7 giugno ore 18:00

SCHEMA DI DECRETO LEGISLATIVO

di 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

IL PRESIDENTE DELLA REPUBBLICA

VISTI gli articoli 76 e 87, quinto comma, della Costituzione;

VISTA la legge 24 dicembre 2012, n. 234, recante «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea» e, in particolare, gli articoli 31 e 32;

VISTA la legge 21 febbraio 2024, n. 15, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea - Legge di delegazione europea 2022-2023» e, in particolare, l'articolo 3;

VISTA la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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;

VISTA la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del l2 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche);

VISTA la raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese;

VISTA la direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio;

VISTO il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011;

VISTA la direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario;

VISTA la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio;

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»;

VISTO il decreto legislativo 1° agosto 2003, n. 259, recante «Codice delle comunicazioni elettroniche»;

VISTO il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale» e, in particolare, le disposizioni in materia di funzioni dell'AgID e di sicurezza informatica;

VISTO il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, recante «Misure urgenti per il contrasto del terrorismo internazionale»;

VISTA la legge 3 agosto 2007, n. 124, recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto»;

VISTO il decreto legislativo 23 giugno 2011, n. 118, recante «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»;

VISTO il decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante «Misure urgenti per la crescita del Paese» e, in particolare, l'articolo 19, che ha istituito l'Agenzia per l'Italia digitale (AgID);

VISTO il decreto legislativo 4 marzo 2014, n. 39, recante «Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI»;

VISTO il decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, recante «Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione»;

VISTO 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;»

VISTO 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»;

VISTO il decreto legislativo adottato ai sensi dell'articolo 5 della legge n. 15 del 2024 per il recepimento della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio;

VISTO il decreto del Presidente del Consiglio dei ministri n. 5 del 6 novembre 2015, recante «Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva», pubblicato nella Gazzetta Ufficiale n. 284 del 5 dicembre 2015;

VISTO il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, concernente «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», pubblicato nella Gazzetta Ufficiale n. 87 del 13 aprile 2017;

SENTITA l'Agenzia per la cybersicurezza nazionale, ai sensi dell'articolo 3 della legge n. 15 del 2024;

VISTA la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del….;

ACQUISITO il parere della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, reso nella seduta del…. ;

ACQUISITI i pareri delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

VISTA la deliberazione del Consiglio dei ministri, adottata nella riunione del ….

SULLA PROPOSTA del Presidente del Consiglio dei ministri e del Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR, di concerto con i Ministri per la pubblica amministrazione, degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, delle imprese e del made in Italy, dell'agricoltura, della sovranità alimentare e delle foreste, dell'ambiente e della sicurezza energetica, delle infrastrutture e dei trasporti, dell'università e della ricerca, della cultura e della salute;

Emana
il seguente decreto legislativo:

Capo I
Disposizioni generali

ART. 1
(Oggetto)

1. Il presente decreto 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.
2. Ai fini del comma 1, il presente decreto prevede:
   a) la Strategia nazionale di cybersicurezza, recante previsioni volte a garantire un livello elevato di sicurezza informatica;
   b) l'integrazione del quadro di gestione delle crisi informatiche, nel contesto dell'organizzazione nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza, di cui all'articolo 10 del decreto-legge 4 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;
   c) la conferma dell'Agenzia per la cybersicurezza nazionale quale:
      1) Autorità nazionale competente NIS, disciplinandone i poteri inerenti all'implementazione e all'attuazione del presente decreto;
      2) Punto di contatto unico NIS, assicurando il raccordo nazionale e transfrontaliero;
      3) Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia);
   d) la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del

Ministero della Difesa, ciascuno per gli ambiti di competenza indicati all'articolo 2, comma 1, lettera g), quali Autorità nazionali di gestione delle crisi informatiche, assicurando la coerenza con il quadro nazionale esistente in materia di gestione generale delle crisi informatiche, ferme restando le competenze del Nucleo per la cybersicurezza di cui all'articolo 9 del decreto-legge 14 giugno 2021, n. 82;

e) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale, supportandone le funzioni svolte quale Autorità nazionale competente NIS e Punto di contatto unico NIS;

f) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;

g) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del presente decreto, in particolare, attraverso la partecipazione nazionale a livello dell'Unione europea:

   1) al Gruppo di cooperazione NIS tra autorità competenti NIS e tra punti di contatto unici degli Stati membri dell'Unione europea, nell'ottica di incrementare la fiducia e la collaborazione a livello unionale;

   2) alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi cibernetiche su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione europea;

   3) alla Rete di CSIRT nazionali nell'ottica di assicurare una cooperazione, sul piano tecnico, rapida ed efficace.

ART. 2
(Definizioni)

1. Ai fini del presente decreto si applicano le definizioni seguenti:

   a) «Strategia nazionale di cybersicurezza»: il quadro coerente che prevede obiettivi strategici e priorità in materia di cybersicurezza e la governance per il loro conseguimento di cui all'articolo 9;

   b) «Agenzia per la cybersicurezza nazionale»: l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

   c) «Nucleo per la cybersicurezza»: Il Nucleo per la cybersicurezza di cui all'articolo 8 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

   d) «Autorità nazionale competente NIS»: l'Agenzia per la cybersicurezza nazionale, quale Autorità nazionale competente NIS di cui all'articolo 10, comma 1;

   e) «Punto di contatto unico NIS»: l'Agenzia per la cybersicurezza nazionale, quale Punto di contatto unico NIS di cui all'articolo 10, comma 2;

f) «Autorità di settore NIS»: le Amministrazioni designate quali Autorità di settore di cui all'articolo 11, commi 1 e 2;

g) «Autorità nazionali di gestione delle crisi informatiche»: per la parte relativa alla resilienza nazionale di cui all'articolo 1 del decreto-legge n. 82 del 2021, l'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e, per la parte relativa alla difesa e sicurezza militare dello Stato, il Ministero della Difesa, quali Autorità nazionali di gestione delle crisi informatiche di cui all'articolo 13, comma 1;

h) «CSIRT nazionali»: i Gruppi nazionali di risposta agli incidenti di sicurezza informatica di cui all'articolo 10, paragrafo 1, della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

i) «CSIRT Italia»: Il Gruppo nazionale di risposta agli incidenti di sicurezza informatica ai sensi dell'articolo 15, comma 1, operante all'interno dell'Agenzia per la cybersicurezza nazionale;

l) «Gruppo di cooperazione NIS»: il Gruppo di cooperazione di cui all'articolo 18, istituito ai sensi dell'articolo 14 della direttiva (UE) 2022/2555;

m) «EU-CyCLONe»: la Rete delle organizzazioni di collegamento per le crisi informatiche di cui all'articolo 19, istituita ai sensi dell'articolo 16 della direttiva (UE) 2022/2555;

n) «Rete di CSIRT nazionali»: la Rete di CSIRT nazionali di cui all'articolo 20, istituita ai sensi dell'articolo 15 della direttiva (UE) 2022/2555;

o) «ENISA»: l'Agenzia dell'Unione europea per la sicurezza informatica, di cui all'articolo 3 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019;

p) «sistema informativo e di rete»:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

q) «sicurezza dei sistemi informativi e di rete»: la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi;

r) «sicurezza informatica»: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche, così come definito dall'articolo 2, punto 1), del regolamento (UE) 2019/881;

s) «cybersicurezza»: ferme restando le definizioni di cui alle lettere q) e r), l'insieme delle attività di cui all'articolo 1, comma 1, lettera a), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

t) «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

u) «quasi-incidente»: cd. *near-miss*, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato;

v) «incidente di sicurezza informatica su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

z) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e recuperare da esso;

aa) «rischio»: la combinazione dell'entità dell'impatto di un incidente, in termini di danno o di perturbazione, e della probabilità che quest'ultimo si verifichi;

bb) «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone, così come definita dall'articolo 2, punto 8), del regolamento (UE) 2019/881;

cc) «minaccia informatica significativa»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informativi e di rete di un soggetto o sugli utenti dei servizi erogati da un soggetto causando perdite materiali o immateriali considerevoli;

dd) «approccio multi-rischio»: cosiddetto approccio *all-hazards*, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati;

ee) «singoli punti di malfunzionamento»: cosiddetto *single points of failure*, singolo componente di un sistema da cui dipende il funzionamento del sistema stesso;

ff) «prodotto TIC»: un elemento o un gruppo di elementi di un sistema informativo o di rete, così come definito dall'articolo 2, punto 12), del regolamento (UE) 2019/881;

gg) «servizio TIC»: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo dei sistemi informativi e di rete così come definito dall'articolo 2, punto 13), del regolamento (UE) 2019/881;

hh) «processo TIC»: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC, così come definito dall'articolo 2, punto 14), del regolamento (UE) 2019/881;

ii) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica;

ll) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012;

mm) «punto di interscambio internet»: cosiddetto *internet exchange point* (IXP), un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico internet, che fornisce interconnessione soltanto ai sistemi autonomi e che non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo né altera o interferisce altrimenti con tale traffico;

nn) «sistema dei nomi di dominio»: cosiddetto *domain name system* (DNS), un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di instradamento e connettività di internet al fine di accedere a tali servizi e risorse;

oo) «fornitore di servizi di sistema dei nomi di dominio»: un soggetto che fornisce:

1) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet; o

2) servizi di risoluzione dei nomi di dominio autoritativi per uso da parte di terzi, fatta eccezione per i server dei nomi radice (cosiddetto *root nameserver*);

pp) «gestore di registro dei nomi di dominio di primo livello»: cosiddetto registro dei nomi TLD (*top level domain*) o *registry*, soggetto cui è stato delegato uno specifico dominio di primo livello e che è responsabile dell'amministrazione di tale dominio di primo livello, compresa la registrazione dei nomi di dominio sotto tale dominio di primo livello, e del funzionamento tecnico di tale dominio di primo livello, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona del dominio di primo livello tra i server dei nomi, indipendentemente dal fatto che una qualsiasi di tali operazioni sia effettuata dal soggetto stesso o sia esternalizzata, ma escludendo le situazioni in cui i nomi di dominio di primo livello sono utilizzati da un registro esclusivamente per uso proprio;

qq) «fornitore di servizi di registrazione di nomi di dominio»: un *registrar* o un agente che agisce per conto di registrar, come un fornitore o un rivenditore di servizi di registrazione per la privacy o di proxy;

rr) «servizio digitale»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015;

ss) «servizio fiduciario»: un servizio fiduciario quale definito all'articolo 3, punto 16), del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2024;

tt) «prestatore di servizi fiduciari»: una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore

di servizi fiduciari non qualificato, quale definito all'articolo 3, punto 19), del regolamento (UE) n. 910/2014;

uu) «servizio fiduciario qualificato»: un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel regolamento (UE) n. 910/2014, ai sensi dell'articolo 3, punto 17) dello stesso;

vv) «prestatore di servizi fiduciari qualificato»: un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato, quale definito all'articolo 3, punto 20), del regolamento (UE) n. 910/2014;

zz) «mercato online»: un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori, quale definito all'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005;

aaa) «motore di ricerca online»: un servizio digitale che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto, quale definito all'articolo 2, punto 5), del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019;

bbb) «servizio di cloud computing»: un servizio digitale che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni;

ccc) «servizio di data center»: un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare in modo centralizzato, interconnettere e far funzionare apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;

ddd) «rete di distribuzione dei contenuti»: cosiddetta *content delivery network* (CDN), una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di internet per conto di fornitori di contenuti e servizi;

eee) «piattaforma di servizi di social network»: una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi, in particolare, attraverso chat, post, video e raccomandazioni;

fff) «rete pubblica di comunicazione elettronica»: una rete di comunicazione elettronica, utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra

i punti terminali di rete, quale definita all'articolo 2, punto 8), della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018;

ggg) «servizio di comunicazione elettronica»: un servizio di comunicazione elettronica quale definito all'articolo 2, punto 4), della direttiva (UE) 2018/1972;

hhh) «soggetto»: una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi;

iii) «fornitore di servizi gestiti»: un soggetto che fornisce servizi relativi all'installazione, alla gestione, al funzionamento o alla manutenzione di prodotti, reti, infrastrutture, applicazioni TIC o di qualsiasi altro sistema informativo e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza;

lll) «fornitore di servizi di sicurezza gestiti»: un fornitore di servizi gestiti che svolge o fornisce assistenza per attività relative alla gestione dei rischi di sicurezza informatica;

mmm) «organismo di ricerca»: un soggetto che ha come obiettivo principale lo svolgimento di attività di ricerca applicata o di sviluppo sperimentale al fine di sfruttare i risultati di tale ricerca a fini commerciali, ma che non comprende gli istituti di istruzione;

nnn) «audit»: attività di verifica, a distanza o in loco, sistematica, documentata e indipendente che ha come scopo quello di vagliare la corrispondenza agli obblighi di cui al capo IV del presente decreto, effettuata da un organismo indipendente qualificato o dall'Autorità nazionale competente NIS.

ART. 3
(Ambito di applicazione)

1. Nell'ambito di applicazione del presente decreto rientrano i soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV che sono sottoposti alla giurisdizione nazionale ai sensi dell'articolo 5. Gli allegati I e II descrivono i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e tipologie di soggetto. Gli allegati III e IV descrivono, rispettivamente, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetto a cui si applica il presente decreto.
2. Il presente decreto si applica ai soggetti delle tipologie di cui all'allegato I e II, che superano i massimali per le piccole imprese ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE.
3. L'articolo 3, paragrafo 4, dell'allegato alla raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, non si applica ai fini del presente decreto.
4. Per determinare se un soggetto è da considerarsi una media o grande impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, si applica l'articolo 6, paragrafo 2, del medesimo allegato, salvo che ciò non sia proporzionato, tenuto anche conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi

informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce.

5. Il presente decreto si applica, indipendentemente dalle loro dimensioni, anche:
   a) ai soggetti che sono identificati come soggetti critici ai sensi del decreto legislativo, che recepisce la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;
   b) ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;
   c) ai prestatori di servizi fiduciari;
   d) ai gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
   e) ai fornitori di servizi di registrazione dei nomi di dominio.
6. Il presente decreto si applica, altresì, indipendentemente dalle loro dimensioni, anche alle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III e che, a tal fine, sono considerate:
   a) amministrazioni centrali;
   b) amministrazioni regionali;
   c) amministrazioni locali;
   d) amministrazioni di tipologia diversa da quelle elencate alle lettere a), b) e c).
7. Sulla base di un criterio di gradualità, dell'evoluzione del grado di esposizione al rischio della pubblica amministrazione, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico, tenuto conto anche dei criteri di cui al comma 9, con uno o più decreti del Presidente del Consiglio dei ministri adottati secondo le modalità di cui all'articolo 40, comma 2, possono essere individuate ulteriori categorie di pubbliche amministrazioni a cui si applica il presente decreto al fine di adeguare l'elenco di categorie di cui all'allegato III.
8. Il presente decreto si applica, altresì, indipendentemente dalle loro dimensioni, anche ai soggetti delle tipologie di cui all'allegato IV, individuati secondo le procedure di cui al comma 13.
9. Il presente decreto si applica, altresì, anche ai soggetti dei settori o delle tipologie di cui agli allegati I, II, III e IV, indipendentemente dalle loro dimensioni, individuati secondo le procedure di cui al comma 13, qualora:
   a) il soggetto sia identificato prima della data di entrata in vigore del presente decreto come operatore di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65;
   b) il soggetto sia l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
   c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato;
f) il soggetto sia considerato critico ai sensi del presente decreto quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti.

10. Il presente decreto si applica, infine, indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:
    a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
    b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
    c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;
    d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.
11. Resta ferma la disciplina in materia di protezione dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e al decreto legislativo 30 giugno 2003, n. 196, nonché in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile di cui al decreto legislativo 4 marzo 2014, n. 39.
12. L'Autorità nazionale competente NIS applica la clausola di salvaguardia di cui al comma 4, secondo i criteri per la determinazione individuati con le modalità di cui all'articolo 40, comma 1.
13. I soggetti di cui ai commi 8 e 9 sono individuati dall'Autorità nazionale competente NIS, su proposta delle Autorità di settore, secondo le modalità di cui all'articolo 40, comma 4. L'Autorità nazionale competente NIS notifica a tali soggetti la loro individuazione ai fini della registrazione di cui all'articolo 7, comma 1.
14. Il presente decreto non si applica ai soggetti identificati come essenziali o importanti che sono sottoposti agli obblighi di cui al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché, ai sensi dell'articolo 2, comma 10, della direttiva, ai soggetti esentati dall'ambito del predetto Regolamento.

ART. 4

(Protezione degli interessi nazionali e commerciali)

1. Il presente decreto lascia impregiudicata la responsabilità dello Stato italiano di tutelare la sicurezza nazionale e il suo potere di salvaguardare altre funzioni essenziali dello Stato,

tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

2. I soggetti di cui all'articolo 3, commi 6 e 7, non ricomprendono il Parlamento italiano, l'Autorità giudiziaria e la Banca d'Italia. Agli Organi costituzionali e di rilievo costituzionale non si applicano le previsioni di cui al capo V.
3. Il presente decreto non si applica agli enti, organi e articolazioni della pubblica amministrazione che operano nei settori, della pubblica sicurezza, della difesa nazionale o dell'attività di contrasto, compresi l'indagine, l' accertamento e il perseguimento di reati, nonché agli organismi di informazione per la sicurezza di cui alla legge 3 agosto 2007, n. 124, all'Agenzia per la cybersicurezza nazionale di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.
4. Con uno o più decreti del Presidente del Consiglio dei ministri adottati, con le modalità di cui all'articolo 40, comma 3, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli enti, organi e articolazioni della pubblica amministrazione di cui al comma 3. A tali soggetti, nell'espletamento di tali attività o servizi, non si applicano gli obblighi di cui al capo IV e le previsioni di cui al capo V.
5. Con decreto del Presidente del Consiglio dei ministri, adottato ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli Organismi di informazione per la sicurezza nazionale di cui agli articoli 4, 5 e 6 della legge n. 124 del 2007. A tali soggetti, nell'espletamento dei predetti attività o servizi, non si applicano gli obblighi di cui al capo IV e le previsioni di cui al capo V. Dei provvedimenti adottati ai sensi del primo periodo viene data comunicazione all'Agenzia per la cybersicurezza nazionale.
6. Ai sensi del comma 4, non possono essere esclusi gli enti, organi e articolazioni della pubblica amministrazione con competenze di regolazione o le cui attività sono solo marginalmente connesse ai settori di cui al medesimo comma. Non possono altresì essere esclusi i soggetti che agiscono in qualità di prestatore di servizi fiduciari. I soggetti di cui al comma 4 assicurano un livello di sicurezza informatica coerente con gli obblighi di cui al capo IV.
7. Gli obblighi stabiliti nel presente decreto non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali dello Stato italiano in materia di sicurezza nazionale, pubblica sicurezza o difesa.
8. Fatto salvo quanto previsto dall'articolo 346 del trattato sul funzionamento dell'Unione europea, le informazioni riservate secondo quanto disposto dalla normativa dell'Unione europea e nazionale, in particolare per quanto concerne la riservatezza degli affari, sono scambiate con la Commissione europea e con le autorità competenti degli Stati membri solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione del presente decreto. Le informazioni scambiate sono pertinenti e commisurate allo scopo. Lo scambio di informazioni ne tutela la riservatezza e protegge la sicurezza e gli interessi commerciali dei soggetti essenziali e importanti.

ART. 5

(Giurisdizione e territorialità)

1. Sono sottoposti alla giurisdizione nazionale i soggetti critici stabiliti sul territorio dello Stato, ad eccezione dei seguenti casi:

a) i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi;
b) i fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono sottoposti la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione ai sensi del comma 2;
c) gli enti della pubblica amministrazione, che sono sottoposti alla giurisdizione dello Stato membro che li ha istituiti.

2. Ai fini di cui al comma 1, lettera b), si considera stabilimento principale nell'Unione quello dello Stato nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Se non è possibile determinare lo Stato membro in cui sono adottate le suddette decisioni o se le stesse non sono adottate nell'Unione, lo stabilimento principale è considerato quello collocato nello Stato in cui sono effettuate le operazioni di cybersicurezza, ovvero, ove ciò non sia possibile, quello dello Stato in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione europea

3.Se i soggetti di cui al comma 1, lettera b), non sono stabiliti nel territorio dell'Unione ma offrono servizi all'interno dello stesso, essi designano un rappresentante nell'Unione, che è stabilito in uno degli Stati in cui sono offerti i predetti servizi ed è sottoposto alla relativa giurisdizione.

4. In assenza della designazione del rappresentante da parte di uno dei soggetti di cui al comma 3, l'Autorità nazionale competente NIS può avviare un'azione legale, nei confronti dei soggetti inadempienti.

5. La designazione del rappresentante di cui al comma 3 non pregiudica le azioni legali che potrebbero essere state già avviate per violazioni degli obblighi di cui al presente decreto, l'imposizione degli obblighi di cui al capo IV e l'esercizio dei poteri di cui al capo V.

ART. 6
(Soggetti essenziali e importanti)

1. Ai fini del presente decreto, sono considerati soggetti essenziali:
   a) i soggetti di cui all'allegato I che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE;

b) indipendentemente dalle loro dimensioni, i soggetti identificati come soggetti critici ai sensi del decreto legislativo, che recepisce la direttiva (UE) 2022/2557;
c) i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui all'articolo 3, comma 5, lettera b), che si considerano medie imprese ai sensi dell'articolo 2 dell'allegato alla raccomandazione 2003/361/CE;
d) indipendentemente dalle loro dimensioni, i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio di cui all'articolo 3, comma 5, lettere c) e d);
e) indipendentemente dalle loro dimensioni, le pubbliche amministrazioni centrali di cui all'articolo 3, comma 6, lettera a).

2. Fermo restando quanto previsto dal comma 1, l'Autorità nazionale competente NIS individua, secondo le modalità di cui all'articolo 40, comma 5, i soggetti di cui all'articolo 3, commi 6, 8, 9 e 10, che, indipendentemente dalle loro dimensioni, sono considerati essenziali.
3. Ai fini del presente decreto, sono considerati soggetti importanti i soggetti di cui all'articolo 3 che non sono considerati essenziali ai sensi dei commi 1 e 2 del presente articolo.

ART. 7

(Identificazione ed elencazione dei soggetti essenziali e importanti)

1. Dal 1° gennaio al 28 febbraio di ogni anno successivo alla data di entrata in vigore del presente decreto, i soggetti di cui all'articolo 3, si registrano o aggiornano la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni attribuite all'Agenzia per la cybersicurezza nazionale anche ai sensi del presente decreto. A tal fine, tali soggetti forniscono o aggiornano almeno le informazioni seguenti:
   a) la ragione sociale;
   b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono;
   c) 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;
   d) ove applicabile, i pertinenti settori, sottosettori e tipologie di soggetto di cui agli allegati I, II, III e IV;
2. Entro il 31 marzo di ogni anno successivo alla data di entrata in vigore del presente decreto, l'Autorità nazionale competente NIS, redige, secondo le modalità di cui all'articolo 40, comma 5, l'elenco dei soggetti essenziali e importanti, sulla base delle registrazioni di cui al comma 1 e delle decisioni adottate ai sensi degli articoli 3, 4, e 6.
3. Tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS comunica ai soggetti registrati di cui al comma 2:
   a) l'inserimento nell'elenco dei soggetti essenziali o importanti;
   b) la permanenza nell'elenco dei soggetti essenziali o importanti;

c) l’espunzione dall’elenco dei soggetti.

4. Dal 15 aprile al 31 maggio di ogni anno successivo alla data di entrata in vigore del presente decreto, tramite la piattaforma digitale di cui al comma 1, i soggetti che hanno ricevuto la comunicazione di cui al comma 3, lettere a) e b), forniscono o aggiornano almeno le informazioni seguenti:
   a) lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto;
   b) ove applicabile, l’elenco degli Stati membri in cui forniscono servizi che rientrano nell’ambito di applicazione del presente decreto;
   c) i responsabili di cui all’articolo 38, comma 5, indicando il ruolo presso il soggetto, i suoi recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono;
   d) un sostituto del punto di contatto di cui al comma 1, lettera c), indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono.
5. I fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, i fornitori di motori di ricerca online e i fornitori di piattaforme di social network, forniscono all'Autorità nazionale competente NIS, secondo le modalità di cui al comma 4, anche:
   a) l'indirizzo della sede principale e delle altre sedi del soggetto nell’Unione europea;
   b) se non è stabilito nell’Unione europea, l’indirizzo della sede del suo rappresentante ai sensi dell'articolo 5, comma 3, unitamente ai dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono.
6. L’Autorità nazionale competente NIS stabilisce, secondo le modalità di cui all’articolo 40, comma 5, termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale di cui al comma 1, indicando altresì eventuali ulteriori informazioni che i soggetti devono fornire ai sensi dei commi 1 e 4, nonché di designazione dei rappresentanti di cui all’articolo 5, comma 3.
7. I soggetti che hanno ricevuto la comunicazione di cui al comma 3, lettere a) e b), notificano all’Autorità nazionale competente NIS, tramite la piattaforma digitale di cui al comma 1, qualsiasi modifica delle informazioni trasmesse ai sensi del presente articolo tempestivamente e, in ogni caso, entro 14 giorni dalla data della modifica.

ART. 8
(Protezione dei dati personali)

1. L’Agenzia per la cybersicurezza nazionale, le Autorità di settore NIS, i soggetti di cui all’articolo 3, trattano i dati personali nella misura necessaria ai fini del presente decreto e conformemente al decreto legislativo 30 giugno 2003, n. 196 e al regolamento (UE) 2016/679.

2. Il trattamento dei dati personali ai sensi del presente decreto da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di servizi di comunicazione elettronica accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione europea in materia di protezione dei dati e della legislazione dell'Unione europea in materia di tutela della vita privata, ai sensi della direttiva 2002/58/CE.

Capo II
Quadro nazionale di sicurezza informatica

ART. 9
(Strategia nazionale di cybersicurezza)

1. La Strategia nazionale di cybersicurezza individua gli obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza.
2. La Strategia nazionale di cybersicurezza comprende almeno:
   a) gli obiettivi e le priorità, che riguardano in particolare i settori di cui agli allegati I, II, III e IV;
   b) un quadro di governance per la realizzazione degli obiettivi e delle priorità di cui alla lettera a), comprendente le misure strategiche di cui al comma 3;
   c) un quadro di governance che chiarisca i ruoli e le responsabilità dei pertinenti portatori di interessi a livello nazionale, a sostegno della cooperazione e del coordinamento a livello nazionale tra le Autorità di settore NIS, l'Agenzia per la cybersicurezza nazionale, in qualità di Autorità nazionale competente NIS, di Punto di contatto unico NIS e di CSIRT Italia, nonché il coordinamento e la cooperazione tra tali organismi e le altre autorità competenti ai sensi degli atti giuridici settoriali dell'Unione europea;
   d) un meccanismo per individuare le risorse e una valutazione dei rischi a livello nazionale;
   e) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;
   f) un elenco delle diverse autorità e dei diversi portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cybersicurezza;
   g) un quadro strategico per il coordinamento rafforzato tra le autorità competenti ai sensi del presente decreto e le autorità competenti di cui al decreto legislativo di recepimento della direttiva (UE) 2022/2557 ai fini della condivisione delle informazioni sui rischi, le minacce e gli incidenti sia informatici che non informatici e dello svolgimento di compiti di vigilanza, in modo adeguato;
   h) un piano, comprendente le misure necessarie, per aumentare il livello generale di consapevolezza dei cittadini in materia di sicurezza informatica.
3. Nell'ambito della strategia nazionale per la cybersicurezza, sono previste, inoltre, le seguenti misure strategiche:

a) la sicurezza informatica nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati dai soggetti per la fornitura dei loro servizi;
b) l'inclusione e la definizione di requisiti concernenti la sicurezza informatica per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cybersicurezza, alla cifratura e all'utilizzo di prodotti di sicurezza informatica open source;
c) la gestione delle vulnerabilità, ivi comprese la promozione e l'agevolazione della divulgazione coordinata delle vulnerabilità di cui all'articolo 16;
d) il sostegno della disponibilità generale, dell'integrità e della riservatezza del nucleo pubblico della rete internet aperta, compresa, se del caso, la sicurezza informatica dei cavi di comunicazione sottomarini;
e) la promozione dello sviluppo e dell'integrazione di tecnologie avanzate rilevanti, volte ad attuare misure all'avanguardia nella gestione dei rischi per la sicurezza informatica;
f) la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di sicurezza informatica, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti;
g) il sostegno agli istituti accademici e di ricerca volto a sviluppare, rafforzare e promuovere la diffusione di strumenti di sicurezza informatica e di infrastrutture di rete sicure;
h) la messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla sicurezza informatica tra soggetti, nel rispetto del diritto dell'Unione europea;
i) il rafforzamento dei valori di riferimento relativi alla resilienza e all'igiene informatica delle piccole e medie imprese, in particolare quelle escluse dall'ambito di applicazione del presente decreto, fornendo orientamenti e sostegno facilmente accessibili per le loro esigenze specifiche;
l) la promozione di una protezione informatica attiva.

4. Ferme restando le funzioni del Presidente del Consiglio dei ministri di cui all'articolo 2, commi 1 e 2, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, l'Agenzia per la cybersicurezza nazionale provvede ai sensi dell'articolo 7 del citato decreto-legge n. 82 del 2021, alla periodica valutazione della Strategia nazionale di cybersicurezza, nonché al suo aggiornamento ove necessario e comunque almeno ogni cinque anni sulla base di indicatori chiave di prestazione, proponendone l'adozione al Presidente del Consiglio dei ministri con le modalità di all'articolo 2, comma 1, lettera b), del medesimo decreto-legge.

ART. 10

(Autorità nazionale competente e Punto di contatto unico)

1. L'Agenzia per la cybersicurezza nazionale è l'Autorità nazionale competente NIS di cui all'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555 e pertanto:
   a) sovrintende all'implementazione e all'attuazione del presente decreto;
   b) predispone i provvedimenti necessari a dare attuazione al presente decreto;
   c) svolge le funzioni e le attività di regolamentazione di cui al presente decreto, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti;
   d) individua i soggetti essenziali e importanti ai sensi degli articoli 3 e 6, nonché redige l'elenco di cui all'articolo 7, comma 2;
   e) partecipa al Gruppo di cooperazione NIS, nonché ai consessi e alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555;
   f) definisce gli obblighi di cui all'articolo 7, comma 6, e al capo IV;
   g) svolge le attività ed esercita i poteri di vigilanza ed esecuzione di cui al capo V.
2. L'Agenzia per la cybersicurezza nazionale è il Punto di contatto unico NIS di cui all'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555, svolgendo una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità nazionali con le autorità pertinenti degli altri Stati membri, la Commissione e l'ENISA.

ART. 11

(Autorità di settore NIS)

1. Al fine di assicurare l'efficace attuazione del presente decreto a livello settoriale, sono individuate le Autorità di settore NIS che supportano l'Autorità nazionale competente NIS e collaborano con essa, secondo le modalità di cui all'articolo 40, comma 2, lettera c).
2. Sono designate quali Autorità di settore NIS:
   a) la Presidenza del Consiglio dei ministri per:
      1) il settore gestione dei servizi TIC, di cui al numero 9 dell'allegato I, in collaborazione con l'Agenzia per la cybersicurezza nazionale;
      2) il settore dello spazio, di cui al numero 10 dell'allegato I;
      3) il settore delle pubbliche amministrazioni, di cui all'articolo 3, commi 6 e 7, e all'allegato III;
      4) le società in house e le società partecipate o a controllo pubblico, di cui al numero 4 dell'allegato IV;
   b) il Ministero dell'economia e delle finanze, per i settori bancario e delle infrastrutture dei mercati finanziari, di cui ai numeri 3 e 4 dell'allegato I, sentite le autorità di vigilanza di settore, Banca d'Italia e Consob;
   c) il Ministero delle imprese e del made in Italy per:
      1) il settore delle infrastrutture digitali, di cui al numero 8 dell'allegato I;
      2) il settore dei servizi postali e di corriere, di cui al numero 1 dell'allegato II;
      3) il settore della fabbricazione, produzione e distribuzione di sostanze chimiche, di cui al numero 3 dell'allegato II, sentito il Ministero dell'ambiente e della sicurezza energetica e il Ministero della salute;

4) i sottosettori della fabbricazione di computer e prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche e della fabbricazione di macchinari e apparecchiature n.c.a., di cui alle lettere b), c) e d) del settore fabbricazione, di cui al numero 5 dell'allegato II;
5) i sottosettori della fabbricazione di autoveicoli, rimorchi e semirimorchi, e della fabbricazione di altri mezzi di trasporto, di cui alle lettere e) e f) del settore fabbricazione, di cui al numero 5 dell'allegato II, sentito il Ministero delle infrastrutture e dei trasporti;
6) i fornitori di servizi digitali, di cui al numero 6 dell'allegato II;

d) il Ministero dell'agricoltura, della sovranità alimentare e delle foreste per il settore produzione, trasformazione e distribuzione di alimenti, di cui al numero 4 dell'allegato II;
e) il Ministero dell'ambiente e della sicurezza energetica per:
1) il settore energia, di cui al numero 1 dell'allegato I;
2) i settori:
2.1) fornitura e distribuzione di acqua potabile, di cui al numero 6 dell'allegato I;
2.2) acque reflue, di cui al numero 7 dell'allegato I;
2.3) gestione rifiuti, di cui al numero 2 dell'allegato II;

f) il Ministero delle infrastrutture e dei trasporti per:
1) il settore trasporti, di cui al numero 2 dell'allegato I;
2) i soggetti che forniscono servizi di trasporto pubblico locale di cui al numero 1 dell'allegato IV;

g) il Ministero dell'università e della ricerca per il settore ricerca di cui al numero 7 dell'allegato II e per gli istituti di istruzione che svolgono attività di ricerca di cui al numero 2 dell'allegato IV;
h) il Ministero della cultura per i soggetti che svolgono attività di interesse culturale di cui al numero 3 dell'allegato IV;
i) il Ministero della salute per:
1) il settore sanitario, di cui al numero 5 dell'allegato I;
2) il sottosettore fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, di cui alla lettera a) del settore fabbricazione, di cui al numero 5 dell'allegato II;

3. Le Amministrazioni di cui al comma 2, per i rispettivi settori di competenza, sono altresì designate Autorità di settore per i soggetti di cui all'articolo 3, commi 9 e 10.
4. Le Autorità di settore NIS, per i rispettivi settori di competenza ai fini di cui al comma 1, procedono, in particolare:
a) alla verifica dell'elenco dei soggetti di cui all'articolo 7, comma 2;
b) al supporto nell'individuazione dei soggetti essenziali e importanti ai sensi degli articoli 3 e 6, in particolare identificando i soggetti essenziali e importanti di cui ai commi 8, 9 e 10 dell'articolo 3;
c) all'individuazione dei soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;

d) al supporto per le funzioni e le attività di regolamentazione di cui al presente decreto secondo le modalità di cui all'articolo 40;
e) all'elaborazione dei contributi per la relazione annuale di cui all'articolo 12, comma 5;
f) all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione settoriale del presente decreto nonché al relativo monitoraggio. Per la partecipazione ai tavoli settoriali non sono previsti gettoni di presenza, compensi o rimborsi di spese;
g) alla partecipazione alle attività settoriali del Gruppo di Cooperazione NIS nonché dei consessi e delle iniziative a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555.

5. Con accordo definito in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono definite modalità di collaborazione tra le Autorità di settore e le regioni interessate, quando il soggetto critico ha carattere regionale ovvero opera esclusivamente sul territorio di una regione nei settori di cui al comma 2, lettere a), numeri 3 e 4, e), numero 2, e i), numero 1.

ART. 12
(Tavolo per l'attuazione della disciplina NIS)

1. Presso l'Agenzia per la cybersicurezza nazionale è costituito, in via permanente, il Tavolo per l'attuazione della disciplina NIS, per assicurare l'implementazione e attuazione del presente decreto.
2. Il Tavolo per l'attuazione della disciplina NIS è presieduto dal direttore generale dell'Agenzia per la cybersicurezza nazionale, o da un suo delegato, ed è composto da un rappresentante di ogni Autorità di settore NIS di cui all'articolo 11 e da due rappresentanti designati da regioni e province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano.
3. I componenti del Tavolo per l'attuazione della disciplina NIS possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati dalle previsioni di cui al presente decreto.
4. Il Tavolo per l'attuazione della disciplina NIS è convocato su indicazione del presidente o su richiesta di almeno tre componenti e si riunisce almeno una volta per trimestre.
5. Per le finalità di cui al comma 1, il Tavolo per l'attuazione della disciplina NIS:
   a) supporta l'Autorità nazionale competente NIS nello svolgimento delle funzioni relative all'implementazione e all'attuazione del presente decreto, con particolare riferimento a quanto previsto dall'articolo 10, comma 1, lettere da a) a f);
   b) formula proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo ai fini dell'efficace attuazione del presente decreto;

c) predispone una relazione annuale sull'attuazione del presente decreto.

6. Per la partecipazione al Tavolo per l'attuazione della disciplina NIS non sono previsti gettoni di presenza, compensi, rimborsi di spese o altri emolumenti, comunque denominati.

ART. 13

(Quadro nazionale di gestione delle crisi informatiche)

1. L'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e il Ministero della Difesa sono individuati quali Autorità nazionali di gestione delle crisi informatiche, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g).
2. Le Autorità nazionali di gestione delle crisi informatiche individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini del presente decreto.
3. Entro dodici mesi dalla data di entrata in vigore del presente decreto, con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale e del Ministero della Difesa, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g), previo parere del Comitato interministeriale per la sicurezza della Repubblica nella composizione di cui all'articolo 10 del decreto-legge n. 82 del 2021, è definito il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala. Il piano di cui al primo periodo è aggiornato periodicamente e, comunque, ogni tre anni.
4. Il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala stabilisce gli obiettivi e le modalità di gestione dei medesimi. In tale piano sono definiti, in particolare:
   a) gli obiettivi delle misure e delle attività nazionali di preparazione;
   b) i compiti e le responsabilità delle Autorità nazionali di gestione delle crisi informatiche;
   c) le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza di cui all'articolo 10 del decreto-legge 4 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, e i canali di scambio di informazioni;
   d) le misure nazionali di preparazione, comprese le esercitazioni e le attività di formazione;
   e) i pertinenti portatori di interessi del settore pubblico e privato e le infrastrutture coinvolte;
   f) le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dell'Italia alla gestione coordinata degli incidenti e delle crisi informatiche su vasta scala a livello dell'Unione europea.
5. I decreti del Presidente del Consiglio dei ministri di cui al presente articolo sono esclusi dall'accesso e non sono soggetti a pubblicazione.

ART. 14

(Cooperazione tra Autorità nazionali)

1. Sono assicurate la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS con l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto), il Garante per la protezione dei dati personali quale autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679, l'Ente nazionale per l'aviazione civile (ENAC) quale autorità nazionale ai sensi dei regolamenti (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, e (UE) 2018/1139, del Parlamento europeo e del Consiglio, del 4 luglio 2018, l'Agenzia per l'Italia digitale (AgID) quale organismo di vigilanza ai sensi del regolamento (UE) n. 910/2014, l'Autorità per le garanzie nelle comunicazioni quale autorità nazionale di regolamentazione ai sensi della direttiva (UE) 2018/1972, con il Ministero della Difesa, quale responsabile in materia di difesa e sicurezza militare dello Stato, nonché con altre autorità nazionali competenti anche ai sensi di altri atti giuridici settoriali dell'Unione europea, ivi incluso lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.
2. Ai fini della cooperazione e della collaborazione di cui al comma 1:
   a) l'Autorità nazionale competente NIS coopera con il Garante per la protezione dei dati personali, ai sensi dell'articolo 7, comma 5, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, nei casi di incidenti che comportano violazioni di dati personali, ai sensi del regolamento (UE) 2016/679, senza pregiudicare la competenza e i compiti di controllo di cui al citato regolamento;
   b) qualora l'Autorità nazionale competente NIS, in sede di vigilanza o di esecuzione, venga a conoscenza del fatto che la violazione degli obblighi di cui all'articolo 24 da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, quale definita all'articolo 4, punto 12), del regolamento (UE) 2016/679, che deve essere notificata ai sensi dell'articolo 33 del medesimo regolamento, ne informa senza indebito ritardo il Garante per la protezione dei dati personali ai sensi dell'articolo 55 o 56 di tale regolamento;
   c) qualora il Garante per la protezione dei dati personali o le autorità di controllo di altri Stati membri di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria ai sensi dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, l'Autorità nazionale competente NIS non procede all'irrogazione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 38 per una violazione di cui alla lettera b) del presente comma, imputabile al medesimo comportamento. L'Autorità nazionale competente NIS può tuttavia esercitare i poteri di esecuzione di cui all'articolo 37;

d) con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro della difesa, è definito, nell'ambito dell'elenco di cui all'articolo 7, comma 2, l'elenco dei soggetti che impattano sulla efficienza dello Strumento militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'Autorità nazionale competente NIS comunica tempestivamente al Ministero della difesa gli incidenti di cui all'articolo 25, nonché, con le modalità previste nel decreto di cui alla presente lettera, le ulteriori informazioni di sicurezza cibernetica;

3. È assicurata la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 3, lettera b), punto 1), con le autorità nazionali competenti di cui al regolamento (UE) 2022/2554 e al decreto legislativo che recepisce la direttiva (UE) 2022/2556, in relazione, tra l'altro, allo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.
4. Ai fini della cooperazione e della collaborazione di cui al comma 3, l'Autorità nazionale competente NIS coopera con le pertinenti autorità nazionali competenti degli altri Stati membri, di cui al regolamento (UE) 2022/2554. In particolare, l'Autorità nazionale competente NIS informa il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercita i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dal presente decreto da parte di un soggetto essenziale designato come fornitore terzo critico di servizi di TIC ai sensi dell'articolo 31 del regolamento (UE) 2022/2554;
5. È assicurata la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS, secondo le modalità di cui all'articolo 40, comma 3, lettera b), punto 2), con le autorità nazionali competenti e il punto di contatto unico ai sensi della direttiva (UE) 2022/2557, anche con lo scambio periodico di informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557, e sulle misure adottate in risposta a tali rischi, minacce e incidenti.
6. Ai fini della cooperazione e della collaborazione di cui al comma 5:
   a) il punto di contatto unico e le autorità competenti di cui al decreto legislativo comunicano tempestivamente all'Autorità nazionale competente NIS i soggetti identificati come soggetti critici ai sensi del decreto legislativo di recepimento della direttiva (UE) 2022/2557 e successivi aggiornamenti;
   b) le autorità nazionali competenti ai sensi del decreto legislativo di recepimento della direttiva (UE) 2022/2557 possono chiedere all'Autorità nazionale competente NIS di svolgere le attività ed esercitare i poteri di cui al capo V in relazione a un soggetto che è stato individuato come soggetto critico ai sensi del citato decreto legislativo.

ART. 15

(Gruppo nazionale di risposta agli incidenti di sicurezza informatica – CSIRT Italia)

1. Il CSIRT Italia, fermo restando quanto previsto dal decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109:
   a) è l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i settori, i sottosettori e le tipologie di soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso;
   b) dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale attraverso la quale scambiare informazioni con i soggetti essenziali o importanti e con gli altri portatori di interesse pertinenti;
   c) coopera e, se opportuno, scambia informazioni pertinenti conformemente all'articolo 17 con comunità settoriali o intersettoriali di soggetti essenziali e importanti;
   d) partecipa alla revisione tra pari di cui all'articolo 21;
   e) garantisce la collaborazione effettiva, efficiente e sicura, nella Rete di CSIRT nazionali di cui all'articolo 20;
   f) ai sensi dell'articolo 7, comma 1, lettera s), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, può stabilire relazioni di cooperazione con gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi. Nell'ambito di tali relazioni di cooperazione, facilita uno scambio di informazioni efficace, efficiente e sicuro con tali CSIRT nazionali, o strutture nazionali equivalenti di Paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, ivi inclusi quelli adottati e sviluppati dalle principali comunità nazionali, europee e internazionali del settore. Il CSIRT Italia può scambiare informazioni pertinenti con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, compresi dati personali ai sensi della normativa nazionale vigente e del diritto dell'Unione europea in materia di protezione dei dati personali;
   g) ai sensi dell'articolo 7, comma 1, lettera s), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, può cooperare con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, in particolare al fine di fornire loro assistenza in materia di sicurezza informatica.
2. Il CSIRT Italia:
   a) è dotato di un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di malfunzionamento e dispone di mezzi che gli permettono di essere contattato e di contattare i soggetti e altri CSIRT nazionali in qualsiasi momento. Il CSIRT Italia indica chiaramente i canali di comunicazione e li rende noti ai soggetti e agli altri CSIRT nazionali;
   b) dispone di locali e sistemi informativi di supporto ubicati in siti sicuri;
   c) utilizza un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;
   d) garantisce la riservatezza e l'affidabilità delle proprie attività;
   e) è dotato di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei propri servizi;

f) partecipa, se del caso, a reti di cooperazione internazionale.

3. Il CSIRT Italia svolge i seguenti compiti:
   a) monitora e analizza le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale e, su richiesta, fornisce assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informativi e di rete, secondo un ordine di priorità delle attività definito dal CSIRT Italia, onde evitare oneri sproporzionati o eccessivi;
   b) emette preallarmi, allerte e bollettini e divulga informazioni ai soggetti essenziali e importanti interessati, nonché alle autorità nazionali competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;
   c) fornisce una risposta agli incidenti e assistenza ai soggetti essenziali e importanti interessati, ove possibile;
   d) raccoglie e analizza dati forensi e fornisce un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla sicurezza informatica;
   e) effettua, su richiesta di un soggetto essenziale o importante, secondo modalità e procedure definite, una scansione proattiva dei sistemi informativi e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;
   f) partecipa alla Rete di CSIRT nazionali di cui all'articolo 20 e fornisce assistenza reciproca secondo le proprie capacità e competenze agli altri membri della Rete di CSIRT nazionali su loro richiesta;
   g) agisce in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 16;
   h) contribuisce allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui al comma 1, lettera b);
   i) può effettuare, secondo modalità e procedure definite, una scansione proattiva e non intrusiva dei sistemi informativi e di rete accessibili al pubblico di soggetti essenziali e importanti. Tale scansione è effettuata per individuare sistemi informativi e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti.
4. Il CSIRT Italia applica un approccio basato sul rischio per stabilire l'ordine di priorità nello svolgimento dei compiti di cui al comma 3.
5. In caso di eventi malevoli per la sicurezza informatica, le strutture pubbliche con funzione di *computer emergency response team* (CERT) collaborano con il CSIRT Italia, anche ai fini di un più efficace coordinamento della risposta agli incidenti.
6. Il CSIRT Italia instaura rapporti di cooperazione con i pertinenti portatori di interesse nazionali del settore privato al fine di perseguire gli obiettivi del presente decreto in relazione alle proprie competenze.
7. Al fine di agevolare la cooperazione di cui al comma 5, il CSIRT Italia promuove l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda:
   a) le procedure di gestione degli incidenti;

b) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 16.

ART. 16

(Divulgazione coordinata delle vulnerabilità)

1. Il CSIRT Italia è designato coordinatore ai fini della divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12 della direttiva (UE) 2022/2555 e agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti.
2. I compiti del CSIRT Italia in veste di coordinatore comprendono:
   a) l'individuazione e il contatto dei soggetti interessati;
   b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità;
   c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti.
3. Le persone fisiche o giuridiche possono segnalare in forma anonima, qualora lo richiedano, una vulnerabilità al CSIRT Italia. Quest'ultimo, in veste di coordinatore, garantisce lo svolgimento di diligenti azioni per dare seguito alla segnalazione di vulnerabilità e assicura l'anonimato della persona fisica o giuridica segnalante. Se la vulnerabilità segnalata è suscettibile di avere un impatto significativo su soggetti in più di uno Stato membro, il CSIRT Italia coopera, ove opportuno, con altri CSIRT designati in qualità di coordinatori nell'ambito della Rete di CSIRT nazionali di cui all'articolo 20.
4. L'Autorità nazionale competente NIS adotta, secondo le modalità di cui all'articolo 40, comma 5, una politica nazionale di divulgazione coordinata delle vulnerabilità in linea con le previsioni del presente decreto e tenuto conto degli orientamenti non vincolanti del Gruppo di cooperazione NIS. L'Agenzia per la cybersicurezza nazionale implementa mezzi tecnici per agevolare l'attuazione della politica nazionale di divulgazione coordinata delle vulnerabilità.

ART. 17

(Accordi di condivisione delle informazioni sulla sicurezza informatica)

1. I soggetti che rientrano nell'ambito di applicazione del presente decreto e laddove opportuno anche ulteriori soggetti, possono scambiarsi, su base volontaria, pertinenti informazioni sulla sicurezza informatica, comprese informazioni relative a minacce informatiche, quasi-incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di sicurezza informatica e raccomandazioni concernenti la configurazione degli

strumenti di sicurezza informatica per individuare le minacce informatiche, se tale condivisione di informazioni:

a) mira a prevenire o rilevare gli incidenti, a recuperare dagli stessi o a mitigarne l'impatto;
b) aumenta il livello di sicurezza informatica, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di mitigazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati.

2. Lo scambio di informazioni di cui al comma 1 avviene nell'ambito di comunità di soggetti essenziali e importanti e, se opportuno, dei loro fornitori o fornitori di servizi. Tale scambio è attuato mediante accordi di condivisione delle informazioni sulla sicurezza informatica che tengono conto della natura potenzialmente sensibile delle informazioni condivise.
3. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, ove possibile, tenuto conto degli orientamenti e delle migliori pratiche non vincolanti elaborati da ENISA, favorisce la conclusione degli accordi di condivisione delle informazioni sulla sicurezza informatica di cui al comma 2 e può specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni. Nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, l'Autorità nazionale competente NIS può imporre condizioni per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, supporta i soggetti essenziali ed importanti per l'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 9, comma 3, lettera h).
4. I soggetti essenziali e importanti notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica di cui al comma 2 al momento della conclusione di tali accordi o, ove applicabile, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.
5. È assicurato l'accesso degli Organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007 alle informazioni riguardanti l'elenco dei soggetti essenziali e importanti, tramite la piattaforma digitale di cui all'articolo 7, le notifiche di cui agli articoli 25 e 26, le vulnerabilità rilevate nell'applicazione del presente decreto, e le ulteriori informazioni rispetto a quelle di cui al primo periodo che dovessero essere ritenute utili, relative alle attività di cui al presente decreto, previe intese tra i predetti Organismi e l'Agenzia per la cybersicurezza nazionale.

Capo III
Cooperazione a livello dell'Unione europea e internazionale

ART. 18
(Gruppo di cooperazione NIS)

1. L'Autorità nazionale competente NIS partecipa al Gruppo di cooperazione NIS.
2. Le Autorità di settore NIS partecipano, su richiesta dell'Autorità nazionale competente NIS, alle iniziative del Gruppo di cooperazione NIS relative al proprio settore di interesse.
3. Ai fini dei commi 1 e 2, l'Autorità nazionale competente NIS, supportata dalle Autorità di settore NIS interessate, provvede a:
   a) tenere conto degli orientamenti non vincolanti del Gruppo di cooperazione NIS in merito al recepimento e all'attuazione della direttiva (UE) 2022/2555;
   b) tenere conto degli orientamenti non vincolanti del Gruppo di cooperazione NIS in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 16;
   c) scambiare migliori prassi e informazioni relative all'attuazione della direttiva (UE) 2022/2555, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi-incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, specifiche tecniche anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012, nonché all'identificazione dei soggetti essenziali e importanti ai sensi del presente decreto;
   d) effettuare scambi di opinioni per quanto riguarda l'attuazione degli atti giuridici settoriali dell'Unione europea che contengono disposizioni in materia di sicurezza informatica;
   e) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 21;
   f) richiedere, se del caso, una discussione sulle relazioni sulle revisioni tra pari di cui all'articolo 21 che coinvolgono l'Autorità nazionale competente NIS e l'elaborazione di conclusioni e di raccomandazioni a riguardo;
   g) discutere casi di assistenza reciproca, ivi incluse le esperienze e i risultati delle azioni di vigilanza comuni transfrontaliere di cui all'articolo 39;
   h) su richiesta di uno o più Stati membri, discutere le richieste specifiche di assistenza reciproca di cui all'articolo 39;
   i) richiedere, se opportuno, la discussione di richieste specifiche di assistenza reciproca di cui all'articolo 39 che coinvolgono l'Autorità nazionale competente NIS;
   l) scambiare opinioni su misure per mitigare la ricorrenza di incidenti e crisi di sicurezza informatica su vasta scala sulla base degli insegnamenti tratti da EU–CyCLONe e dalla Rete di CSIRT nazionali;
   m) partecipare, ove necessario, ai programmi di sviluppo delle capacità, anche prevedendo lo scambio di personale tre le Autorità nazionali e quelle di altri Stati membri;
   n) discutere le attività intraprese per quanto riguarda le esercitazioni in materia di sicurezza informatica, comprese le attività svolte dall'ENISA;

o) partecipare alle riunioni congiunte con il gruppo per la resilienza dei soggetti critici istituito ai sensi della direttiva (UE) 2022/2557, volte a promuovere e ad agevolare la cooperazione strategica e lo scambio di informazioni nell'attuazione della direttiva medesima e della direttiva (UE) 2022/2555.

4. Inoltre, ai fini dei commi 1 e 2, l'Autorità nazionale competente NIS, supportata dalle Autorità di settore NIS interessate, contribuisce:
   a) alla definizione degli orientamenti non vincolanti per le autorità competenti in merito al recepimento e all'attuazione della direttiva (UE) 2022/2555;
   b) alla definizione degli orientamenti non vincolanti del Gruppo di cooperazione NIS in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 16;
   c) alla definizione di pareri non vincolanti e alla cooperazione con la Commissione europea per quanto riguarda le nuove iniziative strategiche in materia di sicurezza informatica e la coerenza dei requisiti settoriali di informatica;
   d) alla definizione di pareri non vincolanti e alla cooperazione con la Commissione europea per quanto riguarda i progetti di atti delegati o di esecuzione adottati ai sensi della direttiva (UE) 2022/2555;
   e) allo scambio delle migliori prassi e di informazioni con le Istituzioni, gli Organismi, gli Uffici e le Agenzie pertinenti dell'Unione europea;
   f) se del caso, all'elaborazione di conclusioni e di raccomandazioni circa le relazioni sulle revisioni tra pari di cui all'articolo 21;
   g) all'elaborazione delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche conformemente all'articolo 22, paragrafo 1, della direttiva (UE) 2022/2555;
   h) alla definizione degli orientamenti strategici per EU–CyCLONe e per la Rete di CSIRT nazionali su specifiche questioni emergenti;
   i) al rafforzamento delle capacità di sicurezza informatica a livello dell'Unione europea;
   l) all'organizzazione di riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato dell'Unione europea per discutere le attività svolte dal Gruppo di cooperazione NIS e raccogliere contributi sulle sfide strategiche emergenti;
   m) alla definizione della metodologia e degli aspetti organizzativi delle revisioni tra pari di cui all'articolo 21 nonché della metodologia di autovalutazione per gli Stati membri e all'elaborazione dei codici di condotta su cui si basano i metodi di lavoro degli esperti di sicurezza informatica designati di cui al medesimo articolo;
   n) all'elaborazione delle relazioni, ai fini del riesame di cui all'articolo 40 della direttiva (UE) 2022/2555, sull'esperienza acquisita a livello strategico e dalle revisioni tra pari sull'attuazione della direttiva stessa;
   o) alla discussione e allo svolgimento periodico di valutazione dello stato di avanzamento delle minacce o degli incidenti informatici, ivi inclusi i ransomware;
   p) alla collaborazione con ENISA e con la Commissione europea per la pubblicazione della relazione biennale sullo stato della sicurezza informatica nell'Unione europea di cui all'articolo 18, paragrafo 1, della direttiva (UE) 2022/2555;

q) alla collaborazione con ENISA, con la Commissione europea e con la Rete di CSIRT nazionali, per la definizione della metodologia di cui all'articolo 18, paragrafo 3, della direttiva (UE) 2022/2555, per l'elaborazione della relazione biennale sullo stato della sicurezza informatica nell'Unione europea.

ART. 19

(Rete delle organizzazioni di collegamento per le crisi informatiche - EU-CyCLONe)

1. L'Autorità nazionale di gestione delle crisi informatiche partecipa alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).
2. Ai fini del comma 1, l'Autorità nazionale di gestione delle crisi informatiche contribuisce a:
   a) aumentare il livello di preparazione per la gestione di incidenti e crisi informatiche su vasta scala;
   b) sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi informatiche su vasta scala;
   c) valutare le conseguenze e l'impatto degli incidenti e delle crisi informatiche su vasta scala e proporre possibili misure di attenuazione;
   d) coordinare la gestione degli incidenti e delle crisi informatiche su vasta scala e sostenere il processo decisionale a livello politico in merito a tali incidenti e crisi;
   e) discutere, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 9, paragrafo 4, della direttiva (UE) 2022/2555;
   f) supportare la collaborazione con il Gruppo di cooperazione NIS al fine di aggiornarlo in merito alla gestione degli incidenti e delle crisi informatiche su vasta scala, nonché in merito alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti;
   g) cooperare con la Rete di CSIRT nazionali;
   h) elaborare la relazione al Parlamento europeo e al Consiglio sulla valutazione del lavoro della Rete di cui all'articolo 16, paragrafo 7, della direttiva (UE) 2022/2555.
3. L'Autorità nazionale di gestione delle crisi informatiche, ai sensi del comma 2, lettera e), può richiedere di discutere il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3.

ART. 20

(Rete di CSIRT nazionali)

1. Il CSIRT Italia partecipa alla Rete di CSIRT nazionali.
2. Il CSIRT Italia, ai fini del comma 1, contribuisce a:
   a) scambiare informazioni per quanto riguarda le capacità dei CSIRT;

b) agevolare, ove possibile, la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT nazionali;

c) scambiare su richiesta di un CSIRT nazionale di uno altro Stato membro potenzialmente interessato da un incidente, informazioni relative a tale incidente, alle minacce informatiche, ai rischi e alle vulnerabilità associate;

d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di sicurezza informatica;

e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni;

f) su richiesta di un membro della Rete di CSIRT nazionali potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente, ai rischi e alle vulnerabilità associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;

g) su richiesta di un membro della Rete di CSIRT nazionali, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

h) fornire assistenza ai CSIRT nazionali di altri Stati membri nel far fronte a incidenti che interessano due o più Stati membri;

i) cooperare e scambiare migliori pratiche con i CSIRT nazionali designati dagli altri Stati membri in qualità di coordinatori ai sensi dell'articolo 12 della direttiva (UE) 2022/2555, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;

l) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a:

1) categorie di minacce informatiche e incidenti;

preallarmi;

2) assistenza reciproca;

3) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;

4) contributi al piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all’articolo 13, comma 3, su richiesta di uno Stato membro;

m) su richiesta di un membro della Rete di CSIRT nazionali, discutere le capacità e lo stato di preparazione del CSIRT nazionale richiedente;

n) cooperare e scambiare informazioni con i centri operativi di sicurezza informatica regionali e a livello dell'Unione europea, al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche a livello dell'Unione europea;

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 21;

p) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi-incidenti, le minacce informatiche, i rischi e le vulnerabilità;

q) informare il Gruppo di cooperazione NIS sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera i) e, se necessario, chiedere orientamenti non vincolanti in merito;

r) fare il punto sui risultati delle esercitazioni di sicurezza informatica, comprese quelle organizzate dall'ENISA;

s) fornire orientamenti non vincolanti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

ART. 21

(Procedura di revisione tra pari)

1. L'Autorità nazionale competente NIS può partecipare alla procedura di revisione tra pari, di cui all'articolo 19 della direttiva (UE) 2022/2555, nel quadro della metodologia di cui all'articolo 18, comma 4, lettera m), del presente decreto:
   a) richiedendo l'esecuzione di una revisione tra pari in relazione all'attuazione della direttiva (UE) 2022/2555 a livello nazionale;
   b) indicando uno o più rappresentanti dell'Agenzia per la cybersicurezza nazionale o delle Autorità di settore NIS quali esperti di sicurezza informatica, di cui all'articolo 19, paragrafo 2, della direttiva (UE) 2022/2555, per eseguire revisioni tra pari presso altri Stati membri, su richiesta di questi ultimi, nel rispetto dei codici di condotta di cui all'articolo 18, comma 4, lettera m), del presente decreto. Eventuali rischi di conflitto di interessi riguardanti gli esperti di sicurezza informatica designati sono condivisi con gli altri Stati membri, il Gruppo di cooperazione NIS, la Commissione europea e l'ENISA prima dell'inizio della revisione tra pari.
2. Ai fini di cui al comma 1, lettera a), l'Autorità nazionale competente NIS:
   a) provvede a identificare almeno un aspetto da sottoporre alla revisione tra pari tra i seguenti:
      1) il livello di attuazione degli obblighi in materia di misure di gestione del rischio e di notifica degli incidenti di cui agli articoli 24 e 25;
      2) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti dell'Autorità medesima;
      3) le capacità operative del CSIRT Italia;
      4) lo stato di attuazione dell'assistenza reciproca di cui all'articolo 39;
      5) lo stato di attuazione degli accordi per la condivisione delle informazioni in materia di sicurezza informatica di cui all'articolo 17;
      6) questioni specifiche di natura transfrontaliera o intersettoriale;
   b) notifica, prima dell'inizio della revisione tra pari, agli Stati membri partecipanti, l'ambito di applicazione della medesima, comprese le questioni specifiche individuate;
   c) effettua, se del caso, un'autovalutazione degli aspetti oggetto della revisione;
   d) seleziona, tra gli esperti di sicurezza informatica indicati dagli altri Stati membri partecipanti, gli esperti idonei da designare. Qualora l'Autorità nazionale competente

NIS si opponga alla designazione di uno o più esperti indicati, comunica allo Stato membro indicante i motivi debitamente giustificati;

e) fornisce, se del caso, l'autovalutazione di cui alla lettera c) agli esperti designati di cui alla lettera d);

f) fornisce agli esperti designati di cui alla lettera d) le informazioni necessarie per la valutazione, anche con visite in loco fisiche o virtuali, nonché scambi di informazioni a distanza;

g) formula, se del caso, osservazioni sulla relazione elaborata dagli esperti designati di cui alla lettera d);

h) può decidere di rendere pubblica la relazione elaborata dagli esperti designati di cui alla lettera d), alla quale sono allegate, in tutto o in parte, le osservazioni di cui alla lettera g).

3. Ai fini di cui al comma 1, lettera b), gli esperti di sicurezza informatica indicati dall'Autorità nazionale competente NIS:

a) non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso delle revisioni tra pari a cui partecipano;

b) partecipano alle attività necessarie allo svolgimento delle revisioni tra pari tramite visite in loco fisiche o virtuali e scambi di informazioni a distanza;

c) contribuiscono all'elaborazione delle relazioni sui risultati e sulle conclusioni delle revisioni tra pari.

4. La condivisione delle informazioni ai sensi del presente articolo è effettuata nel rispetto della legislazione nazionale o dell'Unione europea in materia di tutela delle informazioni protette da classifica di segretezza e di salvaguardia delle funzioni essenziali dello Stato, ivi inclusa la sicurezza nazionale.

ART. 22
(Comunicazioni all'Unione europea)

1. Successivamente alla data di entrata in vigore del presente decreto, la Presidenza del Consiglio dei ministri notifica tempestivamente alla Commissione europea la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS e quale Punto di contatto unico NIS, nonché la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della Difesa, quali Autorità nazionali di gestione delle crisi informatiche, e i relativi ambiti di competenza come indicati all'articolo 2, comma 1, lettera g). Successivamente, ogni ulteriore modifica a tali designazioni o compiti è notificata, senza ingiustificato ritardo, alla Commissione europea. Alle designazioni sono assicurate idonee forme di pubblicità.

2. L'Autorità nazionale competente NIS:

a) trasmette alla Commissione europea la Strategia nazionale di cybersicurezza di cui all'articolo 9 entro tre mesi dalla sua adozione o dal suo aggiornamento. Possono

essere esclusi dalla trasmissione gli elementi della strategia riguardanti la sicurezza nazionale e aspetti ulteriori alle previsioni del presente decreto;

b) comunica entro il 17 gennaio 2025 alla Commissione europea le misure sanzionatorie e le disposizioni che stabiliscono sanzioni nei confronti dei soggetti essenziali e importanti di cui al presente decreto. Successivamente, è comunicata ogni ulteriore modifica a tali misure e disposizioni;

c) comunica entro il 17 aprile 2025 e, successivamente, ogni due anni:

   1) alla Commissione europea e al Gruppo di cooperazione NIS, il numero dei soggetti essenziali e importanti nell'elenco di cui all'articolo 7, comma 2, per ciascun settore e sottosettore di cui agli allegati I, II e III;

   2) alla Commissione europea informazioni pertinenti sul numero di soggetti essenziali e importanti individuati ai sensi dell'articolo 3, comma 9, lettere da b) a e), sui settori e i sottosettori di cui agli allegati I, II e III ai quali appartengono, sul tipo di servizio che forniscono e sui criteri di cui all'articolo 3, comma 9, lettere da b) a e), per i quali sono stati individuati;

d) su richiesta della Commissione europea, può notificare a quest'ultima, in tutto o in parte, le denominazioni dei soggetti essenziali e importanti di cui alla lettera c), numero 2);

e) comunica all'ENISA, senza ingiustificato ritardo e comunque entro quattordici giorni dalla loro ricezione, le informazioni di cui all'articolo 7, comma 1, lettere a), b) e d), comma 4, lettera b), e comma 5, lettere a) e b), fornite dai soggetti di cui a quest'ultimo comma, per l'inserimento nel registro di cui all'articolo 27 della direttiva (UE) 2022/2555. L'Autorità nazionale competente NIS può richiedere ad ENISA l'accesso a tale registro, assicurando la tutela della riservatezza delle informazioni ivi contenute.

3. Il Punto di contatto unico NIS:

   a) successivamente alla data di entrata in vigore del presente decreto, comunica alla Commissione europea, senza ingiustificato ritardo, la designazione l'Agenzia per la cybersicurezza nazionale quale CSIRT nazionale, denominato CSIRT Italia, e quale coordinatore conformemente all'articolo 16, i rispettivi compiti in relazione ai soggetti essenziali e importanti e qualsiasi ulteriore modifica dei medesimi;

   b) trasmette all'ENISA, ogni trimestre a partire dal primo gennaio 2026 una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi-incidenti notificati ai sensi degli articoli 25 e 26;

   c) trasmette, successivamente alla data di entrata in vigore del presente decreto, senza ingiustificato ritardo, le notifiche di incidente con effetti transfrontalieri di cui agli articoli 25 e 26 ai punti di contatto unici degli altri Stati membri interessati e all'ENISA.

4. L'Autorità nazionale di gestione delle crisi informatiche comunica entro tre mesi dall'adozione o dall'aggiornamento del piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3, alla Commissione europea e alla Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) le informazioni pertinenti relative ai requisiti di cui all'articolo 13, comma 4,

in merito al proprio piano nazionale di risposta agli incidenti e delle crisi informatiche su vasta scala, fatto salvo quanto previsto dall'articolo 4, commi 1, 6 e 7.

Capo IV
Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente

ART. 23
(Organi di amministrazione e direttivi)

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti:
   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.
2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti:
   a) sono tenuti a seguire una formazione in materia di sicurezza informatica;
   b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro 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.
3. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.

ART. 24
(Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica)

1. I soggetti essenziali e importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:
   a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;

b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:
   a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
   b) gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;
   c) continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;
   d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
   e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
   f) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
   g) pratiche di igiene di base e di formazione in materia di sicurezza informatica;
   h) politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;
   i) sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
   l) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.
3. Nel valutare quali misure di cui al comma 2, lettera d), siano adeguate, i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.
4. Qualora un soggetto rilevi di non essere conforme alle misure di cui al comma 2, esso adotta, senza indebito ritardo, tutte le misure appropriate e proporzionate correttive necessarie.

ART. 25

(Obblighi in materia di notifica di incidente)

1. I soggetti essenziali e importanti notificano senza ingiustificato ritardo al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi di cui al comma 4, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

2. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente.
3. La notifica non espone il soggetto che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.
4. Un incidente è considerato significativo se:
   a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
   b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.
5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:
   a) senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;
   b) senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
   c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;
   d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:
      1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
      2) il tipo di minaccia o la causa originale (*root cause*) che ha probabilmente innescato l'incidente;
      3) le misure di attenuazione adottate e in corso;
      4) ove noto, l'impatto transfrontaliero dell'incidente;
   e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.
6. In deroga a quanto previsto dal comma 5, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, provvede alla notifica di cui alla medesima lettera, senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.
7. Fermo restando quanto previsto dall’articolo 15, comma 4, senza ingiustificato ritardo e ove possibile entro 24 ore dal ricevimento della pre-notifica di cui al comma 5, lettera a), il CSIRT Italia fornisce una risposta al soggetto notificante, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore supporto tecnico.

8. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT Italia fornisce al soggetto notificante anche orientamenti sulla segnalazione dell'incidente significativo, all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto).
9. Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e importanti comunicano senza ingiustificato ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.
10. I soggetti essenziali e importanti, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, comunicano senza ingiustificato ritardo, ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e importanti comunicano ai medesimi destinatari anche la natura di tale minaccia informatica significativa.
11. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, anche sentendo, se del caso, le autorità competenti e gli CSIRT nazionali degli altri Stati membri interessati, può informare il pubblico riguardo all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico.
12. L'Agenzia per la cybersicurezza nazionale adotta mezzi tecnici e relative procedure per semplificare le notifiche di cui al presente articolo e le notifiche volontarie di cui all'articolo 26, informando i soggetti essenziali e importanti.

ART. 26

(Notifica volontaria di informazioni pertinenti)

1. In aggiunta all'obbligo di notifica di incidente di cui all'articolo 25, possono essere trasmesse, su base volontaria, notifiche al CSIRT Italia, da parte dei:
   a) soggetti essenziali e importanti, per quanto riguarda gli incidenti diversi da quelli di cui all'articolo 25, comma 1, le minacce informatiche e i quasi-incidenti;
   b) soggetti diversi da quelli di cui alla lettera a), indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione del presente decreto, per quanto riguarda gli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi, le minacce informatiche e i quasi-incidenti.
2. Il CSIRT Italia:
   a) tratta le notifiche volontarie applicando la procedura di cui all'articolo 25;
   b) tratta le notifiche di incidente di cui all'articolo 25 prioritariamente rispetto alle notifiche volontarie;

c) tratta le notifiche volontarie soltanto qualora ciò non costituisca un onere sproporzionato o eccessivo.

3. Fatte salve le esigenze di indagine, accertamento e perseguimento di reati, la notifica volontaria di cui al comma 1 non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

ART. 27
(Uso di schemi di certificazione della cybersicurezza)

1. Al fine di dimostrare il rispetto di determinati obblighi di cui all'articolo 24, l'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può imporre ai soggetti essenziali e importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza di cui all'articolo 49 del regolamento (UE) 2019/881. Inoltre, l'Autorità nazionale competente NIS promuove l'utilizzo di servizi fiduciari qualificati da parte dei soggetti essenziali e importanti.
2. Nelle more dell'adozione di pertinenti sistemi europei di certificazione della cybersicurezza di cui all'articolo 49 del regolamento (UE) 2019/881, l'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può imporre ai soggetti essenziali e importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito di schemi di certificazione riconosciuti a livello nazionale o europeo.

ART. 28
(Specifiche tecniche)

1. Per favorire l'attuazione efficace e armonizzata dell'articolo 24, commi 1 e 2, l'Autorità nazionale competente NIS, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, promuove l'uso di specifiche tecniche europee e internazionali, anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012, relative alla sicurezza dei sistemi informativi e di rete.
2. Ai fini del comma 1, l'Autorità nazionale competente NIS tiene conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA ai sensi dell'articolo 25, paragrafo 2, della direttiva (UE) 2022/2555 e può redigere e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica.
3. L'elenco di cui al comma 2 non ha carattere vincolante o esaustivo ed è pubblicato sul sito dell'Agenzia per la cybersicurezza nazionale al fine di fornire un orientamento sulle specifiche tecniche, di cui al comma 1, e sulle norme di settore nazionali ed europee applicabili alle tipologie di soggetti di cui agli allegati I, II, III e IV del presente decreto.

ART. 29

(Banca dei dati di registrazione dei nomi di dominio)

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza dei sistemi di nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio raccolgono e mantengono dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione europea in materia di protezione dei dati personali.
2. Ai fini del comma 1, la banca dei dati di registrazione dei nomi di dominio contiene le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD (*top level domain*). Tali informazioni includono, almeno:
   a) il nome di dominio;
   b) la data di registrazione;
   c) il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione;
   d) l'indirizzo e-mail di contatto e il numero di telefono del punto di contatto che amministra il nome di dominio qualora siano diversi da quelli del soggetto che procede alla registrazione.
3. I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio predispongono e rendono pubbliche politiche e procedure, incluse le procedure di verifica, al fine di garantire che le banche dati di cui al comma 1 contengano informazioni accurate e complete.
4. I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio per i domini di primo livello rendono pubblicamente disponibili, senza ingiustificato ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali.
5. I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio, su richiesta motivata dei soggetti legittimati, forniscono l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione europea in materia di protezione dei dati. I soggetti che gestiscono i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondono senza ingiustificato ritardo e, comunque, entro 72 ore dalla ricezione della richiesta di accesso. Tale risposta reca gli specifici dati di registrazione dei nomi di dominio richiesti, ovvero le motivazioni per cui la richiesta non è stata ritenuta legittima o debitamente motivata. Le politiche e le procedure relative alla divulgazione di tali dati hanno evidenza pubblica.
6. Ai fini del comma 5, l'Agenzia per la cybersicurezza nazionale può richiedere l'accesso ai dati di registrazione dei nomi di dominio e può stipulare appositi protocolli con i gestori di registri dei nomi di dominio di primo livello e i fornitori di registrazione dei nomi di dominio.

7. Al fine di evitare una duplicazione della raccolta di dati di registrazione dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio individuano modalità e procedure di collaborazione per la raccolta e il mantenimento dei dati di cui al comma 1.

ART. 30

(Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi)

1. Ai fini di cui all'articolo 24, comma 1, dal primo maggio al 30 giugno di ogni anno a partire dalla ricezione della prima comunicazione di cui all'articolo 7, comma 3, lettera a), tramite piattaforma digitale di cui all'articolo 7, comma 1, i soggetti essenziali e importanti comunicano e aggiornano un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza.
2. L'Autorità nazionale competente NIS stabilisce, secondo le modalità di cui all'articolo 40, comma 5, anche tenuto conto dei criteri di cui all'articolo 25, comma 1, le categorie di rilevanza nonché il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi di cui al presente articolo.
3. Entro novanta giorni dalla comunicazione tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS fornisce riscontro ai soggetti essenziali e importanti circa la conformità di quanto comunicato rispetto alle modalità e ai criteri di cui al comma 2. Il predetto termine può essere prorogato dall'Autorità nazionale competente NIS, per una sola volta e fino ad un massimo di ulteriori sessanta giorni, qualora sia necessario svolgere approfondimenti. Ove si renda necessario richiedere integrazioni e informazioni aggiuntive ai soggetti essenziali o importanti, i termini di cui al presente comma sono interrotti sino alla data di ricevimento delle predette integrazioni e informazioni, che sono rese entro il termine di trenta giorni dalla richiesta.
4. In assenza del riscontro di cui al comma 3 da parte dall'Autorità nazionale competente NIS entro i termini di cui al medesimo comma, la conformità di cui al comma 3 si intende convalidata.
5. Ai fini del presente articolo, l'Autorità nazionale competente NIS può avvalersi dei tavoli settoriali di cui all'articolo 11.

ART. 31

(Proporzionalità e gradualità degli obblighi)

1. Ai fini di cui agli articoli 23, 24, 25, 27, 28 e 29 l'Autorità nazionale competente NIS stabilisce obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti a rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.
2. L'Autorità nazionale competente NIS stabilisce termini, modalità, specifiche e tempi graduali di implementazione degli obblighi di cui al comma 1, secondo le modalità di cui all'articolo 40, comma 5, anche differenziandoli in relazione:

a) alle categorie di rilevanza di cui all'articolo 30, comma 2, delle attività e dei servizi che i sistemi informativi e di rete supportano, svolgono o erogano;
b) al settore, al sottosettore e alla tipologia di soggetto, tenendo conto del grado di maturità iniziale nell'ambito della sicurezza informatica;
c) all'individuazione del soggetto quale essenziale o importante.

3. L'Autorità nazionale competente NIS individua, se del caso, le fattispecie che determinano la sospensione dei termini di cui al comma 2.
4. L'Autorità nazionale competente NIS può emanare linee guida vincolanti per l'attuazione degli obblighi di cui al presente capo.
5. L'Autorità nazionale competente NIS può emanare raccomandazioni per supportare i soggetti nell'implementazione degli obblighi di cui al presente capo.
6. Ai fini del presente articolo, l'Autorità nazionale competente NIS può avvalersi dei tavoli settoriali di cui all'articolo 11.
7. Le comunicazioni e interazioni dei soggetti con l'Autorità nazionale competente NIS avvengono, in via prioritaria, per mezzo della piattaforma digitale di cui all'articolo 7, comma 1.

ART. 32
(Previsioni settoriali specifiche)

1. Fermo restando quanto previsto dagli articoli 23, 24, 25, 27, 28 e 29, tenuto conto degli impatti sociali e economici di un incidente significativo nella catena di approvvigionamento del settore della pubblica amministrazione, l'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può imporre specifici obblighi proporzionati e graduali ai soggetti essenziali e importanti che forniscono servizi, anche digitali, alla pubblica amministrazione.
2. L'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può individuare obblighi di cui al presente capo che non si applicano:
   a) alle amministrazioni pubbliche di cui all'articolo 3, comma 6, lettere c) e d);
   b) ai soggetti di cui all'articolo 3, comma 8, comma 9, lettera f), e comma 10.
3. Gli obblighi di cui agli articoli 24 e 25 non si applicano ai soggetti che erogano esclusivamente servizi di registrazione dei nomi di dominio. Tali soggetti assicurano un livello di sicurezza informatica coerente con gli obblighi di cui agli articoli 24 e 25.
4. La designazione o la mancata designazione del rappresentante di cui all'articolo 5, comma 3, non pregiudica l'applicabilità degli obblighi di cui al presente capo.

ART. 33
(Coordinamento con la disciplina del Perimetro di sicurezza nazionale cibernetica)

1. Ai fini dell'articolo 4:

a) gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente previsti dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sono considerati almeno equivalenti a quelli previsti dal presente decreto;
b) alle reti, sistemi informativi e servizi informatici inseriti nell'elenco di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, non si applicano le disposizioni di cui al presente decreto. Restano fermi gli obblighi del presente decreto per i sistemi informativi e di rete diversi da quelli di cui al primo periodo;
c) i soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, non sono sottoposti agli obblighi di notifica di cui all'articolo 25 del presente decreto per gli incidenti riconducibili a una notifica effettuata ai sensi dell'articolo 1, comma 3, del decreto-legge medesimo;
d) le informazioni attinenti ai soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, ovvero trasmesse da questi ultimi all'Agenzia per la cybersicurezza nazionale ai sensi del presente decreto, possono essere escluse dagli obblighi di comunicazione di cui all'articolo 22.

Capo V
Monitoraggio, vigilanza ed esecuzione

ART. 34
(Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione)

1. L'Autorità nazionale competente NIS monitora e valuta il rispetto da parte dei soggetti importanti ed essenziali degli obblighi previsti dal capo IV e dall'articolo 7, nonché i relativi effetti sulla sicurezza dei sistemi informativi e di rete, svolgendo attività di vigilanza attraverso:
   a) il monitoraggio, l'analisi e il supporto;
   b) la verifica e le ispezioni;
   c) l'adozione di misure di esecuzione;
   d) l'irrogazione di sanzioni amministrative pecuniarie e accessorie.
2. L'Autorità nazionale competente NIS può conferire priorità alle attività di cui al presente capo adottando un approccio basato sul rischio.
3. L'Autorità nazionale competente NIS provvede affinché le attività di vigilanza imposte ai soggetti per quanto riguarda gli obblighi di cui al presente decreto siano effettive, proporzionate e dissuasive, tenuto conto di ciascuna fattispecie e dei criteri di cui all'articolo 31.

4. L’Autorità nazionale competente NIS vigila sul rispetto, da parte degli enti della pubblica amministrazione, del presente decreto, con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza.
5. L’Autorità nazionale competente NIS espone nei particolari la motivazione per l’adozione dei provvedimenti per lo svolgimento delle attività e l’esercizio dei poteri di cui al presente capo.
6. Le attività e i poteri di cui al presente capo sono rispettivamente svolte ed esercitati rispettando i diritti della difesa nonché tenendo conto delle circostanze di ciascuna fattispecie e almeno degli elementi seguenti:
   a) la gravità della violazione e l’importanza delle disposizioni violate, considerando gravi in particolare:
      1) le violazioni ripetute;
      2) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti;
      3) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dall’Autorità nazionale competente NIS;
      4) l’ostacolo alle attività di vigilanza di cui al presente capo;
      5) la fornitura di informazioni false o gravemente inesatte relative agli obblighi di cui al presente decreto;
   b) la durata della violazione;
   c) eventuali precedenti violazioni pertinenti commesse dal soggetto interessato;
   d) qualsiasi danno materiale o immateriale causato, incluse le perdite finanziarie o economiche, gli effetti sugli altri servizi e il numero di utenti interessati;
   e) un’eventuale condotta intenzionale o negligenza da parte dell’autore della violazione;
   f) qualsiasi misura adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale;
   g) qualsiasi adesione a codici di condotta o meccanismi di certificazione approvati;
   h) il livello di collaborazione delle persone fisiche o giuridiche ritenute responsabili con l’Autorità nazionale competente NIS.
7. Gli audit sulla sicurezza, periodici e mirati, nonché le scansioni di sicurezza di cui agli articoli 35 e 37, sono svolti da organismi indipendenti e si basano su valutazioni del rischio effettuate dall’Autorità nazionale competente NIS o dal soggetto sottoposto ad audit o su altre informazioni disponibili in relazione ai rischi. L’Autorità nazionale competente NIS può richiedere, anche solo in parte, di acquisire gli esiti di tali audit sulla sicurezza e di tali scansioni di sicurezza. I costi di tali audit sulla sicurezza e di tali scansioni di sicurezza sono a carico del soggetto sottoposto ad audit, salvo in casi debitamente giustificati in cui l’Autorità nazionale competente NIS decida altrimenti, in linea con il piano di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all’articolo 13, comma 3.
8. La designazione o la mancata designazione del rappresentante di cui all’articolo 5, comma 3, non pregiudica lo svolgimento delle attività e l’esercizio dei poteri di cui al presente capo.

9. Le comunicazioni e interazioni dei soggetti con l'Autorità nazionale competente NIS avvengono, in via prioritaria, per mezzo della piattaforma digitale di cui all'articolo 7, comma 1.
10. Con decreto del Presidente del Consiglio dei ministri, da adottare secondo le modalità di cui all'articolo 40, comma 1, sono stabiliti i criteri, le procedure e le modalità per lo svolgimento delle attività, l'esercizio dei poteri e l'adozione dei provvedimenti di cui al presente capo.

ART. 35

(Monitoraggio, analisi e supporto)

1. Ai fini dell'articolo 7, l'Autorità nazionale competente NIS verifica e fornisce riscontro circa le informazioni trasmesse e la relativa corrispondenza ai requisiti prescritti per i soggetti registrati, ai fini dell'inserimento nell'elenco di cui all'articolo 7, comma 2, assicurando altresì adeguata pubblicità ai criteri concernenti l'ambito di applicazione del presente decreto e dei relativi obblighi.
2. L'Autorità nazionale competente NIS monitora l'attuazione degli obblighi di cui al presente decreto da parte dei soggetti che rientrano nell'ambito di applicazione di cui all'articolo 3, implementando, altresì, interventi di supporto per i soggetti medesimi.
3. L'Autorità nazionale competente NIS, ai fini dell'attività di monitoraggio di cui al comma 2, può:
   a) richiedere ai soggetti una rendicontazione, anche periodica, ivi incluse autovalutazioni e piani di implementazione, dello stato di attuazione degli obblighi di cui al presente decreto, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali, dichiarando la finalità della richiesta;
   b) richiedere ai soggetti l'esecuzione, periodica o mirata, di audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto;
   c) richiedere ai soggetti l'esecuzione di scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;
   d) emanare raccomandazioni e avvertimenti relativi a presunte violazioni del presente decreto da parte dei soggetti interessati.
4. Ai fini del comma 2, l'Autorità nazionale competente NIS indica modalità e termini ragionevoli e proporzionati per adempiere, nonché per riferire circa lo stato di attuazione degli adempimenti.
5. L'Autorità nazionale competente NIS analizza le risultanze delle attività di cui al presente capo al fine di stabilire l'ordine di priorità degli interventi di supporto di cui al comma 2 nonché di individuare gli indirizzi di sviluppo della regolamentazione di cui all'articolo 31.
6. L'Autorità nazionale competente NIS implementa gli interventi di supporto di cui al comma 2 qualora ciò non costituisca un onere sproporzionato o eccessivo.

7. L’Autorità nazionale competente NIS, nello svolgimento delle attività di cui al presente capo, si può avvalere dei tavoli settoriali di cui all’articolo 11.

ART. 36

(Verifiche e ispezioni)

1. L’Autorità nazionale competente NIS, nell’esercizio dei poteri di verifica e ispettivi nei confronti dei soggetti che rientrano nell’ambito di applicazione del presente decreto, può sottoporre questi ultimi a:
   a) verifiche della documentazione e delle informazioni trasmesse all’Autorità nazionale competente NIS ai sensi del presente decreto;
   b) ispezioni in loco e a distanza, compresi controlli casuali;
   c) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei poteri di cui al presente articolo, dichiarando la finalità della richiesta e specificando le informazioni richieste ai soggetti.
2. Nei confronti dei soggetti importanti, i poteri di verifica e ispettivi si applicano unicamente qualora l’Autorità nazionale competente NIS acquisisca o riceva elementi di prova, indicazioni o informazioni che suggeriscano possibili violazioni del presente decreto.

ART. 37

(Misure di esecuzione)

1. L’Autorità nazionale competente NIS, ai fini dell’esercizio dei suoi poteri di esecuzione, tiene anche conto degli esiti delle attività di monitoraggio, analisi e supporto di cui all’articolo 35 e delle risultanze dell’esercizio dei poteri di verifica e ispettivi di cui all’articolo 36.
2. L’Autorità nazionale competente NIS, nell’esercizio dei suoi poteri di esecuzione può richiedere ai soggetti, dichiarandone la finalità, di fornire i dati che dimostrino l’attuazione di politiche di sicurezza informatica, quali i risultati di audit sulla sicurezza e i relativi elementi di prova, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali anche ai fini:
   a) della valutazione delle misure di gestione dei rischi per la sicurezza informatica;
   b) del rispetto degli obblighi di trasmissione, comunicazione e notifica di cui al presente decreto.
3. L’Autorità nazionale competente NIS, nell’esercizio dei suoi poteri di esecuzione, può intimare ai soggetti:
   a) di eseguire, su base periodica o mirata, audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto. L’Autorità nazionale competente NIS non può prescrivere l’esecuzione periodica di audit di sicurezza ai soggetti importanti;
   b) di eseguire scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con la medesima Autorità;

c) di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza;
d) di adempiere agli obblighi di cui al presente decreto;
e) di porre termine al comportamento che viola il presente decreto e di astenersi dal ripeterlo;
f) di attuare le istruzioni vincolanti impartite dalla medesima Autorità o di porre rimedio alle carenze individuate nell'adempimento degli obblighi di cui al presente decreto o alle conseguenze che derivano da violazioni del presente decreto;
g) ai fini dell'articolo 25, comma 9, di comunicare senza ingiustificato ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;
h) ai fini dell'articolo 25, comma 10, di comunicare senza ingiustificato ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, qualsiasi misura o azione correttiva che tali destinatari possono adottare in risposta a tale minaccia, nonché, se opportuno, la minaccia informatica significativa stessa;
i) ai fini dell'articolo 25, comma 11, di informare il pubblico sugli incidenti occorsi;
l) di rendere pubbliche le violazioni di cui al presente decreto.

4. L'Agenzia per la cybersicurezza nazionale, nell'esercizio dei suoi poteri di esecuzione quale Autorità nazionale competente NIS e di CSIRT Italia, può intimare l'osservanza di istruzioni vincolanti per evitare il verificarsi di un incidente. Le Autorità nazionali di gestione delle crisi informatiche, in raccordo tra loro, nell'ambito delle competenze di cui all'articolo 2, comma 1, lettera g), possono altresì intimare l'osservanza di istruzioni vincolanti per porre rimedio agli incidenti che si sono verificati.
5. L'Autorità nazionale competente NIS può designare un proprio funzionario per supportare il soggetto interessato ai fini dell'adempimento degli obblighi di cui al presente decreto, con compiti ben definiti nell'arco di un periodo di tempo determinato, anche tramite visite in loco e a distanza. Il soggetto interessato assicura la piena collaborazione con il funzionario designato.
6. Qualora il soggetto interessato non adempia alle disposizioni di cui ai commi 2, 3, 4 e 5, secondo periodo, l'Autorità nazionale competente NIS diffida il soggetto ad adempiere a tali disposizioni.
7. Ai fini dei commi 2, 3, 4 e 6, l'Autorità nazionale competente NIS indica modalità e termini ragionevoli e proporzionati per adempiere nonché per riferire circa lo stato di attuazione degli adempimenti.
8. Prima di adottare provvedimenti di cui ai commi 3 e 6, l'Autorità nazionale competente NIS notifica ai soggetti interessati le conclusioni preliminari, concedendo a questi ultimi un termine ragionevole, comunque non inferiore a quindici giorni, per presentare osservazioni.
9. Il comma 8 non trova applicazione nei casi in cui la notifica delle conclusioni preliminari non consente azioni immediate per prevenire un incidente o rispondervi. In tali casi l'Autorità nazionale competente NIS motiva l'omissione della notifica di cui al comma 8.

10. Nei casi di adozione da parte dell'Autorità nazionale competente NIS di più provvedimenti successivi riconducibili alla medesima fattispecie, il comma 8 si applica esclusivamente al primo di questi provvedimenti.

ART. 38

(Sanzioni amministrative)

1. L'Autorità nazionale competente NIS, ai fini dell'esercizio dei suoi poteri sanzionatori, tiene anche conto degli esiti delle attività di monitoraggio, supporto e analisi di cui all'articolo 35, delle risultanze dell'esercizio dei poteri di verifica e ispettivi di cui all'articolo 36, nonché dell'esercizio dei poteri di esecuzione di cui all'articolo 37.
2. Fermi restando i criteri di cui all'articolo 34, comma 6, l'Agenzia per la cybersicurezza nazionale con una o più determinazioni, adottate secondo le modalità dell'articolo 40, comma 5, può specificare laddove necessario i criteri per la determinazione dell'importo delle sanzioni per le violazioni di cui ai commi 8 e 10, adottando tutte le misure necessarie per assicurarne l'effettività, la proporzionalità, la dissuasività e l'applicazione.
3. L'esercizio dei poteri di cui all'articolo 37 non impedisce la contestazione delle violazioni di cui ai commi 8 e 10, nonché la relativa irrogazione di sanzioni amministrative di cui al presente articolo.
4. Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, l'Autorità nazionale competente NIS può sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, ai sensi della normativa vigente, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale. Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7. Le disposizioni di cui al presente comma non si applicano alle pubbliche amministrazioni di cui all'allegato III, nonché ai soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4.
5. Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle previsioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza.
6. Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, l'Autorità nazionale competente NIS può disporre nei confronti delle persone fisiche di cui al comma 5, ivi inclusi gli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali e importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante, l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Tale

sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7.

7. Ai dipendenti pubblici che esercitano i poteri di cui al comma 5, si applicano le norme in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati. In particolare, la violazione degli obblighi di cui al presente decreto può costituire causa di responsabilità disciplinare e amministrativo-contabile.
8. Con le sanzioni amministrative pecuniarie di cui al comma 9 sono punite le seguenti violazioni:
   a) mancata osservanza degli obblighi imposti dall'articolo 23 agli organi di amministrazione e agli organi direttivi, nonché degli obblighi relativi alla gestione del rischio per la sicurezza informatica e alla notifica di incidente, di cui agli articoli 24 e 25, così come disciplinati ai sensi dell'articolo 31;
   b) inottemperanza alle disposizioni adottate dall'Autorità nazionale competente NIS ai sensi dell'articolo 37, commi 3 e 4, e alle relative diffide.
9. Le violazioni di cui al comma 8 sono punite:
   a) per i soggetti essenziali, escluse le pubbliche amministrazioni, con sanzioni amministrative pecuniarie fino a un massimo di 10.000.000 euro o del 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE, se tale importo è superiore, il cui minimo è fissato nella misura di un ventesimo del massimo edittale;
   b) per i soggetti importanti, escluse le pubbliche amministrazioni, con sanzioni amministrative pecuniarie fino a un massimo di 7.000.000 euro o del 1,4% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE, se tale importo è superiore, il cui minimo è fissato nella misura di un trentesimo del massimo edittale;
   c) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti essenziali, con sanzioni amministrative pecuniarie da euro 25.000 a euro 125.000;
   d) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti importanti, le sanzioni amministrative pecuniarie di cui alla lettera c) sono ridotte di un terzo.
10. Con le sanzioni amministrative pecuniarie di cui al comma 11 sono punite le seguenti violazioni:
    a) mancata registrazione, comunicazione o aggiornamento delle informazioni ai sensi dell'articolo 7, commi 1, 3, 4, 5 e 7;
    b) inosservanza delle modalità stabilite dall'Autorità nazionale competente NIS ai sensi dell'articolo 7;

c) mancata comunicazione o aggiornamento dell'elenco delle attività e dei servizi nonché della loro categorizzazione ai sensi dell'articolo 30, comma 1;
d) mancata implementazione o attuazione degli obblighi relativi all'uso di schemi di certificazione, alla banca dei dati di registrazione dei nomi di dominio nonché alle previsioni settoriali specifiche di cui agli articoli 27, 29 e 32, così come disciplinati ai sensi dell'articolo 31.
e) mancata collaborazione con l'Autorità nazionale competente NIS nello svolgimento delle attività e nell'esercizio dei poteri di cui al presente capo;
f) mancata collaborazione con il CSIRT Italia.

11. Le violazioni di cui al comma 10, fermi restando i minimi edittali di cui al comma 9, sono punite:
a) per i soggetti essenziali, con sanzioni amministrative pecuniarie fino a un massimo del 0,1% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE;
b) per i soggetti importanti, con sanzioni amministrative pecuniarie fino a un massimo dello 0,07% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE;
c) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti essenziali, con sanzioni amministrative pecuniarie da euro 10.000 a euro 50.000;
d) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti importanti, le sanzioni amministrative pecuniarie di cui alla lettera c) sono ridotte di un terzo.

12. Si ha reiterazione delle violazioni di cui al presente articolo nei casi regolati dall'articolo 8-bis della legge 24 novembre del 1981, n. 689. Nei casi di reiterazione specifica, la sanzione prevista per la violazione è aumentata fino al doppio. Nei casi di reiterazione non specifica si applica la sanzione prevista per la violazione più grave aumentata fino al triplo.

13. In caso di mancata o tardiva registrazione di cui all'articolo 7, sono comunque contestate tutte le violazioni previste dai commi 8 e 10, e si applica la sanzione prevista per la violazione più grave aumentata fino al triplo.

14. In caso di mancata osservanza degli obblighi relativi alla notifica di incidente di cui all'articolo 25, da parte delle pubbliche amministrazioni di cui all'allegato III, nonché dei soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, le disposizioni di cui al comma 9 si applicano solo in caso di reiterazione specifica nell'arco di cinque anni e l'Autorità nazionale competente NIS può esercitare, durante i dodici mesi successivi all'accertamento della violazione, i poteri di verifica e ispettivi di cui all'articolo 36.

15. Ai fini dell'attuazione del presente articolo, sono individuate, ai sensi dell'articolo 40, comma 1, lettera c), le modalità di applicazione, nell'ambito del procedimento sanzionatorio, dei seguenti strumenti deflattivi del contenzioso:
    a) l'invito a conformarsi che l'Autorità nazionale competente NIS, ove accerti la sussistenza delle violazioni, e fatto salvo il caso di reiterazione delle stesse, invia al trasgressore, assegnando un congruo termine perentorio, proporzionato al tipo e alla gravità della violazione, per conformare la condotta agli obblighi previsti dalla normativa vigente. Ove il trasgressore ottemperi all'obbligo di conformare la condotta nei termini previsti, il procedimento sanzionatorio non prosegue. La disposizione di cui alla presente lettera non si applica al soggetto che sia stato già destinatario della diffida di cui all'articolo 37, comma 6, ovvero ai soggetti e nei casi previsti dal comma 14;
    b) la facoltà di estinguere il procedimento attraverso il pagamento in misura ridotta pari alla terza parte del massimo della sanzione o se più favorevole, e qualora sia stabilito, al doppio del minimo della sanzione edittale, nel termine perentorio di 60 giorni dalla data di notifica della contestazione. In caso di reiterazione si applica l'articolo 8-bis della legge 24 novembre 1981, n. 689;
    c) le fattispecie in cui non è prevista pubblicità dell'irrogazione di sanzioni amministrative.

16. I proventi delle sanzioni amministrative pecuniarie irrogate dall'Autorità nazionale competente NIS ai sensi di quanto previsto dal presente decreto sono versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale.

ART. 39
(Assistenza reciproca)

1. L'Autorità nazionale competente NIS coopera e assiste le autorità competenti degli altri Stati membri interessati, nonché può richiedere la cooperazione e l'assistenza reciproca alle medesime in funzione delle necessità nei seguenti casi:
    a) un soggetto, considerato sotto la giurisdizione nazionale ai sensi dell'articolo 5 o i cui sistemi informativi e di rete sono ubicati sul territorio nazionale, fornisce servizi in uno o più altri Stati membri;
    b) un soggetto, considerato sotto la giurisdizione di altri Stati membri ai sensi dell'articolo 5 o i cui sistemi informativi e di rete sono ubicati sul territorio di altri Stati membri, fornisce servizi sul territorio nazionale.
2. La cooperazione di cui al comma 1 comprende la reciproca:
    a) notifica e consultazione, per il mezzo del Punto di contatto unico NIS, circa le attività ispettive, le misure di esecuzione e l'esercizio dei poteri sanzionatori, nonché la loro applicazione;

b) richiesta giustificata di attività ispettive o di adozione di misure di esecuzione;
c) assistenza proporzionata alle rispettive risorse affinché le attività ispettive e di esecuzione possano essere attuate in maniera efficace, efficiente e coerente.

3. L'assistenza reciproca di cui al comma 2, lettera c), può riguardare richieste di informazioni e attività ispettive, comprese le richieste di effettuare ispezioni in loco o a distanza o audit sulla sicurezza mirati.
4. L'Autorità nazionale competente NIS può respingere una richiesta di assistenza da parte di autorità competenti degli altri Stati membri ai sensi del presente articolo qualora:
   a) l'Autorità nazionale competente NIS non è competente per fornire l'assistenza richiesta;
   b) l'assistenza richiesta non è proporzionata ai compiti ispettivi e di esecuzione previsti dal presente decreto;
   c) la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrarie agli interessi essenziali di sicurezza nazionale, di pubblica sicurezza o di difesa dello Stato.
5. Ai fini del comma 4, prima di respingere una richiesta, l'Autorità nazionale competente NIS consulta le autorità competenti degli Stati membri interessati. Su richiesta di uno degli Stati membri interessati, l'Autorità nazionale competente NIS consulta anche la Commissione europea e l'ENISA.
6. Se opportuno e di comune accordo, l'Autorità nazionale competente NIS e le autorità competenti di altri Stati membri possono svolgere attività ispettive e di esecuzione comuni.
7. L'Autorità nazionale competente NIS può:
   a) a fronte di una richiesta di assistenza reciproca da parte di autorità competenti di altri Stati membri, esercitare i poteri di cui al presente capo nei confronti di un soggetto che soddisfa i criteri di cui al comma 1, lettera a), del presente articolo;
   b) inoltrare una richiesta di assistenza reciproca alle autorità competenti degli altri Stati membri interessati per l'esercizio dei rispettivi poteri di cui al capo VII della Direttiva 2022/2555 nei confronti di un soggetto che soddisfa i criteri di cui al comma 1, lettera b), del presente articolo.

Capo VI
Disposizioni finali e transitorie

ART. 40
(Attuazione)

1. Con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400:

a) sono definiti i criteri per l'applicazione della clausola di salvaguardia di cui all'articolo 3, comma 4;
b) sono stabiliti i criteri, le procedure e le modalità di cui all'articolo 34, comma 10;
c) sono individuate le modalità di applicazione, nell'ambito del procedimento sanzionatorio, degli strumenti deflattivi del contenzioso di cui all'articolo 38, comma 14.

2. Con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, d'intesa con le Autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400:
   a) possono essere stabiliti ulteriori criteri di identificazione delle tipologie di soggetto di cui agli allegati I e II, nonché delle ulteriori tipologie di soggetto di cui all'articolo 3;
   b) possono essere individuate ulteriori categorie di pubbliche amministrazioni di cui all'articolo 3, commi 6 e 7 a cui si applica il presente decreto;
   c) sono stabilite le modalità di raccordo e di collaborazione tra l'Agenzia per la cybersicurezza nazionale e le Autorità di settore NIS ai fini del presente decreto.
3. Con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, d'intesa con le Amministrazioni interessate, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400:
   a) sono individuati gli enti, gli organi e le articolazioni della pubblica amministrazione, nonché i soggetti di cui all'articolo 4, comma 4;
   b) sono stabilite, ove necessario, le modalità di raccordo e collaborazione di cui all'articolo 14.
4. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, su proposta delle Autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS:
   a) sono individuati, ove necessario, i soggetti ai quali si applica la clausola di salvaguardia di cui all'articolo 3, comma 4;
   b) sono individuati i soggetti ai quali si applica il presente decreto ai sensi dell'articolo 3, commi 8 e 9;
5. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS:
   a) ai sensi degli articoli 3 e 6, è stabilito l'elenco dei soggetti essenziali e importanti di cui all'articolo 7, comma 2;
   b) sono stabiliti i termini, le modalità nonché i procedimenti di utilizzo e accesso di cui all'articolo 7, comma 6, le eventuali ulteriori informazioni che i soggetti devono fornire ai sensi dei commi 1 e 4 del medesimo articolo, nonché di designazione dei rappresentanti di cui all'articolo 5, comma 3;

c) sono definiti l'organizzazione e il funzionamento del Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12;
d) è adottata, d'intesa con il Ministero della giustizia, la politica nazionale di divulgazione coordinata delle vulnerabilità di cui all'articolo 16, comma 4;
e) possono essere imposte condizioni per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia nel contesto degli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all'articolo 17;
f) sono stabilite le modalità con cui i soggetti essenziali e importanti notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all'articolo 17;
g) possono essere designati gli esperti di sicurezza informatica di cui all'articolo 21, comma 1, nonché individuate, se necessario, le modalità per l'esecuzione della revisione tra pari di cui al medesimo articolo, commi 2 e 3;
h) può essere imposto l'utilizzo di prodotti TIC, servizi TIC e processi TIC certificati di cui all'articolo 27, definito i relativi termini, criteri e modalità;
i) sono stabilite le categorie di rilevanza nonché le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 30;
l) sono stabiliti obblighi proporzionati e graduali, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 31, le modalità di applicazione dei medesimi obblighi per i soggetti che svolgono attività in più settori o sottosettori e per i soggetti di cui all'articolo 32, commi 1 e 2;
m) sono stabiliti i criteri per la determinazione dell'importo delle sanzioni ai sensi dell'articolo 38, comma 2.

6. Sono esclusi dall'accesso e non sono soggetti a pubblicazione:
   a) i decreti di cui al comma 3, lettera a);
   b) le determinazioni di cui al comma 4, lettera b), e al comma 5, lettera a).
7. Entro 30 giorni dalla data di entrata in vigore del presente decreto sono adottati:
   a) i decreti del Presidente del Consiglio dei ministri di cui al comma 1, lettera a), e al comma 3, lettera a);
   b) le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al comma 4, lettera b), e al comma 5, lettere b) e c).
8. Entro sei mesi dalla data di entrata in vigore del presente decreto, sono adottati:
   a) i decreti del Presidente del Consiglio dei ministri di cui al comma 1, lettere b) e c), e al comma 2, lettera c);
   b) le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al comma 5, lettere d), f) e i).
9. Entro 18 mesi dalla data di entrata in vigore del presente decreto, sono adottate le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al comma 5, lettera h).
10. I decreti del Presidente del Consiglio dei ministri di cui al presente articolo sono aggiornati periodicamente e comunque ogni tre anni.

11. Le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al presente articolo sono aggiornate periodicamente e comunque ogni due anni.

ART. 41

(Abrogazioni e regime transitorio)

1. A decorrere dalla data di entrata in vigore del presente decreto, il decreto legislativo 18 maggio 2018, n. 65, è abrogato. I Capi IV e V del medesimo decreto legislativo continuano a trovare applicazione nei confronti dei soli soggetti di cui all'articolo 3, comma 9, lettera a), fino alla data di adozione dei provvedimenti attuativi di cui all'articolo 40, commi 1, 2, 3, lettera b), 4 e 5, lettere a), b), e) e f).
2. Al decreto legislativo 1° agosto 2003, n. 259:
   a) all'articolo 2, comma 1, la lettera h) è soppressa;
   b) l'articolo 30, comma 26, e gli articoli 40 e 41 sono abrogati.
3. I provvedimenti attuativi degli articoli 40 e 41 continuano a trovare applicazione, per quanto non in contrasto con la legge e con le norme contenute nel presente decreto, fino all'adozione delle determinazioni di cui all'articolo 40, comma 5, lettera l).

ART. 42

(Fase di prima applicazione)

1. In fase di prima applicazione:
   a) ai sensi dell'articolo 7, entro il 17 gennaio 2025, i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del presente decreto, si registrano sulla piattaforma digitale di cui all'articolo dell'articolo 7, comma 1;

   b) sino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 si riunisce almeno una volta ogni 60 giorni;

   c) sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 è fissato in 9 mesi dalla ricezione della comunicazione di cui all'articolo 7, comma 3, lettere *a)* e *b)*, e il termine per l'adempimento degli obblighi di cui agli articoli 23, 24 e 29 è fissato in 18 mesi dalla medesima comunicazione. Ai fini di cui al primo periodo, l'Autorità nazionale competente NIS può stabilire modalità e specifiche di base per assicurare la conformità dei soggetti essenziali e importanti.

2. L'obbligo di cui all'articolo 30, comma 1, si applica a partire dal primo gennaio 2026.

3. Ai sensi dell'articolo 7, comma 1, i soggetti essenziali e importanti possono registrarsi a partire dalla data di pubblicazione della piattaforma di cui al medesimo comma;

ART. 43

(Modifiche normative)

1. Al fine di assicurarne la coerenza con l'architettura nazionale di cybersicurezza e con i compiti dell'Agenzia per la cybersicurezza nazionale, al decreto-legge 14 giugno 2021, n. 82, convertito con modificazione dalla legge 4 agosto 2021, n. 109, sono apportate le seguenti modificazioni:
   a) all'articolo 1, comma 1,
      1) la lettera d) è sostituita dalla seguente:
      «d) decreto legislativo NIS, il decreto legislativo di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;»;
      2) alla lettera e), le parole: «di cui all'articolo 6» sono sostituite dalle seguenti: «di cui all'articolo 9»;
   b) all'articolo 7:
      1) al comma 1:
      1.1) la lettera d) è sostituita dalle seguenti:
      «d) è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettere d) ed e), del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento;
      d-*bis*) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera g), del decreto legislativo NIS;
      d-*ter*) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma 1, lettera i), del decreto legislativo NIS;»;
      1.2) alla lettera n), le parole «CSIRT Italia di cui all'articolo 8» sono sostituite dalle seguenti «CSIRT Italia di cui all'articolo 2, comma 1, lettera i)»;
      1.3) alla lettera n-*bis*) le parole: «di cui all'articolo 3, comma 1, lettere g) e i)» sono sostituite dalle seguenti: «i soggetti essenziali e importanti di cui all'articolo 6 del decreto legislativo NIS»;
      2) il comma 3 è abrogato;
   c) l'articolo 15 è abrogato.
2. Per assicurarne la coerenza con gli obblighi di cui al capo IV e con le previsioni di cui al capo V del presente decreto, all'articolo 1 del decreto-legge del 21 settembre 2019, n. 105, convertito con modificazioni dalla legge del 18 novembre 2019, n. 133, sono apportate le seguenti modificazioni:
   a) il comma 8, è sostituito dal il seguente:
   «8. La notifica d'incidente ai sensi del comma 3, lettera a), effettuata dai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che rientrano nell'ambito di applicazione

del decreto legislativo di recepimento della direttiva (UE) 2022/2555 assolve agli obblighi in materia di notifica di incidente di cui all'articolo 25 del decreto legislativo medesimo.»;

b) dopo il comma 8, è inserito il seguente:

«8-*bis*. Ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che non sono individuati come soggetti essenziali o importanti ai sensi degli articoli 3 e 6 del decreto legislativo di recepimento della direttiva (UE) 2022/2555, si applicano gli obblighi di cui al capo IV e le attività ispettive e sanzionatorie di cui al capo V per i soggetti essenziali ai sensi del medesimo decreto legislativo, limitatamente ai sistemi informativi e di rete diversi da quelli inseriti nell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui all'articolo 1, comma 2, lettera b), del presente decreto. L'Agenzia per la cybersicurezza nazionale, sentito il tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica, stabilisce con propria determina termini, modalità, specifiche e tempi graduali di implementazione degli obblighi di cui al presente comma.»;

c) il comma 3-*bis*, è abrogato;

d) il comma 17, è abrogato.

ART. 44
(Disposizioni finanziarie)

1. Al fine di garantire che l'Autorità nazionale competente NIS e il Punto di contatto unico NIS siano dotati di risorse adeguate a svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi del presente decreto, disponendo di personale sufficiente e formato in modo appropriato, agli oneri derivanti dall'articolo 10, pari a 2.000.000 euro annui a decorrere dall'anno 2025, si provvede ai sensi del comma 5 del presente articolo.
2. Al fine di garantire l'efficiente ed efficace svolgimento dei compiti assegnati dal presente decreto alle Autorità di settore NIS, agli oneri derivanti dall'articolo 11, pari a 1.000.000 euro annui a decorrere dall'anno 2025, si provvede ai sensi del comma 5 del presente articolo.
3. Al fine di garantire che le Autorità nazionali di gestione delle crisi informatiche siano dotate di risorse adeguate a svolgere in modo efficiente ed efficace i compiti assegnati e conseguire in questo modo gli obiettivi del presente decreto, disponendo di personale sufficiente e formato in mod appropriato, agli oneri derivanti dall'articolo 13, comma 1, pari a 1.000.000 euro annui a decorrere dall'anno 2025, si provvede ai sensi del comma 5 del presente articolo.
4. Al fine di garantire che il CSIRT Italia disponga di risorse adeguate a svolgere efficacemente i compiti assegnati dal presente decreto, disponendo di personale sufficiente e formato in modo appropriato, agli oneri derivanti dell'articolo 15, pari a 2.000.000 euro annui a decorrere dall'anno 2025, si provvede ai sensi del comma 5 del presente articolo.
5. Agli oneri di cui ai commi 1, 2, 3 e 4, pari a 6.000.000 euro annui a decorrere dall'anno 2025, si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-bis della legge 24 dicembre 2012, n. 234.

6. Le spese ICT sostenute dalle pubbliche amministrazioni ai sensi degli articoli 10, 11, 13 e 15 del presente decreto e, più in generale le spese ICT sostenute per l'adeguamento dei sistemi informativi al presente decreto, sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell'articolo 1, della legge 28 dicembre 2015, n. 208.
7. Dall'attuazione del presente decreto, ad esclusione degli articoli 10, 11, 13 e 15, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni pubbliche provvedono con le risorse umane, strumentali e finanziarie previste a legislazione vigente.
8. Il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati.

Il presente decreto munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a ….