SEZIONE PRIMA

Deliberazioni della Giunta regionale

DELIBERAZIONE DELLA GIUNTA REGIONALE 7 ottobre 2025, n. 1480

Approvazione del Modello Strategico della cybersecurity regionale in attuazione della disciplina nazionale ed europea (Direttiva UE 2022/2555, L. n. 90/2024 e D. Lgs. n. 138/2024).

LA GIUNTA REGIONALE

VISTI:

- ✓ gli artt. 4, 5 e 6 della L.R. n.7 del 4 febbraio 1997;
- ✓ la Deliberazione della Giunta Regionale n. 3261 del 28 luglio 1998;
- ✓ gli art. 4 e 16 del D. Lgs. n. 165 del 30 marzo 2001 e ss.mm.ii.;
- ✓ gli artt. 43 e 44 dello Statuto della Regione Puglia;
- ✓ il Decreto del Presidente della Giunta Regionale n.22 del 22 gennaio 2021 e ss.mm.ii. recante l'Atto di Alta Organizzazione "*M.A.I.A. 2.0*";
- ✓ il Regolamento interno di questa Giunta;

VISTO il documento istruttorio del Dipartimento per la Transizione Digitale - Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche, concernente l'argomento in oggetto, e la conseguente proposta del Presidente della Giunta regionale;

PRESO ATTO

a) delle sottoscrizioni dei responsabili della struttura amministrativa competente, ai fini dell'attestazione della regolarità amministrativa dell'attività istruttoria e della proposta, ai sensi dell'art.6, co.8 delle Linee guida sul "*Sistema dei controlli interni della Regione Puglia*", adottate con D.G.R. n.1374 del 23 luglio 2019;

b) della dichiarazione del Direttore del Dipartimento in merito a eventuali osservazioni sulla proposta di deliberazione, ai sensi degli artt. 18 e 20 del Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii;

con voto favorevole espresso all'unanimità dei presenti e per le motivazioni contenute nel documento istruttorio che è parte integrante e sostanziale della presente deliberazione;

DELIBERA

1. di condividere quanto esposto in narrativa che qui si intende integralmente riportato;
2. di approvare il Modello di governance e strategia di cybersecurity dell'ecosistema regionale pugliese nonché il Modello organizzativo di cybersecurity di Regione Puglia - Allegato A al presente provvedimento per farne parte integrante e sostanziale;
3. di approvare la matrice di assegnazione delle responsabilità (cd. *matrice RACI*) di cybersecurity di Regione Puglia - Allegato B al presente provvedimento per farne parte integrante e sostanziale;
4. di prendere atto della matrice di assegnazione delle responsabilità (cd. *matrice RACI*) di cybersecurity di InnovaPuglia S.p.A. - Allegato C al presente provvedimento per farne parte integrante e sostanziale;
5. di disporre la pubblicazione del presente provvedimento, ad eccezione degli allegati A, B e C, sul Bollettino Ufficiale della Regione Puglia e nella Sezione "Amministrazione Trasparente", sottosezione "Provvedimenti" del portale regionale;

6. di notificare il presente provvedimento, a cura della Struttura proponente, per gli eventuali adempimenti consequenziali, a tutti i soggetti interessati e, qualora previsto, all'Agenzia per la Cybersicurezza Nazionale.

Il Segretario Generale della Giunta
NICOLA PALADINO

Il Presidente della Giunta
MICHELE EMILIANO

DOCUMENTO ISTRUTTORIO

OGGETTO: Approvazione del Modello Strategico della cybersecurity regionale in attuazione della disciplina nazionale ed europea (Direttiva UE 2022/2555, L. n. 90/2024 e D. Lgs. n. 138/2024).

Visti:

- Il D. Lgs. n. 82 del 7 marzo 2005, "*Codice dell'amministrazione digitale*";
- il Regolamento UE 2016/679 relativo alla "*Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", che abroga la Direttiva 95/46/CE (Reg. generale sulla protezione dei dati) e il D. Lgs. n. 196/2003 ("*Codice Privacy*");
- la Legge n. 241 del 7 agosto 1990 e ss.mm.ii., "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- la D.G.R. n. 1974 del 7 dicembre 2020, con la quale la Giunta regionale ha adottato la Macrostruttura del Modello organizzativo denominato "*MAIA 2.0*", quale atto di alta organizzazione che disciplina l'organizzazione amministrativa della Presidenza e della Giunta Regionale;
- il D.P.G.R. n. 22 del 22 gennaio 2021 pubblicato sul BURP n. 15 del 28.01.2021, che ha emanato l'atto di alta organizzazione relativo alle strutture della Presidenza e della Giunta Regionale "*Adozione Atto di Alta Organizzazione - Modello organizzativo MAIA 2.0*" e successivamente modificato e integrato con i decreti del Presidente della Giunta Regionale n. 45 del 10 febbraio 2021 e n. 380 del 15 settembre 2022;
- il D.P.G.R. n. 430 del 27 novembre 2020, con il quale è stato conferito l'incarico di Consigliere del Presidente per l'informatizzazione, l'e-government ed il social government;
- la D.G.R. n. 282 del 14 marzo 2024, avente oggetto "Modifiche ed integrazioni alla deliberazione di *Giunta Regionale n. 1974 del 7 dicembre 2020 e ss.mm.ii. – Nuove istituzioni, rimodulazioni e soppressioni di strutture dirigenziali*", con cui la Giunta Regionale ha disposto l'istituzione del Dipartimento per la Transizione Digitale contenente, al suo interno, la Sezione Innovazione, Dati e Servizi digitali e la Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche, in tal modo avviando un processo di rafforzamento del percorso di trasformazione digitale, con l'obiettivo ultimo di offrire servizi sempre più efficienti e accessibili alla cittadinanza, alle imprese e a tutti i portatori di interessi del territorio anche sotto il profilo della sicurezza dei dati e dei sistemi;
- la D.G.R. n. 477 del 15 aprile 2024, con cui la Giunta Regionale ha aggiornato le funzioni delle Sezioni del Dipartimento in attuazione della già citata D.G.R. n. 282/2024, dettagliando la declaratoria delle funzioni della nuova struttura dipartimentale Dipartimento per la Transizione Digitale ed in particolare della Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche a cui sono attribuite, tra le altre, le seguenti competenze:
    - definisce e coordina la realizzazione dei piani di sicurezza delle infrastrutture digitali regionali;
    - coordina l'adozione degli standard e framework di sicurezza europea e nazionale in Regione Puglia, anche mediante direttive ed audit presso i dipartimenti, le Agenzie Regionali e le Aziende Sanitarie;

- coordina il CSIRT, il SOC e centro operativo sulla cybersecurity per la Regione Puglia in sinergia con gli enti nazionali;
- definisce e coordina le misure di sicurezza sulle postazioni, sulla rete intranet e Internet delle sedi e sui sistemi di condivisione e di lavoro da remoto;

- la D.G.R. n. 1872 del 23 dicembre 2024, con cui la Giunta Regionale ha conferito l'incarico di Direttore di Dipartimento per la Transizione Digitale all'Ing. Cosimo Elefante;
- la D.G.R. n. 51 del 29 gennaio 2025, con cui la Giunta Regionale ha nominato Responsabile per la Transizione al Digitale [RTD] della Regione Puglia il Direttore pro-tempore del Dipartimento per la Transizione Digitale, Ing. Cosimo Elefante;
- la D.G.R. n. 248 del 4 marzo 2025, con cui la Giunta Regionale ha conferito l'incarico di direzione della Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche, afferente al Dipartimento per la Transizione Digitale, alla dirigente dott.ssa Angela Guerra;
- la D.G.R. n. 1219 del 22 luglio 2021, avente ad oggetto "*Riorganizzazione digitale dell'amministrazione regionale - Linee di indirizzo*", con cui la Giunta Regionale ha stabilito di avviare un percorso di razionalizzazione ed omogeneizzazione dei sistemi informativi regionali;
- la D.G.R. n. 791 del 30 giugno 2022 con cui la Giunta Regionale ha adottato il "*Piano triennale di Riorganizzazione Digitale della Regione Puglia 2022-2024*" e ss.mm.ii.;
- la D.G.R. n. 663 del 16 maggio 2023, avente ad oggetto "*Linee di indirizzo per le infrastrutture tecnologiche digitali regionali*";
- la D.G.R. n. 1760 del 30 novembre 2023, avente ad oggetto "*P.R. Puglia 2021-2027-Azione 1.8-Sub Azione 1.8.2 "Interventi per la transizione digitale della PA" e Fondo Sanitario Regionale - Atto di indirizzo per l'avvio degli interventi. Variazione al bilancio di previsione 2023 e pluriennale 2023-2025 ai sensi dell'art. 51 comma 2 del D. Lgs n. 118/2011 e ss.mm.ii.*";
- la Determinazione Dirigenziale del Dirigente del Servizio Tecnico e Transizione Digitale n. 7 del 7 dicembre 2023, avente ad oggetto "*CUP: B31C23000820006 - PR Puglia FESR - FSE + 2021-2027 – Azione 1.8 – Sub Azione 1.8.2 "Interventi per la transizione digitale della PA" – PRD 2022-2024 e ss.mm.ii. - Piano di Potenziamento della Cybersecurity della Regione Puglia. Accertamento in entrata, impegno di spesa a valere sul Bilancio Vincolato e Autonomo. Approvazione PO e affidamento in house InnovaPuglia Spa*".
- la Legge n. 90 del 28 giugno 2024, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*";
- il D.Lgs. n. 138 del 4 settembre 2024, di "*Recepimento della direttiva (UE) 2022/2555* [cd. NIS2]*, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*";
- la D.G.R. n. 1793 del 16 dicembre 2024, avente ad oggetto "*Legge 28 giugno 2024, n. 90 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", articolo 8 - D. Lgs. 4 settembre 2024, n. 138 di recepimento della Direttiva (UE) 2022/2555, art. 7 - Indirizzi sulla cybersecurity regionale, individuazione della struttura e del referente per la cybersicurezza, designazione Punto di Contatto soggetto NIS*";

- la Determinazione Dirigenziale del Dirigente del Servizio Tecnico e Transizione digitale n. 8 del 30 dicembre 2024, avente ad oggetto "*Approvazione documentazione CSIRT Regione Puglia e indicazioni operative – Seguito DGR n. 1793 del 16.12.2024*";
- la Determinazione del Direttore generale dell'ACN n. 136430 del 12 aprile 2025, ha individuato la Regione Puglia quale *soggetto importante* ai sensi del D.Lgs. 138/2024;
- la Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale n. 164179 del 14 aprile 2025 "*di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo*";
- la Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale n. 283727 del 22 luglio 2025 "*di cui all'articolo 7, comma 6, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, recante termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale*";
- la D.G.R. n. 1258 dell'11 agosto 2025, avente ad oggetto "*D. Lgs. n. 138 del 4 settembre 2024, di recepimento della Direttiva (UE) 2022/2555, art. 7, comma 4, - Individuazione dei componenti degli organi di amministrazione e direttivi e designazione del Sostituto Punto di Contatto soggetto NIS. Scioglimento dell'Osservatorio Regionale sulle attività non autorizzate nei sistemi informativi*".

Viste altresì:

- la D.G.R. n. 1466 del 15 settembre 2021, recante l'approvazione della Strategia regionale per la parità di genere, denominata "*Agenda di Genere*";
- la D.G.R. n. 1295 del 26 settembre 2024, recante "*Valutazione di Impatto di Genere (VIG). Approvazione indirizzi metodologico-operativi e avvio fase strutturale*";

Premesso che:

- con la D.G.R. n. 791 del 30 giugno 2022, la Giunta Regionale ha adottato il "*Piano triennale di Riorganizzazione Digitale della Regione Puglia 2022-2024*" e ha stabilito, tra l'altro, di:
    - "*affidare la governance del Piano Triennale di Riorganizzazione Digitale al RTD, coinvolgendo allo scopo tutti i Dirigenti delle strutture interessate e la società in house InnovaPuglia S.p.A.;*
    - *dare atto che il Piano Triennale di Riorganizzazione Digitale sarà finanziato con fondi a valere sulle risorse regionali, nazionali ed europee che sono stati o saranno individuati per ogni singolo intervento/progetto, impegnando le strutture regionali competenti, in raccordo con il RTD, sulla base delle proposte di dettaglio di ciascun intervento, a provvedere alla formulazione degli atti necessari ad avviare e garantire la piena e puntuale attuazione della strategia regionale;*

- *disporre che per qualsiasi intervento di digitalizzazione, acquisizione o evoluzione di sistemi informativi o infrastrutture tecnologiche, le strutture regionali dovranno coordinarsi e cooperare ex ante con l'Ufficio Responsabile per la Transizione al Digitale, preposto a fornire i relativi pareri in merito agli interventi e alle acquisizioni proposti, al fine di accertarne la coerenza con le strategie ICT adottate con il Piano Triennale di Riorganizzazione Digitale*";

- con il Piano triennale di Riorganizzazione Digitale 2022-2024 [PRD] e relativi aggiornamenti 2023 - 2025 e 2024 - 2026, approvati rispettivamente con D.G.R. n. 791/2022, D.G.R. n. 1094/2023 e D.G.R. n. 1646/2024, l'Amministrazione regionale ha delineato il proprio quadro strategico per la transizione al digitale, prevedendo una serie di obiettivi realizzativi [OR] ed ulteriori strumenti e meccanismi di raccordo con le strutture regionali;
- tra gli interventi di cui al citato PRD 2022-2024 e successivi aggiornamenti, l'Amministrazione ha, tra gli altri, individuato, nell'ambito delle attività dell'OR_20, quello relativo al "*Cyber Security e Networking Infrastructures*", la cui necessità è legata alla rapida evoluzione tecnologica ed al massiccio ricorso ai processi di digitalizzazione, che hanno comportato una crescita ed un'evoluzione del panorama delle minacce informatiche, sempre più frequenti, articolate e sofisticate;
- l'intervento indicato prevede la realizzazione di un Piano Strategico della Cybersecurity, finalizzato alla definizione delle linee di indirizzo regionali in ambito cybersecurity, e ad individuare una serie di iniziative, da attuare nel medio-lungo termine, per rafforzare in modo significativo le capacità della Regione e degli Enti coinvolti, contribuendo così a garantire un ambiente digitale più sicuro e resiliente;

Considerato che:

- con Determinazione Dirigenziale del Dirigente del Servizio Tecnico e Transizione Digitale n. 7 del 7 dicembre 2023, è stato approvato il Piano Operativo, denominato "*Piano di Potenziamento della Cybersecurity della Regione Puglia*", per un importo complessivo di € 11.480.800,00 (di cui € 5.844.200,00 a valere sulle risorse del P.R. Puglia FESR FSE+ 2021-2027 Sub-Azione 1.8.2 e € 5.636.600,00, a valere sul Fondo Sanitario del Bilancio Autonomo), affidando ad InnovaPuglia S.p.A. l'esecuzione del suddetto Piano Operativo ai sensi dell'art. 7, commi 2 e 3 del D. Lgs. n. 36/2023, avente i seguenti *Driver*:
    - Governo omogeneo della cybersecurity;
    - Partecipazione collaborativa;
    - Sistema di Gestione degli Incidenti e delle Crisi;
    - Gestione continua delle minacce e delle esposizioni al rischio;
    - Cultura della cyber sicurezza;
- con la L. n. 90 del 28 giugno 2024, all'art. 8 comma 1, è stato previsto l'obbligo per l'Amministrazione regionale di individuare "*una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede:*
    - *allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;*
    - *alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;*

- *alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;*
- *alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;*
- *alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);*
- *alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;*
- *al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza*";

- con D.G.R. n. 1793 del 16 dicembre 2024, la Giunta regionale ha inteso fornire indirizzi sulla cybersecurity regionale, ed in particolare:
  - è stata individuata "*nell'Ufficio per la Transizione al Digitale, la Struttura presso la quale opera il referente per la cybersicurezza*" ed è stato individuato "*il referente per la Cybersicurezza nel Responsabile per la Transizione al Digitale di Regione Puglia*";
  - ha disposto di "*affidare al Responsabile della Transizione al Digitale di Regione Puglia, in coerenza con la complessiva strategia regionale sull'ICT, il coordinamento, la governance e la definizione di tutti gli indirizzi strategici in ambito di cybersecurity*";
  - ha disposto "*di designare, altresì, il Responsabile per la Transizione al Digitale di Regione Puglia quale Punto di Contatto previsto dall'art. 7 del D. Lgs. n. 138/2024 per tutte le attività ad esso inerenti, in particolare le attività indicate dall'articolo 4 della Determinazione del Direttore Generale di ACN prot. n. 38565 del 26.11.2024";*
- la D.G.R. n. 1258 dell'11 agosto 2025, in attuazione del D. Lgs. n. 138 del 4 settembre 2024, di recepimento della Direttiva (UE) 2022/2555, art. 7, comma 4, ha disposto:
  - di designare *"la Dott.ssa Angela Guerra, quale Dirigente della Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche, come sostituto Punto di Contatto previsto dall'art. 7 del D. Lgs. n. 138/2024 per tutte le attività ad esso inerenti, e in particolare per le attività indicate dall'art. 5 della Determinazione del Direttore generale dell'ACN n. 283727 del 22 luglio 2025";*
  - di demandare "*all'Ing. Cosimo Elefante, Direttore del Dipartimento per la Transizione Digitale, in collaborazione con la Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche e InnovaPuglia S.p.A., il coordinamento, la pianificazione, la progettazione e l'implementazione di tutte le politiche di sicurezza informatica ai sensi dell'art. 23 del D.Lgs. n. 138/2024, anche con il supporto delle altre Strutture regionali attivamente coinvolte, ai fini di una piena implementazione delle misure di gestione dei rischi per la cybersecurity, inclusa la previsione di specifiche attività di formazione e la destinazione di budget dedicati*";
- il rafforzamento delle capacità di cybersecurity del sistema regionale è una priorità per Regione Puglia, quale strumento decisivo per rispondere efficacemente alle crescenti sfide del mondo digitale e dare esecuzione, al contempo, alle strategie nazionali ed europee.

Rilevato che:

- la D.G.R. n. 663 del 16 maggio 2023, avente ad oggetto "*Linee di indirizzo per le infrastrutture tecnologiche digitali regionali*" ha stabilito di "*affidare al RTD della Regione Puglia, in coerenza con la complessiva strategia regionale sull'ICT* [...] *il coordinamento, la governance e la definizione degli ulteriori indirizzi strategici del Polo di Conservazione, del Data Center e dello CSIRT Puglia*";
- la D.G.R. n. 1793 del 16 dicembre 2024, ha disposto:
    - che "*il Computer Security Incident Response Team (CSIRT) Puglia, già interessato dalla ridefinizione degli asset regionali prevista dalla D.G.R. n. 663/2023, sia convertito in CSIRT regionale con la denominazione di "CSIRT della Regione Puglia", mantenendo le finalità e le attività attualmente previste*";
    - che "*le modalità operative ed i servizi erogati dal CSIRT saranno oggetto di progettazione esecutiva e verranno ulteriormente dettagliati nell'ambito del contratto di servizio con InnovaPuglia S.p.A., cui resta affidata l'erogazione dei servizi, lasciando il coordinamento e la governance dell'asset nella competenza di Regione Puglia, in coerenza con la disposizione di cui al precedente punto 1, per il tramite del RTD regionale*";
    - "*di demandare, inoltre, al RTD regionale, nella qualità di cui al punto precedente, tutte le attività e gli eventuali atti necessari e conseguenti, anche per l'eventuale ampliamento e ridefinizione della constituency di riferimento del CSIRT Regione Puglia e delle relative modalità di adesione*";
- con Determinazione Dirigenziale del Dirigente del Servizio Tecnico e Transizione digitale n. 8 del 30 dicembre 2024, sono stati approvati i documenti "*Mandato e Constituency*", "*Modello di Governance*", "*Struttura Organizzativa*" e "*Catalogo Servizi*" dello CSIRT della Regione Puglia;
- con nota n. 646933 del 31 dicembre 2024, avente ad oggetto "*PIANO NAZIONALE DI RIPRESA E RESILIENZA Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 - Avviso n. 6/2023 dell'Agenzia per la Cybersicurezza Nazionale "Attivazione e potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" – Progetto: "Rafforzamento CSIRT Regionale Conseguimento M&T - ID Progetto 5_WP7_A6_Regione Puglia/CUP B34F23009890006 – Avviso n. 6/2023*", il RTD di Regione Puglia ha:
    - trasmesso all'Agenzia per la Cybersicurezza Nazionale la definizione della struttura organizzativa, dei processi, dei flussi, delle procedure operative, delle linee guida e della constituency del CSIRT della Regione Puglia, al fine di soddisfare i requisiti prescritti da ACN per il livello di maturità base secondo quanto indicato dal framework SIM3 Model adottato da ENISA (European Network and Information Security Agency) per l'accreditamento di un CSIRT;
    - confermato la responsabilità delle attività di governo e indirizzo del CSIRT regionale in capo alla Regione Puglia, delegando InnovaPuglia S.p.A. all'espletamento delle attività operative, come stabilito dalla DGR n. 663/2023 "*Linee di indirizzo per le infrastrutture tecnologiche digitali regionali*";

- con nota del 06 maggio 2025, acquisita al prot. n. 236135/2025, l'Agenzia per la Cybersicurezza Nazionale ha attestato che il modello di governo adottato dal CSIRT della Regione Puglia aveva raggiunto il livello di maturità base secondo il modello SIM3 di ENISA e ha comprovato la conclusione dell'iter volto a garantire la piena operatività dello CSIRT regionale, in coerenza con le Linee Guida per la realizzazione di CSIRT versione 2.0;
- con D.P.C.M. dell'8 luglio 2024 recante "*Ripartizione del Fondo per l'attuazione della strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza*", la Regione Puglia risultava destinataria di parte delle risorse quale Amministrazione individuata come responsabile dal Piano di implementazione dell'attuazione della Strategia nazionale di cybersicurezza 2024-26;
- con Determinazione Dirigenziale della Dirigente della Sezione Innovazione, Dati e Servizi Digitali, n. 11 del 22 settembre 2025, è stato approvato il Piano Operativo per la fornitura dei servizi di cui all' "*Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni*" per la realizzazione di un *Clinical SOC*, che abiliti la protezione reattiva dei *dispositivi IoMT* in uso presso gli Enti sanitari della Regione Puglia;
- in riferimento al già citato Piano di Potenziamento di Cybersecurity della Regione Puglia, relativamente alle attività di rafforzamento delle capacità di gestione degli eventi di sicurezza, attraverso la realizzazione di un *Cybersecurity Defence Center* (composto da CSIRT, SOC, Clinical SOC), InnovaPuglia S.p.A. ha elaborato il Piano dei Fabbisogni e il Piano Operativo nonché sottoscritto il Contratto Esecutivo finalizzato alla erogazione di un servizio di *Security Operation Center* (SOC) per garantire monitoraggio, rilevamento, analisi e risposta agli incidenti di sicurezza informatica.

Rilevato, altresì, che:

- con D.G.R. n. 526 del 16 aprile del 2025, è stato approvato il Protocollo di Intesa tra Regione Puglia e Polizia di Stato per la prevenzione dei crimini informatici sui sistemi informativi critici della Regione Puglia, al fine di garantire la continuità dei servizi digitali regionali e favorire lo scambio informativo e la cooperazione tecnica tra il Centro Operativo Sicurezza Cibernetica - Polizia Postale "*Puglia*" e il Dipartimento per la Transizione Digitale;
- il RTD della Regione Puglia, nel biennio 2024 - 2025 ha promosso le seguenti attività di *cyber awareness* e formazione specifica in materia di normativa di cybersecurity:
    - progetto "*Cybersecurity Posture Assessment e Security Awareness Training per migliorare la consapevolezza degli utenti su temi di cyber security e misura delle capacità acquisite*";
    - organizzazione dell'evento "*Cybersecurity & Data Protection*" del 16 gennaio 2025, al fine di supportare gli Enti sanitari, le Agenzie e Società in-house della Regione Puglia nell'applicazione della normativa NIS2 e della L. 90/2024;
    - organizzazione dell'evento "*SICURA: Regione Puglia e ACN in prima linea nella difesa cibernetica del settore sanitario*" del 20 marzo 2025, al fine di innalzare il livello di cybersicurezza in coordinamento con gli Enti sanitari della Regione Puglia;
    - organizzazione di una simulazione delle fasi di un attacco ransomware nell'ambito del "*2° Incontro della Rete dei Responsabili per la Transizione al Digitale*" pugliesi del 16 luglio 2025, finalizzata a fornire strumenti operativi per il rafforzamento della postura di sicurezza delle amministrazioni pubbliche regionali.

Rilevato infine che:

- con la condivisione e il supporto di consulenza e assistenza tecnica svolta dal Consigliere del Presidente per l'informatizzazione, l'e-government ed il social government, nominato con D.P.G.R. n. 430/2020, al Responsabile per la Transizione al Digitale e Direttore del Dipartimento per la Transizione Digitale, sin dall'inizio dell'attività di predisposizione del Piano di Riorganizzazione Digitale, dell'OR_20 e del Piano di Potenziamento della Cybersecurity della Regione Puglia, sono stati forniti indirizzi comuni, al fine di mantenere uniformi regia e processo di tutti gli interventi d'ambito;
- alla luce del percorso di progressivo rafforzamento della capacità regionale in materia di cybersecurity, illustrato nelle premesse, si è proceduto, nell'ambito delle attività previste dal Piano di Potenziamento della Cybersecurity della Regione Puglia, alla definizione di una matrice di assegnazione delle responsabilità (RACI) e di un modello strategico e organizzativo di cybersecurity;
- La matrice RACI (Responsable, Accountable, Consulted, Informed) costituisce uno strumento metodologico di chiara e immediata lettura, volto a rappresentare in modo sistematico i ruoli, le responsabilità e le interazioni tra i diversi soggetti coinvolti nei processi di governance e di gestione della sicurezza informatica regionale. Tale matrice è stata elaborata, con il supporto tecnico-specialistico di InnovaPuglia S.p.A., nell'ambito delle attività di assessment e compliance previste dal citato Piano di Potenziamento;
- L'analisi condotta ha confermato la piena coerenza del modello organizzativo attualmente vigente — centrato sul Dipartimento per la Transizione Digitale e sulla Sezione Cloud, Cybersecurity e Infrastrutture tecnologiche — come già disposto dalle D.G.R. n. 282/2024, n. 477/2024, n. 1258/2025 nonché rispetto ai requisiti previsti dalla normativa nazionale (L. n. 90/2024 e D.Lgs. n. 138/2024) e dalle linee guida dell'Agenzia per la Cybersicurezza Nazionale;
- la presente deliberazione non introduce modifiche all'assetto organizzativo regionale, ma formalizza e approva la matrice RACI quale strumento di ricognizione, validazione e consolidamento del modello organizzativo regionale di cybersecurity già in essere, rafforzando al contempo l'integrazione e la chiarezza delle responsabilità operative tra Regione Puglia e InnovaPuglia S.p.A.

Alla luce delle risultanze istruttorie, si ritiene necessario:

- approvare, in considerazione dei *deliverable* progettuali trasmessi da InnovaPuglia S.p.A. con nota prot. n. 536037 del 02 ottobre 2025 per quanto previsto dal Piano di Potenziamento della Cybersecurity della Regione Puglia, i seguenti documenti:
    - Modello di governance e strategia di cybersecurity dell'ecosistema regionale pugliese e Modello organizzativo di cybersecurity di Regione Puglia - Allegato A al presente provvedimento per farne parte integrante e sostanziale;
    - matrice di assegnazione delle responsabilità (cd. *matrice RACI*) di cybersecurity di Regione Puglia - Allegato B al presente provvedimento per farne parte integrante e sostanziale;
- prendere atto, in considerazione del ruolo che InnovaPuglia S.p.A. svolge quale fornitore strategico di servizi operativi di cybersecurity nei confronti di Regione Puglia come rappresentato nelle premesse del seguente *deliverable* trasmesso:

- matrice di assegnazione delle responsabilità (cd. *matrice RACI*) di cybersecurity di InnovaPuglia S.p.A. - Allegato C al presente provvedimento per farne parte integrante e sostanziale.

Garanzie di riservatezza

La pubblicazione sul BURP, nonché la pubblicazione sull'Albo o sul sito Istituzionale, salve le garanzie previste dalla legge 241/1990 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 679/2016 in materia di protezione dei dati personali, nonché dal D. Lgs. 196/2003 ss.mm.ii., ed ai sensi del vigente Regolamento regionale 5/2006 per Il trattamento dei dati sensibili e giudiziari, in quanto applicabile. Ai fini della pubblicità legale, il presente provvedimento è stato redatto in modo da evitare la diffusione di dati personali identificativi non necessari ovvero il riferimento alle particolari categorie di dati previste dagli articoli 9 e 10 del succitato Regolamento UE.

Esiti Valutazione di impatto di genere: neutro.

SEZIONE COPERTURA FINANZIARIA DI CUI AL D. LGS. 118/2011 E SS. MM. E II.

La presente deliberazione non comporta implicazioni, dirette e/o indirette, di natura economico-finanziaria e/o patrimoniale e dalla stessa non deriva alcun onere a carico del Bilancio Regionale.

Tutto ciò premesso, al fine di procedere all'approvazione e alla presa d'atto dei modelli previsti dal Piano di Potenziamento della Cybersecurity della Regione Puglia, ai sensi dell'art. 4, comma 4, lett. a), d) della L.R. n. 7/97, si propone alla Giunta Regionale:

1. di condividere quanto esposto in narrativa che qui si intende integralmente riportato;
2. di approvare il Modello di governance e strategia di cybersecurity dell'ecosistema regionale pugliese nonché il Modello organizzativo di cybersecurity di Regione Puglia - Allegato A al presente provvedimento per farne parte integrante e sostanziale;
3. di approvare la matrice di assegnazione delle responsabilità (cd. *matrice RACI*) di cybersecurity di Regione Puglia - Allegato B al presente provvedimento per farne parte integrante e sostanziale;
4. di prendere atto della matrice di assegnazione delle responsabilità (cd. *matrice RACI*) di cybersecurity di InnovaPuglia S.p.A. - Allegato C al presente provvedimento per farne parte integrante e sostanziale;
5. di disporre la pubblicazione del presente provvedimento, ad eccezione degli allegati A, B e C, sul Bollettino Ufficiale della Regione Puglia e nella Sezione "Amministrazione Trasparente", sottosezione "Provvedimenti" del portale regionale;
6. di notificare il presente provvedimento, a cura della Struttura proponente, per gli eventuali adempimenti consequenziali, a tutti i soggetti interessati e, qualora previsto, all'Agenzia per la Cybersicurezza Nazionale.

I sottoscritti attestano la regolarità amministrativa dell'attività istruttoria e della proposta, ai sensi dell'art. 6, co.3, lett. da a) ad e) delle Linee guida sul "*Sistema dei controlli interni nella Regione Puglia*", adottate con D.G.R. n. 1374 del 23 luglio 2019.

L'Istruttore
(Dott. Paolo Giannoccaro)

Paolo Giannoccaro
06.10.2025 14:28:16
GMT+02:00

Il Funzionario E.Q.
(Dott. Nicola Lombardi)

Nicola Lombardi
06.10.2025
14:19:39
GMT+02:00

La Dirigente della Sezione Cloud,
Cybersecurity e Infrastrutture tecnologiche
(Dott.ssa Angela Guerra)

Angela Guerra
06.10.2025
14:21:24
GMT+02:00

Il Direttore del Dipartimento ai sensi degli artt. 18 e 20 del Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii., NON RAVVISA la necessità di esprimere osservazioni alla presente proposta di D.G.R.

Il Direttore del Dipartimento per la Transizione Digitale
(Ing. Cosimo Elefante)

REGIONE PUGLIA
Cosimo Elefante
06.10.2025
15:11:26
GMT+02:00

Il Presidente della Giunta, ai sensi del vigente Regolamento della Giunta Regionale,

PROPONE

alla Giunta Regionale l'adozione del presente atto.

Il Presidente della Giunta Regionale
(Dott. Michele Emiliano)

Michele
Emiliano
06.10.2025
18:47:03
GMT+02:00