AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

DELIBERA N. 82/26/CONS

INDIVIDUAZIONE DELLA *GOVERNANCE* PER LA GESTIONE DELLA SICUREZZA INFORMATICA (AI SENSI DEL DECRETO LEGISLATIVO 4 SETTEMBRE 2024, n. 138) E DELLE RELATIVE LINEE DI INDIRIZZO

Nella sua riunione di Consiglio del 25 marzo 2026;

VISTA la legge 14 novembre 1995, n. 481, recante "*Norme per la concorrenza e la regolazione dei servizi di pubblica utilità. Istituzione delle Autorità di regolazione dei servizi di pubblica utilità*";

VISTA la legge 31 luglio 1997, n. 249, recante "*Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo*";

VISTA la legge 7 agosto 1990, n. 241, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";

VISTA la legge 28 giugno 2024, n. 90, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" e, in particolare, l'articolo 8, comma 2, ove è stabilito che "*Presso le strutture di cui al comma 1 opera il referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. Qualora i soggetti di cui all'articolo 1, comma 1, non dispongano di personale dipendente fornito di tali requisiti, possono conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente. Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla presente legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta la medesima amministrazione. A tale fine, il nominativo del referente per la cybersicurezza è comunicato all'Agenzia per la cybersicurezza nazionale*";

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*Recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*" (di seguito, anche "decreto NIS") e in particolare l'articolo 6, comma 1, lettera e) che considera "soggetto essenziale" le pubbliche amministrazioni centrali, tra cui le autorità amministrative indipendenti;

VISTA la delibera n. 223/12/CONS, del 27 aprile 2012, recante "*Adozione del nuovo Regolamento concernente l'organizzazione e il funzionamento dell'Autorità*" (di seguito,

anche "Regolamento"), come modificata, da ultimo, dalla delibera n. 58/25/CONS, del 6 marzo 2025, in particolare gli articoli 21 e 22;

VISTA la delibera n. 201/22/CONS, del 15 giugno 2022, recante "*Organizzazione interna dell'Autorità per le Garanzie nelle Comunicazioni relativa agli adempimenti in materia di trattamento dei dati personali ai sensi dell'articolo 29 del regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e dell'articolo 2-quaterdecies del d.lgs. 30 giugno 2003, n. 196*";

VISTE le Linee guida dell'Agenzia per la cybersicurezza nazionale (di seguito "ACN") del novembre 2024 "*per il rafforzamento della resilienza dei soggetti cui all'articolo 1, comma 1 della Legge 28 giugno 2024, n. 90*" (di seguito Linee guida ACN");

CONSIDERATO che con atto di delega del 23 gennaio 2025, a firma del Presidente, è stato individuato quale "Punto di contatto", ai sensi dell'articolo 7, comma 1, lettera c) del decreto NIS, il Direttore del Servizio Sistemi informativi e digitalizzazione in qualità di Responsabile della cybersicurezza ai sensi della legge 28 giugno 2024, n. 90;

VISTA la delibera n. 204/25/CONS del 30 luglio 2025, recante "*Individuazione della governance per la gestione della sicurezza informatica*";

VISTA la delibera n. 259/25/CONS del 28 ottobre 2025, recante "*Approvazione della politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche*";

VISTA la determinazione ACN n. 379907 del 18 dicembre 2025 "*di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo*", che aggiorna e sostituisce la determinazione ACN n. 164179 del 14 aprile 2025;

VISTA la determinazione ACN n. 250916 del 19 settembre 2025, di cui all'articolo 7, comma 6, del decreto legislativo 4 settembre 2024, n. 138, che "*aggiorna e sostituisce la determinazione ACN n. 283727 del 22 luglio 2025*".

VISTA la determina n. 05/25/SSI del 18 dicembre 2025, recante "*Nomina del referente CSIRT ai sensi dell'articolo 7 della determinazione ACN n. 250916 del 19/09/2025*";

CONSIDERATO che l'Autorità ha completato, tramite il "Punto di contatto", la fase di registrazione richiesta dall'Agenzia per la sicurezza nazionale (di seguito, ACN) ed è stata successivamente individuata - con determinazione ACN n. 136430 del 12 aprile 2025 - quale "soggetto essenziale";

RILEVATO che, nell'ambito degli obblighi individuati dal decreto NIS, come specificati dall'art. 15 comma 1 della determinazione ACN n. 136117 del 10 aprile 2025, il Punto di contatto dei soggetti essenziali, entro il termine del 31 maggio 2025, poi prorogato al 31 luglio con determinazione ACN n. 283727 del 22 luglio 2025, deve

inserire nel portale ACN le informazioni e i dati dei componenti degli "organi di amministrazione e direttivi", ai sensi dell'art. 7, comma 4 del decreto NIS;

CONSIDERATO che la sopra richiamata determinazione, all'articolo 1, comma 1, lettera e), definisce quali "*organi di amministrazione e direttivi*", gli organi di amministrazione e direttivi di cui all'articolo 23 del decreto NIS, ove è chiarito, al comma 1, che: "*a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24; b) sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7; c) sono responsabili delle violazioni di cui al presente decreto*";

CONSIDERATO che l'articolo 31, commi 1 e 2, del decreto NIS prevede che, ai fini dell'attuazione degli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente di cui agli articoli 23, 24, 25, 27, 28 e 29, l'ACN stabilisce obblighi proporzionati, nonché termini, modalità, specifiche e tempi graduali di implementazione, tenuto conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico;

CONSIDERATO, altresì, che l'articolo 40, comma 5, lettera l), del decreto NIS prevede che tali obblighi sono stabiliti con una o più determinazioni dell'ACN e che l'articolo 42, comma 1, lettera c), prevede che in fase di prima applicazione, l'ACN stabilisce le modalità e le specifiche di base per l'adempimento ai predetti obblighi;

CONSIDERATO che le modalità e le specifiche di base sono stabilite, per i "soggetti essenziali", con la determinazione ACN n. 164179 del 14 aprile 2025;

RILEVATO che il decreto NIS prevede come preliminare misura di sicurezza quella relativa alla definizione dell'organizzazione per la sicurezza informatica con individuazione di connessi ruoli e correlate responsabilità, cosiddetta *governance* per la gestione della sicurezza informatica;

RILEVATO l'elevato grado di tecnicismo delle attività inerenti alla sicurezza informatica;

CONSIDERATO che, ai sensi del comma 1 dell'art. 12-*bis* (Funzioni di indirizzo e controllo e funzioni di gestione) del Regolamento "*Salva la competenza degli Organi collegiali ad adottare gli atti previsti dalla legge e dai regolamenti, spettano ai predetti Organi l'indirizzo e il controllo dell'attività amministrativa.*"; mentre, ai sensi del comma 2, "*L'attuazione e la gestione degli indirizzi competono al Segretario generale.*";

CONSIDERATO che alla luce dell'esperienza applicativa si è constatato che i Piani operativi di gestione si sostanziano in misure aventi natura squisitamente tecnica, organizzativa e operativa;

CONSIDERATO, dunque, che le predette misure, in ragione della loro natura tecnica, organizzativa e operativa, sono strettamente afferenti ai ruoli e alle responsabilità dei soggetti che fanno parte della *governance* di gestione della cybersicurezza e non del Consiglio, che è invece titolare delle funzioni di indirizzo e controllo ai sensi dell'art. 12-*bis* del Regolamento;

RITENUTO necessario, pertanto, ridefinire ruoli e responsabilità dei soggetti che fanno parte della *governance*, individuati quali "organi amministravi e direttivi" ai sensi dell'art. 23 del decreto NIS;

RITENUTO, opportuno, sulla base della concreta esperienza applicativa maturata e al fine di garantire una più efficiente applicazione della normativa sulla cybersicurezza, definire con chiarezza il perimetro di competenza tra i soggetti responsabili dell'indirizzo e quelli incaricati della traduzione di tali linee in Piani operativo-amministrativi, in coerenza con la struttura disegnata dal decreto NIS, nonché con i regolamenti interni dell'Autorità;

CONSIDERATO, dunque, che il compito principale della *governance* del sistema di cybersicurezza è quello di tradurre gli indirizzi del Consiglio in Piani di natura operativa-amministrativa e che, pertanto, il Consiglio non può essere qualificato come soggetto che partecipa alla *governance* né, tantomeno, come organo amministravo e direttivo ai sensi del decreto NIS;

CONSIDERATO, altresì, che nella definizione della organizzazione interna occorre garantire che i processi decisionali in situazioni di emergenza siano svolti in tempi rapidi al fine di mitigare i danni;

PRESO ATTO che, in attuazione del decreto NIS, spetta al Consiglio dell'Autorità definire la *governance* della cybersicurezza e impartire indirizzi alla struttura amministrativa;

CONSIDERATO che le Linee guida ACN indirizzano i soggetti destinatari degli obblighi di cui alla legge 28 giugno 2024, n. 90 verso il rafforzamento della propria resilienza tramite l'individuazione di misure di sicurezza minime e fornendo indicazioni per la loro implementazione nel rispetto di quanto previsto all'articolo 8, lettera f), della medesima legge;

CONSIDERATO, in particolare, che l'Autorità è risultata assegnataria del "*Piano strategico degli interventi di potenziamento – AGCOM*" fornito dall'ACN, in conclusione delle attività previste dal Bando 7/2023 nell'ambito dell'Investimento 1.5 – Cybersecurity nell'ambito del PNRR, Missione M1C1 "Digitalizzazione, innovazione e sicurezza nella P.A.";

CONSIDERATO, altresì, che il suddetto Piano descrive in dettaglio gli interventi specifici di potenziamento indicando il relativo tempo di realizzazione e grado di rilevanza, per un totale complessivo di 58 interventi.

RITENUTO opportuno, per una più efficiente attuazione della cybesicurezza individuare quali "organi amministravi e direttivi", di cui all'art. 23 del decreto NIS, il Segretario generale e la *governance* di cui all'art. 2 della presente delibera;

VISTA la proposta del Segretario generale;

UDITA la relazione del Commissario Antonello Giacomelli, relatore ai sensi dell'articolo 31 del "*Regolamento concernente l'organizzazione ed il funzionamento dell'Autorità*";

DELIBERA

Articolo 1

(Disposizioni generali)

1. Nell'esercizio delle sue funzioni di indirizzo, ai sensi dell'art. 12-*bis* del Regolamento, il Consiglio, preso atto delle indicazioni dell'ACN, individua quali "organi amministravi e direttivi", ai sensi dell'art. 23 del decreto NIS, il Segretario generale e i soggetti che partecipano alla *governance* di cui al successivo articolo 2, per l'attuazione delle misure in materia di rafforzamento della cybersicurezza nazionale e di reati informatici tramite specifici Piani operativi di gestione.

2. Il Segretario generale esercita il potere sostitutivo nei confronti dei soggetti che costituiscono la *governance* come indicati nell'articolo 2, in caso di inerzia per la puntuale esecuzione degli adempimenti in materia di cybersicurezza nazionale e di reati informatici.

Articolo 2

(Individuazione della *governance*)

1. Ai sensi dell'art. 23 del decreto NIS, sono individuati quali "organi amministrativi e direttivi" i soggetti che fanno parte della *governance* di gestione della cybersicurezza e sono definite le relative responsabilità.
2. I soggetti che partecipano alla *governance* di gestione della cybersicurezza sono:
   - il Segretario generale;
   - i Vicesegretari generali, ed in particolare il Vicesegretario generale appositamente delegato in materie attinenti alla cybersicurezza, che opera con funzioni di coordinamento e come sostituto del Punto di Contatto;
   - il Responsabile della cybersicurezza;
   - il Punto di Contatto;
   - il Responsabile dell'unità organizzativa di primo livello competente per lo sviluppo e la gestione dell'infrastruttura di rete e dei sistemi informativi (di seguito, anche "Servizio sistemi informativi");
   - i Responsabili delle unità organizzative di primo livello, ove gestiscano direttamente sistemi informativi;
   - il Responsabile dell'unità organizzativa di primo livello competente in materia di acquisizione di beni strumentali e informatici, di servizi software e dei relativi inventari (di seguito, anche "Servizio risorse umane, strumentali e contratti");
   - il Datore di lavoro;
   - il Responsabile della protezione dati personali (di seguito, anche "RPD");
   - il Designato di primo livello.

Articolo 3

(Linee di indirizzo per la gestione del rischio di sicurezza informatica e notifica degli incidenti)

1. Nell'ambito funzioni di indirizzo di cui all'articolo 1, con determina il Segretario generale adotta il Piano operativo di gestione del rischio di sicurezza informatica che individua i programmi di intervento nell'ambito dei quali occorre agire per il rafforzamento della sicurezza informatica e l'individuazione delle relative azioni correttive.

2. Con successive determine il Segretario generale adotta, inoltre, i Piani di cui ai seguenti articoli 4, 5, 6, 7, 8 e 9 del presente provvedimento.

3. Il Piano operativo di gestione del rischio di sicurezza informatica è riesaminato e, se opportuno, adeguato qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Il Piano di gestione del rischio di sicurezza informatica è, comunque, riesaminato con cadenza almeno annuale.

4. Il Responsabile della cybersicurezza riferisce al Segretario generale, con periodicità semestrale, sull'attuazione dei programmi di intervento di cui ai commi 1 e 2. Il Segretario generale informa il Consiglio, con periodicità annuale, sull'efficacia delle misure adottate per la gestione del rischio per la sicurezza informatica.

Articolo 4

(Piano per la gestione e notifica degli incidenti di sicurezza informatica)

1. Con determina il Segretario generale adotta il Piano per la gestione e la notifica al CSIRT Italia degli incidenti di sicurezza informatica, recante i processi interni di gestione degli eventi di sicurezza informatica nelle fasi di prevenzione, rilevamento, segnalazione, risposta e ripristino.

2. Il Piano di cui al comma 1 è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi.

Articolo 5

(Piano per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche)

1. Con determina il Segretario generale adotta il Piano di sensibilizzazione, formazione e sviluppo della consapevolezza delle minacce e dei rischi in materia di sicurezza informatica per tutti i soggetti di cui all'articolo 2, comma 2 e per tutto il personale.

2. Il Piano di cui al comma 1 comprende i percorsi di formazione e sensibilizzazione in materia di sicurezza informatica diversificati in funzione dei relativi destinatari, i relativi programmi di aggiornamento continuo e le eventuali modalità di verifica dell'acquisizione dei contenuti.

Articolo 6

(Piano dei rischi di sicurezza informatica)

1. Con determina il Segretario generale adotta il Piano dei rischi di sicurezza informatica per identificare e gestire i rischi informatici valutando l'eventuale rischio residuo. Nell'ambito del Piano sono definiti anche i processi di gestione dei rischi di sicurezza informatica della catena di approvvigionamento.

2. Il Piano di cui al comma 1 è aggiornato almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

3. Ai fini di cui al comma 1, il Servizio risorse umane, strumentali e contratti e il Servizio Sistemi informativi, con il coordinamento del Vicesegretario generale appositamente delegato dal Segretario generale, definiscono d'intesa, ciascuno per le rispettive competenze, il registro degli *asset* previsto dalla misura ID.AM della determinazione ACN n. 164179 recante un elenco aggiornato dei componenti rilevanti dei sistemi informativi e di rete (*software, hardware* e servizi informatici erogati dai fornitori), con l'indicazione dei sistemi informativi e di rete ai quali è possibile accedere da remoto e la descrizione delle relative modalità di accesso, i criteri per lo sviluppo e la gestione dei sistemi informativi e di rete (ivi inclusi gli apparati ad uso dei dipendenti) in termini di vita utile degli asset, policy di configurazione, assegnazione agli utenti, manutenzione e dismissione, sempre in base alle competenze rispettivamente attribuite dal Regolamento.

4. Ai fini di cui al comma 1, con determina il Segretario generale o il Vicesegretario generale delegato, sentiti il RPD, il Designato di I livello e il Responsabile della Cybersicurezza, stabilisce le modalità di protezione della riservatezza, dell'integrità e della disponibilità dei dati e delle informazioni, nonché le modalità di gestione dei *software* e degli *hardware* in coerenza con la strategia sul rischio di cui all'articolo 3, nonché l'accesso agli asset fisici e logici.

5. In accordo alle esigenze di continuità operativa, il Servizio Sistemi informativi adotta le procedure per effettuare periodicamente i *backup* dei dati e delle configurazioni di rete rilevanti nonché le modalità di gestione di *hardware*, *software* e dei servizi delle piattaforme fisiche e virtuali.

6. Ai fini di cui al comma 1, con determina del Servizio risorse umane, strumentali e contratti, sentito il Servizio Sistemi informativi e d'intesa con il Vicesegretario generale delegato, è istituito, e costantemente aggiornato, un registro dei soggetti le cui forniture hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete.

Articolo 7

(Piano di gestione delle vulnerabilità)

1. Con determina il Segretario generale adotta il Piano di gestione delle vulnerabilità che reca le modalità per identificare le vulnerabilità e per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità.

2. Ai fini di cui al comma 1, con determina il Servizio Sistemi informativi approva la relazione sull'attività svolta per l'identificazione delle vulnerabilità dei sistemi e/o *penetration test,* sugli esiti della stessa, sulle vulnerabilità rilevate, nonché sul loro impatto sulla sicurezza.

Articolo 8

(Piano di risposta agli incidenti)

1. Con determina il Segretario generale adotta il "Piano di risposta agli incidenti" recante il "Piano di continuità operativa" e il "Piano di gestione delle crisi" volti a definire le responsabilità e le azioni da attuare in caso di incidenti di sicurezza informatica.

2. Con determina il Servizio Sistemi informativi adotta la Procedura per il ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica, coordinando con le parti interne e quelle esterne le attività di risposta a seguito di un incidente.

3. Il Piano di risposta agli incidenti di cui al comma 1 e la Procedura di ripristino di cui al comma 2 sono aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Articolo 9

(Gestione dell'autenticazione, delle identità digitali e del controllo accessi)

1. Con determina il Segretario generale definisce le modalità di gestione dell'accesso agli *asset* fisici e logici e le modalità di autenticazione di utenti, servizi e *hardware*.

2. Con determina il Servizio Sistemi informativi nomina gli amministratori di sistema dei sistemi informativi e di rete, i quali sono tenuti al rispetto della riservatezza dei dati e delle informazioni gestiti, anche dopo la cessazione o la modifica del rapporto di lavoro.

Articolo 10

(Misure attuative)

1. L'azione amministrativa in esecuzione dei Piani di cui ai precedenti articoli è svolta nel rispetto dei compiti attribuiti dal Regolamento. In caso di inadempimento, il titolare del potere sostitutivo è il Segretario generale.

2. In attuazione della presente delibera, il Punto di contatto notifica, ai sensi dell'articolo 7, comma 4, del decreto NIS quali organi amministrativi e direttivi dell'Autorità i soggetti di cui all'articolo 2, comma 2.

Articolo 11

(Nomine del Punto di contatto ACN e del sostituto Punto di contatto ACN)

1. Ai sensi dell'articolo 7, comma 1, lettera c), del decreto NIS, il Punto di contatto è il referente ufficiale per tutte le comunicazioni con l'ACN relative alla normativa in materia di sicurezza informatica.

2. Il Punto di contatto per l'Autorità è nominato nella persona del Responsabile del Servizio sistemi informativi anche in qualità di Responsabile della cybersicurezza.

3. In caso di assenza o impedimento del Punto di contatto, opera con le stesse funzioni il sostituto Punto di contatto garantendo la continuità delle attività. Il sostituto Punto di contatto è il Vicesegretario generale appositamente delegato dal Segretario generale**.**

4. Con determina del Servizio sistemi informativi può essere individuato un dipendente dell'Autorità, cui attribuire l'utenza del portale ACN con il ruolo di Segreteria che supporta il Punto di contatto o il suo sostituto nella raccolta e nell'inserimento dei dati richiesti dall'ACN. L'utente con il ruolo di Segreteria non può effettuare trasmissione di comunicazioni ufficiali.

Articolo 12

(Disposizioni finali)

1. I ruoli e le responsabilità dei soggetti che fanno parte della *governance* sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Il Vicesegretario generale appositamente delegato dal Segretario generale, al fine di favorire la collaborazione e, ove prevista, l'intesa fra i servizi e le direzioni, opera con funzione generale di coordinamento. In caso di difficoltà o rischio di ritardo negli adempimenti, per assicurare il rispetto dei tempi, il Vicesegretario delegato può proporre al Segretario generale l'esercizio del potere sostitutivo.

2. La presente delibera entra in vigore il giorno successivo alla sua approvazione.

3. Le delibere n. 204/25/CONS e n. 259/25/CONS sono abrogate.

4. Il Punto di contatto, ai sensi dell'art. 15 della determinazione ACN n. 136117 del 10 aprile 2025, inserisce tempestivamente nel portale ACN, ai sensi dell'art. 7, comma 4, del decreto NIS, tramite la piattaforma digitale, le variazioni dei componenti degli organi amministrativi e direttivi di cui all'articolo 2 del presente provvedimento, con le modifiche apportate dalla presente delibera.

La presente delibera è pubblicata sul sito *web* dell'Autorità ed è trasmessa ai soggetti interessati.

IL PRESIDENTE
Giacomo Lasorella

IL COMMISSARIO RELATORE
Antonello Giacomelli

Per attestazione di conformità a quanto deliberato
IL SEGRETARIO GENERALE
Giovanni Santella