R E G I O N E C A L A B R I A
G I U N T A R E G I O N A L E

Deliberazione n. 784 della seduta del 28 dicembre 2023.

Oggetto: APPROVAZIONE PIANO STRATEGICO DI CYBERSECURITY 2024 – 2027.

Presidente e/o Assessore/i Proponente/i: f.to Dott. Filippo Pietropaolo

Relatore (se diverso dal proponente): _____ (*timbro e firma*) **_____**

Dirigente/i Generale/i: f.to Dott. Tommaso Calabrò

Dirigente di Settore: f.to Ing. Alfredo Pellicanò

Alla trattazione dell'argomento in oggetto partecipano:

			Presente	Assente
1	**ROBERTO OCCHIUTO**	**Presidente**	X	
2	**GIUSEPPINA PRINCI**	**Vice Presidente**	X	
3	**GIOVANNI CALABRESE**	**Componente**	X	
4	**GIANLUCA GALLO**	**Componente**	X	
5	**MARCELLO MINENNA**	**Componente**	X	
6	**FILIPPO PIETROPAOLO**	**Componente**	X	
7	**EMMA STAINE**	**Componente**	X	
8	**ROSARIO VARI'**	**Componente**	X	

Assiste il Segretario Generale della Giunta Regionale.

La delibera si compone di n. 5 pagine compreso il frontespizio e di n. 2 allegati.

Il Dirigente Generale del Dipartimento Bilancio
conferma la compatibilità finanziaria del presente provvedimento
con nota n°580842 del 27 dicembre 2023

LA GIUNTA REGIONALE

PREMESSO CHE:

- Il Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e s.m.i.) ha tracciato il quadro normativo entro cui deve attuarsi la digitalizzazione della Pubblica Amministrazione. Le successive modifiche introdotte dal D.L. 235/2010, hanno poi avviato un ulteriore processo verso una PA moderna, digitale e sburocratizzata;
- Il Codice dell'Amministrazione Digitale, adottato con il Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. (comunemente indicato con l'acronimo CAD), è un atto normativo avente forza di legge, adottato dal Governo italiano sulla base della delega contenuta nell'art. 10 della Legge 29 luglio 2003, n. 229 che raccoglie, in maniera organica e sistematica le disposizioni relative all'utilizzo degli strumenti e delle tecnologie telematiche e della comunicazione nella pubblica amministrazione. In particolare, il CAD mette l'accento sulla capacità delle nuove tecnologie di porsi come strumento privilegiato di dialogo con i cittadini. Il CAD, inoltre, contiene importanti norme che si rivolgono anche ai privati soprattutto per quanto riguarda l'utilizzo della PEC, i documenti informatici e le firme elettroniche. Nel corso del tempo il CAD è stato oggetto di numerosi interventi normativi che ne hanno modificato il contenuto adeguandolo al progresso tecnologico ed alle esigenze emerse in sede applicativa;
- Alcune importanti novità nel Codice dell'Amministrazione Digitale e, in generale, nella normativa che governa il processo di transizione al digitale sono state introdotte dal Decreto Semplificazioni – D.L. 76/2020 - dove vengono intese come una analisi e un cambiamento di radicate modalità lavorative;
- All'interno del Codice, la tematica della sicurezza costituisce un problema immanente, con il quale tutti gli istituti disciplinati devono confrontarsi; in particolare, l'art. 51 del CAD, rubricato "Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", prescrive all'Agenzia per l'Italia Digitale, al comma 1, il compito di adottare Linee Guida, ai sensi dell'art. 71 del CAD, al fine di individuare le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità, la riservatezza dei dati e anche la continuità operativa dei sistemi e delle infrastrutture.

VISTI:

- il decreto legislativo 18 maggio 2018, n. 65 recante "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (direttiva NIS);
- il Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (cd. "Cybersecurity Act");
- il decreto-legge 21 settembre 2019, n. 105 recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 133;
- la legge del 18 novembre 2019, n. 133 convertita, con modificazioni, dal decreto-legge 21 settembre 2019, n. 105, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica";
- il decreto-legge 19 luglio 2020, n. 76, che ha fornito impulso alla digitalizzazione della PA prevedendo che la stessa avvenga osservando i principi di sicurezza cibernetica compresa la formazione del personale e la promozione della consapevolezza circa l'importanza della sicurezza informatica;
- il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione

dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" che prevede l'istituzione dell'Agenzia a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;

- l'articolo 7, comma 1, lettere m) e n), del suddetto decreto-legge n. 82 del 2021, che hanno attribuito all'Agenzia per la Cybersicurezza Nazionale tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale e i compiti di cui all'articolo 33-septies, comma 4, del Decreto Legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221, nonché la responsabilità di sviluppare "capacità nazionali di prevenzione, monitoraggio, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici […]";
- l'articolo 7, comma 1, lettera t), del suddetto decreto-legge n. 82 del 2021, che individua l'Agenzia quale autorità che "promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza nazionale e dei correlati servizi applicativi […]";
- il decreto legislativo 8 novembre 2021, n. 207, di attuazione della Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche e disciplina, tra l'altro, i requisiti di cybersicurezza delle reti pubbliche di comunicazione o dei servizi di comunicazione elettronica accessibili al pubblico, l'obbligo di notifica di incidenti significativi, nonché l'adozione di misure di sicurezza, attribuendo la competenza in materia all'ACN;
- il decreto-legge 21 marzo 2022, n. 21, che ha recato, tra le varie, disposizioni sulla ridefinizione dei poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché di ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud. In particolare, ha ridefinito gli obblighi e le procedure di notifica da parte delle imprese interessate, nonché le procedure di esercizio dei poteri speciali, di monitoraggio e sanzionatori da parte del Governo, prevedendo la partecipazione dell'Agenzia Nazionale per la Cybersicurezza Nazionale, di avvalersi anche del Centro di Valutazione e Certificazione Nazionale (CVCN) e la possibilità di condurre attività ispettive e di verifica;
- la Direttiva (UE) 2022/2555 (direttiva NIS 2) del Parlamento europeo e del Consiglio del 14 dicembre 2022 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, che dovrà essere recepita dagli Stati Membri entro il 18/10/2024;
- il Piano Triennale per l'informatica nella PA 2022-2024, approvato con decreto del Presidente del Consiglio dei Ministri del 22 dicembre 2022;
- la Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di Implementazione che 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.

CONSIDERATO CHE:

- Il Piano Triennale per l'Informatica nella Pubblica Amministrazione nella versione aggiornata 2022-2024 riporta (capitolo 6) tutti i riferimenti e la roadmap che le PA dovranno seguire per la compliance in termini di sicurezza informatica e fà esplicito riferimento alla direttiva NIS 2 anche per le Regioni:'…Benché alle citate Amministrazioni, centrali e regionali, non si applichino le sanzioni previste dalla Direttiva, esse sono soggette agli stessi obblighi previsti per gli altri soggetti essenziali/importanti contemplati dalla Direttiva NIS 2';

- Per attuare la strategia nazionale, come previsto dal Piano triennale per l'informatica nella PA, ogni amministrazione deve predisporre un proprio documento strategico, quali sono le Linee Guida per la Crescita Digitale della Regione Calabria 2022 – 2025, approvate con DGR 413 del 1° settembre 2022;
- In attuazione di quanto previsto dal decreto NIS (d.lgs 18 maggio 2018, n. 65) e dal D.L.82/2021 il 18 Maggio 2022 il Comitato Intermnisteriale per la Cybersicurezza (CIC) ha approvato la Strategia Nazionale per la Cybersicurezza (2022-2026) elaborato dall'ACN Agenzia per la Cybersicurezza Nazionale. Nel piano è stato tracciato, tra l'altro, il coinvolgimento delle pubbliche amministrazioni territoriali come Regioni e Province autonome in alcune tra le 82 misure previste per la sua implementazione;
- È necessario, pertanto delineare un piano strategico in ambito cybersecurity della Regione Calabria individuando l'insieme degli indirizzi per gli interventi da attuare nel breve, medio e lungo termine necessari per il potenziamento delle capacità cyber dell'Ente stesso al fine di contribuire al raggiungimento anche degli obiettivi delle "Linee Guida per la Crescita Digitale della Regione Calabria 2022 – 2025" ed assicurare una transizione digitale cyber resiliente;
- Il Piano Strategico di Cybersecurity 2024 – 2027 contribuisce alla definizione ed attuazione delle linee strategiche della Regione Calabria in ambito cybersecurity, perseguendo la crescita digitale in un'ottica di sistema, e realizzando una transizione digitale cyber resiliente attraverso un rinnovato approccio alla cybersecurity che consentirà di potenziare le capacità cyber dell'Ente per affrontare efficacemente le nuove sfide della sicurezza informatica; in particolare, il Piano contribuisce ad acquisire visibilità, continuativa, sulle minacce informatiche, gestire i rischi cyber in modo sostenibile e favorire la diffusione di una cultura della cybersicurezza.

CONSIDERATO ALTRESÌ il quadro socioeconomico attuale, la situazione derivante all'emergenza COVID-19 e le conseguenti misure legislative introdotte dal Governo per garantire e sostenere la ripartenza del Paese, le quali prevedono interventi anche in ambito digitale con significative modificazioni normative e strategiche e che la sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021 e definitivamente approvato il 13 luglio 2021.

PRESO ATTO della necessità di definire il Piano Strategico di Cybersecurity che individui le linee di indirizzo per gli interventi che la Regione Calabria dovrà realizzare nel breve, medio, lungo termine per l'attuazione della propria strategia di cybersicurezza nell'ambito della strategia di crescita digitale;

RITENUTO che il Piano Strategico di Cybersecurity 2024 – 2027 rappresenta per la Regione Calabria uno strumento essenziale di indirizzo strategico in ambito cybersecurity contenente l'insieme di interventi necessari per il potenziamento delle capacità cyber dell'Ente stesso, al fine di assicurare una transizione digitale cyber resiliente;

VISTI
- Lo Statuto della Regione Calabria;
- La L.R. n. 7 del 13 maggio 1996 recante "Norme sull'ordinamento della struttura organizzativa della Giunta Regionale e sulla dirigenza regionale" ed in particolare l'art.28 che individua compiti e responsabilità del Dirigente con funzioni di Dirigente Generale;
- Il D.P.G.R. n. 354 del 21 giugno 1999 del Presidente della Giunta Regionale recante "separazione dell'attività amministrativa di indirizzo e di controllo da quella di gestione", rettificato con D.P.G.R. n. 206 del 15 dicembre 2000;
- La D.G.R. n. 2661 del 21 giugno 1999 recante "Adeguamento delle norme legislative e regolamentari in vigore per l'attuazione delle disposizioni recate dalla L.R. 7/96 e dal D.lgs. 29/93 e successive modifiche e integrazioni";
- La vigente Struttura della Giunta Regionale di cui al Regolamento Regionale n.12/2022 come, da ultimo modificato, con Regolamento Regionale del 15 dicembre 2023 n. 15;

- la D.G.R. 122 del 31/3/2023 avente ad oggetto “Modifica D.G.R. n. 532 del 10.11.2017” , la Regione Calabria che ha disposto, tra l’ altro, di confermare le funzioni del RTD nel Dirigente Generale pro tempore del Dipartimento Transizione Digitale ed Attività Strategiche;

PRESO ATTO

- Che il Dirigente Generale ed il Dirigente di Settore del Dipartimento proponente attestano che l’istruttoria è completa e che sono stati acquisiti tutti gli atti e i documenti previsti dalle disposizioni di legge e di regolamento che disciplinano la materia.
- Che il Dirigente Generale ed il Dirigente di Settore del Dipartimento proponente ai sensi dell’art. 28, comma 2, lett. a, e dell’art. 30, comma 1, lett. a, della legge regionale 13 maggio 1996 n. 7, sulla scorta dell’istruttoria effettuata, attestano la regolarità amministrativa nonché la legittimità della deliberazione e la sua conformità alle disposizioni di legge e di regolamento comunitarie, nazionali e regionali, ai sensi della normativa vigente e del disciplinare dei lavori di Giunta approvato con D.G.R. n. 17/2020.
- Che il Dirigente Generale ed il Dirigente di Settore del Dipartimento proponente attestano che il presente provvedimento non comporta oneri a carico del bilancio annuale e/o pluriennale della Regione, in quanto di natura programmatica

SU PROPOSTA dell’Assessore Filippo Pietropaolo, con delega alla Transizione Digitale, a voti unanimi.

DELIBERA

1. di approvare il **Piano Strategico di Cybersecurity 2024** – **2027**, quale parte integrante e sostanziale della presente Deliberazione, che costituisce lo strumento di indirizzo strategico in ambito cybersecurity della Regione Calabria, individuando le linee di indirizzo per gli interventi da attuare nel breve, medio e lungo termine per potenziare le capacità cyber dell’Ente e supportare il raggiungimento degli obiettivi di crescita digitale per una digitalizzazione sicura e resiliente;

2. di demandare al Dipartimento Transizione Digitale e Attività Strategiche ogni atto consequenziale, adempimento tecnico e atto amministrativo funzionali all’attuazione del Piano Strategico di Cybersecurity 2024 ‐ 2027;

3. di notificare il presente provvedimento a cura del Dipartimento proponente a tutti i Dipartimenti regionali interessati;

4. di disporre, a cura del Dirigente Generale del Dipartimento proponente, la pubblicazione del provvedimento sul BURC, ai sensi della legge regionale 6 aprile 2011 n. 11 e nel rispetto del Regolamento UE 2016/679, e la contestuale pubblicazione sul sito istituzionale della Regione, ai sensi del d.lgs. 14 marzo 2013 n. 33 (laddove prevista), della legge regionale 6 aprile 2011 n.11 e nel rispetto del Regolamento UE 2016/679.

IL SEGRETARIO GENERALE
f.to MONTILLA

IL PRESIDENTE
f.to OCCHIUTO