

DELIBERAZIONE DELLA GIUNTA REGIONALE 16 dicembre 2024, n. 1793

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 GIUNTA REGIONALE

VISTI:

- ✓ gli artt. 4, 5 e 6 della L.R. 4 febbraio 1997, n.7;
- ✓ la Deliberazione della Giunta Regionale n. 3261 del 28 luglio 1998;
- ✓ gli artt. 4 e 16 del D. Lgs. n. 165 del 30.03.2001 e ss.mm.ii.;
- ✓ gli artt. 43 e 44 dello Statuto della Regione Puglia;
- ✓ il Decreto del Presidente della Giunta Regionale 22 gennaio 2021, n.22 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 Servizio Tecnico e Transizione al Digitale, 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. 23 luglio 2019, n.1374;
- b) della dichiarazione del Capo di Gabinetto, 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 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;
2. di individuare nell’Ufficio per la Transizione al Digitale, la struttura presso la quale opera il referente per la cybersicurezza, ai sensi dell’art. 8 comma 1 della legge n. 90/2024;
3. individuare il referente per la Cybersicurezza nel Responsabile per la Transizione al Digitale di Regione Puglia, ai sensi dell’art. 8, comma 2 della legge n. 90/2024;
4. di demandare al referente individuato la costituzione di un apposito gruppo di lavoro formato da personale di Regione Puglia e di InnovaPuglia S.p.A.;
5. 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;

6. di disporre 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;
7. di disporre 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;
8. 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;
9. di disporre la pubblicazione del presente provvedimento in versione integrale nel Bollettino Ufficiale della Regione Puglia ai sensi della L.R. 18/2023;
10. di disporre la pubblicazione integrale del presente provvedimento sul sito istituzionale della Regione Puglia www.regione.puglia.it nella sezione "Amministrazione Trasparente", sottosezione "Provvedimenti della Giunta Regionale";
11. di notificare il presente provvedimento, a cura della Struttura proponente a tutti i soggetti interessati e, qualora previsto, all'Agenzia per la cybersicurezza nazionale (ACN).

Il Segretario Generale della Giunta

ANNA LOBOSCO

Il Presidente della Giunta

MICHELE EMILIANO

DOCUMENTO ISTRUTTORIO

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.

Visti:

- Il D. Lgs. 7 marzo 2005, n. 82 “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 7 agosto 1990, n. 241 e ss.mm.ii. “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”;
- la D.G.R. 7 dicembre 2020, n. 1974, 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. 22 gennaio 2021, n. 22, 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 del 10 febbraio 2021, n. 45 e del 15 settembre 2022, n. 380;
- il D.P.G.R. 28 settembre 2023, n. 453, con il quale è conferito l’incarico di Direttore Amministrativo del Gabinetto al Dott. Crescenzo Antonio Marino a decorrere dal 01 ottobre 2023;
- il D.P.G.R. 27 novembre 2020 n. 430, 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. 10.05.2021, n. 773 con cui la Giunta Regionale ha individuato il ruolo di Responsabile per la Transizione Digitale (RTD), previsto dall’art. 17 del D. Lgs. 7 marzo 2005, n. 82 in capo al responsabile del Servizio Tecnico e Transizione Digitale della Direzione Amministrativa del Gabinetto, evidenziando la necessità di garantire l’unitarietà di azione strategica nello svolgimento dei compiti previsti dall’art. 17, comma 1, del D. Lgs. n. 82/2005 e ss.mm.ii., nonché quelli previsti dalla Circolare n. 3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione;
- la D.G.R. 22.07.2021, n. 1219 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. 16.05.2023, n. 663 avente ad oggetto “Linee di indirizzo per le infrastrutture tecnologiche digitali regionali”, con cui la Giunta Regionale 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 Legge 28 giugno 2024, n. 90 recante “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici” che, all’art. 8, dispone l’individuazione di un referente per la cybersicurezza e della struttura in cui il referente opera;
- il D. Lgs. 4 settembre 2024, n. 138 di “Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell’Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148”;

Viste altresì:

- la D.G.R. 15.09.2021, n. 1466, che reca l’approvazione della Strategia regionale per la parità di genere, denominata “Agenda di Genere”;
- la D.G.R. 3 luglio 2023, n. 938 recante “D.G.R. n. 302/2022 “*Valutazione di impatto di genere. Sistema di gestione e di monitoraggio*”. Revisione degli allegati”;

Premesso che:

- con la D.G.R. 30.06.2022, n. 791, 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;

- il suddetto Piano Strategico di Cybersecurity intende:
 - potenziare e ottimizzare le capacità di monitoraggio continuo e rilevazione degli eventi di sicurezza;
 - migliorare i processi e i meccanismi di risposta e contenimento degli incidenti di sicurezza;
 - assicurare una gestione efficace delle crisi e salvaguardare la continuità dei processi a supporto dei servizi erogati;
 - Incrementare la visibilità sugli asset, identificando e prioritizzando quelli critici secondo una logica *risk-based* e garantirne una corretta gestione e protezione;
 - assicurare che minacce, rischi e vulnerabilità siano tempestivamente identificati, valutati e mitigati su base continuativa;
 - adottare soluzioni che consentano la protezione della rete da accessi non autorizzati verso tutti quei dispositivi non gestiti direttamente (ad esempio, i laptop personali di utenti che lavorano da remoto o di personale sanitario/farmaceutico che opera sui sistemi software regionali);
 - creare un Cybersecurity Defense Center unico regionale, nel quale confluiranno le attuali funzioni del CSIRT e del SOC, con l'obiettivo di creare una struttura in grado di erogare molteplici servizi di sicurezza verso gli enti regionali [con particolare riferimento ai servizi di monitoraggio continuo, rilevazione e risposta agli eventi/incidenti di sicurezza];
 - ampliare e consolidare le competenze individuali in ambito cybersecurity per le figure professionali della sicurezza informatica;
 - aumentare la consapevolezza del personale sui rischi cyber, promuovendo l'adozione di buone pratiche per contrastare le minacce cyber;

Considerato che:

- con la D.G.R. 16.05.2023 n. 663, la Giunta Regionale ha espresso *“come vincolante l’indirizzo all’utilizzo del Data Center di Regione Puglia presso InnovaPuglia S.p.A per tutti i servizi regionali, di qualsiasi tipologia e ambito, compresi tutti i servizi dei Data Center delle Aziende Sanitarie Locali, delle Aziende Ospedaliere e degli IRCCS pubblici della Regione Puglia”* e 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”* ritenendo che una visione strategica unitaria degli asset di Regione Puglia possa consentire una maggiore capacità realizzativa ed un’aumentata efficacia della governance degli stessi;
- il rafforzamento delle capacità cyber 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;
- il 70% dei sistemi informatici ospitati nel Data Center di Regione Puglia erogano servizi digitali in ambito sanitario e le Aziende Sanitarie Locali, le Aziende Ospedaliere e gli IRCCS pubblici della Regione Puglia stanno completando il percorso di migrazione dei propri servizi digitali sanitari presso il Data Center di Regione Puglia, con conseguente necessità di dover procedere con la massima urgenza ad innalzare il livello di sicurezza delle infrastrutture;
- il CSIRT Puglia è attualmente oggetto di rafforzamento a seguito del finanziamento per euro 1.500.000,00 del progetto *“RAFFORZAMENTO CSIRT REGIONALE”*, concesso con Determinazione Direttoriale dell’Agenzia Nazionale per la Cybersecurity del 30.11.2023 prot. n. 30697, in merito all’Avviso Pubblico n. 06/2023 recante *“Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all’attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti*

informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”M1C1I1.5”;

Rilevato che:

- con Determinazione Dirigenziale del RTD del 07.12.2023, n. 7 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, nel rispetto degli obiettivi generali dell’intervento e degli obiettivi realizzativi descritti nel progetto;

Rilevato altresì che:

- la L. 28 giugno 2024 n. 90, all’art. 8 comma 1, prevede 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:*
 - a) *allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;*
 - b) *alla produzione e all’aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;*
 - c) *alla produzione e all’aggiornamento di un documento che definisca i ruoli e l’organizzazione del sistema per la sicurezza delle informazioni dell’amministrazione;*
 - d) *alla produzione e all’aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell’amministrazione;*
 - e) *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);*
 - f) *alla pianificazione e all’attuazione dell’adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall’Agenzia per la cybersicurezza nazionale;*
 - g) *al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza”;*
- il successivo comma 2 dell’art. 8 sopra menzionato prevede che *“presso le strutture di cui al comma 1 opera il referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza [...]”, che “Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell’amministrazione con l’Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla presente legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta la medesima amministrazione” e che “ a tale fine, il nominativo del referente per la cybersicurezza è comunicato all’Agenzia per la cybersicurezza nazionale”;*
- sempre l’art. 8, al comma 3 dispone che *“la struttura e il referente di cui ai commi 1 e 2 possono essere individuati, rispettivamente, nell’ufficio e nel responsabile per la transizione al digitale [...]”;*

Rilevato, infine, che:

- il D. Lgs. n. 138/2024, all’art. 7 comma 1 lett. c), prevede come obbligo per l’Amministrazione regionale quello della *“designazione di un punto di contatto, indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono”;*

Ritenuto 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 DPGR 430/2020 al Responsabile Transizione Digitale e Dirigente del Servizio Tecnico e Transizione Digitale del Gabinetto del Presidente G.R. - Direzione Amministrativa, sin dall'inizio dell'attività dell'UTD con la predisposizione del Piano di Riorganizzazione Digitale, dell'OR_20 e del Piano di Sicurezza regionale, risulta necessario, per mantenere uniformi regia e processo di tutti gli interventi d'ambito, fornire indirizzi comuni;
- per le medesime motivazioni, è opportuno 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";
- sempre in considerazione dei medesimi obiettivi, è altresì opportuno che siano mantenute le finalità e le attività attualmente previste, ridenominando il CSIRT in "CSIRT della Regione Puglia" e prevedendo la distinzione tra le attività esecutive, affidate a InnovaPuglia S.p.A. e il coordinamento e la governance dell'asset, nella competenza di Regione Puglia per il tramite del RTD regionale;

Ritenuto altresì che:

- alla luce della previsione della legge n. 90/2024 è necessario:
 - 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;
 - individuare il referente per la cybersicurezza, in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza; è opportuno, onde consentire il coordinamento con il Piano di Cybersecurity regionale e con gli altri interventi in materia a regia del RTD regionale, individuare la struttura e il referente di cui sopra, rispettivamente, nell'Ufficio e nel Responsabile per la Transizione al Digitale ai sensi del comma 3, art. 8, Legge n. 90/2024;
- alla luce della previsione del D. Lgs. n. 138/2024 è necessario individuare nel Responsabile per la Transizione al Digitale il Punto di Contatto previsto dall'art. 7 comma 1 lett. c);

Alla luce delle risultanze istruttorie, risulta necessario procedere all'espletamento degli obblighi previsti dalla L. 90/2024, dal D. Lgs. n. 138/2024 e garantire organicità e unitarietà dell'azione regionale in materia di cybersecurity.

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'espletamento degli obblighi previsti dalla L. 90/2024, dal D. Lgs. n. 138/2024 e garantire organicità e unitarietà dell'azione regionale in materia di cybersecurity, ai sensi dell'art. 4, comma 4, lett. a) e d) della L.R. n. 7/97, si propone alla Giunta Regionale:

1. 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;
2. di individuare nell'Ufficio per la Transizione al Digitale, la struttura presso la quale opera il referente per la cybersicurezza, ai sensi dell'art. 8 comma 1 della legge n. 90/2024;
3. individuare il referente per la Cybersicurezza nel Responsabile per la Transizione al Digitale di Regione Puglia, ai sensi dell'art. 8, comma 2 della legge n. 90/2024;
4. di demandare al referente individuato la costituzione di un apposito gruppo di lavoro formato da personale di Regione Puglia e di InnovaPuglia S.p.A.;
5. 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;
6. di disporre 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;
7. di disporre 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;
8. 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;
9. di disporre la pubblicazione del presente provvedimento in versione integrale nel Bollettino Ufficiale della Regione Puglia ai sensi della L.R. 18/2023;
10. di disporre la pubblicazione integrale del presente provvedimento sul sito istituzionale della Regione Puglia www.regione.puglia.it nella sezione "Amministrazione Trasparente", sottosezione "Provvedimenti della Giunta Regionale";
11. di notificare il presente provvedimento, a cura della Struttura proponente a tutti i soggetti interessati e, qualora previsto, all'Agenzia per la cybersicurezza nazionale (ACN).

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. 23 luglio 2019, n. 1374.

L'istruttore
(Dott. Paolo Giannoccaro)



Paolo Giannoccaro
12.12.2024 10:15:18
GMT+02:00

Il Funzionario E.Q. "Project Management
e reingegnerizzazione dei processi di Transizione al Digitale"
(Ing. Diego Catalano)



Diego Catalano
12.12.2024 10:58:01
GMT+02:00

La Funzionaria E.Q. "Supporto giuridico specialistico
per la Transizione alla modalità digitale"
(Avv.ta Maria Morena Ragone)



Maria Morena Ragone
12.12.2024 11:04:13
GMT+02:00

Il Direttore della Direzione Amministrativa del Gabinetto
(Dott. Crescenzo Antonio Marino)



Crescenzo Antonio
Marino
12.12.2024 17:53:08
GMT+02:00

Il Capo di Gabinetto, ai sensi dell'art. 18 e 20 del Decreto del Presidente della Giunta Regionale 22 gennaio 2021, n. 22 e ss.mm.ii., NON RAVVISA osservazioni alla presente proposta di deliberazione

Il Capo di Gabinetto
(Prof. Giuseppe Pasquale Roberto Catalano)



Giuseppe Pasquale
Roberto Catalano
13.12.2024
09:58:07
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
13.12.2024
11:50:22
GMT+02:00