DELIBERAZIONE DELLA GIUNTA REGIONALE 16 aprile 2025, n. 526

Approvazione schema del Protocollo d'Intesa tra Regione Puglia e Polizia di Stato per la prevenzione dei crimini informatici sui sistemi informativi critici della Regione Puglia.

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 art. 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 Dipartimento per la Transizione Digitale concernente l'argomento in oggetto, e la conseguente proposta del Presidente della Giunta

PRESO ATTO

a) delle sottoscrizioni dei responsabili delle strutture amministrative competenti, 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 Direttore del Dipartimento per la Transizione Digitale, in merito a eventuali osservazioni sulla proposta di deliberazione, ai sensi degli art. 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. approvare lo schema di Protocollo d'Intesa ex art. 15, commi 1 e 2 della legge n. 241/1990 (Allegato A) alla presente proposta di deliberazione e parte integrante della stessa, da sottoscriversi tra Regione Puglia e Ministero dell'Interno - Dipartimento della Pubblica Sicurezza, Direzione Centrale per la Polizia Scientifica e per la Sicurezza Cibernetica;
2. di dare atto che il Protocollo d'Intesa allegato sia sottoscritto nelle forme di rito da parte del Presidente della Giunta Regionale e del Direttore Centrale del Dipartimento della Pubblica Sicurezza, Direzione Centrale per la Polizia Scientifica e per la Sicurezza Cibernetica del Ministero dell'Interno;
3. di demandare alla Struttura regionale competente, individuata nel Dipartimento per la Transizione Digitale, l'attuazione delle attività previste nel Protocollo d'Intesa apportandovi eventuali modifiche ed integrazioni non sostanziali che dovessero rendersi necessarie e/o opportune;
4. di stabilire che il Protocollo d'intesa avrà durata di tre anni, a decorrere dalla data della sua sottoscrizione e che potrà essere prorogato, fino al completamento delle iniziative concordate;
5. di pubblicare il presente provvedimento sul BURP in versione integrale;

6. di notificare, a cura del Dipartimento per la Transizione Digitale, il presente provvedimento ai soggetti interessati;
7. di demandare al Dipartimento per la Transizione al Digitale gli adempimenti amministrativi di competenza per l'esatta esecuzione del provvedimento;
8. di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 23 del decreto legislativo 14 marzo 2013, n. 33.

Il Segretario Generale della Giunta
NICOLA PALADINO

Il Presidente della Giunta
MICHELE EMILIANO

DOCUMENTO ISTRUTTORIO

OGGETTO: **Approvazione schema del Protocollo d'Intesa tra Regione Puglia e Polizia di Stato per la prevenzione dei crimini informatici sui sistemi informativi critici della Regione Puglia.**

Visti:

- 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 D.G.R. 7 dicembre 2020, n. 1974 con cui è stato approvato l'atto di Alta organizzazione Modello Ambidestro denominato "MAIA 2.0", successivamente adottato – come previsto dallo Statuto regionale – con Decreto del Presidente della Giunta Regionale n. 22 del 22 gennaio 2021, di seguito modificato e integrato con successivi Decreti del Presidente della Giunta regionale;

- la D.G.R. 15 settembre 2021, n. 1466 recante "Approvazione del documento strategico Agenda di Genere. Strategia Regionale per la Parità di Genere in Puglia";

- la D.G.R. 26 settembre 2024, n. 1295 recante "Valutazione di Impatto di Genere (VIG). Approvazione indirizzi metodologico-operativi e avvio fase strutturale";

- la D.G.R. 03 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" e ss. mm e ii.

Premesso che:

- l'art. 15 della Legge 7 agosto 1990, n. 241 stabilisce che le Amministrazioni Pubbliche possono concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;

- la legge 31 luglio 1997, n. 249, ha istituito l'Autorità per le garanzie nelle comunicazioni dettando norme sui sistemi delle telecomunicazioni e radiotelevisivo;

- l'art. 1, commi 13 e 15 della legge 31 luglio 1997, n. 249, con decreto del Ministro dell'Interno, adottato di concerto con il Ministro delle Comunicazioni e con il Ministro del Tesoro, del Bilancio e della Programmazione Economica, in data 19 gennaio 1999, ha individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;

- il decreto legge 27 luglio 2005 n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005 n. 155, recante "Misure urgenti per il contrasto del terrorismo internazionale", ed in particolare l'art. 7 bis, comma 1, che ha disposto con decreto del Ministro dell'Interno che fossero individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;

- il Decreto del 7 febbraio 2024 del Ministro dell'Interno, di concerto con il Ministro dell'Economia e delle Finanze, ha istituito la Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, tra le cui articolazioni è incardinato il Servizio Polizia Postale e per la Sicurezza Cibernetica (già Servizio Polizia Postale e delle Comunicazioni della Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato);

- la Legge 28 giugno 2024, n. 90 recante “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici” introduce disposizioni per il rafforzamento della cybersicurezza nazionale e la prevenzione dei reati informatici prevedendo di aumentare la sicurezza informatica del Paese e migliorando la capacità di risposta a emergenze cibernetiche e coordinando meglio gli interventi in caso di attacchi informatici;

- il D. Lgs. 4 settembre 2024, n. 138 prevede il “Recepimento della direttiva (UE) 2022/2555, 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”;

- il già citato D.Lgs. 4 settembre 2024 n. 138 ha confermato quale Autorità di contrasto ai reati cibernetici il Servizio Polizia Postale e della Sicurezza Cibernetica in qualità di Organo Centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione;

Considerato che:

- la D.G.R. n. 663 del 16 maggio 2023, relativa alle Linee di indirizzo per le infrastrutture tecnologiche digitali regionali ha come obiettivo principale la razionalizzazione e omogeneizzazione dei sistemi informativi regionali, migliorando l'efficienza e la sicurezza delle infrastrutture digitali;

- la D.G.R. n. 1793 del 16 dicembre 2024, prevede il rafforzamento delle capacità cyber del sistema regionale e la designazione del Responsabile per la Transizione Digitale quale Punto di Contatto previsto dall’art. 7 del D. Lgs. n. 138/2024;

Considerato, altresì, che:

- con D.G.R. n. 282 del 14 marzo 2024 ad oggetto “Modifiche ed integrazioni alla deliberazione di Giunta Regionale 7 dicembre 2020 n. 1974 e s.m.i. – Nuove istituzioni, rimodulazioni e soppressioni di strutture dirigenziali”, 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;

- con la D.G.R. n. 477 del 15 aprile 2024, la Giunta Regionale ha aggiornato le funzioni delle Sezioni di 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 e che tra i suoi compiti rientrano 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;

    - definisce e coordina le politiche delle abilitazioni ai servizi informatici, agli applicativi regionali e alle risorse di rete;

- definisce e coordina le politiche regionali relative ai servizi infrastrutturali della Amministrazione regionale, connettività (fissa e wireless) intranet e internet delle sedi;
- coordina il servizio di supporto informatico e presidio IT;
- sistemi IT di mappatura e monitoraggio degli asset regionali;
- acquista le attrezzature informatiche e i relativi servizi di assistenza;
- definisce e coordina il processo di migrazione da parte di Regione Puglia, degli enti collegati, delle Aziende Sanitarie e degli enti del territorio (in raccordo per questi ultimi con il Dipartimento Sviluppo Economico) al datacenter regionale e al cloud regionale;
- definisce e coordina le infrastrutture di rete e le piattaforme tecnologiche della Regione Puglia;
- coordina la gestione del DataCenter regionale, del Sistema Cloud e dei relativi livelli di servizio, alta affidabilità e sicurezza;
- definisce e coordina i servizi digitali di base utilizzati dall'Ente: PEO, PEC, Firma Digitale, IAM e tutte le piattaforme abilitanti regionali;
- coordina il polo di conservazione regionale e tutti i processi di dematerializzazione di Regione;
- partecipa ai tavoli tecnici europei, nazionali, interregionali e ai Centri di Competenza regionali, e a progetti a finanziamento europeo e nazionale nelle materie di competenza;

- con D.G.R. n. 1872 del 23 dicembre 2024 la Giunta Regionale ha conferito l'incarico di Direttore di Dipartimento per la Transizione Digitale all' Ing. Cosimo Elefante;
- con D.G.R. n. 51 del 29 gennaio 2025 la Giunta Regionale ha nominato Responsabile della Transizione al Digitale (RTD) della Regione Puglia il Direttore pro-tempore del Dipartimento per la Transizione Digitale, Ing. Cosimo Elefante;
- con D.G.R. n. 248 del 4 marzo 2025 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;

Dato atto che:

- la minaccia dei crimini informatici impone l'adozione di misure di prevenzione e contrasto in collaborazione con le Autorità competenti;
- la Polizia di Stato, attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), svolge un ruolo primario nella prevenzione e repressione degli attacchi informatici alle infrastrutture strategiche;
- il Centro Operativo Sicurezza Cibernetica - Polizia Postale "Puglia" provvede, come organo periferico del Servizio Polizia Postale e per la Sicurezza Cibernetica del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e per la Sicurezza Cibernetica, con particolare riferimento alla prevenzione e repressione dei reati commessi avvalendosi delle specifiche potenzialità tecniche dei servizi o mezzi di comunicazione, anche ad alta tecnologia, ovvero alterando il normale funzionamento degli stessi;

- la Regione Puglia gestisce sistemi informativi regionali critici per l'erogazione di servizi pubblici essenziali e la tutela del patrimonio informativo dell'amministrazione e per il supporto alle proprie funzioni istituzionali a favore di cittadini, imprese ed Enti oltre a svolgere il ruolo di soggetto aggregatore per questi ultimi, promuovendo sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali ai sensi dell'art.14, comma 2-bis del D.Lgs. 82/2005 "Codice dell'Amministrazione Digitale";

- i sistemi informatici e le reti telematiche di supporto alle funzioni istituzionali di Regione Puglia sono da considerare infrastrutture critiche di interesse nazionale e che, pertanto, risulta necessario prevenire e contrastare ogni forma di accesso illecito, anche tentato, con finalità di:

  a) interruzione dei servizi di pubblica utilità;

  b) indebita sottrazione di informazioni;

  c) attacchi cibernetici su vasta scala volti a compromettere la sicurezza del "Sistema Paese";

  d) porre in essere qualsiasi ulteriore attività illecita;

Tenuto conto che:

- a conclusione di specifici incontri tecnici tra i rappresentanti del Centro Operativo per la Sicurezza Cibernetica Puglia della Polizia di Stato e il Dipartimento per la Transizione Digitale della Regione Puglia è stato elaborato un progetto di collaborazione per la prevenzione ed il contrasto dei crimini informatici che ha per oggetto, nella loro complessità, i sistemi ed i servizi informatici critici della Regione Puglia;
- la cooperazione tra il Centro Operativo per la Sicurezza Cibernetica e la Regione Puglia, volta alla prevenzione e alla repressione dei crimini informatici, ispirata al principio di sicurezza partecipata, nell'intento di assicurare in via sinergica ed efficiente le risorse del Sistema Paese a vantaggio dell'intera collettività, contribuisce al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati attraverso sistemi informatici e di telecomunicazioni.
- è necessario formalizzare una collaborazione tra la Regione Puglia e la Polizia di Stato per garantire un efficace sistema di monitoraggio e prevenzione delle minacce cyber;
- il Protocollo d'Intesa tra Regione Puglia e Polizia di Stato disciplina gli ambiti di collaborazione, le modalità operative e gli obblighi reciproci;

Alla luce delle risultanze istruttorie si propone di:

approvare lo schema del Protocollo d'Intesa tra Regione Puglia e Polizia di Stato per la prevenzione dei crimini informatici sui sistemi informativi critici della Regione Puglia, Allegato A al presente provvedimento e parte integrante dello stesso, per le finalità sopra descritte.

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 del 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: Neutra

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 approvare il Protocollo d'Intesa tra Regione Puglia e Polizia di Stato, finalizzato alla prevenzione e al contrasto dei crimini informatici ai danni dei sistemi informativi critici regionali, ai sensi dell'art. 4, comma 4, lettera a) ed e) della L.R. n. 7/97, di concerto con il Consigliere del Presidente per l'informatizzazione, e–government ed il social government, nominato con DPGR n. 430/2020, si propone alla Giunta Regionale:

1. di approvare lo schema di Protocollo d'Intesa ex art. 15, commi 1 e 2 della legge n. 241/1990 (Allegato A) alla presente proposta di deliberazione e parte integrante della stessa, da sottoscriversi tra Regione Puglia e Ministero dell'Interno - Dipartimento della Pubblica Sicurezza, Direzione Centrale per la Polizia Scientifica e per la Sicurezza Cibernetica;

2. di dare atto che il Protocollo d'Intesa allegato sia sottoscritto nelle forme di rito da parte del Presidente della Giunta Regionale e del Direttore Centrale del Dipartimento della Pubblica Sicurezza, Direzione Centrale per la Polizia Scientifica e per la Sicurezza Cibernetica del Ministero dell'Interno;

3. di demandare alla Struttura regionale competente, individuata nel Dipartimento per la Transizione Digitale, l'attuazione delle attività previste nel Protocollo d'Intesa apportandovi eventuali modifiche ed integrazioni non sostanziali che dovessero rendersi necessarie e/o opportune;

4. di stabilire che il Protocollo d'intesa avrà durata di tre anni, a decorrere dalla data della sua sottoscrizione e che potrà essere prorogato, fino al completamento delle iniziative concordate;

5. di pubblicare il presente provvedimento sul BURP in versione integrale;

6. di notificare, a cura del Dipartimento per la Transizione Digitale, il presente provvedimento ai soggetti interessati;

7. di demandare al Dipartimento per la Transizione al Digitale gli adempimenti amministrativi di competenza per l'esatta esecuzione del provvedimento;

8. di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 23 del decreto legislativo 14 marzo 2013, n. 33.

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

Il Funzionario
(Dott. Nicola Lombardi)

Nicola Lombardi
16.04.2025
13:06:22
GMT+02:00

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

Angela Guerra
16.04.2025
13:13:13
GMT+02:00

Il Direttore 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 osservazioni alla presente proposta di DGR.

Il Direttore del Dipartimento per la Transizione Digitale

(Ing. Cosimo Elefante)

REGIONE PUGLIA
Cosimo Elefante
16.04.2025
13:24:07
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

(Michele Emiliano)

Michele
Emiliano
16.04.2025
14:38:37
GMT+02:00

***

Dalla pagina successiva segue l'Allegato A, le cui pagine sono numerate in modo consecutivo, a partire dalla pagina 1 fino all'ultima pagina dell'allegato.

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

PROTOCOLLO D'INTESA
PER LA PREVENZIONE DEI CRIMINI INFORMATICI
SUI SISTEMI INFORMATIVI CRITICI DELLA REGIONE PUGLIA

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

Il Ministero dell'Interno – Dipartimento della Pubblica Sicurezza, Direttore Centrale per la Polizia Scientifica e per la Sicurezza Cibernetica *pro-tempore*, Dirigente Generale di Pubblica Sicurezza dr. Luigi Rinella, domiciliato per la sua funzione in Roma, Via Tuscolana n. 1558,

e

La Regione Puglia, avente sede legale in Bari, Lungomare N. Sauro, 33, rappresentata dal Presidente della Regione dott. ……. (P.E.C.: ……), domiciliato per la carica nella sede di Bari, Lungomare N. Sauro 33, in qualità di legale rappresentante;

d'ora innanzi, congiuntamente, "*Parti*"

PREMESSO CHE

- l'art. 15 della Legge 7 agosto 1990, n. 241 stabilisce che le Amministrazioni Pubbliche possono concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;
- la legge 31 luglio 1997, n. 249, ha istituito l'Autorità per le garanzie nelle comunicazioni dettando norme sui sistemi delle telecomunicazioni e radiotelevisivo;
- in relazione all'art. 1, commi 13 e 15 della citata legge, con decreto del Ministro dell'Interno, adottato di concerto con il Ministro delle Comunicazioni e con il Ministro del Tesoro, del Bilancio e della Programmazione Economica, in data 19 gennaio 1999, è stato individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;
- il decreto legge 27 luglio 2005 n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005 n. 155, recante "*Misure urgenti per il contrasto del terrorismo internazionale*", ed in particolare l'art. 7 bis, comma 1, dispone che con decreto del Ministro dell'Interno siano individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;
- in attuazione dell'articolo 7 bis, comma 1, del decreto legge 27 luglio 2005, n.144, convertito con modificazioni dalla legge 31 luglio 2005, n. 155, il Ministro dell'Interno, con proprio decreto, in data 9 gennaio 2008 ha previsto:

  a) all'art. 1, comma 1, le infrastrutture critiche informatizzate di interesse nazionale, quali i sistemi ed i servizi informatici di supporto alle funzioni istituzionali di una definita serie di enti, pubblici e privati, operanti nei settori strategici per il Paese;

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

b) all'art. 1, comma 2, che i collegamenti telematici necessari per assicurare protezione alle infrastrutture critiche informatizzate siano definiti mediante apposite convenzioni stipulate, ai sensi dell'art. 15 della legge 7 agosto 1990, n. 241 e dell'art. 39 della legge 16 gennaio 2003 n. 3, tra i soggetti titolari delle infrastrutture critiche ed il Ministero dell'Interno – Dipartimento della Pubblica Sicurezza;

c) all'art. 3, l'istituzione del C.N.A.I.P.I.C. - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, quale unità incardinata nel Servizio Polizia Postale e delle Comunicazioni;

d) che con decreto del Capo della Polizia – Direttore Generale della Pubblica Sicurezza - adottato in data 7 agosto 2008, venisse formalizzato l'assetto organizzativo e funzionale del C.N.A.I.P.I.C.;

- che il D.P.C.M. del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, definisce all'art.1 l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali;
- che il D.P.C.M. del 27 gennaio 2014 ha adottato il "Quadro Strategico Nazionale per la Sicurezza Nazionale dello Spazio Cibernetico" e con DPCM 31/03/2017 è stato ridefinito il "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica";
- che con il Decreto 19 settembre 2017, n. 215 del Ministero dell'Interno, di concerto con i Ministri dello Sviluppo Economico e dell'Economia e delle Finanze, è stato adottato il "*Regolamento recante individuazione delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato e al Corpo nazionale dei vigili del fuoco, nonché le modalità attuative ai fini della loro concessione in uso temporaneo a terzi*";
- che la Direttiva del Ministro dell'Interno del 15 agosto 2017 "sui comparti delle Specialità e sulla razionalizzazione dei Presidi di Polizia" ha ribadito al punto 1.4 la competenza della Polizia Postale e delle Comunicazioni in materia di protezione delle infrastrutture critiche nonché di sicurezza e regolarità dei servizi di telecomunicazione;
- che con decreto del Capo della Polizia del 28 giugno 2022, è stata attuata la complessiva revisione dell'assetto ordinativo delle articolazioni periferiche dell'Amministrazione della Pubblica Sicurezza e, in particolare, dei Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) quale nuova denominazione dei Compartimenti di Polizia Postale e delle Comunicazioni, al cui interno sono stati istituiti i Nuclei Operativi Sicurezza Cibernetica (N.O.S.C.);
- che con il Decreto del 7 febbraio 2024 del Ministro dell'Interno, di concerto con il Ministro dell'Economia e delle Finanze, è stata istituita la Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, tra le cui articolazioni è incardinato il Servizio Polizia Postale e per la Sicurezza Cibernetica (già Servizio Polizia Postale e delle Comunicazioni della Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato);

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

- che con il D.Lgs. 4 settembre 2024 n. 138 è stata recepita la Direttiva (UE) 2022/2555 relativa alle *misure per un livello comune elevato di cibersicurezza nell'Unione"* (c.d. Direttiva NIS2), che conferma quale Autorità di contrasto il Servizio Polizia Postale e della Sicurezza Cibernetica in qualità di Organo Centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155, così come individuato dal Decreto Interministeriale del 10 gennaio 1999;
- che nell'ambito del Piano integrato di Attività e organizzazione del Ministero dell'Interno datato 30 gennaio 2024, il Ministro dell'Interno, in ordine agli obiettivi operativi, nel ribadire l'esigenza di ampliare la sfera di tutela del C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) per le infrastrutture critiche informatizzate e delle infrastrutture sensibili presenti sul territorio (piccole e medie imprese – Pubbliche Amministrazioni Locali) da realizzarsi tramite l'incremento di accordi bilaterali tra l'Amministrazione e gli enti gestori di sistemi e servizi informatici strategici, ha altresì previsto il rafforzamento – attraverso le risorse del PNRR – delle difese cibernetiche, aumentando il grado di resilienza informatica dell'amministrazione attraverso la creazione di sezioni operative per la sicurezza cibernetica distrettuali, di laboratori operativi dotati delle infrastrutture per le attività forensi (CLABS) e il potenziamento della sala server, al fine di prevedere o rilevare tempestivamente attacchi e incidenti informatici;

tenuto conto

- che il Centro Operativo Sicurezza Cibernetica - Polizia Postale "Puglia" provvede, come organo periferico del Servizio Polizia Postale e per la Sicurezza Cibernetica del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e per la Sicurezza Cibernetica, con particolare riferimento alla prevenzione e repressione dei reati commessi avvalendosi delle specifiche potenzialità tecniche dei servizi o mezzi di comunicazione, anche ad alta tecnologia, ovvero alterando il normale funzionamento degli stessi;
- che Regione Puglia gestisce i sistemi informativi regionali per il supporto alle proprie funzioni istituzionali a favore di cittadini, imprese ed Enti oltre a svolgere il ruolo di soggetto aggregatore per questi ultimi, promuovendo sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali ai sensi dell'art.14, comma 2-bis del D.Lgs. 82/2005 "Codice dell'Amministrazione Digitale";
- che i sistemi informatici e le reti telematiche di supporto alle funzioni istituzionali di Regione Puglia sono da considerare infrastrutture critiche di interesse nazionale. Risulta, pertanto, necessario prevenire e contrastare ogni forma di accesso illecito, anche tentato, con finalità di:

  a) interruzione dei servizi di pubblica utilità;

  b) indebita sottrazione di informazioni;

  c) attacchi cibernetici su vasta scala volti a compromettere la sicurezza del "Sistema Paese";

  d) porre in essere qualsiasi ulteriore attività illecita;

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

- che a conclusione di specifici incontri tecnici tra i rappresentanti del centro operativo per la sicurezza cibernetica Puglia e il Dipartimento per la Transizione Digitale della Regione Puglia è stato elaborato un progetto di collaborazione per la prevenzione ed il contrasto dei crimini informatici che ha per oggetto, nella loro complessità, i sistemi ed i servizi informatici critici della Regione Puglia;
- che la cooperazione tra il Centro Operativo per la Sicurezza Cibernetica e la Regione Puglia, volta alla prevenzione e alla repressione dei crimini informatici, ispirata al principio di sicurezza partecipata, nell'intento di assicurare in via sinergica ed efficiente le risorse del Sistema Paese a vantaggio dell'intera collettività, contribuisce al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati attraverso sistemi informatici e di telecomunicazioni.

premesso inoltre

- che l'articolo 39 della legge 16 gennaio 2003, n. 3, recante: "Disposizioni ordinamentali in materia di pubblica amministrazione" prevede che il Dipartimento della Pubblica Sicurezza, nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione, può stipulare convenzioni con soggetti, pubblici e privati, dirette a fornire, con la contribuzione degli stessi soggetti, servizi specialistici, finalizzati ad incrementare la sicurezza pubblica;
- Il Decreto Legislativo 30 giugno 2003, n.196, concernente "Codice in materia di protezione dei dati personali", come integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101;
- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- che con il D.Lgs. 18 maggio 2018 n. 51, recante "Attuazione della Direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016" sono state ridefinite le regole riguardanti il trattamento dei dati personali effettuato per "finalità di polizia", ovvero direttamente collegate all'attività di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica;

TUTTO CIO' PREMESSO

LE PARTI STIPULANO E CONVENGONO QUANTO SEGUE

Articolo 1

(Oggetto della convenzione)

1. Le *Parti* si impegnano reciprocamente a collaborare in relazione:

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

a) alla condivisione e all'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture critiche informatiche della Regione Puglia per le finalità meglio in premessa specificate;

b) alla segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione;

c) all'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche gestite dalla Regione Puglia o che traggano origine dalle medesime;

d) alla prevenzione e al supporto nella gestione di situazioni di crisi cibernetiche;

e) all'avvio di percorsi formativi congiunti per il personale del perimetro regionale (Regione, Agenzie regionali, in house, Aziende ed Enti del Sistema Sanitario Regionale pugliese) finalizzati a costituire una base minima di conoscenze in tema di cybersecurity, per riconoscere e prevenire le minacce cyber e fornire competenze pratiche per proteggere sistemi e dati. L'attività formativa può essere organizzata anche in accordo con altre strutture regionali, istituzioni, imprese e istituti scolastici e di formazione sul territorio, per garantire un approccio integrato ed efficace alla sicurezza informatica nell'intera Regione;

f) all'analisi e monitoraggio del "territorio digitale" attraverso lo scambio di informazioni e dati tra la Regione Puglia e la Polizia Postale per identificare nuove minacce informatiche e monitorare l'andamento dei crimini informatici sul territorio regionale;

g) allo sviluppo di sistemi di allerta precoce (*early warning)* per allertare tempestivamente le autorità in caso di minacce informatiche imminenti;

h) alla organizzazione di eventi e iniziative per promuovere la cultura della sicurezza informatica sul territorio della Regione Puglia;

i) alla realizzazione di materiale informativo (brochure, video, infografiche) da distribuire online e offline;

j) alla sensibilizzazione degli utenti telematici pugliesi al corretto utilizzo della rete e delle piattaforme social in relazione alle minacce cyber.

2. Le attività necessarie al conseguimento degli obiettivi di cui al precedente comma 1 verranno assicurate dal Centro operativo per la sicurezza cibernetica "Puglia" e dal Dipartimento per la Transizione Digitale della Regione Puglia.

Articolo 2
(Oneri delle parti)

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

1. Dall'attuazione della presente Convenzione non devono derivare nuovi o maggiori oneri a carico del bilancio del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, che provvede con le risorse umane e strumentali disponibili a legislazione vigente.
2. Nessun onere economico specifico deriva dal presente accordo per l'Amministrazione della Pubblica Sicurezza.
3. La Regione Puglia, ove dovesse rendersi necessario, si impegna, al fine del conseguimento degli obiettivi di cui al precedente articolo 1, comma 1, ad estendere al Centro Operativo per la Sicurezza Cibernetica "Puglia" e alle dipendenti Sezioni Operative regionali quali articolazioni periferiche del Servizio Polizia Postale e per la Sicurezza Cibernetica, la rete in "*fibra ad alta velocità*", già in uso agli Uffici Regionali.
4. La Regione Puglia, qualora lo ritenga opportuno, potrà fornire eventuali tecnologie necessarie per l'assolvimento di compiti istituzionali previsti all'art. 1. Sono a suo carico eventuali oneri di attuazione, comunque concordati preventivamente per singola progettualità, in coerenza con l'articolo 39, comma 2, della legge 16 gennaio 2003, n. 3 e saranno oggetto di successivi atti aggiuntivi alla presente Convenzione.

Articolo 3

(Formazione)

1. Le *Parti* potranno sviluppare, attraverso il C.O.S.C. Puglia ed il competente Dipartimento per la Transizione Digitale della Regione, attività formativa reciproca o congiunta sui sistemi e sulle tecnologie informatiche utilizzate, nonché sulle procedure di intervento atte a prevenire e contrastare gli accessi illeciti o i tentativi di accesso illecito ai danni di tali sistemi e tecnologie nonché i fenomeni delittuosi di cui all'art. 1. L'attività formativa avrà inoltre lo scopo di favorire l'interscambio e la partecipazione del rispettivo personale (dipendente) ai percorsi di formazione specifica ritenuti di interesse dalle Parti.

Articolo 4

(Impegni delle parti)

1. Per le finalità di cui all'art. 1, le *Parti* si impegnano a definire ed individuare:

   a) i sistemi ed i servizi informativi e telematici critici della Regione Puglia, come classificati nei Piani di migrazione al Cloud regionali e delle Aziende ed Enti del Sistema Sanitario Regionale pugliese;

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

b) i sistemi di trasferimento sicuri per la comunicazione delle informazioni d'interesse, nel rispetto delle disposizioni in materia di circolazione e protezione dei dati personali, l'utilizzo e l'accesso alle informazioni di polizia nonché di quelle sul segreto d'indagine e la tutela delle informazioni classificate.

Articolo 5

(Trattamento dei dati personali)

1. Le parti, ciascuna per le rispettive competenze, opereranno in qualità di titolari autonomi e si impegneranno a trattare i dati personali eventualmente derivanti dalle attività previste dalla presente intesa unicamente per le finalità concesse con la sua esecuzione e comunque nel rispetto del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, del dl.gs 30 giugno 2023 n.196 come integrato nelle modifiche introdotte dal Decreto Legislativo 10 agosto 2018 n. 101 e del D. lgs. n.51/2018.

Articolo 6

(Riservatezza e privacy)

1. Le *Parti* si impegnano a trattare e a custodire i dati e le informazioni tecniche ordinariamente acquisite nell'ambito delle attività previste dalla presente Convenzione, definendo ruoli, responsabilità e idonee misure nel rispetto della normativa in materia di protezione dei dati personali.
2. Ciascuna *Parte* si impegna a mantenere riservati ed a non utilizzare i risultati delle attività svolte in comune senza il preventivo consenso scritto dell'altra *Parte*.
3. L'obbligo di riservatezza di cui al comma che precede permarrà anche successivamente all'estinzione della presente Convenzione.

Articolo 7

(Attività di promozione e comunicazione)

1. Le *Parti* si impegnano a sviluppare iniziative congiunte, concordate preventivamente, volte a valorizzare il reciproco rapporto di collaborazione, anche attraverso iniziative volte alla promozione ed alla diffusione della cultura della legalità, tramite l'utilizzo delle denominazioni, degli stemmi, degli emblemi della Regione Puglia, nonchè degli altri segni distintivi in uso esclusivo alla Polizia di Stato nel rispetto del decreto del Ministro dell'Interno 19 settembre 2017, n. 215.
2. Con riferimento al precedente comma 1, la Regione Puglia si impegna a promuovere le iniziative congiunte intraprese ai sensi della presente convenzione, anche attraverso la

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

realizzazione di spot dedicati da trasmettere su media, network televisivi e piattaforme social ovvero a mezzo stampa sui principali quotidiani, con il coordinamento della Struttura Speciale Comunicazione Istituzionale.

Articolo 8

(Sottoscrizione, durata, recesso, referenti)

1. Il presente Protocollo sottoscritto con firma digitale, ai sensi dell'art. 15, comma 2-bis, della legge 7 agosto 1990, n. 241, o con firma elettronica avanzata o qualificata, soggetto agli obblighi di pubblicazione ai sensi dell'articolo 23, comma 1,lettera d), del decreto legislativo 14 marzo 2013, n. 33, entra in vigore dalla data della sottoscrizione ed ha durata di tre anni al termine dei quali si intende rinnovato automaticamente salvo contraria espressa dichiarazione di una delle Parti.
2. Le *Parti* possono procedere, periodicamente, alla verifica congiunta dei risultati ottenuti e all'individuazione degli obiettivi da conseguire nell'anno successivo sulla base di metodologie e criteri da stabilire con separato allegato tecnico.
3. Ciascuna delle *Parti* ha la facoltà di recedere dalla presente Convenzione in ogni momento, dandone comunicazione scritta all'altra con un preavviso di almeno tre mesi.
4. Le *Parti* individuano i propri referenti in relazione alle attività previste dall'accordo. Il referente per il Dipartimento della Pubblica Sicurezza è: …….. e le comunicazioni dovranno essere inviate al seguente indirizzo PEC: …….
   Il referente per Regione Puglia è l'ing. Cosimo Elefante e le comunicazioni dovranno essere inviate al seguente indirizzo PEC: resp.transizionedigitale@pec.rupar.puglia.it

Articolo 9

(Clausola finale e foro competente)

1. Ogni controversia relativa all'interpretazione e all'esecuzione della presente Convenzione viene esaminata bonariamente dalle *Parti*.
2. Qualora non risulti possibile addivenire ad una composizione della controversia, con un preavviso di 60 giorni naturali e consecutivi, le *Parti* potranno adire le competenti sedi giurisdizionali.
3. A tutti gli effetti di legge, Regione Puglia dichiara di eleggere domicilio in Bari, Lungomare N. Sauro, 33 .
   P.E.C.: resp.transizionedigitale@pec.rupar.puglia.it

Letto, approvato e sottoscritto.

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

REGIONE PUGLIA

Bari, data come da firme digitali

Il Direttore Centrale
per la Polizia Scientifica e la Sicurezza Cibernetica
del Dipartimento della P.S.
……..

Il Presidente
della Giunta Regionale
……..