Roma, 24 Luglio 2019

CIRCOLARE N. 11/2019

Prot. 97/2019
Sez. II/1

A TUTTI GLI ISTITUTI ASSOCIATI
LORO SEDI

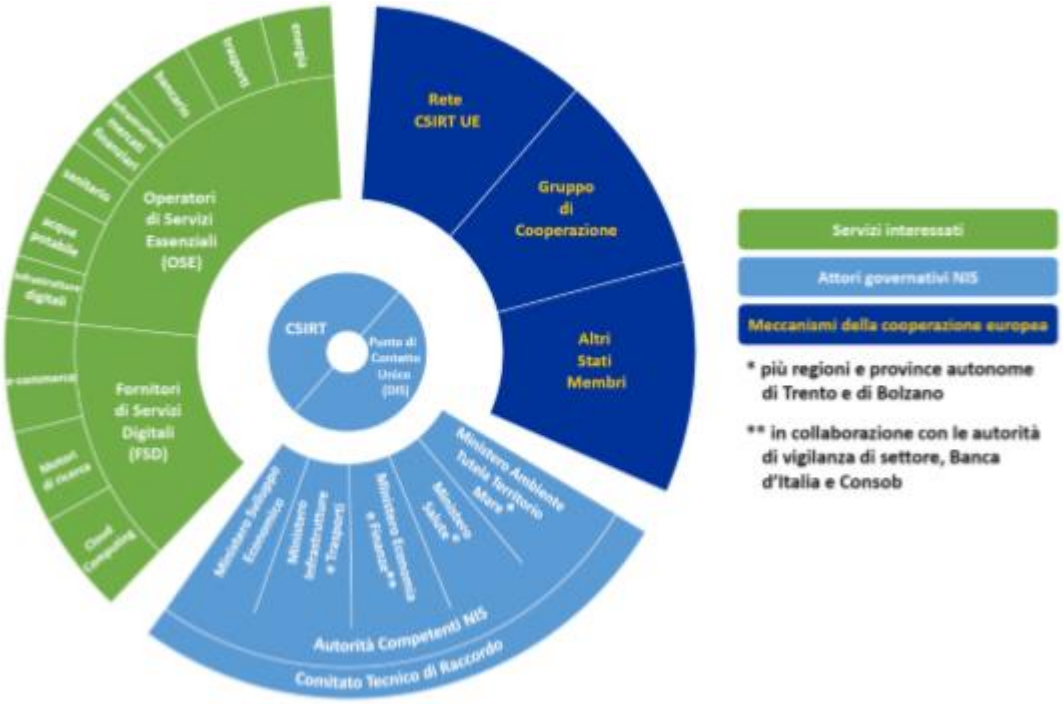
Oggetto: ***La sicurezza nazionale cibernetica alla luce della Direttiva Network and Information Security.***

Vista la crescente dipendenza della vita quotidiana e delle economie dalle tecnologie digitali, i cittadini sono sempre più esposti a gravi incidenti informatici. Per far fronte alle sfide crescenti, l'Unione Europea ha intensificato le sue attività nel settore della sicurezza informatica, promuovendo un ecosistema cibernetico sicuro e affidabile.
Nel 2016 infatti l'Unione ha adottato le sue prime misure nel settore della cibersicurezza attraverso la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio sulla sicurezza delle reti e dei sistemi informativi, la così detta Direttiva NIS (Network and Information Security). **Questa è stata recepita dall'Italia con il decreto legislativo n.65/2018 pubblicato sulla Gazzetta Ufficiale il 9 giugno ed efficace dal 24 giugno 2018 (doc. 1).**

La direttiva è volta a migliorare le difese delle infrastrutture critiche degli Stati membri, puntando sulla intelligence e prevenzione per raggiungere un adeguato livello di sicurezza cibernetica e di resilienza dei sistemi critici nazionali. L'obiettivo è quello di creare misure volte a garantire un livello comune elevato di sicurezza delle reti e delle informazioni che sia uniforme in tutta l'Unione europea. Ciò, attraverso l'adozione di misure tecniche e organizzative che consentano di ridurre i rischi e l'impatto degli incidenti informatici. In quest'ottica, la Direttiva si sviluppa su tre piani:

- promuovere la cultura della gestione del rischio e della segnalazione degli incidenti tra i principali attori economici, in particolare tra gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali, così come tra i fornitori di servizi digitali;
- migliorare le capacità nazionali in materia di sicurezza cibernetica;
- rafforzare la cooperazione in questo settore a livello nazionale e in ambito europeo.

L'applicazione della direttiva NIS riguarda principalmente le aziende che verranno identificate come Operatori di servizi essenziali (OSE) o Fornitori di servizi digitali (FSD).
Tanto gli OSE che gli FSD sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio. Hanno inoltre l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al Computer Security Incident Response Team (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.



I soggetti giuridici non identificati come OSE e che non sono FSD possono inoltrare al CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati. Ciò poiché l'intento della Direttiva NIS e del relativo decreto di recepimento è quello di favorire la più ampia diffusione di una consapevole cultura nel campo della cybersecurity e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni.
Il decreto 65/2018 resta molto fedele al testo della direttiva europea e identifica otto settori di intervento: energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile, infrastrutture digitali, servizi digitali (quali motori di ricerca, servizi cloud e piattaforme di commercio elettronico).

Si prevede, inoltre, l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team, detto CSIRT italiano, che andrà a sostituire, fondendoli, gli attuali CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale).

Gli operatori di servizi essenziali dovranno adottare misure tecnico-organizzative "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici. Il decreto specifica che nell'adottare tali misure gli operatori dovranno tenere in debita considerazione le linee guida che sono state recentemente predisposte dal Gruppo di Cooperazione. Le autorità competenti NIS potranno inoltre imporre l'adozione di misure di sicurezza specifiche, sentiti gli operatori di servizi essenziali.

Analoghi obblighi in materia di sicurezza sono previsti a carico dei **fornitori di servizi digitali**, i quali dovranno adottare misure tecniche-organizzative per la gestione dei rischi e per la riduzione dell'impatto di eventuali incidenti informatici.

Per l'adozione di tali misure i soggetti coinvolti possono utilizzare framework come quello elaborato dal NIST U.S. (l'Istituto Nazionale degli Standard e della Tecnologia), o la certificazione ISO 27001, quali soluzioni di best practice, allo scopo di valutare il loro livello di sicurezza IT e impostare obiettivi per migliorare le procedure utilizzate per proteggere i dati sensibili. I livelli del Cybersecurity framework (parziale, consapevole del rischio informatico, replicabile e adattivo), spiegano quanto deve essere profonda l'implementazione della sicurezza informatica e con riferimento alle categorie e sottocategorie, è possibile stabilire dove siano le lacune e scegliere i piani d'azione più adeguati per colmarle. La ISO 27001 adotta un approccio più ampio poichè la sua metodologia si basa sul ciclo Plan-Do-Check-Act (PDCA), ovvero costruire un sistema di gestione che non solo progetta e implementa la cyber security, ma mantiene e migliora anche l'intero sistema di gestione delle informazioni.

Tornando alla Direttiva NIS, in ossequio a quanto richiesto dall'Articolo 7, il decreto di recepimento prevede l'adozione di una strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei Ministri. La strategia dovrà prevedere in particolare le misure di preparazione, risposta e recupero dei servizi a seguito di incidenti informatici, la definizione di un piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione in materia di sicurezza informatica.

Così nel mese di luglio 2019 il nostro Paese ha visto, da un lato, la realizzazione e la diffusione delle *Linee guida per* gli OSE in ambito NIS e, dall'altro, lo *"Schema di disegno di legge in materia di perimetro di sicurezza nazionale cibernetica*". Tutti questi interventi legislativi sembrerebbero tessere di un mosaico che si colloca in maniera coerente con l'evoluzione che ormai da tempo si sta ravvisando nello scenario nazionale e internazionale in tema di cyber security e sicurezza delle informazioni.

Il Consiglio dei Ministri ha infatti approvato proprio qualche giorno fa un disegno di legge in materia di perimetro di sicurezza nazionale cibernetica per a*ssicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione o servizio essenziale dello Stato per il mantenimento di attività civili, sociali o economiche fondamentali e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.*

A questo scopo, il disegno di legge prevede:

1. la definizione delle finalità del perimetro e delle modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle rispettive reti, dei sistemi informativi e dei servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica per i quali si applicano le misure di sicurezza e le procedure introdotte;
2. l'istituzione di un meccanismo teso ad assicurare un procurement più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti;
3. l'individuazione delle competenze del Ministero dello sviluppo economico – per i soggetti privati inclusi nel perimetro – e dell'Agenzia per l'Italia Digitale (AgID) – per le amministrazioni pubbliche;
4. l'istituzione di un sistema di vigilanza e controllo sul rispetto degli obblighi introdotti;
5. lo svolgimento delle attività di ispezione e verifica da parte delle strutture specializzate in tema di protezione di reti e sistemi nonché, per quanto riguarda la prevenzione e il contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti.

Le conseguenze dell' approvazione di questa legge saranno numerose: questo infatti potrebbe rappresentare il primo vero momento di diffusione delle buone pratiche di *security by design e by default*. Alla aziende, alle PA, si chiederà un nuovo sforzo di cambio di mentalità e un forte impegno nello studio di soluzioni sostenibili e intelligenti per promuovere il progresso, la tecnologia, lo sviluppo e la sicurezza.

In tale ottica e con gli attuali scenari presenti, l'asse della sicurezza si sta spostando da un punto di vista solo fisico ad un approccio olistico della cybersecurity.

La sicurezza fisica delle infrastrutture è fondamentale ma anche la sicurezza cibernetica non deve essere sottovalutata.

Un problema della cybersecurity è che questa non ha confini spaziali e temporali. Se devo compiere un furto fisico, devo per forza farlo sul posto, viene fatto una sola volta e da una sola entità. Un furto informatico invece, può essere compiuto da qualsiasi luogo nel mondo, può essere compiuto più volte e da diversi attaccanti, che possono compiere nello stesso tempo più furti su più soggetti.

Il percorso virtuoso che dovranno seguire gli istituti di vigilanza sarà quello di far tesoro delle loro competenze di sicurezza, migrandole verso scenari più competitivi e diversamente pericolosi come la sicurezza cibernetica, non limitandosi ad una "sorveglianza esterna" ma mirando ad una sorveglianza e ad una difesa proattiva trasversale.

Cordiali saluti.

Dott.ssa Federica Calì
Privacy Specialist

Dott. Stefano Gorla
Privacy e Sicurezza dati
DPO certificato 001 FAC Certifica

All.

1. D.Lgs n. 65 del 18 Maggio 2018

DECRETO LEGISLATIVO 18 maggio 2018, n. 65

Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (18G00092)

Vigente al: 23-7-2019

Capo I
Disposizioni generali

IL PRESIDENTE DELLA REPUBBLICA

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

Vista la legge 24 dicembre 2012, n. 234, recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017;

Vista la direttiva (UE) 1148/2016 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

Visto il regolamento (CE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

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

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

Visto il Regolamento di esecuzione della Commissione n. 2018/151/UE del 30 gennaio 2018 recante modalita' di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente;

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

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

Vista la legge 3 agosto 2007, n. 124, recante sistema di

informazione per la sicurezza della Repubblica e nuova disciplina del segreto;

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

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

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

Visto il decreto legislativo 11 aprile 2011, n. 61, attuativo della direttiva 2008/114/CE, recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessita' di migliorarne la protezione;

Visto il regolamento adottato con decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5, recante disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva;

Vista la direttiva adottata con decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, pubblicato nella Gazzetta Ufficiale n. 87 del 13 aprile 2017;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il codice in materia di protezione dei dati personali;

Visto il decreto legislativo 1° agosto 2003, n. 259, recante il codice delle comunicazioni elettroniche;

Visto il decreto legislativo 23 giugno 2011, n. 118, recante disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione dell'8 febbraio 2018;

Acquisito il parere della Conferenza Unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, reso nella seduta del 19 aprile 2018;

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

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 16 maggio 2018;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro dello sviluppo economico, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, della giustizia, dell'interno, della difesa, della salute e dell'economia e delle finanze;

Emana

il seguente decreto legislativo:

Art. 1

Oggetto e ambito di applicazione

1. Il presente decreto stabilisce misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea.

2. Ai fini del comma 1, il presente decreto prevede:

a) l'inclusione nella strategia nazionale di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;

b) la designazione delle autorita' nazionali competenti e del punto di contatto unico, nonche' del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti di cui all'allegato I;

c) il rispetto di obblighi da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;

d) la partecipazione nazionale al gruppo di cooperazione europeo, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea, nonche' dell'incremento della fiducia tra di essi;

e) la partecipazione nazionale alla rete CSIRT nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace.

3. Le disposizioni in materia di misure di sicurezza e di notifica degli incidenti di cui al presente decreto non si applicano alle imprese soggette agli obblighi di cui agli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, ne' ai prestatori di servizi fiduciari soggetti agli obblighi di cui all'articolo 19 del regolamento (UE) n. 910/2014.

4. Il presente decreto si applica fatto salvo quanto previsto dal decreto legislativo 11 aprile 2011, n. 61, e dalla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI, del Consiglio.

5. Fatto salvo quanto previsto dall'articolo 346 del trattato sul funzionamento dell'Unione europea, le informazioni riservate secondo quanto disposto dalla normativa dell'Unione europea e nazionale, in particolare per quanto concerne la riservatezza degli affari, sono scambiate con la Commissione europea e con altre autorita' competenti NIS solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione del presente decreto. Le informazioni scambiate sono pertinenti e commisurate allo scopo. Lo scambio di informazioni ne tutela la riservatezza e protegge la sicurezza e gli interessi commerciali degli operatori di servizi essenziali e dei fornitori di servizi digitali.

6. Il presente decreto lascia impregiudicate le misure adottate per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, nei casi in cui la divulgazione sia ritenuta contraria agli interessi essenziali di sicurezza e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati.

7. Qualora gli obblighi previsti per gli operatori di servizi essenziali o i fornitori di servizi digitali di assicurare la sicurezza delle loro reti e dei loro sistemi informativi o di notificare gli incidenti siano oggetto di uno specifico atto giuridico dell'Unione europea, si applicano le disposizioni di detto

atto giuridico nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui al presente decreto.

Art. 2

Trattamento dei dati personali

1. Il trattamento dei dati personali in applicazione del presente decreto e' effettuato ai sensi del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni.

Art. 3

Definizioni

1. Ai fini del presente decreto si intende per:

a) autorita' competente NIS, l'autorita' competente per settore, in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;

b) CSIRT, gruppo di intervento per la sicurezza informatica in caso di incidente, di cui all'articolo 8;

c) punto di contatto unico, l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea;

d) autorita' di contrasto, l'organo centrale del Ministero dell'interno per la sicurezza e per 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;

e) rete e sistema informativo:

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

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

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

f) sicurezza della rete e dei sistemi informativi, la capacita' di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilita', l'autenticita', l'integrita' o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi;

g) operatore di servizi essenziali, soggetto pubblico o privato, della tipologia di cui all'allegato II, che soddisfa i criteri di cui all'articolo 4, comma 2;

h) servizio digitale, servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di un tipo elencato nell'allegato III;

i) fornitore di servizio digitale, qualsiasi persona giuridica che fornisce un servizio digitale;

l) incidente, ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;

m) trattamento dell'incidente, tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e

l'intervento in caso di incidente;

n) rischio, ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi;

o) rappresentante, la persona fisica o giuridica stabilita nell'Unione europea espressamente designata ad agire per conto di un fornitore di servizi digitali che non e' stabilito nell'Unione europea, a cui l'autorita' competente NIS o il CSIRT Nazionale puo' rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi del presente decreto;

p) norma, una norma ai sensi dell'articolo 2, primo paragrafo, numero 1), del regolamento (UE) n. 1025/2012;

q) specifica, una specifica tecnica ai sensi dell'articolo 2, primo paragrafo, numero 4), del regolamento (UE) n. 1025/2012;

r) punto di interscambio internet (IXP), una infrastruttura di rete che consente l'interconnessione di piu' di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, ne' altera o interferisce altrimenti con tale traffico;

s) sistema dei nomi di dominio (DNS), e' un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio;

t) fornitore di servizi DNS, un soggetto che fornisce servizi DNS su internet;

u) registro dei nomi di dominio di primo livello, un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD);

v) mercato online, un servizio digitale che consente ai consumatori ovvero ai professionisti, come definiti rispettivamente all'articolo 141, comma 1, lettere a) e b), del decreto legislativo 6 settembre 2005, n. 206, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato on line;

z) motore di ricerca on line, un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;

aa) servizio di cloud computing, un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

Art. 4

Identificazione degli operatori di servizi essenziali

1. Entro il 9 novembre 2018, con propri provvedimenti, le autorita' competenti NIS identificano per ciascun settore e sottosettore di cui all'allegato II, gli operatori di servizi essenziali con una sede nel territorio nazionale. Gli operatori che prestano attivita' di assistenza sanitaria sono individuati con decreto del Ministro della salute, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. Gli operatori che forniscono e distribuiscono acque destinate al consumo

umano sono individuati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

2. I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti:

a) un soggetto fornisce un servizio che e' essenziale per il mantenimento di attivita' sociali e/o economiche fondamentali;

b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;

c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Oltre ai criteri indicati nel comma 2, nell'individuazione degli operatori di servizi essenziali si tiene conto dei documenti prodotti al riguardo dal Gruppo di cooperazione di cui all'articolo 10.

4. Ai fini del comma 1, prima dell'adozione dei provvedimenti previsti dalla medesima disposizione, qualora un soggetto fornisca un servizio di cui al comma 2, lettera a), sul territorio nazionale e in altro o altri Stati membri dell'Unione europea, le autorita' competenti NIS consultano le autorita' competenti degli altri Stati membri.

5. E' istituito presso il Ministero dello sviluppo economico un elenco nazionale degli operatori di servizi essenziali.

6. L'elenco degli operatori di servizi essenziali identificati ai sensi del comma 1 e' riesaminato con le medesime modalita' di cui al comma 1 e, se del caso, aggiornato su base regolare, ed almeno ogni due anni dopo il 9 maggio 2018, a cura delle autorita' competenti NIS ed e' comunicato al Ministero dello sviluppo economico.

7. Entro il 9 novembre 2018, e in seguito ogni due anni, il punto di contatto unico trasmette alla Commissione europea le informazioni necessarie per la valutazione dell'attuazione del presente decreto, in particolare della coerenza dell'approccio in merito all'identificazione degli operatori di servizi essenziali.

8. Le informazioni di cui al comma 7 comprendono almeno:

a) le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali;

b) l'elenco dei servizi di cui al comma 2;

c) il numero degli operatori di servizi essenziali identificati per ciascun settore di cui all'allegato II ed un'indicazione della loro importanza in relazione a tale settore;

d) le soglie, ove esistano, per determinare il pertinente livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio di cui all'articolo 5, comma 1, lettera a), o all'importanza di tale particolare operatore di servizi essenziali di cui all'articolo 5, comma 1, lettera f).

Art. 5

Effetti negativi rilevanti

1. Ai fini della determinazione della rilevanza degli effetti negativi di cui all'articolo 4, comma 2, lettera c), le autorita' competenti NIS considerano i seguenti fattori intersettoriali:

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;

b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;

c) l'impatto che gli incidenti potrebbero avere, in termini di entita' e di durata, sulle attivita' economiche e sociali o sulla

pubblica sicurezza;

d) la quota di mercato di detto soggetto;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilita' di strumenti alternativi per la fornitura di tale servizio.

2. Al fine della determinazione degli effetti negativi rilevanti di un incidente sono altresi' considerati, ove opportuno, fattori settoriali.

Capo II

Contesto strategico e istituzionale

Art. 6

Strategia nazionale di sicurezza cibernetica

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

2. Nell'ambito della strategia nazionale di sicurezza cibernetica, 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 sicurezza cibernetica.

4. La Presidenza del Consiglio dei ministri trasmette la strategia nazionale in materia di sicurezza cibernetica 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' nazionali competenti e punto di contatto unico

1. Sono designate quali Autorita' competenti NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III:

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

b) il Ministero delle infrastrutture e dei trasporti 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 delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

e) il Ministero dell'ambiente e della tutela del territorio e del mare 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. Le Autorita' competenti NIS sono responsabili dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigilano sull'applicazione del presente decreto a livello nazionale esercitando altresi' le relative potesta' ispettive e sanzionatorie.

3. Il Dipartimento delle informazioni per la sicurezza (DIS) e' designato 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 delle autorita' competenti 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. Le autorita' competenti NIS e il punto di contatto unico consultano, conformemente alla normativa vigente, l'autorita' di contrasto ed il Garante per la protezione dei dati personali e collaborano con essi.

7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella delle autorita' competenti 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 a decorrere dal 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 la Presidenza del Consiglio dei ministri, 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. 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. Per lo svolgimento delle funzioni del CSIRT italiano, la Presidenza del Consiglio dei ministri si avvale di un contingente massimo di trenta unita' di personale, di cui quindici scelti tra dipendenti di altre amministrazioni pubbliche, in posizione di comando o fuori ruolo, per i quali si applica l'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, e quindici da assumere, nel limite della dotazione organica vigente, in aggiunta alle ordinarie facolta' assunzionali della Presidenza del Consiglio dei ministri, nel limite di spesa annuo di 1.300.000 di euro a decorrere dal 2018. Ai relativi oneri si provvede ai sensi dell'articolo 22.

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.

10. Per le spese di funzionamento del CSIRT italiano e' autorizzata la spesa di 2.700.000 euro per l'anno 2018, di cui 2.000.000 per le spese di investimenti, e di 700.000 annui a decorrere dall'anno 2019. A tali oneri si provvede ai sensi dell'articolo 22.

Art. 9

Cooperazione a livello nazionale

1. Le autorita' competenti NIS, il punto di contatto unico e il CSIRT italiano collaborano per l'adempimento degli obblighi di cui al presente decreto. A tal fine e' istituito, presso la Presidenza del Consiglio dei ministri, un Comitato tecnico di raccordo, composto da rappresentanti delle amministrazioni statali competenti ai sensi dell'articolo 7, comma 1, 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, da adottare su proposta dei Ministri per la semplificazione e la pubblica amministrazione e dello sviluppo economico, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi 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 e il punto di contatto unico in merito alle notifiche di incidenti trasmesse ai sensi del presente decreto.

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.

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

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.

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.

5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorita' competente NIS, 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 sicurezza della Repubblica (CISR), delle attivita' di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento.

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.

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.

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.

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.

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.

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

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.

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. 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.

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.

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 e, per conoscenza, all'autorita' competente NIS, 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.

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.

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.

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.

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.

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.

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 dalle autorita' competenti NIS.

2. Con successivo Accordo tra Governo, Regioni e Province autonome di Trento e di Bolzano sono definiti i criteri uniformi in ambito nazionale per lo svolgimento delle attivita' di ispezione e verifica, necessarie per le misure previste dagli articoli 12, 13, 14 e 15, che riguardano le reti e i sistemi informativi utilizzati dagli operatori che prestano attivita' di assistenza sanitaria, nonche' in merito al settore fornitura e distribuzione di acqua potabile.

Art. 20

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

1. Le autorita' competenti NIS di cui all'articolo 7, comma 1, lettere a), b), c), d) ed e), per i rispettivi settori e sottosettori di riferimento di cui all'allegato II e per i servizi di cui all'allegato III, sono competenti 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.

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 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 esercita attivita' di «fornitura» quale all'articolo 2, comma

1. Energia	a) Energia elettrica	25-sexies, di tale decreto legislativo
		Gestori del sistema di distribuzione quali definiti all'articolo 2, comma 25-ter, del decreto legislativo 16 marzo 1999, 79
		Gestori del sistema di trasmissione quali definiti all'articolo 2, comma 25-bis, del decreto legislativo 16 marzo 1999, 79
	b) Petrolio	Gestori di oleodotti
		Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		Imprese fornitrici quali definite all'articolo 2, comma 1, lettera kk-septies), del decreto legislativo 23 maggio 2000, n. 164
	c) Gas	Gestori del sistema di distribuzione quali definiti all'articolo 2, comma 1, lettera kk-sexies), del decreto legislativo 23 maggio 2000, n. 164
		Gestori del sistema di trasmissione quali definiti all'articolo 2, comma 1, lettera kk-quater), del decreto legislativo 23 maggio 2000, n. 164
		Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, comma 1, lettera kk-nonies), del decreto legislativo 23 maggio 2000, n. 164
		Gestori del sistema GNL quali definiti all'articolo 2, comma 1, lettera kk-decies), del decreto legislativo 23 maggio 2000,

		n. 164
		Imprese di gas naturale quale quali definite all'articolo 2, comma 1, lettera t), del decreto legislativo 23 maggio 2000, n. 164
		Gestori di impianti di raffinazione e trattamento di gas naturale
2. Trasporti	a) Trasporto aereo	Vettori aerei quali definiti all'articolo 3, primo paragrafo, numero 4), del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio
		Gestori aeroportuali quali definiti all'articolo 72, comma 1, lettera b), del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27, aeroporti quali definiti a all'articolo 72, comma 1, lettera a), di tale decreto-legge, compresi gli aeroporti centrali di cui all'allegato II, punto 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, e soggetti che gestiscono impianti annessi situati in aeroporti
		Operatori attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo quale definito all'articolo 2, primo paragrafo, numero 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio
	b) Trasporto ferroviario	Gestori dell'infrastruttura quali definiti all'articolo 3, comma 1, lettera b), del decreto legislativo 15 luglio 2015, n. 112
		Imprese ferroviarie quali

		definite all'articolo 3, comma 1, lettera a), del decreto legislativo 15 luglio 2015, n. 112, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, comma 1, lettera n), del decreto legislativo 15 luglio 2015, n. 112,
		compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite nell'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, escluse le singole navi gestite da tale compagnia
	c) Trasporto per vie d'acqua	organi di gestione dei porti quali definiti all'articolo 2, comma 1, lettera a), del decreto legislativo 6 novembre 2007, n. 203, compresi i relativi impianti portuali quali definiti all'articolo 2, primo paragrafo, numero 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 quali definiti all'articolo 2, comma 1, lettera p), del decreto legislativo 19 agosto 2005, n. 196
		Autorita' stradali quali definite all'articolo 2, punto 12, del regolamento delegato (UE) 2015/962 della Commissione responsabili del controllo della gestione del traffico
	d) Trasporto su strada	Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 1, comma 1, lettera a), del

		decreto del Ministro delle infrastrutture e dei trasporti 1 febbraio 2013
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, paragrafo 1, numero 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio
4. Infrastrutture dei mercati finanziari		Gestori delle sedi di negoziazione quali definite all'articolo 1, comma 5-octies, lettera c), del decreto legislativo 24 febbraio 1998, n. 58
		Controparte centrale quale definita all'articolo 2, primo paragrafo, numero 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio
5. Settore sanitario	Istituti sanitari (compresi ospedali e cliniche private)	Prestatori di assistenza sanitaria quali definiti all'articolo 3, comma 1, lettera h), del decreto legislativo 4 marzo 2014, n. 38
6. Fornitura e distribuzione di acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definite all'articolo 2, comma 1, lettera a), del decreto legislativo 2 febbraio 2001, n. 31, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano e' solo una parte della loro attivita' generale di distribuzione di altri prodotti e beni che non sono considerati servizi essenziali
7. Infrastrutture digitali		IXP DNS TLD

Allegato III

(di cui all'art. 3, comma 1, lettera h)

TIPI DI SERVIZI DIGITALI

1. Mercato online
2. Motore di ricerca online
3. Servizi di cloud computing