AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

DELIBERA N. 204/25/CONS

INDIVIDUAZIONE DELLA *GOVERNANCE* PER LA GESTIONE DELLA SICUREZZA INFORMATICA DI CUI ALLA DETERMINAZIONE ACN N. 164179 DEL 14 APRILE 2025

Nella sua riunione di Consiglio del 30 luglio 2025;

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");

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*";

VISTA la decisione assunta dal Consiglio nella seduta dell'11 dicembre 2024 di individuare 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 n. 90/2024;

VISTA la determinazione ACN n. 164179 del 14 aprile 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"* (di seguito, anche "Determinazione ACN");

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. 36117 del 10 aprile 2025, il Punto di contatto dei soggetti essenziali, entro il termine del 31 maggio 2025, poi prorogato al 31 luglio, 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;

CONSIDERATO che dette misure di gestione dei rischi hanno natura tecnica, organizzativa e operativa e includono principalmente:

- Politica per la gestione del rischio di sicurezza informatica
- Politica per la gestione e notifica degli incidenti di sicurezza informatica
- Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche
- Piano della gestione del rischio di sicurezza informatica
- Piano di gestione delle vulnerabilità
- Piano di risposta agli incidenti
- Gestione dell'autenticazione, delle identità digitali e del controllo accessi

RILEVATO che la Determinazione ACN 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;

RITENUTO opportuno, ai fini della definizione della predetta *governance*, mantenere una separazione tra i soggetti che hanno la responsabilità di adottare le Politiche generali in materia di sicurezza informatica e i soggetti che, invece, hanno il compito di tradurle in Piani di natura operativa-amministrativa, in linea con la struttura disegnata dal decreto NIS, nonché con i regolamenti interni dell'Autorità;

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;

RAVVISATA, dunque, la necessità di definire in modo chiaro ruoli e responsabilità dei diversi soggetti coinvolti, così da garantire la realizzazione di processi decisionali idonei a risolvere in tempi rapidi le situazioni di emergenza;

RAVVISATA, dunque, la necessità di un pieno coinvolgimento di tutti coloro che in Autorità ricoprono incarichi di responsabilità di amministrazione e direzione ai fini dell'attuazione della normativa NIS;

VISTA la proposta del Segretario generale;

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

DELIBERA

Articolo 1

(Finalità e ambito di applicazione)

1. Ai sensi del decreto legislativo n. 138/2024, sono individuati i soggetti che fanno parte della *governance* di gestione della sicurezza informatica e sono definite le relative responsabilità.
2. I soggetti che partecipano alla *governance* di gestione della sicurezza informatica sono:
   - il Consiglio dell'Autorità;
   - il Segretario generale;
   - i Vicesegretari generali, ed in particolare il Vicesegretario generale appositamente delegato in materie attinenti alla sicurezza informatica, 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 2

(Politica per la gestione del rischio di sicurezza informatica)

1. Con delibera del Consiglio, su proposta del Segretario generale, è approvata la politica per la gestione del rischio di sicurezza informatica che individua i relativi programmi di intervento.

2. La politica di cui al comma 1 ed i relativi programmi di intervento sono riesaminati e, se opportuno, adeguati periodicamente e comunque almeno con cadenza annuale, nonché 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.

3. Il Segretario generale riferisce al Consiglio, con periodicità semestrale, sugli esiti dei programmi di cui al comma 1 e sull'efficacia delle misure di gestione del rischio per la sicurezza informatica.

Articolo 3

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

1. Con delibera del Consiglio, su proposta del Segretario generale, è approvata la politica per la gestione e la notifica al CSIRT Italia degli incidenti di sicurezza informatica.

2. La politica di cui al comma 1 è riesaminata e, se opportuno, aggiornata periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi.

Articolo 4

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

1. Con delibera del Consiglio, su proposta del Segretario generale, è approvata la politica 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 1, comma 2 e per tutto il personale.

2. La politica 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 5

(Piano della gestione del rischio di sicurezza informatica)

1. Con determina del Segretario generale è adottato il Piano di gestione del rischio di sicurezza informatica per identificare e gestire i rischi informatici valutando l'eventuale rischio residuo. Nell'ambito del Piano di gestione del rischio di sicurezza informatica 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 ROF.

4. Ai fini di cui al comma 1, con determina del Segretario generale o del Vicesegretario generale delegato, sentiti il RPD, il Designato di I livello e il Responsabile della Cybersicurezza, sono stabilite 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 2, 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 istituto, e costantemente aggiornato, un registro dei soggetti le cui forniture hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete.

Articolo 6

(Piano di gestione delle vulnerabilità)

1. Con determina del Segretario generale è adottato 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 del Servizio Sistemi informativi è approvata 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 7

(Piano di risposta agli incidenti)

1. Con determina del Segretario generale è approvato 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 del Servizio Sistemi informativi è adottata 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 8

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

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

2. Con determina del Servizio Sistemi informativi sono nominati 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 9

(Misure attuative)

1. L'azione amministrativa in esecuzione delle Politiche e 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 1, comma 2.

3. Le Politiche e i Piani di cui all'articolo 3 sono adottati entro il 14 gennaio 2026 ai sensi dell'articolo 3, comma 2, della Determinazione ACN.

4. Le Politiche e i Piani di cui agli articoli 2, 4, 5, 6, 7, 8 sono adottati entro il 14 ottobre 2026 ai sensi dell'articolo 3, comma 1, della Determinazione ACN.

Articolo 10

(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 11

(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.

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

IL PRESIDENTE
Giacomo Lasorella

IL COMMISSARIO RELATORE
Laura Aria

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