CONSIGLIO REGIONALE DELLA SARDEGNA

UFFICIO DI PRESIDENZA

DELIBERAZIONE in seduta del 23 ottobre 2025, N. 74

Oggetto: Individuazione struttura e conferimento incarico di "Referente" per la cybersicurezza ai sensi dell'art. 8 della L. 90/24 e conferma dell'individuazione del "Punto di contatto" ai sensi dell'art. 7 del D.Lgs. 138/24

PRESIEDE l'On. Giampietro COMANDINI - Presidente del Consiglio

Sono presenti:

On. Giampietro COMANDINI	*- Presidente del Consiglio*
On. Giuseppe FRAU	*- Vice Presidente del Consiglio*
On. Aldo SALARIS	*- Vice Presidente del Consiglio*
On. Lorenzo COZZOLINO	*- Questore del Consiglio*
On. Emanuele MATTA	*- Segretario del Consiglio*
On. Ivan PIRAS	*- Segretario del Consiglio*

Sono assenti:

On. Giuseppe Marco DESSENA	*- Questore del Consiglio*
On. Gianluigi RUBIU	*- Questore del Consiglio*
On. Giuseppino CANU	*- Segretario del Consiglio*
On. Ivan PINTUS	*- Segretario del Consiglio*
On. Alberto URPI	*- Segretario del Consiglio*

SEGRETARIO: Dott. Danilo FADDA *Segretario Generale del Consiglio*

TESTO DELLA DELIBERAZIONE

L'UFFICIO DI PRESIDENZA

VISTO l'articolo 19 della legge costituzionale 26 febbraio 1948, n. 3, recante lo Statuto speciale per la Sardegna e ss.mm.ii.;

VISTI gli articoli 11 e 131 del Regolamento interno del Consiglio regionale;

VISTO il Regolamento dei Servizi del Consiglio regionale, approvato con deliberazione n. 127 del 20 luglio 2016 e ss.mm.ii.;

VISTO il Regolamento interno di disciplina dell'organizzazione e del funzionamento del Collegio dei Questori e dell'Ufficio di Presidenza approvato dall'Ufficio di Presidenza con deliberazione n. 4 del 21 maggio 2024;

VISTO il Regolamento del personale consiliare come modificato dalla deliberazione n. 101 del 3 dicembre 2020;

PREMESSO che:

la digitalizzazione della Pubblica Amministrazione ha garantito un deciso miglioramento della qualità dei servizi pubblici offerti, ma ha esposto la stessa a nuovi rischi e minacce da affrontare. La P.A. custodisce un ampio patrimonio di informazioni e dati personali ed eroga servizi importanti ed essenziali che è fondamentale proteggere con tecnologie idonee, con l'adozione di processi e politiche di sicurezza solidi, con lo sviluppo costante di competenze;

le contingenze in ambito nazionale e internazionale - dalla superata emergenza sanitaria, ai più recenti conflitti bellici, ai continui e attuali attacchi informatici nei confronti di istituzioni nazionali pubbliche e private che assicurano l'erogazione di servizi essenziali o critici (es: energetici, finanziari, informativi) - hanno contribuito a catalizzare l'attenzione dei legislatori, nazionale e sovranazionale, sulla cybersecurity nella consapevolezza che essa non costituisce solo un fattore di regolamentazione utile allo sviluppo di un mercato digitale unico, ma anche una strategia fondamentale per provvedere alla sicurezza degli Stati nazionali;

il quadro normativo nazionale in materia di cybersecurity ha visto nel corso del 2024 una significativa evoluzione imputabile a una azione del Legislatore improntata ad affrontare il complesso quadro dei rischi e dei gravi incidenti informatici verificatisi a nocumento di importanti Istituzioni ed Enti per mano terza;

PRESO ATTO che la recente legge n. 90 del 28 giugno 2024 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" contiene importanti adempimenti per le pubbliche amministrazioni rientranti nel perimetro di applicazione e risponde alla ratio di

rafforzare la sensibilità e la protezione dei predetti soggetti rispetto ai rischi informatici aventi impatto su reti, sistemi informativi e servizi informatici;

VALUTATO che il decreto legislativo 4 settembre 2024 n.138, "Recepimento della direttiva (UE) 14/12/2022, n. 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", recepisce la Direttiva c.d. **NIS 2** *(Network and Information Security),* completando il percorso di adeguamento dell'ordinamento interno alla normativa euro-unitaria;

CONSIDERATO che le due normative hanno un carattere complementare, in alcuni ambiti dispongono in modo convergente, a volte in modo simile o identico. In particolare, ai fini del presente provvedimento si evidenzia che entrambe stabiliscono un obbligo di notifica degli "incidenti informatici" in un tempo contingentato a pena di sanzioni; obblighi in tema di governance e gestione del rischio cyber con la individuazione di ruoli chiari e definiti nell'ambito di ciascuna organizzazione, tra i quali si evidenzia, in questa sede, il ruolo del soggetto incaricato di notificare gli incidenti alle autorità preposte, nelle forme e nei tempi previsti dalla normativa;

VALUTATO inoltre che la legge 28 giugno 2024, n. 90 prevede:

l'obbligo di segnalazione e notifica a CSIRT *(Computer Security Incident Response Team)* istituito presso l'Agenzia per la Cybersecurity, degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici e l'adozione tempestiva degli interventi risolutivi segnalati dall'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità;

l'individuazione di una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che sviluppi politiche e procedure di sicurezza delle informazioni e che produca un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

CONSIDERATO CHE dovere degli enti è quello di segnalare senza ritardo, entro termini massimi - o di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute - qualunque incidente riconducibile alle tipologie per cui è previsto l'obbligo di segnalazione e che la segnalazione e la successiva notifica sono effettuate tramite le

apposite procedure stabilite da ACN (Agenzia per la Cybersicurezza Nazionale);

VERIFICATO che al comma 3 dell'articolo 7 della legge 28 giugno 2024, n. 90, si prevede inoltre 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 previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.";

CONSIDERATO che il decreto legislativo 4 settembre 2024, n. 138, introduce una rilevante novità in tema di governane della cybersecurity, ossia l'estensione della responsabilità per inosservanza degli obblighi in capo agli organi di amministrazione e direttivi delle pubbliche amministrazioni rientranti nel suo perimetro di applicazione;

VALUTATO che gli organi di amministrazione e gli organi direttivi approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, sovrintendono all'implementazione degli obblighi, sono tenuti a seguire una formazione in materia di sicurezza informatica e promuovono l'offerta periodica di una formazione ai dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti, al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti;

VISTO che il D.lgs. 138/24 impone di individuare almeno un "punto di contatto" tra il singolo ente e l'ACN, quale anello di congiunzione tra il soggetto NIS e l'Autorità che monitora il corretto adempimento delle misure di governance e gestione del rischio da incidente informatico. Che, nello specifico, l'art. 7, rubricato "Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti", sancisce l'obbligo anche per la PA della registrazione e aggiornamento della stessa sulla piattaforma digitale resa disponibile dall'Autorità nazione competente **NIS,** e richiede in fase di registrazione specifici dati identificativi e di contatto dell'ente e "la 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";

PRECISATO che

- in fase di prima applicazione del Decreto la scadenza per completare la registrazione era prevista entro il 28 febbraio 2025;
- entro il 31 marzo 2025 l'Autorità nazionale competente in materia di **NIS,** ha provveduto a redigere l'elenco dei soggetti essenziali e dei soggetti importanti, sulla base delle registrazioni avvenute per la

successiva definizione di un quadro di misure di sicurezza differenziato e proporzionato alla strategicità dell'ambito in cui i soggetti operano;

- con Determinazione del Direttore generale di ACN prot. n. 38565 del 26 novembre 2024, sono stati stabiliti modalità di utilizzo e accesso al Portale ACN e, in particolare, ai Servizi NIS, nonché le ulteriori informazioni che i soggetti NIS devono fornire all'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni attribuite dal decreto NIS;
- l'art. 4 della Determinazione del Direttore generale di ACN, definisce, al comma 1, la figura del "Punto di contatto" come "una persona fisica designata dal soggetto NIS con il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso. In particolare, il punto di contatto accede al Portale ACN e ai Servizi NIS, effettua, per conto del soggetto, la registrazione di cui all'articolo 7 del decreto **NIS,** e interloquisce, per conto del soggetto **NIS,** con l'Autorità nazionale competente **NIS.";**
- sempre l'art. 4 della Determinazione del Direttore generale di **ACN,** al comma 7, afferma che "La designazione del punto di contatto da parte dei soggetti di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90, che rientrano nell'ambito di applicazione del decreto NIS, può soddisfare l'obbligo di nomina e comunicazione del referente per la cybersicurezza di cui all'articolo 8, comma 2, della medesima legge."

VERIFICATO che con comunicazione ns prot. 4211/2025 l'ACN comunicava alla Amministrazione del Consiglio regionale della Sardegna: «In relazione alla dichiarazione DNISA00017214, preso atto delle valutazioni dell'Autorità di settore NIS interessata, si comunica che con la Determinazione del Direttore Generale n. 136430 del 12 aprile 2025, codesta organizzazione Consiglio regionale della Sardegna (92027820924) è stata individuata quale soggetto *Importante* in relazione alla/e tipologia/e di soggetto di seguito indicata/e.

1. Amministrazioni centrali, regionali, locali e di altro tipo (allegato lii);

1.1. Regioni e Province autonome;

Si rende noto, altresì, che a codesta organizzazione è stato attribuito il codice identificativo ITW2DGUY che dovrà essere utilizzato in occasione di tutte le comunicazioni con questa Autorità»;

RITENUTO che le attività relative alla sicurezza informatica, riguardano azioni e strategie che richiedono una organica visione prospettica e di insieme e coinvolgono aspetti fondamentali dell'assetto organizzativo dell'Amministrazione consiliare che sono all'esame della stessa al fine di elaborare, nel lungo periodo, soluzioni ottimali;

CONSIDERATO che il Regolamento dei Servizi del Consiglio regionale della Sardegna, approvato con Deliberazione dell'Ufficio di Presidenza n. 127 del 20 luglio 2016 e s.m.i., conferisce al Segretario generale, vertice amministrativo, il compito di assicurare l'unità di indirizzo dell'Amministrazione in conformità agli obiettivi indicati dagli organi politici del Consiglio;

PRESO ATTO della proposta, formulata dal Segretario generale nel corso della seduta, di attribuire al Dott. Michele Sias, Vice Segretario generale e Capo del Servizio Amministrazione - nominato Responsabile della Transizione Digitale dall'Ufficio di Presidenza con deliberazione numero 40 del 30 gennaio 2025 – il ruolo di "Referente" per la cybersicurezza ai sensi dell'art. 8 della L. 90/24 e di confermare il medesimo quale "Punto di contatto" ai sensi dell'art. 7 del D.Lgs. 138/24;

VISTI il curriculum, lo stato di servizio, i provvedimenti di nomina del Referendario consiliare dott. Michele Sias a Vice Segretario generale e a Capo del Servizio Amministrazione, nonché la dichiarazione di insussistenza di cause di inconferibilità e di incompatibilità di incarichi resa dallo stesso dott. Sias;

RITENUTO, pertanto, di nominare il dott. Michele Sias quale "Referente" per la cybersicurezza ai sensi dell'art. 8 della L. 90/24 e, nel contempo, di confermarne l'individuazione quale "Punto di contatto" ai sensi dell'art. 7 del D.Lgs. 138/24;

PRESO ATTO del parere favorevole del Segretario Generale,

DELIBERA

Art. 1
Nomina di Referente per la cybersicurezza

1. Il dott. Michele Sias è nominato, ai sensi dell'articolo 8 della L. 90/24 quale "Referente" per la cybersicurezza nell'Amministrazione consiliare.

2. L'incarico di "Referente" per la cybersicurezza conferito al dott. Michele Sias, al pari di quello di Responsabile per la transizione digitale, è differenziato e aggiuntivo ed è assegnato nell'ambito delle funzioni di Vice

Segretario generale. Pertanto, allo stesso non sono connessi ulteriori emolumenti retributivi.

3. Il Segretario Generale è incaricato dell'adozione, d'intesa con il Referente per la cybersicurezza, degli appositi atti organizzativi interni, ai sensi dell'art. 7 del vigente Regolamento dei Servizi, finalizzati alla costituzione di un supporto amministrativo per il Referente per la cybersicurezza, costituito dalle professionalità necessarie per lo svolgimento dei compiti allo stesso attribuiti e in premessa meglio individuati e tipizzati, da individuare presso il Servizio Amministrazione.

Art. 2
Pubblicazione ed entrata in vigore

1. La presente deliberazione è pubblicata sul sito istituzionale del Consiglio regionale della Sardegna sezione "Amministrazione Trasparente", ed entra in vigore il giorno della pubblicazione.

Art.3
Adempimenti consequenziali

1. Il Referente per la cybersicurezza è incaricato di provvedere all'aggiornamento dei dati nelle costituite e costituende piattaforme previste dalle disposizioni normative in materia di cybersicurezza.

EGRET **IL PRESIDENTE**