1. Il Presidente del Consiglio dei ministri adotta, sentito il ***((Comitato interministeriale per la cybersicurezza (CIC)))***, la strategia nazionale di ***((cybersicurezza))*** per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

2. Nell'ambito della strategia nazionale di ***((cybersicurezza))***, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto:

a) gli obiettivi e le priorita' in materia di sicurezza delle reti e dei sistemi informativi;

b) il quadro di governance per conseguire gli obiettivi e le priorita', inclusi i ruoli e le responsabilita' degli organismi pubblici e degli altri attori pertinenti;

c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;

d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

e) i piani di ricerca e sviluppo;

f) un piano di valutazione dei rischi;

g) l'elenco dei vari attori coinvolti nell'attuazione.

3. Con la procedura di cui al comma 1 sono adottate linee di indirizzo per l'attuazione della strategia nazionale di ***((cybersicurezza))***.

4. ***((L'Agenzia per la cybersicurezza))*** trasmette la strategia nazionale in materia di ***((cybersicurezza))*** alla Commissione europea entro tre mesi dalla sua adozione. Puo' essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.

Art. 7

(Autorita' nazionale competente e punto di contatto unico).

1. L'Agenzia per la cybersicurezza nazionale e' designata quale autorita' nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III. Sono designate quali autorita' di settore:

a) il Ministero dello sviluppo economico, per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonche' per i servizi digitali;

b) il Ministero delle infrastrutture e della mobilita' sostenibili, per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;

c) il Ministero dell'economia e delle finanze, per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorita' di vigilanza di settore, Banca d'Italia e Consob, secondo modalita' di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;

d) il Ministero della salute, per l'attivita' di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori

dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso, e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorita' sanitarie territorialmente competenti, per le attivita' di assistenza sanitaria prestata dagli operatori autorizzati e accreditati ***((dalle Regioni))*** o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

e) il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio;

f) il Ministero della transizione ecologica e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorita' territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

2. L'autorita' nazionale competente NIS e' responsabile dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigila sull'applicazione del presente decreto a livello nazionale, esercitando altresi' le relative potesta' ispettive e sanzionatorie.

3. L'Agenzia per la cybersicurezza nazionale e' designata quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.

4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera dell'autorita' nazionale competente NIS con le autorita' competenti degli altri Stati membri, nonche' con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.

5. Il punto di contatto unico collabora nel gruppo di cooperazione in modo effettivo, efficiente e sicuro con i rappresentanti designati dagli altri Stati.

6. L'Agenzia per la cybersicurezza nazionale, in qualita' di autorita' nazionale competente NIS e di punto di contatto unico, consulta, conformemente alla normativa vigente, l'autorita' di contrasto ed il Garante per la protezione dei dati personali e collabora con essi.

7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella dell'autorita' nazionale competente NIS, i relativi compiti e qualsiasi ulteriore modifica. Alle designazioni sono assicurate idonee forme di pubblicita'.

8. Agli oneri derivanti dal presente articolo ***((,))*** pari a 1.300.000 euro ***((annui a decorrere dall'anno))*** 2018, si provvede ai sensi dell'articolo 22.

Art. 8

Gruppi di intervento per la sicurezza informatica in caso di incidente - CSIRT

1. E' istituito, presso ***((l'Agenzia per la cybersicurezza))*** nazionale, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-bis del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, gia' operante presso l'Agenzia per l'Italia digitale ai

sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82. (2)

2. L'organizzazione e il funzionamento del CSIRT italiano sono disciplinati con decreto del Presidente del Consiglio dei ministri ai sensi dell'articolo 7 del decreto legislativo 30 luglio 1999, n. 303, da adottare entro il 9 novembre 2018. PERIODO SOPPRESSO DAL D.L. 30 DICEMBRE 2019, N. 162, CONVERTITO CON MODIFICAZIONI DALLA L. 28 FEBBRAIO 2020, N. 8. PERIODO SOPPRESSO DAL D.L. 30 DICEMBRE 2019, N. 162, CONVERTITO CON MODIFICAZIONI DALLA L. 28 FEBBRAIO 2020, N. 8.

3. Nelle more dell'adozione del decreto di cui al comma 2, le funzioni di CSIRT italiano sono svolte dal CERT nazionale unitamente al CERT-PA in collaborazione tra loro.

4. Il CSIRT italiano assicura la conformita' ai requisiti di cui all'allegato I, punto 1, svolge i compiti di cui all'allegato I, punto 2, si occupa dei settori di cui all'allegato II e dei servizi di cui all'allegato III e dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale.

5. Il CSIRT italiano definisce le procedure per la prevenzione e la gestione degli incidenti informatici.

6. Il CSIRT italiano garantisce la collaborazione effettiva, efficiente e sicura, nella rete di CSIRT di cui all'articolo 11.

7. La Presidenza del Consiglio dei ministri comunica alla Commissione europea il mandato del CSIRT italiano e le modalita' di trattamento degli incidenti a questo affidati.

8. Il CSIRT italiano, per lo svolgimento delle proprie funzioni, puo' avvalersi anche dell'Agenzia per l'Italia digitale.

9. Le funzioni svolte dal Ministero dello sviluppo economico in qualita' di CERT nazionale ai sensi dell'articolo 16-bis, del decreto legislativo 1° agosto 2003, n. 259, nonche' quelle svolte da Agenzia per l'Italia digitale in qualita' di CERT-PA, ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, sono trasferite al CSIRT italiano a far data dalla entrata in vigore del decreto di cui al comma 2. ***((4))***

10. Per le spese relative al funzionamento del CSIRT italiano e' autorizzata la spesa di 2.000.000 di euro annui a decorrere dall'anno 2020. A tali oneri si provvede ai sensi dell'articolo 22. (2)

AGGIORNAMENTO (2)

Il D.L. 30 dicembre 2019, n. 162, convertito con modificazioni dalla L. 28 febbraio 2020, n. 8, ha disposto (con l'art. 26, comma 1, alinea) che le presenti modifiche hanno efficacia dal 1° gennaio 2020.

AGGIORNAMENTO (4)

Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera a)) che "Nel decreto legislativo NIS:

a) ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni di cui all'articolo 7,

comma 1, lettera a), del medesimo decreto legislativo, come sostituito dal comma 1, lettera g), del presente articolo".

Art. 9

Cooperazione a livello nazionale

1. Le autorita' di settore collaborano con l'autorita' nazionale competente NIS per l'adempimento degli obblighi di cui al presente decreto. A tal fine e' istituito presso l'Agenzia per la cybersicurezza ***((nazionale un))*** Comitato tecnico di raccordo. Il Comitato e' presieduto dall'autorita' nazionale competente NIS ed e' composto dai rappresentanti delle amministrazioni statali individuate quali autorita' di settore e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato e' definita con decreto del Presidente del Consiglio dei ministri, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi ***((di))*** spese.

2. Gli operatori di servizi essenziali e i fornitori di servizi digitali inviano le notifiche relative ad incidenti al CSIRT italiano.

3. Il CSIRT italiano informa le autorita' competenti NIS, il punto di contatto unico e l'organo del Ministero dell'interno per la sicurezza e la regolarita' dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, in merito alle notifiche di incidenti trasmesse ai sensi del presente decreto. ***((4))***

AGGIORNAMENTO (4)

Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera c)) che "Nel decreto legislativo NIS: [...]

c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Capo III
Cooperazione

Art. 10

Gruppo di cooperazione

1. Il punto di contatto unico partecipa alle attivita' del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'Unione europea per la

sicurezza delle reti e dell'informazione (ENISA) e, in particolare, contribuisce a:

a) condividere buone pratiche sullo scambio di informazioni relative alla notifica di incidenti di cui all'articolo 12 e all'articolo 14;

b) scambiare migliori pratiche con gli Stati membri e, in collaborazione con l'ENISA, fornire supporto per la creazione di capacita' in materia di sicurezza delle reti e dei sistemi informativi;

c) discutere le capacita' e lo stato di preparazione degli Stati membri e valutare, su base volontaria, le strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi e l'efficacia dei CSIRT e individuare le migliori pratiche;

d) scambiare informazioni e migliori pratiche in materia di sensibilizzazione e formazione;

e) scambiare informazioni e migliori pratiche in materia di ricerca e sviluppo riguardo alla sicurezza delle reti e dei sistemi informativi;

f) scambiare, ove opportuno, esperienze in materia di sicurezza delle reti e dei sistemi informativi con le istituzioni, gli organi e gli organismi pertinenti dell'Unione europea;

g) discutere le norme e le specifiche di cui all'articolo 17 con i rappresentanti delle pertinenti organizzazioni di normazione europee;

h) fornire informazioni in relazione ai rischi e agli incidenti;

i) esaminare, su base annuale, le relazioni sintetiche di cui al comma 4;

l) discutere il lavoro svolto riguardo a esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, programmi di istruzione e formazione, comprese le attivita' svolte dall'ENISA;

m) con l'assistenza dell'ENISA, scambiare migliori pratiche connesse all'identificazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere riguardo a rischi e incidenti;

n) discutere modalita' per la comunicazione di notifiche di incidenti di cui agli articoli 12 e 14.

2. Le autorita' competenti NIS, attraverso il punto di contatto unico, assicurano la partecipazione al gruppo di cooperazione al fine di elaborare ed adottare orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti, compresi i parametri di cui all'articolo 12, comma 8.***((4))***

3. Il punto di contatto unico, ove necessario, chiede alle autorita' competenti NIS interessate, nonche' al CSIRT, la partecipazione al gruppo di cooperazione. ***((4))***

4. Entro il 9 agosto 2018 e in seguito ogni anno, il punto di contatto unico trasmette una relazione sintetica al gruppo di cooperazione in merito alle notifiche ricevute, compresi il numero di notifiche e la natura degli incidenti notificati e alle azioni intraprese ai sensi degli articoli 12 e 14.

AGGIORNAMENTO (4)

Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2,

lettera c)) che "Nel decreto legislativo NIS: [...]
c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Art. 11

Rete di CSIRT

1. Il CSIRT italiano partecipa alla rete di CSIRT, composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.
2. Il CSIRT italiano, ai fini del comma 1, provvede a:
a) scambiare informazioni sui servizi, sulle operazioni e sulle capacita' di cooperazione dei CSIRT;
b) su richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente e i rischi associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;
c) scambiare e mettere a disposizione su base volontaria informazioni non riservate su singoli incidenti;
d) su richiesta di un rappresentante di un CSIRT di un altro Stato membro, discutere e, ove possibile, individuare un intervento coordinato per un incidente rilevato nella giurisdizione di quello stesso Stato membro;
e) fornire sostegno agli altri Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria;
f) discutere, esaminare e individuare ulteriori forme di cooperazione operativa, anche in relazione a:
1) categorie di rischi e di incidenti;
2) preallarmi;
3) assistenza reciproca;
4) principi e modalita' di coordinamento, quando gli Stati membri intervengono in relazione a rischi e incidenti transfrontalieri;
g) informare il gruppo di cooperazione in merito alle proprie attivita' e a ulteriori forme di cooperazione operativa discusse sulla scorta della lettera f) e chiedere orientamenti in merito;
h) discutere gli insegnamenti appresi dalle esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA;
i) formulare orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

Capo IV
Sicurezza della rete e dei sistemi informativi degli operatori di servizi essenziali

Art. 12

Obblighi in materia di sicurezza e notifica degli incidenti

1. Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze piu' aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuita' di tali servizi.

3. Nell'adozione delle misure di cui ai commi 1 e 2, gli operatori di servizi essenziali tengono conto delle linee guida predisposte dal gruppo di cooperazione di cui all'articolo 10, nonche' delle linee guida di cui al comma 7.

4. Fatto salvo quanto previsto dai commi 1, 2 e 3, le autorita' competenti NIS possono, se necessario, definire specifiche misure, sentiti gli operatori di servizi essenziali. ***((4))***

5. Gli operatori di servizi essenziali notificano al CSIRT italiano senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuita' dei servizi essenziali forniti.

6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il Comitato interministeriale per la cybersicurezza (CIC), delle attivita' di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento. (4)

7. Le notifiche includono le informazioni che consentono al CSIRT italiano di determinare un eventuale impatto transfrontaliero dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilita' rispetto a quella derivante dall'incidente. Le autorita' competenti NIS possono predisporre linee guida per la notifica degli incidenti. ***((4))***

8. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri:

a) il numero di utenti interessati dalla perturbazione del servizio essenziale;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente.

9. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, il CSIRT italiano informa gli eventuali altri Stati membri interessati in cui l'incidente ha un impatto rilevante sulla continuita' dei servizi essenziali.

10 Ai fini del comma 9, il CSIRT italiano preserva, conformemente al diritto dell'Unione europea e alla legislazione nazionale, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonche' la riservatezza delle informazioni fornite nella notifica secondo quanto previsto dall'articolo 1, comma 5.

11. Ove le circostanze lo consentano, il CSIRT italiano fornisce

all'operatore di servizi essenziali, che effettua la notifica, le pertinenti informazioni relative al seguito della notifica stessa, nonche' le informazioni che possono facilitare un trattamento efficace dell'incidente.

12. Su richiesta dell'autorita' competente NIS o del CSIRT italiano, il punto di contatto unico trasmette, previa verifica dei presupposti, le notifiche ai punti di contatto unici degli altri Stati membri interessati. ***((4))***

13. Previa valutazione da parte dell'organo di cui al comma 6, l'autorita' competente NIS, d'intesa con il CSIRT italiano, dopo aver consultato l'operatore dei servizi essenziali notificante, puo' informare il pubblico in merito ai singoli incidenti, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso. ***((4))***

14. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Gli operatori di servizi essenziali provvedono agli adempimenti previsti dal presente articolo a valere sulle risorse finanziarie disponibili sui propri bilanci.

AGGIORNAMENTO (4)

Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera c)) che "Nel decreto legislativo NIS: [...]

b) ogni riferimento al DIS, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Art. 13

Attuazione e controllo

1. Le autorita' competenti NIS valutano il rispetto da parte degli operatori di servizi essenziali degli obblighi previsti dall'articolo 12, nonche' i relativi effetti sulla sicurezza della rete e dei sistemi informativi. ***((4))***

2. Ai fini del comma 1, gli operatori di servizi essenziali sono tenuti a fornire all'autorita' competente NIS: ***((4))***

a) le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;

b) la prova dell'effettiva attuazione delle politiche di sicurezza, come i risultati di un audit sulla sicurezza svolto dall'autorita' competente NIS o da un revisore abilitato e, in quest'ultimo caso, metterne a disposizione dell'autorita' competente NIS i risultati, inclusi gli elementi di prova. ***((4))***

3. Quando richiede le informazioni o le prove di cui al comma 2, l'autorita' competente NIS indica lo scopo delle richieste

specificando il tipo di informazioni da fornire. ***((4))***

4. A seguito della valutazione delle informazioni o dei risultati degli audit sulla sicurezza di cui al comma 2, l'autorita' competente NIS puo' emanare istruzioni vincolanti per gli operatori di servizi essenziali al fine di porre rimedio alle carenze individuate. ***((4))***

5. Nei casi di incidenti che comportano violazioni di dati personali, l'autorita' competente NIS opera in stretta cooperazione con il Garante per la protezione dei dati personali. ***((4))***

AGGIORNAMENTO (4)

Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera c)) che "Nel decreto legislativo NIS: [...]

c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Capo V
Sicurezza della rete e dei sistemi informativi dei fornitori di servizi digitali

Art. 14

Obblighi in materia di sicurezza e notifica degli incidenti

1. I fornitori di servizi digitali identificano e adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi di cui all'allegato III all'interno dell'Unione europea.

2. Tenuto conto delle conoscenze piu' aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi:

a) la sicurezza dei sistemi e degli impianti;
b) trattamento degli incidenti;
c) gestione della continuita' operativa;
d) monitoraggio, audit e test;
e) conformita' con le norme internazionali.

3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuita' di tali servizi.

4. I fornitori di servizi digitali notificano al CSIRT italiano senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.

5. Le notifiche includono le informazioni che consentono al CSIRT italiano di determinare la rilevanza di un eventuale impatto transfrontaliero. La notifica non espone la parte che la effettua a

una maggiore responsabilita' rispetto a quella derivante dall'incidente.

6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo di cui all'articolo 12, comma 6.

7. Al fine di determinare la rilevanza dell'impatto di un incidente, sono tenuti in considerazione, in particolare, i seguenti parametri:

a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio digitale per la fornitura dei propri servizi;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente;

d) la portata della perturbazione del funzionamento del servizio;

e) la portata dell'impatto sulle attivita' economiche e sociali.

8. L'obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente con riferimento ai parametri di cui al comma 7.

9. Qualora un operatore di servizi essenziali dipenda da una terza parte fornitrice di servizi digitali per la fornitura di un servizio che e' indispensabile per il mantenimento di attivita' economiche e sociali fondamentali, l'operatore stesso notifica qualsiasi impatto rilevante per la continuita' di servizi essenziali dovuto ad un incidente a carico di tale operatore.

10. Qualora l'incidente di cui al comma 4 riguardi due o piu' Stati membri, il CSIRT italiano informa gli altri Stati membri coinvolti.

11. Ai fini del comma 9, il CSIRT italiano tutela, nel rispetto del diritto dell'Unione europea e della legislazione nazionale, la sicurezza e gli interessi commerciali del fornitore del servizio digitale nonche' la riservatezza delle informazioni fornite.

12. Previa valutazione da parte dell'organo di cui all'articolo 12, comma 6, l'autorita' competente NIS, d'intesa con il CSIRT italiano, dopo aver consultato il fornitore di servizi digitali interessato e, se del caso, le autorita' competenti o i CSIRT degli altri Stati membri interessati, puo' informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestirne uno in corso, o qualora sussista comunque un interesse pubblico alla divulgazione dell'incidente. ***((4))***

13. I fornitori di servizi digitali applicano le disposizioni di attuazione degli atti di esecuzione della Commissione europea che specificano ulteriormente le misure tecnico-organizzative di cui al comma 1 e i parametri, ivi compresi formati e procedure, relativi agli obblighi di notifica di cui al comma 4.

14. Fatto salvo quanto previsto dall'articolo 1, comma 7, non sono imposti ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali.

15. Il presente capo non si applica alle microimprese e alle piccole imprese quali definite nella raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE.

AGGIORNAMENTO (4)
Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera c)) che "Nel decreto legislativo NIS: [...]
c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Art. 15

Attuazione e controllo

1. Nel caso in cui sia dimostrato il mancato rispetto degli obblighi di cui all'articolo 14 da parte dei fornitori di servizi digitali, l'autorita' competente NIS puo' adottare misure di vigilanza ex post adeguate alla natura dei servizi e delle operazioni. La dimostrazione del mancato rispetto degli obblighi puo' essere prodotta dall'autorita' competente di un altro Stato membro in cui e' fornito il servizio. ***((4))***
2. Ai fini del comma 1, i fornitori di servizi digitali sono tenuti a:
a) fornire le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;
b) porre rimedio ad ogni mancato adempimento degli obblighi di cui all'articolo 14.
3. Se un fornitore di servizi digitali ha lo stabilimento principale o un rappresentante in uno Stato membro, ma la sua rete o i suoi sistemi informativi sono ubicati in uno o piu' altri Stati membri, l'autorita' competente dello Stato membro dello stabilimento principale o del rappresentante e le autorita' competenti dei suddetti altri Stati membri cooperano e si assistono reciprocamente in funzione delle necessita'. Tale assistenza e cooperazione puo' comprendere scambi di informazioni tra le autorita' competenti interessate e richieste di adottare le misure di vigilanza di cui al comma 1.

AGGIORNAMENTO (4)
Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera c)) che "Nel decreto legislativo NIS: [...]
c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Art. 16

Giurisdizione e territorialita'

1. Ai fini del presente decreto, un fornitore di servizi digitali e' considerato soggetto alla giurisdizione dello Stato membro in cui ha lo stabilimento principale. Un fornitore di servizi digitali e' comunque considerato avere il proprio stabilimento principale in uno Stato membro quando ha la sua sede sociale in tale Stato membro.

2. Un fornitore di servizi digitali che non e' stabilito nell'Unione europea, ma offre servizi di cui all'allegato III all'interno dell'Unione europea, designa un rappresentante nell'Unione europea.

3. Il rappresentante e' stabilito in uno di quegli Stati membri in cui sono offerti i servizi. Il fornitore di servizi digitali e' considerato soggetto alla giurisdizione dello Stato membro in cui e' stabilito il suo rappresentante.

4. La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali.

Capo VI
Normazione e notifica volontaria

Art. 17

Normazione

1. Ai fini dell'attuazione armonizzata dell'articolo 12, commi 1 e 2, e dell'articolo 14, commi 1, 2 e 3, le autorita' competenti NIS promuovono l'adozione di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza della rete e dei sistemi informativi, senza imporre o creare discriminazioni a favore dell'uso di un particolare tipo di tecnologia. ***((4))***

2. Le autorita' competenti NIS tengono conto dei pareri e delle linee guida predisposti dall'ENISA, in collaborazione con gli Stati membri, riguardanti i settori tecnici da prendere in considerazione in relazione al comma 1, nonche' le norme gia' esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.***((4))***

AGGIORNAMENTO (4)

Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 15, comma 2, lettera c)) che "Nel decreto legislativo NIS: [...]

c) ogni riferimento alle autorita' competenti NIS, ovunque ricorra, deve intendersi riferito all'autorita' nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo, come modificato dalla lettera d) del presente comma".

Art. 18

Notifica volontaria

1. I soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali possono

notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuita' dei servizi da loro prestati.

2. Nel trattamento delle notifiche, il CSIRT italiano applica la procedura di cui all'articolo 12.

3. Le notifiche obbligatorie sono trattate prioritariamente rispetto alle notifiche volontarie.

4. Le notifiche volontarie sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo.

5. La notifica volontaria non puo' avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

Capo VII
Disposizioni finali

Art. 19

Poteri ispettivi

1. L'attivita' di ispezione e verifica necessarie per le misure previste dagli articoli 12, 13, 14 e 15, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica, sono svolte ***((dall'autorita' nazionale competente NIS))***.

2. ***((COMMA ABROGATO DAL D.L. 14 GIUGNO 2021, N. 82))***.

Art. 20

Autorita' competente e regime dell'accertamento e dell'irrogazione delle sanzioni amministrative

1. ***((L'autorita' nazionale competente NIS e' competente))*** per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative previste dal presente decreto.

2. Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 1, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

Art. 21

Sanzioni amministrative

1. Salvo che il fatto costituisca reato, l'operatore di servizi essenziali che non adotta le misure tecniche e organizzative adeguate e proporzionate per la gestione del rischio per la sicurezza della rete e dei sistemi informativi, ai sensi dell'articolo 12, comma 1, e' soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro. La sanzione e' ridotta di un terzo se lo stesso fatto e' commesso da un fornitore di servizio digitale, in violazione degli obblighi di cui all'articolo 14, comma 1.

2. Salvo che il fatto costituisca reato, l'operatore di servizi essenziali che non adotta le misure adeguate per prevenire e

minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, ai sensi dell'articolo 12, comma 2, e' soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro. La sanzione e' ridotta di un terzo se lo stesso fatto e' commesso da un fornitore di servizio digitale, in violazione degli obblighi di cui all'articolo 14, comma 3.

3. Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla continuita' dei servizi essenziali forniti, ai sensi dell'articolo 12, comma 5, e' soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

4. Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non ottempera agli obblighi, ai sensi dell'articolo 13, comma 2, e' soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.

5. Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non osserva le istruzioni, ai sensi dell'articolo 13, comma 4, e' soggetto ad una sanzione amministrativa pecuniaria da 15.000 euro a 150.000 euro.

6. Salvo che il fatto costituisca reato, il fornitore di servizio digitale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla fornitura di un servizio fornito, ai sensi dell'articolo 14, comma 4, e' soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

7. Salvo che il fatto costituisca reato, l'operatore di servizi essenziali dipendente da terze parti che fornisce servizi digitali per la fornitura di un servizio che e' indispensabile per il mantenimento di attivita' economiche e sociali fondamentali, che ometta la notifica, ai sensi dell'articolo 14, comma 9, e' soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.

8. Salvo che il fatto costituisca reato, il fornitore di servizi digitali che non osserva gli obblighi ai sensi dell'articolo 15, comma 2, e' soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.

9. Si ha reiterazione delle violazioni di cui al presente articolo nei casi regolati dall'articolo 8-bis della legge 24 novembre del 1981, n. 689. La reiterazione determina l'aumento fino al triplo della sanzione prevista.

Art. 22

Disposizioni finanziarie

1. Agli oneri derivanti dagli articoli 7 e 8, pari a 5.300.000 euro per l'anno 2018 e 3.300.000 euro annui a decorrere dall'anno 2019, si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-bis della legge 24 dicembre 2012, n. 234.

2. Le spese ICT sostenute dalle pubbliche amministrazioni ai sensi degli articoli 7, 8 e 12 del presente decreto e piu' in generale le spese ICT sostenute per l'adeguamento dei sistemi informativi al

presente decreto sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell'articolo 1, della legge 28 dicembre 2015, n. 208.

3. Dall'attuazione del presente decreto, ad esclusione degli articoli 7 e 8, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni pubbliche provvedono con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

4. Il Ministro dell'economia e delle finanze e' autorizzato ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati.

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

Dato a Roma, addi', 18 maggio 2018

MATTARELLA

Gentiloni Silveri, Presidente del Consiglio dei ministri

Calenda, Ministro dello sviluppo economico

Alfano, Ministro degli affari esteri e della cooperazione internazionale

Orlando, Ministro della giustizia

Minniti, Ministro dell'interno

Pinotti, Ministro della difesa

Lorenzin, Ministro della salute

Padoan, Ministro dell'economia e delle finanze

Visto, il Guardasigilli: Orlando

Allegato I

(di cui all'art. 8)

REQUISITI E COMPITI DEI GRUPPI DI INTERVENTO PER LA SICUREZZA INFORMATICA IN CASO DI INCIDENTE (CSIRT)

I requisiti e i compiti del CSIRT sono adeguatamente e chiaramente definiti ai sensi del presente decreto e del decreto del Presidente del Consiglio dei ministri di cui all'art. 8, comma 2. Essi includono quanto segue:

1. Requisiti per il CSIRT

a) Il CSIRT garantisce un alto livello di disponibilita' dei

propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano.

b) I locali del CSIRT e i sistemi informativi di supporto sono ubicati in siti sicuri.

c) Continuita' operativa:

i. il CSIRT e' dotato di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi;

ii. il CSIRT dispone di personale sufficiente per garantirne l'operativita' 24 ore su 24;

iii. il CSIRT opera in base a un'infrastruttura di cui e' garantita la continuita'. A tal fine e' necessario che siano disponibili sistemi ridondanti e spazi di lavoro di backup.

d) Il CSIRT ha la possibilita', se lo desidera, di partecipare a reti di cooperazione internazionale;

((d-bis) il CSIRT Italia conforma i propri servizi e la propria attivita' alle migliori pratiche internazionalmente riconosciute in materia di prevenzione, gestione e risposta rispetto a eventi di natura cibernetica)).

2. Compiti del CSIRT

a) I compiti del CSIRT comprendono almeno:

i. monitoraggio degli incidenti a livello nazionale;

ii. emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;

iii. intervento in caso di incidente;

iv. analisi dinamica dei rischi e degli incidenti, nonche' sensibilizzazione situazionale;

v. partecipazione alla rete dei CSIRT;

b) il CSIRT stabilisce relazioni di cooperazione con il settore privato;

c) per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate ***((, secondo le migliori pratiche internazionalmente riconosciute,))*** nei seguenti settori:

i. procedure di trattamento degli incidenti e dei rischi;

ii. sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Allegato II

(di cui articolo 3, comma 1, lettera g)

OPERATORI DI SERVIZI ESSENZIALI

Settore	Sottosettore	Tipo di soggetto
		Impresa elettrica quale definita all'articolo 2, comma 25-terdecies, del decreto legislativo 16 marzo 1999, 79, che