della strategia nazionale di cybersicurezza;

- € 5.258.170 per la gestione della cybersicurezza, ai sensi dell'articolo 1, comma 899, lettera a), della legge 29 dicembre 2022, n. 197.

DATO ATTO pertanto, che sussiste la necessità di regolare l'attuazione dell'intervento mediante apposita Convenzione tra la Regione e l'Azienda Regionale per la Salute Sardegna;

Tutto ciò premesso si conviene e si stipula in modalità elettronica, con sottoscrizione digitale, quanto segue:

Articolo 1

PREMESSE

Le premesse fanno parte integrante e sostanziale della presente Convenzione.

Articolo 2

OGGETTO DELLA CONVENZIONE

1. La presente Convenzione disciplina i rapporti fra le Parti e fissa le modalità di utilizzo, da parte del Beneficiario ARES, del finanziamento per realizzare l'intervento "Consolidamento della strategia di cybersecurity – Attuatore responsabile ARES Sardegna" finanziato dall'Agenzia Nazionale per la Cybersicurezza relativo alla STRATEGIA NAZIONALE DELLA CYBERSICUREZZA 2022-2026 sulla Misura "Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR - MISURA #55" i cui documento è allegato alla presente convenzione;
2. Le azioni da realizzare sono contenute nella proposta d'intervento approvata dall'Agenzia Nazionale per la Cybersicurezza, le cui attività sono riportate nella seguente tabelle:

ID	Attività	Milestone
A1	Avvio attività SOC	Definizione piano delle attività per il roll'out progressivo sui vari enti e per tipologia di sistemi (i.e. IT, IoT, MD) e definizione degli use case per il SOC
G1	Erogazione servizi SOC	Monitoraggio "real-time" eventi di sicurezza e minacce, Contenimento gestione eventi, Gestione degli Incidenti di Sicurezza
A2	Avvio attività Vulnerability management	Definizione del piano di monitoraggio del perimetro e definizione dei criteri di misurazione/classificazione delle potenziali vulnerabilità
G2	Erogazione servizi Vulnerability management	Monitoraggio continuo del perimetro, ricerca delle vulnerabilità, categorizzazione del potenziale impatto delle vulnerabilità rilevate, pianificazione delle azioni di rimedio per le vulnerabilità rilevate
A3	Avvio attività Threat Intelligence (solo AREUS)	Definizione Linee Guida e pianificazione dell'integrazione col servizio SOC

ID	Attività	Milestone
G3	Erogazione servizi Threat Intelligence (solo AREUS)	Monitoraggio dei threat actor, analisi delle common Vulnerability, data feed al servizio SOC, elaborazione di Report e Alert
A4	Avvio attività Next Generation Firewall (NGFW)	Definizione del perimetro e configurazione dello strumento di NGFW
G4	Erogazione servizi Next Generation Firewall (NGFW)	Gestione continuativa delle politiche e delle configurazioni, stima degli impatti e del rischio sulle configurazioni da implementare (o implementate), rilevamento avanzato malware, analisi predittiva della sfruttabilità delle vulnerabilità e gestione degli accessi in modalità multifattore per le utenze privilegiate
A5	Avvio attività Web Application Firewall (WAF) (solo AREUS)	Definizione del perimetro, configurazione dello strumento di WAF e definizione del piano di automazione
G5	Erogazione servizi Web Application Firewall (WAF) (solo AREUS)	Behavioral Analytics, analisi e discriminazione del traffico web lecito e malevolo
G6	Formazione e Security Awareness	Definizione del programma di training, presa in carico del servizio, configurazione piattaforma di e-learning e coinvolgimento del personale tecnico dell'Amministrazione, erogazione della formazione e creazione reportistica
G7	Migrazione sicura in cloud	"Analisi e Discovery" del livello di sicurezza dei servizi, progettazione "Security by design", configurazione degli apparati di sicurezza, della "landing zone e definizione dei security test
G8	Governance	Guida e condivisione avanzamenti attività progettuali

3. I soggetti Destinatari, oltre al Beneficiario ARES, sono anche gli Enti di seguito elencati, ciascuno in relazione alla peculiare tipologia di intervento previsto per ciascuna Azione:
   - Azienda regionale dell'emergenza e urgenza della Sardegna (AREUS);
   - Azienda di rilievo nazionale ed alta specializzazione "G. Brotzu" (ARNAS)
   - Aziende ospedaliero-universitarie (AOU) di Cagliari e Sassari;
   - Azienda socio-sanitaria locale (ASL 1 Sassari)
   - Azienda socio-sanitaria locale (ASL 2 Gallura)
   - Azienda socio-sanitaria locale (ASL 3 Nuoro)
   - Azienda socio-sanitaria locale (ASL 4 Ogliastra)
   - Azienda socio-sanitaria locale (ASL 5 Oristano)

- Azienda socio-sanitaria locale (ASL 6 Medio Campidano)
- Azienda socio-sanitaria locale (ASL 7 Sulcis)
- Azienda socio-sanitaria locale (ASL 8 Cagliari)

4. L'Ares assume il ruolo di soggetto attuatore dell'intervento, mentre la Direzione generale dell'innovazione e sicurezza IT assume il ruolo di monitoraggio, verifica e gestione finanziaria per il trasferimento delle somme;

Articolo 3

IMPORTO DELLA CONVENZIONE E OBIETTIVI DI RISULTATO

1. Il finanziamento ammissibile per l'intervento oggetto della presente Convenzione è pari a Euro 9.735.260, così suddivisi in:

   - € 4.477.090 per l'attuazione della strategia nazionale di cybersicurezza,

   - € 5.258.170 per la gestione della cybersicurezza,

   ai sensi dell'articolo 1, comma 899, lettera a), della legge 29 dicembre 2022, n. 197.

2. Il Beneficiario è tenuto a contribuire al raggiungimento degli obiettivi progettuali. A tal fine, il Beneficiario è tenuto, nella progettazione degli interventi e nella definizione dei cronoprogrammi di spesa, ad ottimizzare e massimizzare le tempistiche di spesa, accelerando e anticipando il più possibile l'avvio dell'esecuzione, e, in ogni caso, a rispettare le indicazioni e la compilazione di tutta la documentazione propedeutica al monitoraggio dell'Agenzia Nazionale per la Cybersicurezza che saranno inoltrati e vidimati dalla Regione;

Articolo 4

DURATA ED EFFICACIA DELLA CONVENZIONE

1. La presente Convenzione ha validità dalla data della sua sottoscrizione fino al 31 dicembre 2026, eventualmente prorogabile per ulteriori 24 mesi finalizzati a garantire il monitoraggio o l'attuazione in relazione ad eventuali proroghe concesse dall'Agenzia Nazionale per la Cybersicurezza. L'intervento

dovrà essere attuato da ARES nel rispetto dei rispettivi cronoprogrammi e in ogni caso risultare conclusi, funzionanti e in uso entro la data di conclusione della Convenzione.

Articolo 5

SOGGETTI RESPONSABILI DEL FINANZIAMENTO E DELL'ATTUAZIONE

1. I soggetti responsabili per il coordinamento generale dell'intervento sono il Direttore generale dell'innovazione e Sicurezza IT e il Direttore generale dell'Ares, che identificano Direttore del Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica dell'ARES quale responsabile dell'attuazione e il Direttore del Servizio Sistemi della Direzione generale dell'innovazione e sicurezza IT quale responsabile del finanziamento e monitoraggio nei confronti dell'Agenzia Nazionale per la Cybersicurezza;
2. Il responsabile del finanziamento, monitoraggio e della cura dei rapporti con l'Agenzia Nazionale per la Cybersicurezza è il Direttore del Servizio Sistemi della Direzione generale dell'innovazione e sicurezza IT che avrà il compito di:
    a. Provvedere al trasferimento delle somme all'Ares concesse per l'attuazione dell'intervento dall'Agenzia Nazionale per la Cybersicurezza;
    b. Cura il monitoraggio dell'intervento e la trasmissione delle informazioni di rendicontazione presentate dall'Ares Sardegna, secondo gli schemi dall'Agenzia Nazionale per la Cybersicurezza, per l'invio periodico;
    c. Cura i rapporti e informa dell'andamento progettuale l'Agenzia Nazionale per la Cybersicurezza
3. Il responsabile dell'attuazione tecnica è identificato nel Direttore del Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica dell'ARES della Direzione generale dell'Ares che avrà il compito di:
    a. Attuare tecnicamente l'intervento come stabilito dalla proposta progettuale inoltrata all'Agenzia Nazionale per la Cybersicurezza relativo al "Consolidamento della strategia di cybersecurity – Attuatore responsabile ARES Sardegna"
    b. Rispettare tutte le regole tecniche indicate nell'attuazione del progetto, indicatori e cronogrammi, redigere il monitoraggio periodico ed informare tempestivamente il Servizio Sistemi che notificherà Agenzia Nazionale per la Cybersicurezza di eventuali scostamenti e

rimedi attuativi utilizzando report, modelli e qualsivoglia documentazione indicata dall'Agenzia Nazionale per la cybersicurezza;

c. Svolgere tutte le azioni per la corretta tenuta del fascicolo di progetto con la relativa documentazione in appalto;

d. Nominare tutte le figure professionali tecniche, amministrative e amministrative-contabili per curare l'intervento nelle fasi di esecuzione e collaudo

4. Qualsiasi modifica alla Convenzione, derivante dalle varie circostanze normate dalla stessa, dovrà essere preventivamente annunciata e discussa con i responsabili di cui al comma 1, al fine di condividere le reciproche posizioni, valutare gli impatti e rilevare eventuali criticità.

5. Le strutture Regionali e di Ares potranno operare sia in modalità sincrona (riunione collegiale in presenza o tele/video-conferenza) che in modalità asincrona (tramite scambi di note, email, PEC, etc.). I componenti potranno nominare propri delegati per ogni seduta o attività.

Articolo 6

MODALITÀ DI ATTUAZIONE

1. Il Beneficiario provvederà all'attuazione delle attività dell'intervento allegato alla presente Convenzione, al fine di concorrere al raggiungimento degli obiettivi strategici, tecnici e finanziari previsti;

2. Il Beneficiario è tenuto a segnalare tempestivamente e con congruo anticipo alla Regione il manifestarsi di criticità o anche solo di rischi sopraggiunti che possano determinare potenziali ritardi nel cronoprogramma, rappresentando contestualmente le contromisure messe in campo per scongiurare o recuperare il ritardo tecnico previsto. Qualora si renda necessario apportare rimodulazioni a quanto pianificato, il Beneficiario è tenuto a presentare, anticipatamente rispetto all'eventuale manifestarsi di ritardi, apposita proposta di aggiornamento dei cronoprogrammi approvati.

Articolo 7

UTILIZZO DELLE RISORSE E SPESE AMMISSIBILI

1. Il Beneficiario è tenuto ad utilizzare le somme concesse solo ed esclusivamente per la realizzazione dell'intervento allegato, nel rispetto della normativa nazionale e regionale in materia di appalti pubblici e

di ammissibilità delle spese per le attività indicate nell'intervento approvato dall'Agenzia Nazionale per la Cybersicurezza.

2. Ogni eventuale spesa eccedente l'importo autorizzato o risultata non ammissibile a seguito delle verifiche effettuate in fase di controllo, rimarrà a totale carico del Beneficiario che provvederà alla relativa copertura con propri mezzi finanziari e nel rispetto della normativa vigente.

Articolo 8

MODALITÀ DI EROGAZIONE DELLE RISORSE

1. Il Beneficiario si impegna a rispettare il cronoprogramma di spesa pluriennale di cui ai successivi articoli. Il Beneficiario, in corso di attuazione della Convenzione e in motivato caso di necessità, avrà facoltà di presentare una proposta di modifica e aggiornamento del cronoprogramma, la cui approvazione sarà sottoposta al competente Direttore del Servizio Sistemi della Direzione generale dell'innovazione e sicurezza IT responsabile del finanziamento.
2. La Regione provvederà a trasferire il finanziamento in favore del Beneficiario secondo le seguenti modalità.

   Per ciascuna annualità oggetto del cronoprogramma di cui al comma 1 sarà erogata:

   a) una tranche in anticipazione pari al 100% della previsione di spesa per la prima annualità, (la prima tranche sarà erogata a seguito della stipula della Convenzione, una volta perfezionato il relativo impegno di spesa registrato contabilmente);

   b) una tranche in anticipazione pari al 50% della previsione di spesa per annualità successiva, su richiesta del Beneficiario;

   c) una tranche di saldo a conclusione delle attività e delle relative rendicontazioni e monitoraggi.
3. L'erogazione delle risorse sarà in ogni caso vincolata al rispetto del cronoprogramma procedurale e finanziario, eventualmente aggiornato solo dietro specifica autorizzazione della Regione.
4. Le somme erogate costituiscono entrate con destinazione specifica. Come precisato dei precedenti articoli, ai fini del finanziamento si terrà conto delle sole spese effettivamente sostenute dal Beneficiario e riconosciute ammissibili e certificabili in sede di verifica.
5. La Regione si riserva il diritto di esercitare, in ogni momento, con le modalità che riterrà più opportune, verifiche e controlli al fine di accertare la puntuale ed esatta rispondenza di quanto dichiarato dal Beneficiario a giustificazione delle richieste di trasferimento delle singole rate di finanziamento.

Articolo 9

IMPEGNI E OBBLIGHI DEL BENEFICIARIO

1. Il Beneficiario è obbligato al rispetto di quanto previsto nel presente atto ed in generale di tutta la normativa comunitaria, nazionale e regionale, nonché di quanto specificato negli adempimenti previsti dall'Agenzia Nazionale della Cybersicurezza.
2. Il Beneficiario si obbliga a garantire la generazione di un Codice Unico di Progetto (CUP) in relazione a ciascuna operazione.

Articolo 10

OBBLIGHI DI TRACCIABILITÀ DEI FLUSSI FINANZIARI E OBBLIGHI PREVISTI DAL DPR 602/73

1. I contratti tra il Beneficiario e i propri appaltatori dovranno essere conformi a quanto previsto dalla L. 13 agosto 2010, n. 136 "Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia" e s.m.i.
2. Il Beneficiario è obbligato a verificare negli atti di liquidazione di propria competenza l'assenza di impedimenti nei confronti del fisco, nei casi disciplinati dal Decreto n. 40 del 18/01/2008 del MEF recante modalità di attuazione dell'art. 48 bis del DPR n. 602 del 29 settembre 1973 in materia di pagamenti delle pubbliche amministrazioni.

Articolo 11

CLAUSOLE DI SALVAGUARDIA

1. Il Beneficiario assume la piena e incondizionata responsabilità – con risorse finanziarie del proprio bilancio – circa la funzionalità di tutte le opere inerenti agli interventi di cui al presente atto. La Regione è totalmente estranea da qualsiasi responsabilità amministrativa, civile e contabile derivante dalla realizzazione dell'intervento. In particolare, il Beneficiario non potrà rivalersi nei confronti della Regione per danni cagionati a terzi o cose derivanti dalla realizzazione degli interventi.

Articolo 12

DEFINIZIONE DELLE CONTROVERSIE

1. Le eventuali controversie che insorgessero tra il Beneficiario e la Regione dovranno essere sottoposte ad un tentativo di risoluzione amministrativa tra i soggetti del comma 1- Articolo 5.
2. Il Beneficiario non potrà, di conseguenza, adire l'Autorità Giudiziaria prima che la Regione abbia emesso la decisione amministrativa o prima che sia decorso inutilmente il termine per provvedervi (90 giorni dalla notifica).
3. Le parti attribuiscono al Foro di Cagliari la competenza esclusiva a conoscere delle eventuali controversie giudiziarie nascenti dalla presente convenzione.

Articolo 13

RICHIAMO ALLE NORME DI LEGGI VIGENTI

1. Per quanto non espressamente previsto, si richiamano tutte le norme di legge vigenti applicabili all'oggetto e alle modalità di attuazione della presente Convenzione, nonché i regolamenti, le direttive e le altre disposizioni nazionali, regionali e comunitarie in materia che, anche se non allegati alla presente Convenzione, ne costituiscono parte integrante e sostanziale.

Articolo 14

RECESSO

1. Le Parti possono recedere dalla presente Convenzione in caso di sopravvenienza di motivi superiori di pubblico interesse;

Articolo 15

COPERTURA FINANZIARIA, CRONOGRAMMA FINANZIARIO E ALLEGATI

1. I finanziamenti di cui alla presente Convenzione troveranno copertura finanziaria a valere sul Bilancio Regionale annualità 2025 e successive, secondo cronoprogramma di spesa allegato, assegnati al Centro di Responsabilità 00.02.01.05 - Servizio Sistemi della Direzione generale dell'innovazione e sicurezza IT:
   - Capitolo SC09.4924 - Descrizione capitolo: Trasferimenti correnti ad ARES per la realizzazione del progetto integrato in attuazione della strategia nazionale di cybersicurezza. Finanziamento OPEX (DPCM 8 luglio 2024). Rif. capitolo di entrata EC211.127
     - PCF.LIV4 - Codice: U.1.04.01.02.000 Descrizione: TRASFERIMENTI CORRENTI A AMMINISTRAZIONI LOCALI
     - Esercizio 2025: 4.979.551,00 €

- Esercizio 2026: 2.775.688,00 €

- Capitolo SC09.4925 - Descrizione capitolo: Trasferimenti in conto capitale ad ARES per la realizzazione del progetto integrato in attuazione della strategia nazionale di cybersicurezza. Finanziamento CAPEX (DPCM 8 luglio 2024). Rif. capitolo di entrata EC421.384
  - PCF.LIV4 - Codice: U.2.03.01.02.000 Descrizione: CONTRIBUTI AGLI INVESTIMENTI A AMMINISTRAZIONI LOCALI
  - Esercizio 2025: 1.865.759,00 €
  - Esercizio 2026: 114.262,00 €

2. Alla presente Convenzione è allegato l'allegato tecnico contenente la descrizione di dettaglio dell'intervento.

Letto, approvato e sottoscritto digitalmente

Per la Regione Autonoma della Sardegna

Il Direttore Generale dell'innovazione e sicurezza IT

Marco Melis

MARCO MELIS
16.12.2025 12:30:41 GMT+00:00

Per il Beneficiario ARES

Il Direttore Generale

Giuseppe Pintor

PINTOR GIUSEPPE
Firmato digitalmente da PINTOR GIUSEPPE
Data: 2025.12.16 17:51:56 +01'00'

SCHEDA INTERVENTO

ATTORE RESPONSABILE

Regione Sardegna - ARES

PIANO DI IMPLEMENTAZIONE

STRATEGIA NAZIONALE DI CYBERSICUREZZA

2022 – 2026

Indice

Data	Versione Scheda	Nome intervento	Cap./Sez. modificati
15/02/2024	1.0	*Consolidamento della strategia di cybersecurity*	*[nel caso di un secondo invio del file, indicare il capitolo o la sezione oggetto di eventuali modifiche]*

1 Anagrafica intervento

ID Misura	*55*
Descrizione misura	Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR.
Attore responsabile misura	DTD, ACN

ID intervento	*55.2*
Titolo intervento	*Consolidamento della strategia di cybersecurity*
Attore responsabile	*Regione Autonoma della Sardegna – Direzione Generale dell'Innovazione e Sicurezza IT*
Tipologia intervento *(in caso di intervento misto selezionare entrambe le tipologie)*	☒Attuazione ☒Gestione *[Nel caso di intervento di sola "gestione", indicare l'eventuale intervento di "attuazione" correlato]*
Stato Intervento	☒Da avviare ☐In corso ☐Concluso
Data inizio	01/03/2024
Data fine	31/12/2026

Risorse finanziarie disponibili	☒SI ☐NO e non sono necessari ulteriori risorse ☐NO e si richiedono risorse a valere sui Fondi della Strategia
Tipologia di risorse finanziarie disponibili *(in caso sia selezionato il SI al punto precedente selezionare ai fini del monitoraggio la natura dei fondi)*	☒PNRR indicare la Misura PNRR di riferimento: Multimisura 1.1 e 1.2 ☐altri fondi EU indicare quali _____ ☐fondi ordinari
Richiesta di fabbisogno sui Fondi della Strategia *(in caso di intervento misto selezionare entrambe le tipologie)*	☒Attuazione € 4.477.070,74 (IVA inclusa) ☒Gestione € 5.258.159,24 (IVA inclusa)

2 Dettaglio intervento

Descrizione intervento	Il progetto ha l'obiettivo di gestire il nuovo e complesso contesto della sicurezza digitale dei servizi sanitari all'interno dell'intero ecosistema tecnologico sanitario regionale e secondo le necessità dei progetti PNRR avviati e in corso di attivazione nel settore della sanità digitale e di assicurare, in questo contesto, la conformità normativa alle norme cogenti di tutti gli Enti sanitari della Regione Sardegna. La proposta progettuale consiste, da una parte, nell'attivazione di nuove tecnologie, servizi e processi e, dall'altra, nel potenziamento e l'integrazione di quanto già esistente e pienamente operativo. 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.
Contributo al raggiungimento delle misure della Strategia	In linea con la strategia della Sanità Digitale a livello nazionale, Regione Sardegna, in collaborazione con ARES Sardegna, ha l'obiettivo di mettere a disposizione di tutte le aziende sia i sistemi di gestione dei **Dossier Sanitari Elettronici** che i singoli verticali offrendoli in modalità SaaS a tutti gli enti sanitari del territorio e garantire l'alimentazione del **Fascicolo Sanitario Elettronico** della Regione Sardegna. Per fare ciò, ha necessità di qualificarsi come **Fornitore SaaS per la Pubblica Amministrazione**, secondo quanto indicato dalla circolare AGID n. 3 del 9 aprile 2018.
Obiettivi e risultati attesi	L'intervento si propone di consolidare la strategia di cybersecurity finora attuata dall'Amministrazione regionale, per il tramite di ARES, e di coinvolgere e sensibilizzare le altre Amministrazioni (8 ASL, 3 AO e AREUS), con l'obiettivo di porre le basi per una governance della sicurezza allargata e rafforzare la resilienza al rischio cyber sul perimetro di competenza. I meccanismi di governance nell'ambito del progetto e applicati anche a tutte le iniziative afferenti al Piano Triennale riguarderanno: • i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip; • l'inquadramento o categorizzazione degli interventi delle Amministrazioni, realizzati mediante la sottoscrizione di uno o più contratti esecutivi afferenti alle iniziative del Piano Strategico, nel framework del Piano Triennale; • l'individuazione, da parte delle Amministrazioni beneficiarie, secondo quanto fornito in documentazione di gara, degli indicatori di digitalizzazione con i quali gli Organismi di coordinamento e controllo analizzeranno e valuteranno gli interventi realizzati dalle Amministrazioni con i contratti afferenti alle Gare strategiche; • la valutazione e l'attuazione della revisione dei servizi previsti dagli Accordi Quadro e/o dei relativi prezzi, per le Gare Strategiche che lo prevedono in documentazione di gara e in funzione dell'evoluzione tecnologica del mercato e/o della normativa applicabile; • l'analisi e la verifica di coerenza, rispetto al perimetro di ogni Gara Strategica, degli interventi delle Amministrazioni realizzati mediante contratti attuativi afferenti alle Gare Strategiche; • le modalità e le tempistiche con cui i fornitori dovranno consegnare i dati relativi ai contratti esecutivi, con particolare riferimento alla fase di chiusura degli Accordi Quadro.

Ulteriori attori coinvolti	**Collaboratori:** - ARES Sardegna **Beneficiari:** - ASL 1 Sassari - ASL 2 Gallura - ASL 3 Nuoro - ASL 4 Ogliastra - ASL 5 Oristano - ASL 6 Medio Campidano - ASL 7 Sulcis - ASL 8 Cagliari - ARNAS G Brotzu + ARNAS Broztsu Businico - AOU CA Policlinico Monserrato - AOU SS Santissima Annunziata - AREUS (2 sedi) -
Eventuali interventi correlati	Intervento di migrazione al cloud PSN e di migrazione al CSP dei dati e servizi critici e ordinari gestiti dagli Enti del S.S.R., a valere sui fondi ottenuti a seguito dell'adesione all'Avviso multimisura 1.1 e 1.2

3 Cronoprogramma

Nella tabella di seguito si richiede di fornire la **macro-pianificazione delle attività** da svolgere per la realizzazione dell'intervento e delle relative **milestone di progetto** da conseguire, intese come output previsti per ogni attività.
Per ogni attività va indicato se è di tipologia "ATTUAZIONE" (con ID sequenziale A1…An) oppure "GESTIONE" (con ID sequenziale G1…Gn)

ID	Attività	Milestone	Data inizio	Data fine
A1	Avvio attività SOC	Definizione piano delle attività per il roll'out progressivo sui vari enti e per tipologia di sistemi (i.e. IT, IoT, MD) e definizione degli use case per il SOC	01/03/2024	30/06/2024
G1	Erogazione servizi SOC	Monitoraggio "real-time" eventi di sicurezza e minacce, Contenimento gestione eventi, Gestione degli Incidenti di Sicurezza	01/07/2024	31/12/2026
A2	Avvio attività Vulnerability management	Definizione del piano di monitoraggio del perimetro e definizione dei criteri di misurazione/classificazione delle potenziali vulnerabilità	01/03/2024	30/06/2024
G2	Erogazione servizi Vulnerability management	Monitoraggio continuo del perimetro, ricerca delle vulnerabilità, categorizzazione del potenziale impatto delle vulnerabilità rilevate, pianificazione delle azioni di rimedio per le vulnerabilità rilevate	01/07/2024	31/12/2026
A3	Avvio attività Threat Intelligence (solo AREUS)	Definizione Linee Guida e pianificazione dell'integrazione col servizio SOC	01/03/2024	30/06/2024
G3	Erogazione servizi Threat Intelligence (solo AREUS)	Monitoraggio dei threat actor, analisi delle common Vulnerability, data feed al servizio SOC, elaborazione di Report e Alert	01/07/2024	31/12/2026

ID	Attività	Milestone	Data inizio	Data fine
A4	Avvio attività Next Generation Firewall (NGFW)	Definizione del perimetro e configurazione dello strumento di NGFW	01/03/2024	31/07/2024
G4	Erogazione servizi Next Generation Firewall (NGFW)	Gestione continuativa delle politiche e delle configurazioni, stima degli impatti e del rischio sulle configurazioni da implementare (o implementate), rilevamento avanzato malware, analisi predittiva della sfruttabilità delle vulnerabilità e gestione degli accessi in modalità multifattore per le utenze privilegiate	01/08/2024	31/12/2026
A5	Avvio attività Web Application Firewall (WAF) (solo AREUS)	Definizione del perimetro, configurazione dello strumento di WAF e definizione del piano di automazione	01/03/2024	31/07/2024
G5	Erogazione servizi Web Application Firewall (WAF) (solo AREUS)	Behavioral Analytics, analisi e discriminazione del traffico web lecito e malevolo	01/08/2024	31/12/2026
G6	Formazione e Security Awareness	Definizione del programma di training, presa in carico del servizio, configurazione piattaforma di e-learning e coinvolgimento del personale tecnico dell'Amministrazione, erogazione della formazione e creazione reportistica	01/03/2024	30/06/2024
G7	Migrazione sicura in cloud	"Analisi e Discovery" del livello di sicurezza dei servizi, progettazione "Security by design", configurazione degli apparati di sicurezza, della "landing zone e definizione dei security test	01/03/2024	31/12/2026
G8	Governance	Guida e condivisione avanzamenti attività progettuali	01/03/2024	31/12/2026

4 Meccanismi di verifica e monitoraggio

Nella tabella di seguito si richiede di **indicare i meccanismi** per la verifica dell'effettivo e corretto conseguimento delle milestone riportate nella sezione 3. Cronoprogramma.

ID Attività / Milestone	**Meccanismi di verifica del raggiungimento della milestone** *(documenti quali report e verbali, link, pagine web etc.)*
A1	- Piano delle attività per il roll-out - Elenco use case implementati
G1	- Report attività di monitoraggio
A2	- Piano Attività di Vulnerability Management
G2	- Report periodici su vulnerabilità rilevate e azioni suggerite
A3	- Tempi e modalità di reporting
G3	- Report e Alert dalle attività di threat intelligence
A4	- NGFW configurati
G4	- Report periodici sull'attività di sicurezza perimetrale rilevati dal NGFW
A5	- NGFW configurati

ID Attività / Milestone	**Meccanismi di verifica del raggiungimento della milestone** *(documenti quali report e verbali, link, pagine web etc.)*
G5	- Report periodici sull'attività di sicurezza applicativa rilevati dal WAF
G6	- Iniziative di awareness completate (e.g. corsi di formazione, simulazioni, etc)
G7	- Linee guida "Security by design"
G8	- Numero di Verbali dei Comitati prodotti durante il periodo di riferimento

5 Pianificazione finanziaria

In questa sezione si richiede di **indicare il budget complessivo necessario per la realizzazione dell'intervento, e il dettaglio** delle **risorse finanziarie disponibili,** già assegnate all'Amministrazione (provenienti da altri fondi, trasferimenti, etc.) e delle **risorse che l'Amministrazione intende richiedere all'ACN** attraverso la compilazione e la trasmissione della presente scheda. Devono essere indicati **gli importi richiesti in relazione ai singoli fondi disponibili** a seconda della tipologia di attività che verrà svolta.
(Nella tabella indicare la cifra per intero. Es. 2.800.000,00 €)

Tipologia Budget Intervento	Totale intervento
Budget già disponibile (A): *risorse già assegnate all'Amministrazione, anche non ancora incassate. In tal caso bisogna specificare la fonte delle risorse già disponibili (PNRR, Bilancio dello Stato, Altro)*	€ 1.838.769,36
Fabbisogno finanziario richiesto su fondo Attuazione - CAPEX (B): *risorse a valere sul Fondo di Attuazione istituito dalla Legge di Bilancio 2023 che si intende richiedere per la realizzazione dell'intervento (in aggiunta a quelle già disponibili se presenti)*	€ 4.477.070,74
Fabbisogno finanziario richiesto su fondo Gestione - OPEX (C): *risorse a valere sul Fondo di Gestione istituito dalla Legge di Bilancio 2023 che si intende richiedere per la realizzazione dell'intervento (in aggiunta a quelle già disponibili se presenti)*	€ 5.258.159,24
Budget complessivo (A+B+C): *risorse necessarie alla realizzazione dell'intervento*	€ 11.573.999,34

Ai fini del monitoraggio progettuale e finanziario delle attività da parte dell'ACN, si richiede di fornire nella tabella di seguito una pianificazione finanziaria pluriennale degli importi sopra riportati.
(Nella tabella indicare la cifra per intero. Es. 2.800.000,00 €)

Tipologia Budget Intervento	Pianificazione finanziaria pluriennale			
	2024	2025	2026	Totale Intervento
Budget già disponibile (A)	€ 1.838.769,36	€ 0	€ 0	€ 1.838.769,36
Fonte budget già disponibile (A)	☒PNRR ☐Bilancio dello Stato ☐Altro	☐PNRR ☐Bilancio dello Stato ☐Altro	☐PNRR ☐Bilancio dello Stato ☐Altro	
Se "Altro" specificare (ad es. fondi UE)				
Fabbisogno finanziario richiesto su fondo Attuazione (B)	€ 1.985.234,83	€ 1.349.223,76	€ 1.142.612,15	€ 4.477.070,74
Fabbisogno finanziario richiesto su fondo Gestione (C)	€ 1.405.816,13	€ 2.105.019,83	€ 1.747.323,28	€ 5.258.159,24
Budget complessivo (A+B+C)	€ 5.229.820,32	€ 3.454.243,59	€ 2.889.935,43	€ 11.573.999,34

6 Metriche impattate

In questa sezione si richiede di compilare i **target** relativi ai soli **indicatori** della misura che risultano impattati dall'attuazione dell'intervento in oggetto. Per ogni indicatore riportare le **quantità target prefissate per ciascun anno** (es. "n. 30 corsi di formazione erogati entro il 31/12/2024").
Per maggiori dettagli sulle **metriche** e sulle **modalità di misurazione** si rimanda alle **linee guida** presenti nel **Manuale Operativo.**

ID	Indicatore	Target 2024	Target 2025	Target 2026
55a	Numero di iniziative volte a promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, portate a termine nel periodo di riferimento.	N/A	N/A	N/A
55b	Numero di iniziative volte a rafforzare la cybersicurezza nella Pubblica Amministrazione, portate a termine nel periodo di riferimento.	- 10 coppie di FW implementate - SOC implementato sui sistemi IT su 8 enti	- SOC implementato sui sistemi IT su tutti gli enti - SOC implementato sui sistemi IoT su 8 enti - Completata attività di Awareness	- SOC implementato sui sistemi IoT su tutti gli enti
55c	Ammontare dei fondi ottenuti e utilizzati per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, nel periodo di riferimento.	N/A	N/A	N/A
55d	Ammontare dei fondi PNRR ottenuti e utilizzati per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, nel periodo di riferimento.	N/A	N/A	N/A

ID	Indicatore	Target 2024	Target 2025	Target 2026
55e	Ammontare dei fondi ottenuti e utilizzati per rafforzare la cybersicurezza nella Pubblica Amministrazione, nel periodo di riferimento.	0	0	0
55f	Ammontare dei fondi PNRR ottenuti e utilizzati per rafforzare la cybersicurezza nella Pubblica Amministrazione, nel periodo di riferimento.	€ 1.838.769,36 di € 17.049.563,44 totali	0	0
55g	Numero di enti e distribuzione territoriale (a livello di Regione) che hanno ottenuto e utilizzato fondi per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, nel periodo di riferimento.	*N/A*	*N/A*	*N/A*
55h	Numero di enti e distribuzione territoriale (a livello di Regione) che hanno ottenuto e utilizzato fondi per rafforzare la cybersicurezza nella Pubblica Amministrazione, nel periodo di riferimento.	*N/A*	*N/A*	*N/A*

(*) ipotesi di onboarding di tutti gli enti ad eccezione di quelli del Gruppo 5

7 Approvazione intervento

Si chiede di firmare digitalmente il presente documento:

Data	Attore responsabile	Responsabile ACN
15/02/2024	***Firma Digitale***	***Firma Digitale***