Giunta Regionale della Campania

DECRETO DIRIGENZIALE

DIRETTORE GENERALE/
DIRIGENTE UFFICIO/STRUTTURA
DIRIGENTE UNITA' OPERATIVA DIR. /
DIRIGENTE STAFF

MASSIMO BISOGNO

DECRETO N°	DEL	DIREZ. GENERALE / UFFICIO / STRUTT.	UOD / STAFF
349	**15/07/2025**	**6011**	**00**

Oggetto:

PNRR, M1C1 – Investimento 1.5 "Cybersecurity" - Codice d'investimento M1C1I 1.5. Progetto "CSIRT – Campania" – CUP B27H23002720006. Approvazione procedure III Aggiornamento.

IL DIRIGENTE

PREMESSO CHE

a. la Raccomandazione (UE) 2017/1584 della Commissione, pubblicata il 13 settembre 2017, fornisce indicazioni in merito alla risposta coordinata agli incidenti e alle crisi di cybersicurezza su vasta scala;
b. la Direttiva (UE) 2022/2555 del Parlamento europeo e del consiglio, del 14 dicembre 2022, interviene e potenzia le "misure per un livello comune elevato di cybersicurezza nell'Unione", modifica il regolamento (UE) n. 910/2014 e la direttiva (UE) 2018/1972 e abroga la direttiva (UE) 2016/1148 (Direttiva NIS 2);
c. il Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 aggiorna il funzionamento dell'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e introduce la cybersicurezza per le tecnologie dell'informazione e della comunicazione (cd. "Cybersecurity Act");
d. il Regolamento di esecuzione (UE) 2024/482 che stabilisce le norme per l'applicazione del regolamento (UE) 2019/881 per quanto riguarda l'adozione del sistema europeo volontario di certificazione della cibersicurezza basato sui criteri comuni (EUCC) con l'obiettivo di garantire livelli di garanzia «elevati» o «sostanziali» di sicurezza per i prodotti TIC, come hardware e software, compresi componenti quali chip e smart card;
e. l'articolo 32 del Regolamento Generale sulla Protezione dei Dati (GDPR) "sicurezza del trattamento" dei dati personali che impone ai titolari e responsabili del trattamento di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato ai rischi associati al trattamento dei dati;
f. il decreto legislativo 7 marzo 2005, n. 82, con lo scopo di incentivare l'innovazione digitale nell'amministrazione pubblica, incentivando l'efficienza, la trasparenza e l'accessibilità dei servizi offerti reca, in particolare all'art 51, disposizioni in materia di sicurezza informatica, laddove è previsto che le pubbliche amministrazioni debbano adottare misure tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture;
g. il decreto legislativo n. 65 del 18 maggio 2018, detta la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS;
h. il decreto-legge n. 105 del 2019 come convertito dalla L. 18 novembre 2019, n.133 è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi;
i. il DPCM n. 131/2020 recante "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105 convertito con modificazioni, dalla legge 18 novembre 2019, n. 133*" stabilisce le modalità e i criteri procedurali per l'identificazione dei soggetti, sia pubblici che privati, che rientrano nel perimetro di cui al punto precedente;
j. il decreto-legge 14 giugno 2021, n. 82, come convertito dalla L. 4 agosto 2021, n. 109 (in G.U. 4/8/2021, n. 185) ha definito l'architettura nazionale di cybersicurezza ed ha previsto l'istituzione dell'Agenzia per la cybersicurezza nazionale, nonché l'operatività del Centro di Valutazione e Certificazione Nazionale (CVCN) ai sensi del DPCM n.54 del 5 febbraio 2021 ed il DPCM del 15 giugno 2021;
k. il decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, ha approvato il "Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale";
l. la Legge del 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" interviene su vari fronti, tra cui la prevenzione degli attacchi informatici e la protezione delle infrastrutture critiche nazionali, rendendo obbligatoria la creazione di strutture interne dedicate alla cybersicurezza nelle Pubbliche Amministrazioni;

m. il Decreto Legislativo 4 settembre 2024, n. 138, recepisce la Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS2), stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno;
n. la Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di Implementazione definiscono come pianificare, coordinare e attuare misure tese al potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente. In particolare, la Misura #33 avente ad oggetto "Accrescere le capacità di risposta e ripristino a seguito di crisi cibernetiche implementando una rete di CERT settoriali integrata con il CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati, con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici";
o. il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026 pone una forte enfasi sulla cybersicurezza come pilastro centrale per la trasformazione digitale della PA e tra gli obiettivi principali per il rafforzamento delle difese cibernetiche delle amministrazioni pubbliche individua la protezione delle infrastrutture critiche e sulla resilienza dei sistemi, il monitoraggio proattivo

PREMESSO altresì che

a. la Cybersecurity è uno dei sette investimenti della Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo" del PNRR;
b. in data 11/08/2023 l'Agenzia per la cybersicurezza nazionale, in qualità di Soggetto attuatore, ha pubblicato l'avviso pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali, ossia di strutture di "Computer Security Incident Response Team" incardinati presso le Amministrazioni regionali, per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici, nell'ambito della Missione 1 Componete 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5 del PNRR finalizzato a contribuire all'attuazione di investimenti finalizzati al rafforzamento delle capacità tecniche nazionali in materia di prevenzione e risoluzione di incidenti cyber, mediante l'attivazione di squadre di pronto intervento informatico deputate alla gestione degli incidenti e degli attacchi informatici sui propri sistemi informativi;
c. l'avviso è destinato a finanziare, mediante procedura a sportello, per un valore complessivo di 28M€ – secondo l'ordine cronologico di presentazione delle Istanze di partecipazione e fino alla concorrenza delle risorse disponibili – progettualità cd. a regia volte all'attivazione o al potenziamento di Computer Security Incident Response Team (CSIRT) da costituirsi o già costituiti presso le Regioni e le Province autonome, coerentemente con i requisiti minimi individuati dalle "Linee Guida per la realizzazione di uno CSIRT";
d. con Delibera di Giunta Regionale n. 537 del 22/09/2023 è stato disposto di aderire all'Avviso Pubblico del 11/08/2023 dell'Agenzia per la cybersicurezza nazionale 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, a valere sul PNRR, Missione 1 Componete 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5;
e. in data 30 novembre 2023 (prot.n. 0030697.30-11-2023.I) è stata firmata dal Direttore Generale dell'Agenzia di Cybersicurezza Nazionale la determina avente ad oggetto "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". Determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse;

f. con la suddetta determina sono stati approvati la graduatoria definitiva a valere sull'Avviso 6/2023 e i relativi allegati: (Allegato A) graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili, (Allegato B) graduatoria definitiva proposte progettuali ammesse e parzialmente finanziabili, (Allegato C) graduatoria definitiva proposte progettuali idonee ma non finanziabili, (Allegato D) elenco delle proposte progettuali non ammesse".
g. la proposta progettuale "CSIRT Campania" della Regione Campania è risultata tra le proposte ammesse e totalmente finanziabili per un importo complessivo pari ad € 1.499.904,60

RILEVATO che

a. il complesso degli interventi dell'Investimento 1.5 PNRR rappresenta un elemento fondante per la transizione digitale sicura della PA ed un'opportunità imprescindibile per irrobustire le infrastrutture e i servizi digitali, nonché le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza;
b. la Strategia Nazionale di Cybersicurezza 2022-2026 si focalizza su tre obiettivi principali ovvero: protezione degli asset strategici nazionali, risposta alle minacce cibernetiche e sviluppo di tecnologie digitali sicure. La strategia include l'implementazione di 82 misure entro il 2026 e promuove l'autonomia strategica nazionale in ambito digitale, puntando a innalzare la resilienza cibernetica del Paese;
c. Il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026 sottolinea l'importanza dei CERT (Computer Emergency Response Team) nel rafforzare la cybersicurezza all'interno delle pubbliche amministrazioni e, in particolare, evidenzia il ruolo centrale di CERT-AGID – per coordinare le attività di monitoraggio delle minacce informatiche, gestire incidenti cyber e fornire supporto tecnico alle amministrazioni – indirizzando le PA che intendono istituire i CERT di prossimità a far riferimento alle Linee guida per lo sviluppo e la definizione del modello di riferimento per i CERT di prossimità;
d. è interesse della Regione Campania, in conformità alla Strategia Nazionale di Cybersicurezza 2022-2026 ed al Piano operativo per la digitalizzazione della Regione Campania 2023-25, raggiungere i seguenti obiettivi:
    - protezione degli asset strategici, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese;
    - risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale;
    - sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.
e. la Regione Campania ha già realizzato un sistema di sicurezza informatica per proteggere i propri sistemi informativi e, contestualmente, ha anche incardinato nell'Ufficio Speciale per la crescita e la transizione al digitale il personale con specifiche competenze in materia di gestione digitale dei sistemi informativi, istituendo con D.D. n° 139 del 12/10/2022 il Security Operation Center (SOC), costituito da personale interno all'Ente con esperienza diretta nel campo di applicazione delle tecnologie informatiche per la sicurezza, che ha come obiettivo quello di innalzare il livello di resilienza cibernetica dei servizi critici erogati ai cittadini, con particolare attenzione ai settori dei trasporti e della sanità, attraverso la protezione degli asset, delle infrastrutture IT e dei sistemi posti alla base dell'erogazione di suddetti servizi da minacce di natura cyber;
f. l'Agenzia per la Cybersicurezza Nazionale, nell'ambito della quale è istituito il CSIRT Italia, ha adottato le "Linee Guida per la realizzazione di CSIRT", prot. n. 21392 del 07/08/2023, come aggiornate in data 24 luglio 2024, rivolte alle organizzazioni orientate ad istituire o potenziare un Cyber Security Incident Response Team (CSIRT) seguendo le migliori prassi e standard internazionali e definendo i requisiti di squadre di pronto intervento informatico dedicate al rilevamento, all'analisi e alla risposta degli incidenti di sicurezza informatica, nonché ad attività di prevenzione e mitigazione del rischio cyber;

g. i CSIRT regionali si pongono come strutture istituite e operanti sul territorio con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell'ambito del dominio costituito dalle Pubbliche Amministrazioni Locali (PAL);
h. le attività critiche dei CSIRT regionali comprendono, limitatamente alle proprie costituency, una serie di servizi, tra cui:
   - fornire supporto nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
   - agevolare la diffusione di informazioni tempestive su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cyber indirizzati a specifici settori e possibili impatti per le PAL e la loro utenza;
   - incentivare a livello locale l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite a livello nazionale;
   - facilitare le attività di prevenzione e monitoraggio sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale, mediante azioni di aggregazione dei servizi per le PAL;
   - collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle PAL in materia di cyber security;
   - accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi.
   - aiutare le PAL a conformarsi alle normative vigenti in materia di sicurezza informatica, come la direttiva europea NIS e NIS2 e il decreto italiano sul perimetro di sicurezza nazionale cibernetica, che prevedono l'obbligo di notifica e di adozione di misure di sicurezza per gli operatori classificati come essenziali o importanti.

RILEVATO altresì che

a. con Delibera di Giunta regionale n. 551 del 24.10.2024 è stato disposto di:
   - prendere atto della Determina dell'Agenzia Nazionale per la Cybersicurezza prot. n. 0030697.30-11-2023 di ammissione a finanziamento del progetto presentato dalla Regione Campania per un importo complessivo pari ad € 1.499.904,60;
   - prendere atto del Decreto del Presidente del Consiglio dei Ministri del 8 luglio 2024 recante la *"Ripartizione del Fondo per l'attuazione della strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza"* di ammissione a finanziamento del progetto presentato dalla Regione Campania per un importo complessivo pari ad € 14.000.000;
   - prendere atto del documento "Tech Strategy Regionale sulla Cybersecurity" allegato alla presente deliberazione a costituirne parte integrante e sostanziale;
   - di istituire il Computer Security Incident Response Team (CSIRT) della Regione Campania demandando all'Ufficio speciale per la crescita e la transizione digitale, anche in qualità di RTD dell'Ente, tutti gli adempimenti necessari per l'attivazione del CSIRT nonché, le modalità di integrazione per lo svolgimento delle funzioni regionali assegnate in qualità di Autorità di settore dalla disciplina NIS;
   - di stabilire che il CSIRT, in fase di avvio, svolga la propria attività con riferimento alle strutture della Regione Campania, con possibilità futura di integrare ed ampliare la realizzazione di un servizio a supporto del territorio nella prevenzione e risposta agli incidenti di sicurezza informatica, operando in un'ottica di filiera, con tutti gli Enti del territorio regionale;
   - di individuare, ai sensi della Legge 28 giugno 2024, n. 90 art. 8 "Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza", l'Ufficio Speciale per la crescita e la transizione digitale quale struttura responsabile della gestione e del coordinamento della sicurezza informatica;
   - di demandare all'Ufficio speciale per la crescita e la transizione digitale l'individuazione della struttura di governo, le tecnologie, la precisazione dei servizi inclusi nella soluzione di CERT Regionale, dei ruoli

e delle tempistiche di attuazione, la definizione della constituency, delle competenze e professionalità, delle responsabilità e modalità di funzionamento del modello organizzativo, dei processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, delle regola e dei costi di gestione annuali, dei modelli di adesione e di partecipazione alla spesa;

b. con Decreto Dirigenziale n. 379 del 30/12/2024 sono stati approvati i seguenti documenti:
   - PG617871 del 30.12.2024_CSIRT_MACON_ID_01 - Mandato del CSIRT e Constituency
   - PG617875 del 30.12.2024_CSIRT_ORGAN_ID_01 - Modello Organizzativo del CSIRT
   - PG617877 del 30.12.2024_CSIRT_SERVI_ID_01 - Modello di Servizio del CSIRT
   - PG617865 del 30.12.2024_CSIRT_AUDIT_PR_01 - Procedura di Gestione degli Audit
   - PG617883 del 30.12.2024_CSIRT_COMUN_PR_01 - Procedura di Comunicazione interna ed esterna;

c. Con Decreto Dirigenziale n. 224 del 13/0572025 è stata approvata la versione 2.0 dei seguenti documenti, allegati al presente provvedimento a costituirne parte integrante e sostanziale:
   - PG/2025/0235700 del 12.05.2025_CSIRT_MACON_ID_01 - Mandato del CSIRT e Constituency
   - PG/2025/0235704 del 12.05.2025_CSIRT_ORGAN_ID_01 - Modello Organizzativo del CSIRT
   - PG/2025/0235705 del 12.05.2025_CSIRT_SERVI_ID_01 - Modello di Servizio del CSIRT
   - PG/2025/0235692 del 12.05.2025_CSIRT_AUDIT_PR_01 - Procedura di Gestione degli Audit
   - PG/2025/0235698 del 12.05.2025_CSIRT_COMUN_PR_01 - Procedura di Comunicazione interna ed esterna;

CONSIDERATO che

a. a seguito della precedente approvazione della documentazione tecnica funzionale all'avvio del CSIRT regionale aggiornata con Decreto Dirigenziale n. 224 del 13/05/2025 (versione 2.0), si è reso necessario un ulteriore e più ampio aggiornamento e potenziamento del corpus documentale del CSIRT Regione Campania, in linea con:
   - l'evoluzione dei requisiti operativi e normativi nazionali (Direttiva NIS2, Strategia Nazionale di Cybersicurezza, Linee Guida ACN);
   - la crescente complessità degli scenari di rischio cyber, che richiedono strumenti più dettagliati per la risposta agli incidenti;
   - la necessità di formalizzare procedure operative specifiche e playbook di risposta per tipologie concrete di attacco;

b. i nuovi documenti, allegati al presente provvedimento, rafforzano e completano l'impianto organizzativo e tecnico del CSIRT regionale, articolandosi in:

   - procedure operative e gestionali per la classificazione delle informazioni, la comunicazione, la gestione degli incidenti e delle crisi, il monitoraggio delle fonti informative e la condivisione informativa (infosharing);
   - policy specialistiche in ambito di gestione delle chiavi crittografiche;
   - strumenti formativi e di sensibilizzazione, come la procedura di training e awareness;
   - playbook tecnici dedicati alle principali minacce informatiche (phishing, DDoS, ransomware, web attack), utili a standardizzare e velocizzare le risposte operative del CSIRT;
   - documentazione descrittiva, come l'RFC 2350, che rappresenta il profilo ufficiale del CSIRT Regione Campania in conformità agli standard internazionali.

c. tali documenti costituiscono un corpus strutturato, coerente con gli standard europei e nazionali, in grado di supportare operativamente il funzionamento del CSIRT e rafforzare la resilienza cyber dell'Ente e, in prospettiva, del territorio regionale.

RITENUTO

a. di dover approvare i seguenti documenti, benché non materialmente allegati, che costituiscono parte integrante e sostanziale del presente atto, in quanto rappresentano il necessario aggiornamento e ampliamento della documentazione tecnica di riferimento del CSIRT Regione Campania:
   - PG353560_15.07.2025 Procedura di Training e Awareness
   - PG353565_15.07.2025 Procedura di Classificazione delle Informazioni
   - PG353575_15.07.2025 Procedura di Comunicazione interna ed esterna
   - PG353583_15.07.2025 Policy di Gestione delle Chiavi Crittografiche
   - PG353593_15.07.2025 Classificazione Incidenti di Sicurezza
   - PG353614_15.07.2025 Procedura di Gestione degli Eventi e Incidenti di sicurezza
   - PG353625_15.07.2025 Procedura di Infosharing
   - PG353774_15.07.2025 Procedura di Gestione e Monitoraggio delle Informazioni e delle Fonti
   - PG354074_15.07.2025 Playbook DDoS
   - PG354102_15.07.2025 Playbook Phishing
   - PG354122_15.07.2025 Playbook Web Attack
   - PG354305_15.07.2025 Procedura per la Gestione della Crisi
   - PG354315_15.07.2025 Playbook Ransomware
   - PG354333_15.07.2025 RFC 2350 (descrittivo del CSIRT)

VISTI

- tutti gli atti richiamati;
- la Legge 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- il Decreto Legislativo 7 marzo 2005, n. 82 recante "Codice dell'Amministrazione digitale" (CAD) e ss.mm.ii. e relative Regole Tecniche e Linee Guida e disposizioni attuative;
- la legge 24 dicembre 2007, n. 244, "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato";
- il D. Lgs. n. 118/2011 "Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42";
- il D. Lgs. n°33 del 14 marzo 2013 - Attuazione della Trasparenza Amministrativa;
- l'articolo 1, comma 513, della legge 28 dicembre 2015, n. 208;
- il Decreto Legislativo 31 marzo 2023, n. 36 recante "Codice dei contratti pubblici";
- la L. R. 23/2017, "Regione Campania Casa di Vetro. Legge Annuale di Semplificazione 2017";
- il Regolamento Regionale n. 5 del 7 giugno 2018, "Regolamento di Contabilità Regionale in attuazione dell'articolo 10 della legge regionale 5 dicembre 2017 n. 37";
- la deliberazione della Giunta regionale della Campania n. 90 del 09 marzo 2021 con cui è stato approvato il Codice di comportamento, pubblicata sul Bollettino Ufficiale della Regione Campania n. 24 del 15 marzo 2021;
- il Decreto del Presidente della Giunta Regionale n. 72 del 14 aprile 2021 con il quale è stato conferito al dott. Massimo Bisogno l'incarico di Responsabile dell'Ufficio Speciale per la Crescita e la Transizione Digitale;
- Legge regionale 30 dicembre 2024, n. 25 "Disposizioni per la formazione del bilancio di previsione finanziario per il triennio 2025-2027 della Regione Campania - Legge di stabilità regionale per il 2025;
- Legge regionale 30 dicembre 2024, n. 26 "Bilancio di previsione finanziario per il triennio 2025-2027 della Regione Campania";
- Delibera di Giunta regionale n. 773 del 27/12/2024 " Documento Tecnico di Accompagnamento al Bilancio di previsione 2025/2027";

- Delibera di Giunta regionale n. 1 del 07/01/2025 "Approvazione Bilancio gestionale 2025/2027 - Determinazioni ".
- Delibera di Giunta Regionale n. 188 del 23/04/2024 - Funzioni dirigenziali. Determinazioni;
- Delibera di Giunta Regionale n. 370 del 25/07/2024 - Funzioni dirigenziali. Determinazioni;
- Delibera di Giunta Regionale n. 763 del 27/12/2024 - "Funzioni dirigenziali. Determinazioni"
- Delibera di Giunta Regionale n. 105/2025 - Funzioni dirigenziali. Determinazioni"
- Delibera di Giunta Regionale n. 227/2025 - Funzioni dirigenziali. Determinazioni"
- Delibera di Giunta Regionale n. 369/2025 - Funzioni dirigenziali. Determinazioni"
- Tutti gli atti richiamati

alla stregua dell'istruttoria compiuta dall'Ufficio Speciale per la crescita e la transizione digitale, nonché dell'espressa dichiarazione di regolarità formale del presente atto resa dal Direttore dell'Ufficio Speciale per la Crescita e la Transizione digitale

DECRETA

Per i motivi espressi in narrativa che qui si intendono integralmente riportati e confermati:

1. di approvare i seguenti documenti, benché non materialmente allegati, che costituiscono parte integrante e sostanziale del presente atto, in quanto rappresentano il necessario aggiornamento e ampliamento della documentazione tecnica di riferimento del CSIRT Regione Campania:
   - PG353560_15.07.2025 Procedura di Training e Awareness
   - PG353565_15.07.2025 Procedura di Classificazione delle Informazioni
   - PG353575_15.07.2025 Procedura di Comunicazione interna ed esterna
   - PG353583_15.07.2025 Policy di Gestione delle Chiavi Crittografiche
   - PG353593_15.07.2025 Classificazione Incidenti di Sicurezza
   - PG353614_15.07.2025 Procedura di Gestione degli Eventi e Incidenti di sicurezza
   - PG353625_15.07.2025 Procedura di Infosharing
   - PG353774_15.07.2025 Procedura di Gestione e Monitoraggio delle Informazioni e delle Fonti
   - PG354074_15.07.2025 Playbook DDoS
   - PG354102_15.07.2025 Playbook Phishing
   - PG354122_15.07.2025 Playbook Web Attack
   - PG354305_15.07.2025 Procedura per la Gestione della Crisi
   - PG354315_15.07.2025 Playbook Ransomware
   - PG354333_15.07.2025 RFC 2350 (descrittivo del CSIRT)
2. di dare atto che il provvedimento in questione non è soggetto alla pubblicazione in attuazione del disposto del D. Lgs. 33/2013;
3. di inviare il presente provvedimento al Gabinetto del Presidente, all'Ufficio competente per la pubblicazione nella Sezione relativa agli adempimenti previsti dalla L.R. n. 23 del 28/07/2017 "Regione Campania Casa di Vetro" e nella "sezione trasparenza" del sito istituzionale della Regione Campania.

DOTT. MASSIMO BISOGNO