►**B** **DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

del 14 dicembre 2022

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

(Testo rilevante ai fini del SEE)

(GU L 333 del 27.12.2022, pag. 80)

Rettificata da:

►**C1** Rettifica, GU L 112 del 27.4.2023, pag. 51 (2022/2555)
►**C2** Rettifica, GU L 90206 del 22.12.2023, pag. 1 (2022/2555)

▼B

DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

(Testo rilevante ai fini del SEE)

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

▼C1

Oggetto

▼B

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno.

2. A tal fine, la presente direttiva stabilisce:

▼C1

a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di cibersicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT);

▼B

b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557;

c) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza;

d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica ai soggetti pubblici o privati delle tipologie di cui all'allegato I o II che sono considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione.

▼B

L'articolo 3, paragrafo 4, dell'allegato a tale raccomandazione non si applica ai fini della presente direttiva.

2. La presente direttiva si applica anche ai soggetti, indipendentemente dalle loro dimensioni, delle tipologie di cui all'allegato I o II qualora:

a) i servizi siano forniti da:

   i) fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;

   ii) prestatore di servizi di fiducia;

   iii) registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;

b) il soggetto sia l'unico fornitore in uno Stato membro 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 regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;

f) il soggetto è un ente della pubblica amministrazione:

   i) dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale; o

   ii) a livello regionale quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche.

3. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557.

▼B

4. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, che forniscono servizi di registrazione dei nomi di dominio.

5. Gli Stati membri possono prevedere che la presente direttiva si applichi a:

a) enti della pubblica amministrazione a livello locale;

b) istituti di istruzione, in particolare ove svolgano attività di ricerca critiche.

6. La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

7. La presente direttiva non si applica agli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.

8. Gli Stati membri possono esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o del contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui al paragrafo 7 del presente articolo, dal rispetto degli obblighi di cui all'articolo 21 o all'articolo 23 per quanto riguarda tali attività o servizi. In tali casi, le misure di vigilanza e di applicazione di cui al capo VII non si applicano in relazione a tali attività o servizi specifici. Qualora i soggetti svolgano attività o prestino servizi esclusivamente del tipo di cui al presente paragrafo, gli Stati membri possono anche decidere di esentare tali enti dagli obblighi di cui agli articoli 3 e 27.

9. I paragrafi 7 e 8 non si applicano quando un soggetto agisce in qualità di prestatore di servizi fiduciari.

10. La presente direttiva non si applica ai soggetti che gli Stati membri hanno esentato dall'ambito di applicazione del regolamento (UE) 2022/2554 ai sensi dell'articolo 2, paragrafo 4, di tale regolamento.

11. Gli obblighi stabiliti nella presente direttiva non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

12. La presente direttiva si applica fatti salvi il regolamento (UE) 2016/679, la direttiva 2002/58/CE, le direttive 2011/93/UE ([1]) e 2013/40/UE ([2]) del Parlamento europeo e del Consiglio e la direttiva (UE) 2022/2557.

([1]) Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

([2]) 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 (GU L 218 del 14.8.2013, pag. 8).

▼B

13. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione o nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti conformemente alla presente direttiva solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali di soggetti interessati.

14. I soggetti, le autorità competenti, i punti di contatto unici e i CSIRT trattano i dati personali nella misura necessaria ai fini della presente direttiva e conformemente al regolamento (UE) 2016/679, in particolare tale trattamento si basa sull'articolo 6 dello stesso.

Il trattamento dei dati personali a norma della presente direttiva da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di comunicazioni elettroniche accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione in materia di protezione dei dati e della legislazione dell'Unione in materia di riservatezza, segnatamente la direttiva 2002/58/CE.

Articolo 3

Soggetti essenziali e importanti

1. Ai fini della presente direttiva, sono considerati soggetti essenziali i seguenti:

a) 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) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni;

c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2, dell'allegato alla raccomandazione 2003/361/CE;

d) i soggetti della pubblica amministrazione di cui all'articolo 2, paragrafo 2, lettera f), punto i);

e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

f) soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557, di cui all'articolo 2, paragrafo 3 della presente direttiva;

g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale.

▼B

2. Ai fini della presente direttiva, sono considerati soggetti importanti i soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali ai sensi del paragrafo 1 del presente articolo. Ciò comprende soggetti identificati dagli Stati membri come soggetti importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

3. Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. Successivamente, gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano.

▼C1

4. Ai fini della compilazione dell'elenco di cui al paragrafo 3, gli Stati membri impongono ai soggetti di cui a tale paragrafo di presentare alle autorità competenti almeno le informazioni seguenti:

▼B

a) il proprio nome;

b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail, le serie di IP e i numeri di telefono;

c) se del caso, i settori e sottosettori pertinenti di cui all'allegato I o II; e

d) se del caso, un elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione della presente direttiva.

I soggetti di cui al paragrafo 3 notificano tempestivamente qualsiasi modifica delle informazioni trasmesse a norma del primo comma del presente paragrafo e in ogni caso entro due settimane dalla data della modifica.

La Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), fornisce senza indebito ritardo orientamenti e modelli relativi agli obblighi di cui al presente paragrafo.

▼C1

Gli Stati membri possono istituire meccanismi nazionali che consentano ai soggetti di registrarsi.

▼B

5. Entro il 17 aprile 2025 e successivamente ogni due anni, le autorità competenti notificano:

▼C1

a) alla Commissione e al gruppo di cooperazione, il numero dei soggetti essenziali e importanti elencati ai sensi del paragrafo 3 per ciascun settore e sottosettore di cui all'allegato I o II; e

▼B

b) alla Commissione informazioni pertinenti sul numero di soggetti essenziali e importanti individuati ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e), sul settore e il sottosettore di cui all'allegato I o II cui appartengono, sul tipo di servizio che forniscono e sulla fornitura, tra quelli stabiliti all'articolo 2, paragrafo 2, lettere da b) a e), ai sensi dei quali sono stati individuati.

▼B

6. Sino al 17 aprile 2025 e su richiesta della Commissione, gli Stati membri possono notificare alla Commissione i nomi dei soggetti essenziali e importanti di cui al paragrafo 5, lettera b).

Articolo 4

Atti giuridici settoriali dell'Unione

1. Qualora gli atti giuridici settoriali dell'Unione facciano obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare gli incidenti significativi, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, a tali soggetti non si applicano le pertinenti disposizioni della presente direttiva, comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VII. Qualora gli atti giuridici settoriali dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva continuano ad applicarsi ai soggetti non contemplati da tali atti giuridici settoriali dell'Unione.

2. I requisiti di cui al paragrafo 1 del presente articolo sono considerati di effetto equivalente agli obblighi stabiliti dalla presente direttiva qualora:

a) gli effetti delle misure di gestione dei rischi di cibersicurezza siano almeno equivalenti a quelli delle misure di cui all'articolo 21, paragrafi 1 e 2; oppure

b) l'atto giuridico settoriale dell'Unione preveda l'accesso immediato, se del caso automatico e diretto, alle notifiche degli incidenti da parte dei CSIRT, delle autorità competenti o dei punti di contatto unici a norma della presente direttiva e qualora gli obblighi di notifica degli incidenti significativi abbiano un effetto almeno equivalente a quelli di cui all'articolo 23, paragrafi da 1 a 6, della presente direttiva.

3. La Commissione, entro il 17 luglio 2023, fornisce orientamenti che chiariscano l'applicazione dei paragrafi 1 e 2. La Commissione rivede tali orientamenti periodicamente. Nella preparazione di detti orientamenti, la Commissione tiene conto delle osservazioni del gruppo di cooperazione e dell'ENISA.

Articolo 5

Armonizzazione minima

La presente direttiva non impedisce agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione.

Articolo 6

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

▼C1

1) «sistema informativo e di rete»:

▼B

a) una rete di comunicazione elettronica quale definita all'articolo 2, punto 1, della direttiva (UE) 2018/1972;

b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali; o

c) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

▼C1

2) «sicurezza dei sistemi informativi e di rete»: la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di confidenza, 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;

▼B

3) «cibersicurezza»: la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881;

4) «strategia nazionale per la cibersicurezza»: un quadro coerente di uno Stato membro che prevede priorità e obiettivi strategici in materia di cibersicurezza e la governance per il loro conseguimento in tale Stato membro;

▼C1

5) «quasi incidente»: un evento che avrebbe potuto compromettere 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, ma che è stato efficacemente evitato o non si è verificato;

6) «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;

▼B

7) «incidente di cibersicurezza 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;

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

▼B

9) «rischio»: la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi;

10) «minaccia informatica»: una minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

▼C1

11) «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 degli utenti di tali servizi del soggetto causando perdite materiali o immateriali considerevoli;

▼B

12) «prodotto TIC»: un prodotto TIC quale definito all'articolo 2, punto 12), del regolamento (UE) 2019/881;

13) «servizio TIC»: un servizio TIC quale definito all'articolo 2, punto 13), del regolamento (UE) 2019/881;

14) «processo TIC»: un processo TIC quale definito all'articolo 2, punto 14), del regolamento (UE) 2019/881;

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

16) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([3]);

17) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012;

18) «punto di interscambio internet»: 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;

19) «sistema dei nomi di dominio» o «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 inoltro e connettività di internet al fine di accedere a tali servizi e risorse;

([3]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

▼B

20) «fornitore di servizi DNS»: un soggetto che fornisce:

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

b) servizi di risoluzione dei nomi di dominio autorevoli per uso da parte di terzi, fatta eccezione per i server dei nomi radice;

21) «registro dei nomi di dominio di primo livello» o «registro dei nomi TLD»: un soggetto cui è stato delegato uno specifico dominio di primo livello (TLD) e che è responsabile dell'amministrazione di tale TLD, compresa la registrazione dei nomi di dominio sotto tale TLD, e del funzionamento tecnico di tale TLD, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona TLD 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 TLD sono utilizzati da un registro esclusivamente per uso proprio;

22) «soggetto che fornisce 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;

23) «servizio digitale»: un servizio quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([4]);

24) «servizio fiduciario»: un servizio fiduciario quale definito all'articolo 3, punto 16), del regolamento (UE) n. 910/2014;

25) «prestatore di servizi fiduciari»: un prestatore di servizi fiduciari quale definito all'articolo 3, punto 19), del regolamento (UE) n. 910/2014;

26) «servizio fiduciario qualificato»: un servizio fiduciario qualificato quale definito all'articolo 3, punto 17), del regolamento (UE) n. 910/2014;

27) «prestatore di servizi fiduciari qualificato»: un prestatore di servizi fiduciari qualificato quale definito all'articolo 3, punto 20), del regolamento (UE) n. 910/2014;

28) «mercato online»: un mercato online quale definito all'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio ([5]);

29) «motore di ricerca online»: un motore di ricerca online quale definito all'articolo 2, punto 5), del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio ([6]);

([4]) Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

([5]) Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali») (GU L 149 dell'11.6.2005, pag. 22).

([6]) Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (GU L 186 dell'11.7.2019, pag. 57).

▼B

30) «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.

31) «servizio di data center»: un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato 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;

32) «rete di distribuzione dei contenuti (*content delivery network*)»: 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;

33) «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;

34) «rappresentante»: una persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di un fornitore di servizi DNS, un registro dei nomi TLD, un soggetto che fornisce servizi di registrazione di nomi di dominio, un fornitore di servizi di cloud computing, un fornitore di servizi di data center, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti, o un fornitore di mercato online, di un motore di ricerca online o di una piattaforma di servizi di social network che non è stabilito nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del soggetto per quanto riguarda gli obblighi di quest'ultimo a norma della presente direttiva;

35) «ente della pubblica amministrazione»: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, che non comprende la magistratura, i parlamenti e le banche centrali, che soddisfa i criteri seguenti:

a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;

b) è dotato di personalità giuridica o è autorizzato per legge ad agire a nome di un altro soggetto dotato di personalità giuridica;

c) è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico, la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico;

d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali;

▼B

36) «rete pubblica di comunicazione elettronica»: una rete pubblica di comunicazione elettronica quale definita all'articolo 2, punto 8), della direttiva (UE) 2018/1972;

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

38) «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;

▼C1

39) «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;

▼B

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

41) «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.

CAPO II

QUADRI COORDINATI IN MATERIA DI CIBERSICUREZZA

Articolo 7

Strategia nazionale per la cibersicurezza

1. Ogni Stato membro adotta una strategia nazionale per la cibersicurezza che prevede 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 cibersicurezza. La strategia nazionale per la cibersicurezza comprende:

a) gli obiettivi e le priorità della strategia per la cibersicurezza dello Stato membro, che riguardano in particolare i settori di cui agli allegati I e II;

b) un quadro di governance per la realizzazione degli obiettivi e delle priorità di cui alla lettera a) del presente paragrafo, comprendente le misure strategiche di cui al paragrafo 2;

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 competenti, i punti di contatto unici e i CSIRT ai sensi della presente direttiva, nonché il coordinamento e la cooperazione tra tali organismi e le autorità competenti ai sensi degli atti giuridici settoriali dell'Unione;

▼B

d) un meccanismo per individuare le risorse e una valutazione dei rischi nello Stato membro in questione;

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 cibersicurezza;

g) un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e le autorità competenti a norma 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, se del caso;

▼C1

h) un piano, comprendente le misure necessarie, per aumentare il livello generale di consapevolezza dei cittadini in materia di cibersicurezza.

▼B

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare misure strategiche riguardanti:

a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi;

b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source;

c) la gestione delle vulnerabilità, ivi comprese la promozione e l'agevolazione della divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1;

▼C1

d) il sostegno della disponibilità generale, dell'integrità e della riservatezza del nucleo pubblico della rete internet aperta, compresa, se del caso, la cibersicurezza dei cavi di comunicazione sottomarini;

▼B

e) la promozione dello sviluppo e dell'integrazione di tecnologie avanzate pertinenti miranti ad attuare misure di avanguardia nella gestione dei rischi di cibersicurezza;

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 cibersicurezza, 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 cibersicurezza e di infrastrutture di rete sicure;

▼B

h) la messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla cibersicurezza tra soggetti, nel rispetto del diritto dell'Unione;

i) il rafforzamento dei valori di riferimento relativi alla ciberresilienza e all'igiene informatica delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, fornendo orientamenti e sostegno facilmente accessibili per le loro esigenze specifiche;

j) la promozione di una protezione informatica attiva.

3. Gli Stati membri notificano le loro strategie nazionali per la cibersicurezza alla Commissione entro tre mesi dall'adozione. Gli Stati membri possono omettere dalla notifica informazioni relative alla propria sicurezza nazionale.

4. Gli Stati membri valutano le proprie strategie nazionali per la cibersicurezza periodicamente e almeno ogni cinque anni sulla base di indicatori chiave di prestazione e, se necessario, le aggiornano. L'ENISA assiste gli Stati membri, su richiesta di questi ultimi, nell'elaborazione o aggiornamento di una strategia nazionale per la cibersicurezza e di indicatori chiave di prestazione per la relativa valutazione, onde allinearla ai requisiti e agli obblighi di cui alla presente direttiva.

Articolo 8

Autorità competenti e punti di contatto unici

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza di cui al capo VII (autorità competenti).

2. Le autorità competenti di cui al paragrafo 1 controllano l'attuazione della presente direttiva a livello nazionale.

3. Ogni Stato membro designa o istituisce un punto di contatto unico. Se uno Stato membro designa o istituisce soltanto un'autorità competente a norma del paragrafo 1, quest'ultima è anche il punto di contatto unico per tale Stato membro.

4. Ogni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro.

5. Gli Stati membri garantiscono che le proprie autorità competenti e i propri punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva.

6. Ogni Stato membro notifica alla Commissione, senza indebiti ritardi, l'identità dell'autorità competente di cui al paragrafo 1 e del punto di contatto unico di cui al paragrafo 3, i compiti di tali autorità e qualsiasi ulteriore modifica dei medesimi. Ciascuno Stato membro rende pubblica l'identità della propria autorità competente. La Commissione elabora un elenco dei punti di contatto unici disponibili.

▼B

Articolo 9

Quadri nazionali di gestione delle crisi informatiche

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala (autorità di gestione delle crisi informatiche). Gli Stati membri provvedono affinché tali autorità dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente. Gli Stati membri assicurano la coerenza con i quadri nazionali esistenti di gestione generale delle crisi.

2. Se uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche ai sensi del paragrafo 1, esso indica chiaramente quale di tali autorità deve fungere da coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala.

3. Ogni Stato membro individua le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini della presente direttiva.

4. Ogni Stato membro adotta un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala in cui sono stabiliti gli obiettivi e le modalità della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala. 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 di gestione delle crisi informatiche;

c) le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale generale di gestione delle crisi 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 dello Stato membro alla gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello dell'Unione.

5. Entro tre mesi dalla designazione o istituzione dell'autorità di gestione delle crisi informatiche di cui al paragrafo 1, ciascuno Stato membro notifica alla Commissione l'identità della propria autorità e qualsiasi ulteriore modifica alla stessa. Gli Stati membri presentano alla Commissione e alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) le informazioni pertinenti relative ai requisiti di cui al paragrafo 4 in merito ai propri piani nazionali di risposta agli incidenti e delle crisi di cibersicurezza su vasta scala entro tre mesi dall'adozione di tali piani. Gli Stati membri possono omettere informazioni se e nella misura in cui ciò sia necessario ai fini della loro sicurezza nazionale.

▼B

Articolo 10

Team di risposta agli incidenti di sicurezza informatica (CSIRT)

1. Ogni Stato membro designa o istituisce uno o più CSIRT. È possibile designare o istituire i CSIRT all'interno di un'autorità competente. I CSIRT sono conformi ai requisiti di cui all'articolo 11, paragrafo 1, si occupano almeno dei settori, dei sottosettori e dei tipi di soggetto di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita.

2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 11, paragrafo 3.

3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente attraverso la quale scambiare informazioni con i soggetti essenziali e importanti e con gli altri portatori di interesse pertinenti. A tal fine gli Stati membri provvedono affinché ogni CSIRT contribuisca allo sviluppo di strumenti sicuri per la condivisione delle informazioni.

4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 29 con comunità settoriali o intersettoriali di soggetti essenziali e importanti.

5. I CSIRT partecipano alle revisioni tra pari organizzate conformemente all'articolo 19.

6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT.

7. I CSIRT possono stabilire relazioni di cooperazione con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi. Nell'ambito di tali relazioni di cooperazione, gli Stati membri facilitano uno scambio di informazioni efficace, efficiente e sicuro con tali team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, compreso il protocollo TLP (*Traffic Light Protocol*). I CSIRT possono scambiare informazioni pertinenti con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, compresi dati personali a norma del diritto dell'Unione in materia di protezione dei dati.

8. I CSIRT possono cooperare con team 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 cibersicurezza.

9. Ogni Stato membro notifica alla Commissione senza indebiti ritardi l'identità del CSIRT di cui al paragrafo 1 del presente articolo e del CSIRT designato come coordinatore conformemente all'articolo 12, paragrafo 1, i rispettivi compiti in relazione ai soggetti essenziali e importanti e qualsiasi ulteriore modifica dei medesimi.

10. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo dei CSIRT.

▼B

Articolo 11

Requisiti, capacità tecniche e compiti dei CSIRT

1. I CSIRT soddisfano i requisiti seguenti:

a) i CSIRT garantiscono un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di vulnerabilità (*single points of failure*) e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento; essi indicano chiaramente i canali di comunicazione e li rendono noti alla loro base di utenti e ai partner con cui collaborano;

b) i locali e i sistemi informatici di supporto dei CSIRT sono ubicati in siti sicuri;

c) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;

d) i CSIRT garantiscono la riservatezza e l'affidabilità delle loro operazioni;

e) i CSIRT dispongono di personale sufficiente per garantire la disponibilità dei loro servizi in qualsiasi momento e garantiscono che il loro personale sia formato in modo appropriato;

f) i CSIRT sono dotati di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei loro servizi.

I CSIRT hanno la possibilità di partecipare a reti di cooperazione internazionale.

2. Gli Stati membri assicurano che i loro CSIRT dispongano congiuntamente delle capacità tecniche necessarie a svolgere i compiti di cui al paragrafo 3. Gli Stati membri provvedono affinché ai propri CSIRT siano assegnate risorse sufficienti per garantire un organico adeguato al fine di consentire ai CSIRT di sviluppare le proprie capacità tecniche.

3. I CSIRT svolgono i compiti seguenti:

▼C1

a) monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale, e, su richiesta, forniscono 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;

▼B

b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti interessati, nonché alle autorità competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;

c) forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati, se del caso;

▼B

d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza;

▼C1

e) effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informativi e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;

▼B

f) partecipano alla rete di CSIRT e forniscono assistenza reciproca secondo le loro capacità e competenze agli altri membri della rete di CSIRT su loro richiesta.

g) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1;

h) contribuiscono allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui all'articolo 10, paragrafo 3.

▼C1

I CSIRT possono effettuare 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.

▼B

Nello svolgimento dei compiti di cui al primo comma, i CSIRT possono dare priorità a determinati compiti sulla base di un approccio basato sul rischio.

4. I CSIRT instaurano rapporti di cooperazione con i pertinenti portatori di interesse del settore privato al fine di perseguire gli obiettivi della presente direttiva.

5. Al fine di agevolare la cooperazione di cui al paragrafo 4, i CSIRT promuovono 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 gestione delle crisi; e

c) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1.

Articolo 12

Divulgazione coordinata delle vulnerabilità e banca dati europea delle vulnerabilità

1. Ogni Stato membro designa uno dei propri CSIRT come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato 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. I compiti del CSIRT designato come coordinatore comprendono:

▼B

a) l'individuazione e il contatto dei soggetti interessati;

b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità, e

c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti.

Gli Stati membri provvedono affinché le persone fisiche o giuridiche possano segnalare in forma anonima, qualora lo richiedano, una vulnerabilità al CSIRT designato come coordinatore. Il CSIRT designato come 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 designato di ciascuno Stato membro interessato coopera, se del caso, con altri CSIRT designati in qualità di coordinatori nell'ambito della rete di CSIRT.

2. L'ENISA elabora e mantiene, previa consultazione del gruppo di cooperazione, una banca dati europea delle vulnerabilità. ►C1 A tal fine l'ENISA istituisce e gestisce i sistemi informativi, le misure strategiche e le procedure adeguati e adotta le necessarie misure tecniche e organizzative per garantire la sicurezza e l'integrità della banca dati europea delle vulnerabilità, in particolare al fine di consentire ai soggetti, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, e ai relativi fornitori di sistemi informativi e di rete, di divulgare e registrare, su base volontaria, le vulnerabilità pubblicamente note presenti nei prodotti TIC o nei servizi TIC. ◄ Tutti i portatori di interessi hanno accesso alle informazioni sulle vulnerabilità contenute nella banca dati europea delle vulnerabilità. La banca dati contiene:

a) informazioni che illustrano la vulnerabilità;

b) i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata;

▼C1

c) la disponibilità di relative patch e, qualora queste non fossero disponibili, gli orientamenti forniti dalle autorità competenti o dai CSIRT rivolti agli utenti dei prodotti TIC e dei servizi TIC vulnerabili sulle possibili modalità di mitigazione dei rischi derivanti dalle vulnerabilità divulgate.

▼B

Articolo 13

Cooperazione a livello nazionale

1. Se sono separati, le autorità competenti, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva.

▼B

2. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti, ricevano le notifiche degli incidenti significativi a norma dell'articolo 23, nonché degli incidenti, delle minacce informatiche e dei quasi incidenti (*near miss*) a norma dell'articolo 30.

▼C1

3. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti informino i loro punti di contatto unici delle notifiche relative agli incidenti, alle minacce informatiche e ai quasi incidenti trasmesse a norma della presente direttiva.

▼B

4. Al fine di garantire l'efficace adempimento dei compiti e degli obblighi delle autorità competenti, dei punti di contatto unici e dei CSIRT, gli Stati membri, nella misura del possibile, provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra i suddetti organismi e le autorità di contrasto, le autorità di protezione dei dati, le autorità nazionali ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139, gli organismi di vigilanza a norma del regolamento (UE) n. 910/2014, le autorità competenti a norma del regolamento (UE) 2022/2554, le autorità nazionali di regolamentazione a norma della direttiva (UE) 2018/1972, le autorità competenti a norma della direttiva (UE) 2022/2557, nonché le autorità competenti ai sensi di altri atti giuridici settoriali dell'Unione.

5. Gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma della direttiva (UE) 2022/2557 collaborino e si scambino periodicamente informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti essenziali identificati come critici a norma della direttiva (UE) 2022/2557, e sulle misure adottate in risposta a tali rischi, minacce e incidenti. Gli Stati membri provvedono inoltre affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma del regolamento (UE) n. 910/2014, del regolamento (UE) 2022/2554 e della direttiva (UE) 2018/1972 si scambino periodicamente informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

6. Gli Stati membri semplificano la comunicazione mediante i mezzi tecnici per le notifiche di cui agli articoli 23 e 30.

CAPO III

COOPERAZIONE A LIVELLO DELL'UNIONE E INTERNAZIONALE

Articolo 14

Gruppo di cooperazione

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri, nonché di rafforzare la fiducia, è istituito un gruppo di cooperazione.

2. Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali di cui al paragrafo 7.

▼B

3. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Il Servizio europeo per l'azione esterna partecipa alle attività del gruppo di cooperazione in qualità di osservatore. Le autorità europee di vigilanza (AEV) e le autorità competenti a norma del regolamento (UE) 2022/2554 possono partecipare alle attività del gruppo di cooperazione conformemente all'articolo 47, paragrafo 1, di tale regolamento.

Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori il Parlamento europeo e i rappresentanti dei pertinenti portatori di interessi.

La Commissione ne assicura il segretariato.

4. Il gruppo di cooperazione svolge i compiti seguenti:

a) fornire orientamenti alle autorità competenti in merito al recepimento e all'attuazione della presente direttiva;

b) fornire orientamenti alle autorità competenti in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 7, paragrafo 2, lettera c);

c) scambiare migliori prassi e informazioni relative all'attuazione della presente direttiva, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, norme e specifiche tecniche, nonché l'identificazione dei soggetti essenziali e importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

d) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda le nuove iniziative strategiche in materia di cibersicurezza e la coerenza globale dei requisiti settoriali di cibersicurezza;

e) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda i progetti di atti delegati o di esecuzione adottati a norma della presente direttiva;

f) scambiare migliori prassi e informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione;

g) effettuare scambi di opinioni per quanto riguarda l'attuazione degli atti giuridici settoriali dell'Unione che contengono disposizioni in materia di cibersicurezza;

h) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9 ed elaborare conclusioni e raccomandazioni;

i) effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche conformemente all'articolo 22, paragrafo 1;

▼C1

j) discutere i casi di assistenza reciproca, fra cui le esperienze e i risultati delle azioni di vigilanza congiunte transfrontaliere di cui all'articolo 37;

▼B

k) su richiesta di uno o più Stati membri interessati, discutere le richieste specifiche di assistenza reciproca di cui all'articolo 37;

l) fornire orientamenti strategici alla rete di CSIRT ed EU–CyCLONe su specifiche questioni emergenti;

▼C1

m) effettuare scambi di opinioni sulla politica in materia di azioni intraprese a seguito di incidenti e crisi di cibersicurezza su vasta scala sulla base delle lezioni apprese dalla rete di CSIRT e da EU-CyCLONe;

▼B

n) contribuire alle capacità di cibersicurezza in tutta l'Unione agevolando lo scambio di funzionari nazionali attraverso un programma di sviluppo delle capacità che coinvolga il personale delle autorità competenti o dei CSIRT;

o) organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo di cooperazione e raccogliere contributi sulle sfide strategiche emergenti;

p) discutere le attività intraprese per quanto riguarda le esercitazioni di cibersicurezza, compreso il lavoro svolto dall'ENISA;

q) stabilire la metodologia e gli aspetti organizzativi delle revisioni tra pari di cui all'articolo 19, paragrafo 1, nonché stabilire, con l'assistenza della Commissione e dell'ENISA, la metodologia di autovalutazione per gli Stati membri a norma dell'articolo 19, paragrafo 4, ed elaborare, in collaborazione con la Commissione e l'ENISA, i codici di condotta su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati a norma dell'articolo 19, paragrafo 6;

r) elaborare relazioni, ai fini del riesame di cui all'articolo 40, sull'esperienza acquisita a livello strategico e dalle revisioni tra pari;

s) discutere e svolgere periodicamente una valutazione dello stato di avanzamento delle minacce o degli incidenti informatici, come il ransomware.

Il gruppo di cooperazione presenta le relazioni di cui al primo comma, lettera r), alla Commissione, al Parlamento europeo e al Consiglio.

5. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro rappresentanti in seno al gruppo di cooperazione.

6. Il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati.

7. Entro il 1º febbraio 2024 e successivamente ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti.

▼B

8. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo comma del presente paragrafo, conformemente al paragrafo 4, lettera e).

9. Il gruppo di cooperazione si riunisce periodicamente, e in ogni caso una volta all'anno, con il gruppo per la resilienza dei soggetti critici istituito a norma della direttiva (UE) 2022/2557 al fine di promuovere e agevolare la cooperazione strategica e lo scambio di informazioni.

Articolo 15

Rete di CSIRT

1. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

2. La rete di CSIRT è composta da rappresentanti dei CSIRT designati o istituiti a norma dell'articolo 10 e della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE). La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'ENISA ne assicura il segretariato e fornisce attivamente assistenza alla cooperazione fra i CSIRT.

3. La rete di CSIRT svolge i compiti seguenti:

a) scambiare informazioni per quanto riguarda le capacità dei CSIRT;

b) agevolare 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;

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

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

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 potenzialmente interessato da un incidente, scambiare e discutere informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati;

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

▼B

h) fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva;

i) cooperare e scambiare migliori pratiche con i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, 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;

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

   i) categorie di minacce informatiche e incidenti;

   ii) preallarmi;

   iii) assistenza reciproca;

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

   v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4, su richiesta di uno Stato membro;

k) informare il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera j) e, se necessario, chiedere orientamenti in merito;

l) fare il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA;

m) su richiesta di un singolo CSIRT, discutere le capacità e lo stato di preparazione di tale CSIRT;

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

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9;

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

4. Entro il 17 gennaio 2025, e successivamente ogni due anni, ai fini del riesame di cui all'articolo 40, la rete di CSIRT valuta i progressi compiuti nella cooperazione operativa ed elabora una relazione. Nella relazione, in particolare, vengono elaborate conclusioni e raccomandazioni sulla base del risultato delle revisioni tra pari di cui all'articolo 19, che sono effettuate in relazione ai CSIRT nazionali. Tale relazione è trasmessa al gruppo di cooperazione.

5. La rete di CSIRT adotta il proprio regolamento interno.

6. La rete di CSIRT ed EU-CyCLONe concordano le modalità procedurali e cooperano su tale base.

▼B

Articolo 16

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

1. EU-CyCLONe è istituita al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza 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.

2. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, nei casi in cui un incidente di cibersicurezza su vasta scala potenziale o in corso abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nell'ambito di applicazione della presente direttiva, della Commissione. Negli altri casi, la Commissione partecipa alle attività di EU-CyCLONe in qualità di osservatore.

L'ENISA assicura il segretariato di EU-CyCLONe e sostiene lo scambio sicuro di informazioni, oltre a fornire gli strumenti necessari per sostenere la cooperazione tra gli Stati membri garantendo uno scambio sicuro di informazioni.

Ove opportuno, EU-CyCLONe può invitare i rappresentanti dei pertinenti portatori di interessi a partecipare ai suoi lavori in qualità di osservatori.

3. EU-CyCLONe svolge i compiti seguenti:

▼C1

a) aumentare il livello di preparazione per la gestione di incidenti e crisi su vasta scala;

▼B

b) sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi di cibersicurezza su vasta scala;

▼C1

c) valutare le conseguenze e l'impatto dei pertinenti incidenti e delle pertinenti crisi di cibersicurezza su vasta scala e proporre possibili misure di mitigazione;

▼B

d) coordinare la gestione degli incidenti e delle crisi di cibersicurezza 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 di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4.

4. EU-CyCLONe adotta il proprio regolamento interno.

5. EU-CyCLONe riferisce periodicamente al gruppo di cooperazione in merito alla gestione degli incidenti e delle crisi di cibersicurezza su vasta scala, nonché in merito alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti.

▼B

6. EU-CyCLONe coopera con la rete di CSIRT sulla base di modalità procedurali concordate previste all'articolo 15, paragrafo 6.

7. Entro il 17 luglio 2024 e successivamente ogni 18 mesi, EU-CyCLONe presenta al Parlamento europeo e al Consiglio una relazione di valutazione del proprio lavoro.

Articolo 17

Cooperazione internazionale

Ove opportuno, l'Unione può concludere accordi internazionali, conformemente all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di EU-CyCLONe. Tali accordi sono conformi al diritto dell'Unione in materia di protezione dei dati.

Articolo 18

Relazione sullo stato della cibersicurezza nell'Unione

▼C1

1. L'ENISA, in collaborazione con la Commissione e con il gruppo di cooperazione, pubblica una relazione biennale sullo stato della cibersicurezza nell'Unione e la presenta al Parlamento europeo. La relazione è resa disponibile, fra l'altro, in un formato leggibile da dispositivo automatico e comprende gli aspetti seguenti:

▼B

a) una valutazione del rischio di cibersicurezza a livello dell'Unione, che tenga conto del panorama delle minacce informatiche;

b) una valutazione dello sviluppo delle capacità di cibersicurezza nei settori pubblico e privato nell'Unione;

c) una valutazione del livello generale di consapevolezza in materia di cibersicurezza e di igiene informatica tra i cittadini e i soggetti, comprese le piccole e medie imprese;

d) una valutazione aggregata del risultato delle revisioni tra pari di cui all'articolo 19;

e) una valutazione aggregata del livello di maturità delle capacità e delle risorse di cibersicurezza nell'Unione, comprese quelle a livello settoriale, nonché del livello di allineamento delle strategie nazionali di cibersicurezza degli Stati membri.

2. La relazione contiene raccomandazioni strategiche specifiche, finalizzate a porre rimedio alle carenze e ad aumentare il livello di cibersicurezza nell'Unione, e una sintesi delle conclusioni tratte per quel determinato periodo nelle relazioni sulla situazione tecnica della cibersicurezza nell'Unione per quanto riguarda gli incidenti e le minacce informatiche, elaborate dall'ENISA conformemente all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881.

3. L'ENISA, in collaborazione con la Commissione, il gruppo di cooperazione e la rete di CSIRT, elabora la metodologia, ivi comprese le variabili pertinenti — come ad esempio indicatori quantitativi e qualitativi — della valutazione aggregata di cui al paragrafo 1, lettera e).

▼B

Articolo 19

Revisioni tra pari

1. Con l'assistenza della Commissione e dell'ENISA nonché, se del caso, della rete CSIRT ed entro il 17 gennaio 2025, il gruppo di cooperazione stabilisce la metodologia e gli aspetti organizzativi delle revisioni tra pari con l'obiettivo di trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e migliorare le capacità e le politiche di cibersicurezza degli Stati membri necessarie per attuare la presente direttiva. La partecipazione alle revisioni tra pari è volontaria. Le revisioni tra pari sono condotte da esperti di cibersicurezza. Gli esperti di cibersicurezza sono designati da almeno due Stati membri, diversi dallo Stato membro oggetto di revisione.

Le revisioni tra pari riguardano almeno uno degli aspetti seguenti:

a) il livello di attuazione delle misure di gestione e delle prescrizioni in materia di segnalazione dei rischi di cibersicurezza enunciate agli articoli 21 e 23;

b) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti delle autorità competenti;

c) le capacità operative dei CSIRT;

d) il livello di attuazione dell'assistenza reciproca di cui all'articolo 37;

e) il livello di attuazione degli accordi per la condivisione delle informazioni in materia di cibersicurezza di cui all'articolo 29;

f) le questioni specifiche di natura transfrontaliera o intersettoriale.

2. La metodologia di cui al paragrafo 1 comprende criteri obiettivi, non discriminatori, equi e trasparenti sulla base dei quali gli Stati membri designano esperti di cibersicurezza idonei a eseguire le revisioni tra pari. La Commissione e l'ENISA partecipano alle revisioni tra pari in qualità di osservatori.

3. Gli Stati membri possono individuare questioni specifiche di cui al paragrafo 1, lettera f), ai fini di una revisione tra pari.

4. Prima dell'inizio di una revisione tra pari di cui al paragrafo 1, gli Stati membri notificano agli Stati membri partecipanti il suo ambito di applicazione, comprese le questioni specifiche individuate ai sensi del paragrafo 3.

5. Prima dell'inizio della revisione tra pari, gli Stati membri possono effettuare un'autovalutazione degli aspetti oggetto della revisione e fornire tale autovalutazione agli esperti di cibersicurezza designati. Il gruppo di cooperazione, con l'assistenza della Commissione e dell'ENISA, stabilisce la metodologia per l'autovalutazione degli Stati membri.

▼B

6. Le revisioni tra pari comportano visite in loco fisiche o virtuali e scambi di informazioni a distanza. In linea con il principio di buona collaborazione, lo Stato membro sottoposto alla revisione tra pari fornisce agli esperti di cibersicurezza designati le informazioni necessarie per la valutazione, fatta salva la legislazione nazionale o dell'Unione in materia di protezione di informazioni riservate o classificate e di salvaguardia delle funzioni essenziali dello Stato, quali la sicurezza nazionale. Il gruppo di cooperazione, in collaborazione con la Commissione e con l'ENISA, elabora codici di condotta adeguati, su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati. Le informazioni ottenute mediante la revisione tra pari sono utilizzate unicamente a tal fine. Gli esperti di cibersicurezza che partecipano alla revisione tra pari non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso di tale revisione tra pari.

7. Una volta sottoposti a revisione tra pari, i medesimi aspetti esaminati in uno Stato membro non sono più soggetti a ulteriori revisioni tra pari in tale Stato membro per i due anni successivi alla conclusione della revisione, a meno che non sia diversamente richiesto o stabilito dallo Stato membro su proposta del gruppo di cooperazione.

8. Gli Stati membri provvedono affinché gli eventuali rischi di conflitto di interessi riguardanti gli esperti di cibersicurezza designati siano rivelati agli altri Stati membri, al gruppo di cooperazione, alla Commissione e all'ENISA prima dell'inizio della revisione tra pari. Lo Stato membro che è sottoposto alla revisione tra pari può opporsi alla designazione di particolari esperti di cibersicurezza per motivi debitamente giustificati, comunicati allo Stato membro designante.

9. Gli esperti di cibersicurezza che partecipano alle revisioni tra pari elaborano relazioni sui risultati e sulle conclusioni delle revisioni tra pari. Gli Stati membri sottoposti a revisione tra pari possono formulare osservazioni sui progetti di relazione che li riguardano e tali osservazioni sono allegate alle relazioni. Le relazioni contengono raccomandazioni che consentono di migliorare gli aspetti sottoposti alla revisione tra pari. Le relazioni sono presentate al gruppo di cooperazione e alla rete di CSIRT, se del caso. Uno Stato membro sottoposto alla revisione tra pari può decidere di rendere pubblica la sua relazione o una sua versione espunta.

CAPO IV

MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE

Articolo 20

Governance

1. Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21, sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo.

L'applicazione del presente paragrafo lascia impregiudicato il diritto nazionale per quanto riguarda le norme in materia di responsabilità applicabili alle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

▼B

2. Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

Articolo 21

Misure di gestione dei rischi di cibersicurezza

▼C1

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i 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.

Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informativi e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;

▼B

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

▼C1

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

▼B

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

▼B

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) 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, se del caso.

3. Gli Stati membri provvedono affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), del presente articolo, siano adeguate, i soggetti tengano conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Gli Stati membri provvedono inoltre affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), siano adeguate, i soggetti siano tenuti a tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22, paragrafo 1.

4. Gli Stati membri provvedono affinché, qualora un soggetto constati di non essere conforme alle misure di cui al paragrafo 2, esso adotti, senza indebito ritardo, tutte le misure correttive necessarie, appropriate e proporzionate.

5. Entro il 17 ottobre 2024, la Commissione adotta atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure di cui al paragrafo 2 per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, 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, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, nonché i prestatori di servizi fiduciari.

La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici e metodologici, nonché, se necessario, i requisiti settoriali relativi alle misure di cui al paragrafo 2 per quanto riguarda i soggetti essenziali e importanti diversi da quelli di cui al primo comma del presente paragrafo.

Nell'elaborare gli atti di esecuzione di cui al primo e secondo comma del presente paragrafo, la Commissione segue, nella misura del possibile, le norme europee e internazionali, nonché le pertinenti specifiche tecniche. La Commissione scambia pareri e coopera con il gruppo di cooperazione e con l'ENISA in merito ai progetti di atto di esecuzione conformemente all'articolo 14, paragrafo 4, lettera e).

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 22

Valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche

1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi TIC, sistemi TIC o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici.

▼B

2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, nonché, ove necessario, dei pertinenti portatori di interessi, identifica i servizi TIC, i sistemi TIC o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata del rischio per la sicurezza di cui al paragrafo 1.

Articolo 23

Obblighi di segnalazione

1. Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al paragrafo 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi quali indicati al paragrafo 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi. Ciascuno Stato membro provvede affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente. La sola notifica non espone il soggetto che la effettua a una maggiore responsabilità.

Qualora i soggetti interessati notifichino all'autorità competente un incidente significativo conformemente al primo comma, lo Stato membro provvede affinché l'autorità competente inoltri la notifica al CSIRT dopo averla ricevuta.

In caso di incidente significativo transfrontaliero o intersettoriale, gli Stati membri provvedono affinché i loro punti di contatto unici ricevano in tempo utile informazioni pertinenti notificate conformemente al paragrafo 4.

2. Se opportuno, gli Stati membri provvedono affinché i soggetti essenziali e importanti comunichino senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari sono in grado di adottare in risposta a tale minaccia. Se opportuno, i soggetti informano tali destinatari anche della minaccia informatica significativa stessa.

3. 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) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente:

a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

▼B

b) senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, 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 di un CSIRT o, se opportuno, di un'autorità competente, 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:

i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;

ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

▼C1

iii) le misure di mitigazione adottate e in corso;

▼B

iv) se opportuno, l'impatto transfrontaliero dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), gli Stati membri provvedono affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

In deroga al primo comma, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, informa il CSIRT o, se opportuno, l'autorità competente senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.

5. ►C1 Senza indebito ritardo e ove possibile entro 24 ore dal ricevimento del preallarme di cui al paragrafo 4, lettera a), il CSIRT o l'autorità competente fornisce una risposta al soggetto notificante, comprendente un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza operativa sull'attuazione di possibili misure di mitigazione. ◄ Se il CSIRT non è il destinatario iniziale della notifica di cui al paragrafo 1, gli orientamenti sono forniti dall'autorità competente in cooperazione con il CSIRT. Su richiesta del soggetto interessato, il CSIRT fornisce ulteriore supporto tecnico. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT o l'autorità competente fornisce anche orientamenti sulla segnalazione dell'incidente significativo alle autorità di contrasto.

6. Se opportuno, e in particolare se l'incidente significativo interessa due o più Stati membri, il CSIRT, l'autorità competente o il punto di contatto unico ne informa senza indebito ritardo gli altri Stati membri interessati e l'ENISA. Tali informazioni includono o il tipo di informazioni ricevute a norma del paragrafo 4. Nel fare ciò, il CSIRT, l'autorità competente o il punto di contatto unico tutelano, in conformità al diritto dell'Unione o nazionale, la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite.

▼B

7. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente significativo o affrontare un incidente significativo in corso, o qualora la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato il CSIRT di uno Stato membro o, se del caso, la sua autorità competente e, se opportuno, i CSIRT o le autorità competenti degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente significativo o imporre al soggetto di farlo.

8. Su richiesta del CSIRT o dell'autorità competente, il punto di contatto unico inoltra le notifiche ricevute a norma del paragrafo 1 ai punti di contatto unici degli altri Stati membri interessati.

9. Il punto di contatto unico trasmette ogni tre mesi all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30. Al fine di contribuire alla fornitura di informazioni comparabili, l'ENISA può adottare orientamenti tecnici sui parametri delle informazioni da includere nella relazione di sintesi. Ogni sei mesi l'ENISA informa il gruppo di cooperazione e la rete di CSIRT delle sue constatazioni in merito alle notifiche ricevute.

▼C1

10. I CSIRT o, se opportuno, le autorità competenti forniscono alle autorità competenti a norma della direttiva (UE) 2022/2557 le informazioni sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30 dai soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557.

▼B

11. La Commissione può adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura di trasmissione di una notifica a norma del paragrafo 1 del presente articolo e dell'articolo 30 e di una comunicazione trasmessa a norma del paragrafo 2 del presente articolo.

Entro il 17 ottobre 2024 la Commissione adotta, per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, 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, nonché i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, atti di esecuzione che specifichino ulteriormente i casi in cui un incidente debba essere considerato significativo come indicato al paragrafo 3. La Commissione può adottare tali atti di esecuzione in relazione ad altri soggetti essenziali e importanti.

La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo e secondo comma del presente paragrafo conformemente all'articolo 14, paragrafo 4, lettera e).

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

▼B

Articolo 24

Uso dei sistemi europei di certificazione della cibersicurezza

1. Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 21, gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati 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 cibersicurezza adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. Inoltre, gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati.

2. Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 38 al fine di integrare la presente direttiva specificando quali categorie di soggetti essenziali e importanti sono tenute a utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o a ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881. Tali atti delegati sono adottati qualora siano stati individuati livelli insufficienti di cibersicurezza e includono un periodo di attuazione.

Prima di adottare tali atti delegati, la Commissione effettua una valutazione d'impatto e procede a consultazioni conformemente all'articolo 56 del regolamento (UE) 2019/881.

3. Qualora non siano disponibili sistemi di europei di certificazione della cibersicurezza adeguati ai fini del paragrafo 2 del presente articolo, la Commissione può chiedere all'ENISA, previa consultazione del gruppo di cooperazione e del gruppo europeo per la certificazione della cibersicurezza, di preparare una proposta di sistema a norma dell'articolo 48, paragrafo 2, del regolamento (UE) 2019/881.

Articolo 25

Normazione

▼C1

1. Per promuovere l'attuazione convergente dell'articolo 21, paragrafi 1 e 2, gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informativi e di rete.

▼B

2. L'ENISA, in cooperazione con gli Stati membri e, se opportuno, previa consultazione dei pertinenti portatori di interessi, elabora documenti di consulenza e orientamento riguardanti tanto i settori tecnici da prendere in considerazione in relazione al paragrafo 1, quanto le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.

CAPO V

GIURISDIZIONE E REGISTRAZIONE

Articolo 26

Giurisdizione e territorialità

1. I soggetti che rientrano nell'ambito di applicazione della presente direttiva sono considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti, ad eccezione dei casi seguenti:

▼B

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 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 considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione a norma del paragrafo 2;

c) gli enti della pubblica amministrazione, che sono considerati sotto la giurisdizione dello Stato membro che li ha istituiti.

2. Ai fini della presente direttiva, si considera che un soggetto di cui al paragrafo 1, lettera b), abbia il proprio stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui sono effettuate le operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione.

3. Se un soggetto di cui al paragrafo 1, lettera b), non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Nell'assenza di un rappresentante nell'Unione designato a norma del presente paragrafo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per violazione degli obblighi della presente direttiva.

4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1, lettera b), fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso.

▼C1

5. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a un soggetto di cui al paragrafo 1, lettera b), possono, entro i limiti della richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che fornisce servizi o che ha un sistema informativo e di rete nel loro territorio.

▼B

Articolo 27

Registro dei soggetti

1. L'ENISA crea e mantiene un registro di fornitori di servizi DNS, registri dei nomi di dominio di primo livello, soggetti che forniscono 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, fornitori di servizi di sicurezza gestiti, nonché fornitori di mercati online, di motori di

▼B

ricerca online e di piattaforme di servizi di social network sulla base delle informazioni ricevute dai punti di contatto unici conformemente al paragrafo 4. Su richiesta, l'ENISA consente alle autorità competenti di accedere a tale registro, assicurando nel contempo la tutela della riservatezza delle informazioni, se del caso.

2. Gli Stati membri esigono che i soggetti di cui al paragrafo 1 trasmettano entro il 17 gennaio 2025, le informazioni seguenti alle autorità competenti:

a) il proprio nome;

b) il settore, il sottosettore e il tipo di soggetto di cui all'allegato I o II, se del caso;

c) l'indirizzo dello stabilimento principale e degli altri stabilimenti legali del soggetto nell'Unione o, se non è stabilito nell'Unione, del suo rappresentante a norma dell'articolo 26, paragrafo 3;

d) i dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono del soggetto, e, se opportuno, del suo rappresentante a norma dell'articolo 26, paragrafo 3;

e) gli Stati membri in cui il soggetto fornisce i suoi servizi; e

f) le serie di IP del soggetto.

▼C1

3. Gli Stati membri provvedono affinché i soggetti di cui al paragrafo 1 notifichino all'autorità competente qualsiasi modifica delle informazioni trasmesse a norma del paragrafo 2 tempestivamente e, in ogni caso, entro tre mesi dalla data della modifica.

▼B

4. In seguito alla ricezione delle informazioni di cui ai paragrafi 2 e 3, ad eccezione di quelle di cui al paragrafo 2, lettera f), il punto di contatto unico dello Stato membro interessato, senza ritardo, le inoltra all'ENISA.

5. Se opportuno, le informazioni di cui ai paragrafi 2 e 3 del presente articolo sono trasmesse attraverso il meccanismo nazionale di cui all'articolo 3, paragrafo 4, quarto comma.

Articolo 28

Banca dati dei dati di registrazione dei nomi di dominio

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza del DNS, gli Stati membri impongono ai registri dei nomi di TLD e ai soggetti che forniscono servizi di registrazione dei nomi di dominio di raccogliere e mantenere dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione in materia di protezione dei dati per quanto riguarda i dati personali.

2. Ai fini del paragrafo 1, gli Stati membri esigono che la banca dati dei dati di registrazione dei nomi di dominio contenga 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. Tali informazioni includono:

▼B

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. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio predispongano politiche e procedure, incluse procedure di verifica, per garantire che le banche dati di cui al paragrafo 1 comprendano informazioni accurate e complete. Gli Stati membri esigono che tali politiche e procedure siano rese pubbliche.

4. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD rendano pubblicamente disponibili, senza indebito ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali.

5. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio, su richiesta legittima e debitamente motivata di legittimi richiedenti l'accesso, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondano senza indebito ritardo e comunque entro 72 ore dalla ricezione delle richieste di accesso. Gli Stati membri esigono che le politiche e le procedure relative alla divulgazione di tali dati siano rese pubbliche.

6. Il rispetto degli obblighi di cui ai paragrafi da 1 a 5 non comportano una duplicazione della raccolta di dati di registrazione dei nomi di dominio. A tal fine, gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio collaborino tra loro.

CAPO VI

CONDIVISIONE DELLE INFORMAZIONI

Articolo 29

Accordi di condivisione delle informazioni sulla cibersicurezza

1. Gli Stati membri provvedono affinché i soggetti che rientrano nell'ambito di applicazione della presente direttiva e, se del caso, altri soggetti che non rientrano nell'ambito di applicazione della presente direttiva siano in grado di scambiarsi, su base volontaria, pertinenti informazioni sulla cibersicurezza, 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 cibersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cibersicurezza per individuare le minacce informatiche, se tale condivisione di informazioni:

▼B

a) mira a prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto;

▼C1

b) aumenta il livello di cibersicurezza, 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.

▼B

2. Gli Stati membri provvedono affinché lo scambio di informazioni avvenga 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 cibersicurezza che tengono conto della natura potenzialmente sensibile delle informazioni condivise.

3. Gli Stati membri facilitano la conclusione degli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 del presente articolo. Gli Stati membri possono 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, gli Stati membri possono imporre condizioni per le informazioni messe a disposizione dalle autorità competenti o dai CSIRT. Gli Stati membri offrono assistenza per l'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 7, paragrafo 2, lettera h).

4. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.

5. L'ENISA offre assistenza per la conclusione di accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 fornendo orientamenti e provvedendo allo scambio delle migliori pratiche.

Articolo 30

Notifica volontaria di informazioni pertinenti

1. Gli Stati membri provvedono affinché, in aggiunta all'obbligo di notifica di cui all'articolo 23, possano essere trasmesse, su base volontaria, notifiche ai CSIRT o, se opportuno, alle autorità competenti, da parte dei:

a) soggetti essenziali e importanti, per quanto riguarda gli incidenti, le minacce informatiche e i quasi incidenti;

▼B

b) soggetti diversi da quelli di cui alla lettera a), indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, per quanto riguarda gli incidenti significativi, le minacce informatiche e i quasi incidenti.

2. Gli Stati membri trattano le notifiche di cui al paragrafo 1 del presente articolo secondo la procedura di cui all'articolo 23. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie.

Se necessario, i CSIRT e, se del caso, le autorità competenti forniscono ai punti di contatto unici le informazioni sulle notifiche ricevute a norma del presente articolo, garantendo nel contempo la riservatezza e la tutela adeguata delle informazioni fornite dal soggetto notificante. Fatti salvi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, la segnalazione volontaria non ha l'effetto di imporre al soggetto notificante alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

CAPO VII

VIGILANZA ED ESECUZIONE

Articolo 31

Aspetti generali relativi alla vigilanza e all'esecuzione

1. Gli Stati membri provvedono affinché le proprie autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva.

2. Gli Stati membri possono consentire alle proprie autorità competenti di conferire priorità ai compiti di vigilanza. Tale priorità si fonda su un approccio basato sul rischio. A tal fine, nell'esercizio dei rispettivi compiti di vigilanza di cui agli articoli 32 e 33, le autorità competenti possono stabilire metodologie di vigilanza che consentano di conferire priorità a tali compiti secondo un approccio basato sul rischio.

3. Le autorità competenti operano in stretta cooperazione con le autorità di controllo ai sensi del regolamento (UE) 2016/679 nei casi di incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti delle autorità di controllo di cui a tale regolamento.

4. Fatti salvi i quadri legislativi e istituzionali nazionali, gli Stati membri provvedono affinché nel vigilare sul rispetto, da parte degli enti della pubblica amministrazione, della presente direttiva e nell'imporre misure di esecuzione in caso di violazione della presente direttiva, le autorità competenti dispongano dei poteri adeguati per svolgere tali compiti con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza. Gli Stati membri possono decidere di imporre misure di vigilanza e di esecuzione adeguate, proporzionate ed efficaci in relazione a tali enti conformemente ai quadri legislativi e istituzionali nazionali.

▼B

Articolo 32

Misure di vigilanza e di esecuzione relative a soggetti essenziali

1. Gli Stati membri provvedono affinché le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso.

▼C2

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti essenziali, abbiano il potere di sottoporre tali soggetti come minimo a:

▼B

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;

b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;

c) audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione della presente direttiva da parte del soggetto essenziale;

d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato, comprese le politiche di cibersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;

g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi.

I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto ad audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti.

3. Nell'esercizio dei loro poteri di cui al paragrafo 2, lettera e), f) o g), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le proprie autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, abbiano il potere come minimo di:

▼B

a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati;

b) adottare istruzioni vincolanti, ivi incluso per quanto riguarda le misure richieste per evitare il verificarsi di un incidente o porvi rimedio, nonché i termini per l'attuazione di tali misure e per riferire in merito alla loro attuazione, o un'ingiunzione che impongano ai soggetti interessati di porre rimedio alle carenze individuate o alle violazioni della direttiva;

c) imporre ai soggetti interessati di porre termine al comportamento che viola la presente direttiva e di astenersi dal ripeterlo;

d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione del rischio di cibersicurezza siano conformi all'articolo 21 o di adempiere gli obblighi di segnalazione di cui all'articolo 23 in una maniera ed entro un termine specificati;

e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività che sono potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia, nonché in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre ai soggetti interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

▼C1

g) designare un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato al fine di vigilare sul rispetto degli articoli 21 e 23;

▼B

h) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata;

i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo il diritto nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a qualsiasi delle misure di cui al presente paragrafo, lettere da a) a h).

5. Qualora le misure di esecuzione adottate a norma del paragrafo 4, lettere da a) a d), e lettera f), si rivelino inefficaci, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di fissare un termine entro il quale il soggetto essenziale è tenuto ad adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni di tali autorità. Se le misure richieste non sono adottate entro il termine stabilito, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di:

a) sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, 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;

b) chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto.

▼B

Le sospensioni o i divieti temporanei a norma del presente paragrafo sono applicati solo finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le misure di esecuzione sono state applicate. L'imposizione di tali sospensioni o divieti temporanei è soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta, inclusi il diritto a un ricorso effettivo e ad un giusto processo, la presunzione di innocenza e i diritti della difesa.

Le misure di esecuzione previste dal presente paragrafo non sono applicabili agli enti della pubblica amministrazione che sono soggetti alla presente direttiva.

6. Gli Stati membri provvedono affinché qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale sulla base del potere di rappresentarlo, dell'autorità di prendere decisioni per suo conto o dell'autorità di esercitare un controllo su di esso abbia il potere di garantirne il rispetto della presente direttiva. Gli Stati membri provvedono affinché tali persone fisiche possano essere ritenute responsabili dell'inadempimento dei loro doveri di garantire il rispetto della presente direttiva.

Per quanto riguarda gli enti della pubblica amministrazione, il presente paragrafo lascia impregiudicato il diritto nazionale in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

7. Nell'adottare qualsiasi misura di esecuzione di cui al paragrafo 4 o 5, le autorità competenti rispettano i diritti della difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti:

a) la gravità della violazione e l'importanza delle disposizioni violate, essendo le violazioni seguenti, tra l'altro, da considerarsi gravi:

   i) le violazioni ripetute;

   ii) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti;

   iii) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti;

   iv) l'ostacolo degli audit o delle attività di monitoraggio imposte dall'autorità competente a seguito del rilevamento di una violazione;

   v) la fornitura di informazioni false o gravemente inesatte relative alle misure in materia di gestione o segnalazione del rischio di cibersicurezza di cui agli articoli 21 e 23;

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;

▼B

e) un'eventuale condotta intenzionale o negligenza da parte dell'autore della violazione;

f) qualsiasi misure 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 le autorità competenti.

8. Le autorità competenti espongono nei particolari la motivazione delle loro misure di esecuzione. Prima di adottare tali misure le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari. Esse concedono inoltre a tali soggetti un tempo ragionevole per presentare osservazioni, salvo in casi debitamente giustificati in cui ciò impedirebbe di agire con immediatezza per prevenire un incidente o rispondervi.

9. Gli Stati membri provvedono affinché le loro autorità competenti di cui alla presente direttiva informino le autorità competenti pertinenti all'interno dello stesso Stato membro a norma della direttiva (UE) 2022/2557 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto identificato come critico a norma della direttiva (UE) 2022/2557. Se del caso, le autorità competenti di cui alla direttiva (UE) 2022/2557 possono chiedere alle autorità competenti di cui alla presente direttiva di esercitare i propri poteri di vigilanza e di esecuzione in relazione a un soggetto che è stato individuato come soggetto critico ai sensi della direttiva (UE) 2022/2557.

10. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto essenziale designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554

Articolo 33

Vigilanza ed esecuzione relative a soggetti essenziali

1. Se ricevono elementi di prova, indicazioni o informazioni secondo cui un soggetto importante non rispetta presumibilmente la presente direttiva, in particolare dagli articoli 21 e 23 della medesima, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post. Gli Stati membri provvedono affinché tali misure siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a:

▼B

a) ispezioni in loco e vigilanza ex post a distanza, effettuate da professionisti formati;

b) audit sulla sicurezza mirati svolti da un organismo indipendente o da un'autorità competente;

c) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario, con la cooperazione del soggetto interessato;

(d) richieste di qualsiasi informazione necessaria a valutare ex post le misure di gestione dei rischi di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

e) richieste di accesso a dati, documenti e/o informazioni necessari allo svolgimento dei propri compiti di vigilanza;

f) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi.

I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto a audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti.

3. Nell'esercizio dei loro poteri a norma del paragrafo 2, lettere d), e) o f), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti importanti, abbiano il potere come minimo di:

a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati;

b) adottare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi della presente direttiva;

c) imporre ai soggetti interessati di porre termine alle condotte in violazione della presente direttiva e di astenersi dal ripeterle;

d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione dei rischi di cibersicurezza siano conformi all'articolo 21 o i loro obblighi di segnalazione conformi alle prescrizioni di cui all'articolo 23 in una maniera ed entro un termine specificati;

▼B

e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia e alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre agli interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata;

h) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo la legislazione nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a una qualsiasi delle misure di cui al presente paragrafo, lettere da a) a g).

5. L'articolo 32, paragrafi 6, 7 e 8, si applica mutatis mutandis alle misure di vigilanza ed esecuzione di cui al presente articolo per soggetti importanti.

6. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto importante designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554.

Articolo 34

Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti

1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni della presente direttiva siano effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

2. Le sanzioni amministrative pecuniarie sono imposte in aggiunta a qualsiasi delle misure di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g).

3. Nel decidere se imporre una sanzione amministrativa pecuniaria e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno degli elementi di cui all'articolo 32, paragrafo 7.

4. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti essenziali siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

▼B

5. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti importanti siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

6. Gli Stati membri possono prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto essenziale o importante di cessare una violazione della presente direttiva conformemente a una precedente decisione dell'autorità competente.

7. Fatti salvi i poteri delle autorità competenti a norma degli articoli 32 e 33, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere imposte sanzioni amministrative pecuniarie agli enti della pubblica amministrazione.

8. Se l'ordinamento giuridico di uno Stato membro non prevede sanzioni amministrative pecuniarie, lo Stato membro in questione provvede affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Lo Stato membro notifica alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 17 ottobre 2024 e ne comunicano senza ritardo ogni successiva modifica.

Articolo 35

Violazioni che comportano una violazione dei dati personali

1. Qualora le autorità competenti, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto che la violazione degli obblighi di cui agli articoli 21 e 23 della presente direttiva 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 a norma dell'articolo 33 del medesimo regolamento, ne informano senza indebito ritardo le autorità di controllo competenti a norma dell'articolo 55 o 56 di tale regolamento.

2. Qualora le autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, le autorità competenti non impongono una sanzione amministrativa pecuniaria a norma dell'articolo 34 della presente direttiva per una violazione di cui al presente articolo, paragrafo 1, imputabile al medesimo comportamento punito con l'ammenda amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del regolamento (UE) 2016/679. Le autorità competenti possono tuttavia imporre le misure di esecuzione di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g) della presente direttiva.

3. Qualora l'autorità di controllo competente a norma del regolamento (UE) 2016/679 sia stabilita in uno Stato membro diverso rispetto all'autorità competente, l'autorità competente informa l'autorità di controllo stabilita nel proprio Stato membro della potenziale violazione dei dati personali di cui al paragrafo 1.

▼B

Articolo 36

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle misure nazionali adottate in attuazione della presente direttiva e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri comunicano alla Commissione, entro il 17 gennaio 2025, tali norme e misure e la informano, immediatamente, di qualsiasi modifica apportata successivamente.

Articolo 37

Assistenza reciproca

▼C1

1. Se un soggetto fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e i suoi sistemi informativi e di rete sono ubicati in uno o più altri Stati membri, le autorità competenti degli Stati membri interessati cooperano e si assistono reciprocamente in funzione delle necessità. Tale cooperazione comprende, almeno, gli aspetti seguenti:

▼B

a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano, attraverso il punto di contatto unico, le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate;

b) un'autorità competente può chiedere a un'altra autorità competente di adottare misure di vigilanza o esecuzione;

c) un'autorità competente, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente, fornisce a tale altra autorità competente un'assistenza reciproca proporzionata alle proprie risorse affinché le misure di vigilanza o esecuzione possano essere attuate in maniera efficace, efficiente e coerente.

L'assistenza reciproca di cui al primo comma. Lettera c), può riguardare richieste di informazioni e misure di vigilanza, comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che non abbia stabilito che essa non è competente per fornire l'assistenza richiesta, che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente o che la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrari agli interessi essenziali della sicurezza nazionale, la pubblica sicurezza o la difesa dello Stato membro in questione. Prima di respingere tale richiesta, l'autorità competente consulta le altre autorità competenti interessate e, su richiesta di uno degli Stati membri interessati, la Commissione e l'ENISA,

▼C1

2. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza congiunte.

▼B

CAPO VIII

ATTI DELEGATI E ATTI DI ESECUZIONE

Articolo 38

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 24, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 16 gennaio 2023.

3. La delega di potere di cui all'articolo 24, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato a norma dell'articolo 24, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 39

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

▼B

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

CAPO IX

DISPOSIZIONI FINALI

Articolo 40

Riesame

Entro il 17 ottobre 2027 e successivamente ogni 36 mesi, la Commissione riesamina il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La relazione valuta in particolare la pertinenza delle dimensioni dei soggetti interessati, e i settori, sottosettori e tipologie di soggetti di cui agli allegati I e II per il funzionamento dell'economia e della società in relazione alla cibersicurezza. A tal fine e allo scopo di intensificare ulteriormente la cooperazione strategica e operativa, la Commissione tiene conto delle relazioni del gruppo di cooperazione e della rete di CSIRT sull'esperienza acquisita a livello strategico e operativo. La relazione è corredata, se necessario, di una proposta legislativa.

Articolo 41

Recepimento

1. Entro il 17 ottobre 2024, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

Essi applicano tali disposizioni a decorrere dal 18 ottobre 2024.

2. Le disposizioni di cui al paragrafo 1 adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 42

Modifica del regolamento (UE) n. 910/2014

Nel regolamento (UE) n. 910/2014, l'articolo 19 è soppresso con effetto a decorrere dal 18 ottobre 2024.

Articolo 43

Modifica della direttiva (UE) 2018/1972

Nella direttiva (UE) 2018/1972, gli articoli 40 e 41 sono soppressi. con effetto a decorrere dal 18 ottobre 2024.

▼B

Articolo 44

Abrogazione

La direttiva (UE) 2016/1148 è abrogata con effetto a decorrere dal 18 ottobre 2024.

I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva e vanno letti secondo la tavola di concordanza di cui all'allegato III.

Articolo 45

Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 46

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

▼B

ALLEGATO I

SETTORI AD ALTA CRITICITÀ

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio ([1]) che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio ([2]) — Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944 — Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio ([3])
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio ([4])
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio ([5])
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE
		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE

▼B

Settore	Sottosettore	Tipo di soggetto
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE;
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio ([6]), aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio ([7]), e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio ([8])
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([9])
		— Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio ([10]), escluse le singole navi gestite da tale compagnia

▼B

Settore	Sottosettore	Tipo di soggetto
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio ([11]), compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([12])
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione ([13]) responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio ([14])
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([15])
4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([16])
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([17])
5. Settore sanitario		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([18])
		— Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio ([19])
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio ([20]) — Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio ([21])

▼B

Settore	Sottosettore	Tipo di soggetto
6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio ([22]), ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni
7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio ([23]), escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale
8. Infrastrutture digitali		— Fornitori di punti di interscambio internet
		— Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice
		— Registri dei nomi di dominio di primo livello (TLD)
		— Fornitori di servizi di cloud computing
		— Fornitori di servizi di data center
		— Fornitori di reti di distribuzione dei contenuti (content delivery network)
		— Fornitori di servizi fiduciari
		— Fornitori di reti pubbliche di comunicazione
		— Fornitori di servizi di comunicazione elettronica accessibili al pubblico
9. Gestione dei servizi TIC (business-to-business)		— Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti
10. Pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale
		— Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale

▼B

Settore	Sottosettore	Tipo di soggetto
11. Spazio		Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica

([1]) Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).
([2]) Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54).
([3]) Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82).
([4]) Direttiva 2009/119/CE del Consiglio, del 14 settembre 2009, che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (GU L 265 del 9.10.2009, pag. 9).
([5]) Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).
([6]) Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).
([7]) Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).
([8]) Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo («regolamento quadro») (GU L 96 del 31.3.2004, pag. 1).
([9]) Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).
([10]) Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).
([11]) Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).
([12]) Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10)
([13]) Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).
([14]) Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).
([15]) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).
([16]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).
([17]) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).
([18]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).
([19]) Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio, del 23 novembre 2022, relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE (GU L 314 del 6.12.2022, pag. 26).
([20]) Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano (GU L 311 del 28.11.2001, pag. 67).
([21]) Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici (GU L 20 del 31.1.2022, pag. 1).
([22]) Direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio del 16 dicembre 2020 concernente la qualità delle acque destinate al consumo umano (GU L 435 del 23.12.2020, pag. 1).
([23]) Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane (GU L 135 del 30.5.1991, pag. 40).

▼B

ALLEGATO II

ALTRI SETTORI CRITICI

Settore	Sottosettore	Tipo di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali quali definiti all'articolo 2, punto 1 *bis*), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio ([1]), escluse quelle per cui la gestione dei rifiuti non è la principale attività economica
3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio ([2]) e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio ([3]) che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio ([4]) e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ([5]) ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2

▼B

Settore	Sottosettore	Tipo di soggetto
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2
	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di servizi di social network
7. Ricerca		Organizzazioni di ricerca

([1]) Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, relativa ai rifiuti e che abroga alcune direttive (GU L 312 del 22.11.2008, pag. 3).
([2]) Regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE (GU L 396 del 30.12.2006, pag. 1).
([3]) Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare (GU L 31 dell'1.2.2002, pag. 1).
([4]) Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).
([5]) Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

▼B

ALLEGATO III

TAVOLA DI CONCORDANZA

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 1, paragrafo 1	Articolo 1, paragrafo 1
Articolo 1, paragrafo 2	Articolo 1, paragrafo 2
Articolo 1, paragrafo 3	—
Articolo 1, paragrafo 4	Articolo 2, paragrafo 12
Articolo 1, paragrafo 5	Articolo 2, paragrafo 13
Articolo 1, paragrafo 6	Articolo 2, paragrafi 6 e 11
Articolo 1, paragrafo 7	Articolo 4
Articolo 2	Articolo 2, paragrafo 14
Articolo 3	Articolo 5
Articolo 4	Articolo 6
Articolo 5	—
Articolo 6	—
Articolo 7, paragrafo 1	Articolo 7, paragrafi 1 e 2
Articolo 7, paragrafo 2	Articolo 7, paragrafo 4
Articolo 7, paragrafo 3	Articolo 7, paragrafo 3
Articolo 8, paragrafi da 1 a 5	Articolo 8, paragrafi da 1 a 5
Articolo 8, paragrafo 6	Articolo 13, paragrafo 4
Articolo 8, paragrafo 7	Articolo 8, paragrafo 6
Articolo 9, paragrafi 1, 2 e 3	Articolo 10, paragrafi 1, 2 e 3
Articolo 9, paragrafo 4	Articolo 10, paragrafo 9
Articolo 9, paragrafo 5	Articolo 10, paragrafo 10
Articolo 10, paragrafi 1, 2 e 3, primo comma	Articolo 13, paragrafi 1, 2 e 3
Articolo 10, paragrafo 3, secondo comma	Articolo 23, paragrafo 9
Articolo 11, paragrafo 1	Articolo 14, paragrafi 1 e 2
Articolo 11, paragrafo 2	Articolo 14, paragrafo 3
Articolo 11, paragrafo 3	Articolo 14, paragrafo 4, primo comma, lettere da a) a q) e s), e paragrafo 7

▼B

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 11, paragrafo 4	Articolo 14, paragrafo 4, primo comma, lettera r), e secondo comma
Articolo 11, paragrafo 5	Articolo 14, paragrafo 8
Articolo 12, paragrafi da 1 a 5	Articolo 15, paragrafi da 1 a 5
Articolo 13	Articolo 17
Articolo 14, paragrafi 1 e 2	Articolo 21, paragrafi da 1 a 4
Articolo 14, paragrafo 3	Articolo 23, paragrafo 1
Articolo 14, paragrafo 4	Articolo 23, paragrafo 3
Articolo 14, paragrafo 5	Articolo 23, paragrafi 5, 6 e 8
Articolo 14, paragrafo 6	Articolo 23, paragrafo 7
Articolo 14, paragrafo 7	Articolo 23, paragrafo 11
Articolo 15, paragrafo 1	Articolo 31, paragrafo 1
Articolo 15, paragrafo 2, primo comma, lettera a)	Articolo 32, paragrafo 2, lettera e)
Articolo 15, paragrafo 2, primo comma, lettera b)	Articolo 32, paragrafo 2, lettera g)
articolo 15, paragrafo 2, secondo comma	Articolo 32, paragrafo 3
Articolo 15, paragrafo 3	Articolo 32, paragrafo 4, lettera b)
Articolo 15, paragrafo 4	Articolo 31, paragrafo 3
Articolo 16, paragrafi 1 e 2	Articolo 21, paragrafi da 1 e 4
Articolo 16, paragrafo 3	Articolo 23, paragrafo 1
Articolo 16, paragrafo 4	Articolo 23, paragrafo 3
Articolo 16, paragrafo 5	—
Articolo 16, paragrafo 6	Articolo 23, paragrafo 6
Articolo 16, paragrafo 7	Articolo 23, paragrafo 7
Articolo 16, paragrafi 8 e 9	Articolo 21, paragrafo 5, e articolo 23, paragrafo 11
Articolo 16, paragrafo 10	—
Articolo 16, paragrafo 11	Articolo 2, paragrafi 1, 2 e 3
Articolo 17, paragrafo 1	-Articolo 33, paragrafo 1
Articolo 17, paragrafo 2, lettera a)	Articolo 32, paragrafo 2, lettera e)
Articolo 17, paragrafo 2, lettera b)	Articolo 32, paragrafo 4, lettera b)

▼B

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 17, paragrafo 3	Articolo 37, paragrafo 1, lettere a) e b)
Articolo 18, paragrafo 1	Articolo 26, paragrafo 1, lettera b), e paragrafo 2
Articolo 18, paragrafo 2	Articolo 26, paragrafo 3
Articolo 18, paragrafo 3	Articolo 26, paragrafo 4
Articolo 19	Articolo 25
Articolo 20	Articolo 30
Articolo 21	Articolo 36
Articolo 22	Articolo 39
Articolo 23	Articolo 40
Articolo 24	—
Articolo 25	Articolo 41
Articolo 26	Articolo 45
Articolo 27	Articolo 46
Allegato I, punto 1	Articolo 11, paragrafo 1
Allegato I, punto 2, lettera a), punti da i) a iv)	Articolo 11, paragrafo 2, lettere da a) a d)
Allegato I, punto 2, lettera a), punto v)	Articolo 11, paragrafo 2, lettera f)
Allegato I, punto 2, lettera b)	Articolo 11, paragrafo 4
Allegato I, punto 2, lettera c), punti i) e ii)	Articolo 11, paragrafo 5, lettera a)
Allegato II	Allegato I
Allegato III, punti 1 e 2	Allegato II, punto 6
Allegato III, punto 3	Allegato I, punto 8