DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 17 febbraio 2017

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. (17A02655)

(GU n.87 del 13-4-2017)

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 3 agosto 2007, n. 124, recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», come modificata e integrata dalla legge 7 agosto 2012, n. 133, e, in particolare, l'art. 1, comma 3-bis, che dispone che il Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), adotti apposite direttive per rafforzare le attivita' di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali;

Visti altresi', l'art. 5, della legge n. 124 del 2007, che disciplina le funzioni del CISR cui sono attribuiti compiti di consulenza, proposta e deliberazione sugli indirizzi e sulle finalita' generali della politica dell'informazione per la sicurezza, nonche' di elaborazione degli indirizzi generali e degli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza;

Visto il decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, ed in particolare l'art. 7-bis, comma 5, che attribuisce al CISR, convocato dal Presidente del Consiglio dei ministri in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, compiti di consulenza, proposta e deliberazione, secondo modalita' stabilite con regolamento adottato ai sensi dell'art. 43, della legge n. 124 del 2007;

Visto l'art. 4, comma 3, lettera d-bis), della legge n. 124 del 2007, ai sensi del quale il Dipartimento delle informazioni per la sicurezza coordina le attivita' di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

Vista la 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 (c.d. Direttiva NIS);

Vista la legge 1° aprile 1981, n. 121, recante «Nuovo ordinamento dell'Amministrazione della Pubblica sicurezza», ed in particolare l'art. 1;

Visti 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 che, all'art. 7-bis, dispone che, ferme restando le competenze dei Servizi di informazione per la sicurezza, i competenti organi del Ministero dell'interno assicurano i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale ed il decreto del Ministro dell'interno 9 gennaio 2008, con il quale sono state individuate le predette infrastrutture ed e' stata prevista l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC);

Visti l'art. 14 del decreto legislativo 30 luglio 1999, n. 300, recante «Riforma dell'organizzazione del Governo, a norma dell'art. 11 della legge 15 marzo 1997, n. 59», che attribuisce, tra l'altro, al Ministero dell'interno competenze in materia di difesa civile ed

il decreto del Ministro dell'interno 28 settembre 2001 che istituisce la Commissione interministeriale tecnica di difesa civile;

Visto il decreto legislativo 15 marzo 2010, n. 66, recante «Codice dell'ordinamento militare» e, in particolare, l'art. 89 che individua le attribuzioni delle Forze armate e le disposizioni e direttive conseguenti che disciplinano i compiti attinenti alla difesa cibernetica;

Visto il decreto legislativo 1° agosto 2003, n. 259, recante «Codice delle comunicazioni elettroniche» e, in particolare, le disposizioni che affidano al Ministero dello sviluppo economico competenze in materia di sicurezza ed integrita' delle reti pubbliche di comunicazione e dei servizi di comunicazione elettronica accessibili al pubblico;

Visto il decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, e successive modificazioni, 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;

Vista la legge 24 febbraio 1992, n. 225, recante «Istituzione del Servizio nazionale della protezione civile»;

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 l'art. 5, comma 2, lettera h), della legge 23 agosto 1988, n. 400;

Visto il decreto legislativo 30 luglio 1999, n. 303, recante «Ordinamento della Presidenza del Consiglio dei ministri a norma dell'art. 11 della legge 15 marzo 1997, n. 59»;

Visto il regolamento recante «Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva», adottato con decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5, ai sensi dell'art. 4, comma 3, lettera l), della legge n. 124 del 2007;

Visto il regolamento recante «Ordinamento ed organizzazione del Dipartimento delle informazioni per la sicurezza», adottato con decreto del Presidente del Consiglio dei ministri 26 ottobre 2012, n. 2, ed in particolare l'art. 4, comma 5, ai sensi del quale presso il Dipartimento delle informazioni per la sicurezza e' istituito un organismo collegiale permanente, c.d. CISR Tecnico, per l'espletamento, a supporto del Comitato interministeriale per la sicurezza della Repubblica, di attivita' di istruttoria, di approfondimento e di valutazione anche con riferimento a specifiche situazioni di crisi;

Vista la direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, adottata con decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, che ha definito, in un contesto unitario, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali;

Considerato l'attuale quadro legislativo, improntato alla distribuzione di funzioni e compiti aventi rilievo per la sicurezza cibernetica tra molteplici soggetti istituzionali competenti nelle diverse fasi: della prevenzione degli eventi dannosi nello spazio cibernetico; dell'elaborazione di linee guida e standard tecnici di sicurezza; della difesa dello Stato da attacchi nello spazio cibernetico; della prevenzione e repressione dei crimini informatici; della preparazione e della risposta nei confronti di eventi cibernetici;

Considerato che sul richiamato quadro legislativo e' intervenuto l'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge n. 198 del 2015, che ha attribuito al CISR funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale;

Ravvisata pertanto la necessita' di aggiornare, anche nelle more del recepimento, entro il 9 maggio 2018, della citata direttiva (UE) 2016/1148, la predetta architettura istituzionale alla luce delle previsioni recate dall'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge n. 198 del 2015, cosi' da ricondurre a sistema e unitarieta' le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento;

Ritenuto in tale quadro di procedere, altresi', ad una razionalizzazione e semplificazione della predetta architettura istituzionale, prevedendo che le funzioni di coordinamento e raccordo delle attivita' di prevenzione, preparazione e gestione di eventuali situazioni di crisi di natura cibernetica siano attestate presso strutture che assicurino un piu' diretto ed efficace collegamento con il Comitato interministeriale per la sicurezza della Repubblica;

Ritenuto per quanto sopra di dover procedere all'adozione di un nuovo provvedimento che sostituisca il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013;

Sentito il Comitato interministeriale per la sicurezza della Repubblica;

Dispone:

Art. 1

Oggetto

1. Il presente decreto definisce, in un contesto unitario e integrato, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione delle vulnerabilita', della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalita' dei sistemi in caso di crisi.

2. I soggetti compresi nell'architettura istituzionale di cui al comma 1 operano nel rispetto delle competenze gia' attribuite dalla legge a ciascuno di essi.

3. Il modello organizzativo-funzionale delineato con il presente decreto persegue la piena integrazione con le attivita' di competenza del Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, nonche' con quelle espletate dalle strutture del Ministero della difesa dedicate alla protezione delle proprie reti e sistemi nonche' alla condotta di operazioni militari nello spazio cibernetico, dalle strutture del Ministero dell'interno, dedicate alla prevenzione e al contrasto del crimine informatico e alla difesa civile, e quelle della protezione civile.

Art. 2

Definizioni

1. Ai fini del presente decreto si intende per:

a) Presidente: il Presidente del Consiglio dei ministri;

b) CISR: il Comitato interministeriale per la sicurezza della Repubblica di cui all'art. 5, della legge 3 agosto 2007, n. 124;

c) «CISR tecnico»: l'Organismo di supporto al CISR di cui all'art. 5;

d) DIS: il Dipartimento delle informazioni per la sicurezza di cui all'art. 4, della legge n. 124 del 2007;

e) Agenzie: l'Agenzia informazioni e sicurezza esterna e l'Agenzia informazioni e sicurezza interna di cui agli articoli 6 e 7, della legge n. 124 del 2007;

f) organismi di informazione per la sicurezza: il DIS, l'AISE e l'AISI di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007;

g) Consigliere militare: il Consigliere militare del Presidente

del Consiglio dei ministri di cui all'art. 11, del decreto del Presidente del Consiglio dei ministri 1° ottobre 2012;

h) spazio cibernetico: l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonche' delle relazioni logiche, comunque stabilite, tra di essi;

i) sicurezza cibernetica: condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

l) minaccia cibernetica: complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia in particolare, nelle azioni di singoli individui od organizzazioni, statali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a controllare indebitamente, danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

m) evento cibernetico: avvenimento significativo, di natura volontaria o accidentale, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

n) allarme: comunicazione di avviso di evento cibernetico da valutarsi ai fini dell'attivazione di misure di risposta pianificate;

o) situazione di crisi cibernetica: situazione in cui l'evento cibernetico assume dimensioni, intensita' o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale;

p) operatori di servizi essenziali: gli operatori di cui all'allegato II 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 (c.d. direttiva NIS);

q) fornitori di servizi digitali: i fornitori di cui all'allegato III della direttiva NIS.

Art. 3

Presidente del Consiglio dei ministri

1. Il Presidente, quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica, ai fini della tutela della sicurezza nazionale anche nello spazio cibernetico:

a) assume le determinazioni ai sensi dell'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito con modificazioni dalla legge 11 dicembre 2015, n. 198, provvedendo, nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale, a convocare il CISR secondo le modalita' stabilite con il regolamento ivi previsto;

b) adotta, curandone l'aggiornamento, su proposta del CISR, il quadro strategico nazionale per la sicurezza dello spazio cibernetico, contenente l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilita' dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, e di quelli nazionali operanti al di fuori del territorio del Paese, l'individuazione degli strumenti e delle procedure con cui perseguire l'accrescimento della capacita' del Paese di prevenzione e risposta rispetto ad eventi nello spazio cibernetico, anche in un'ottica di diffusione della cultura della sicurezza;

c) adotta, su deliberazione del CISR, il Piano nazionale per la

protezione cibernetica e la sicurezza informatica nazionali contenente gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale;

d) emana le direttive ed ogni atto d'indirizzo necessari per l'attuazione del Piano di cui alla lettera c);

e) impartisce, sentito il CISR, le direttive al DIS e alle Agenzie ai sensi dell'art. 1, comma 3-bis, della legge n. 124 del 2007.

Art. 4

Comitato interministeriale per la sicurezza della Repubblica

1. Nella materia della sicurezza dello spazio cibernetico, il CISR:

a) partecipa, in caso di crisi cibernetica, alle determinazioni del Presidente, con funzioni di consulenza e di proposta, nonche' di deliberazione nei casi indicati all'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito con modificazioni dalla legge n. 198 del 2015;

b) propone al Presidente l'adozione del quadro strategico nazionale di cui all'art. 3, comma 1, lettera b);

c) delibera il Piano nazionale per la sicurezza dello spazio cibernetico di cui all'art. 3, comma 1, lettera c), ai fini dell'adozione da parte del Presidente;

d) esprime parere, ai sensi dell'art. 5, comma 2, lettera h), della legge n. 400 del 1988, sulle direttive del Presidente di cui all'art. 3, comma 1, lettera d);

e) e' sentito, ai sensi dell'art. 1, comma 3-bis, della legge n. 124 del 2007, ai fini dell'adozione delle direttive del Presidente agli organismi di informazione per la sicurezza;

f) esercita l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;

g) approva linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonche' per la condivisione delle informazioni e per l'adozione di best pratices e di misure rivolte all'obiettivo della sicurezza cibernetica;

h) elabora, ai sensi dell'art. 5, della legge n. 124 del 2007, gli indirizzi generali e gli obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali da perseguire nel quadro della politica dell'informazione per la sicurezza da parte degli organismi di informazione per la sicurezza, ciascuno per i profili di rispettiva competenza;

i) promuove l'adozione delle iniziative necessarie per assicurare, in forma coordinata, la piena partecipazione dell'Italia ai diversi consessi di cooperazione internazionale, sia in ambito bilaterale e multilaterale, ivi compresa la NATO, e dell'UE, al fine della definizione e adozione di politiche e strategie comuni di prevenzione e risposta;

l) formula le proposte di intervento normativo ed organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi.

2. Si applicano le disposizioni dell'art. 5, commi 4 e 5, della legge n. 124 del 2007.

Art. 5

Organismo di supporto al CISR - «CISR tecnico»

1. Alle attivita' di supporto per lo svolgimento da parte del CISR delle funzioni di cui all'art. 4 del presente decreto, provvede l'organismo collegiale di coordinamento, presieduto dal Direttore generale del DIS, nella composizione di cui all'art. 4, comma 5, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 26 ottobre 2012, n. 2, recante l'organizzazione ed il funzionamento del Dipartimento delle informazioni per la sicurezza.

2. L'organismo collegiale di coordinamento di cui al comma 1:

a) svolge attivita' preparatoria delle riunioni del CISR dedicate

alla materia della sicurezza cibernetica;

b) assicura l'istruttoria per l'adozione degli atti e per l'espletamento delle attivita', da parte del CISR, di cui all'art. 4, comma 1, del presente decreto;

c) espleta le attivita' necessarie a verificare l'attuazione degli interventi previsti dal Piano nazionale per la sicurezza dello spazio cibernetico e l'efficacia delle procedure di coordinamento tra i diversi soggetti, pubblici e privati, chiamati ad attuarli;

d) coordina, in attuazione degli indirizzi approvati dal CISR e sulla base degli elementi forniti dalle amministrazioni ed enti competenti, dagli organismi di informazione per la sicurezza, dal Nucleo per la sicurezza cibernetica di cui all'art. 8 e dagli operatori privati, la formulazione delle indicazioni necessarie allo svolgimento delle attivita' di individuazione delle minacce alla sicurezza dello spazio cibernetico, al riconoscimento delle vulnerabilita', nonche' per l'adozione di best practices e misure di sicurezza;

3. Per le finalita' di cui al comma 2, l'organismo collegiale di coordinamento compie approfondimenti ed acquisisce ogni utile contributo e valutazione ritenuti necessari.

Art. 6

Linee di azione per la sicurezza cibernetica

1. Il direttore generale del DIS, per le finalita' di tutela della sicurezza nazionale di cui al presente decreto, adotta le iniziative idonee a definire le necessarie linee di azione di interesse generale con l'obiettivo di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilita' dei piu' adeguati ed avanzati supporti tecnologici in funzione della preparazione alle azioni di prevenzione, contrasto e risposta in caso di crisi cibernetica da parte delle amministrazioni ed enti pubblici e degli operatori privati di cui all'art. 11.

2. Per la realizzazione delle linee di azione indicate al comma 1, il direttore generale del DIS predispone gli opportuni moduli organizzativi, di coordinamento e di raccordo, prevedendo il ricorso anche a professionalita' delle pubbliche amministrazioni, degli enti di ricerca pubblici e privati, delle universita' e di operatori economici privati.

3. Il direttore generale del DIS, per le finalita' di cui al presente articolo, puo' fare ricorso a convenzioni e intese con le pubbliche amministrazioni e soggetti privati, ai sensi dell'art. 13 della legge n. 124 del 2007 ed all'affidamento di incarichi ad esperti esterni ai sensi dell'art. 21 della predetta legge.

Art. 7

Organismi di informazione per la sicurezza

1. Il DIS e le Agenzie svolgono la propria attivita' nel campo della sicurezza cibernetica avvalendosi degli strumenti e secondo le modalita' e le procedure stabilite dalla legge n. 124 del 2007.

2. Per le finalita' di cui al comma 1, il direttore generale del DIS, sulla base delle direttive adottate dal Presidente ai sensi dell'art. 1, comma 3-bis, della legge n. 124 del 2007 e alla luce degli indirizzi generali e degli obiettivi fondamentali individuati dal CISR, cura, ai sensi dell'art. 4, comma 3, lettera d-bis), della citata legge, il coordinamento delle attivita' di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

3. Il DIS, attraverso i propri uffici, assicura il supporto al direttore generale per l'espletamento delle attivita' di coordinamento di cui al comma 2. Il DIS provvede, altresi', sulla base delle informazioni acquisite ai sensi dell'art. 4, comma 3, lettera c), della legge n. 124 del 2007, alla luce delle acquisizioni provenienti dallo scambio informativo di cui all'art. 4, comma 3, lettera e), della citata legge, e dei dati acquisiti ai sensi dell'art. 13, commi 1 e 2, della medesima legge, alla formulazione di

analisi, valutazioni e previsioni sulla minaccia cibernetica. Provvede, in base a quanto disposto dal presente decreto, alla trasmissione di informazioni rilevanti ai fini della sicurezza cibernetica alle pubbliche amministrazioni e agli altri soggetti, anche privati, interessati all'acquisizione di informazioni, ai sensi dell'art. 4, comma 3, lettera f), della citata legge, nonche' alla condivisione delle stesse informazioni nell'ambito del Nucleo per la sicurezza cibernetica di cui all'art. 8.

4. Le Agenzie, ciascuna nell'ambito delle rispettive attribuzioni, svolgono, secondo gli indirizzi definiti dalle direttive del Presidente e le linee di coordinamento delle attivita' di ricerca informativa stabilite dal direttore generale del DIS ai sensi del comma 2, le attivita' di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali.

5. Per lo svolgimento delle attivita' previste dal presente articolo, il DIS e le Agenzie, secondo le forme di coordinamento definite ai sensi dell'art. 4, comma 3, lettera d-bis), della legge n. 124 del 2007, corrispondono con le pubbliche amministrazioni, i soggetti erogatori di servizi di pubblica utilita', le universita' e con gli enti di ricerca, stipulando a tal fine apposite convenzioni ai sensi dell'art. 13, comma 1, della medesima legge. Possono accedere, per le medesime finalita', agli archivi informatici dei soggetti di cui all'art. 13, comma 2, della legge n. 124 del 2007, secondo le modalita' e con le procedure indicate dal regolamento ivi previsto.

6. Il DIS, ai sensi dell'art. 4, comma 3, lettera m), della legge n. 124 del 2007, pone in essere ogni iniziativa volta a promuovere e diffondere la conoscenza e la consapevolezza in merito ai rischi derivanti dalla minaccia cibernetica e sulle misure necessarie a prevenirli.

Art. 8

Nucleo per la sicurezza cibernetica

1. Presso il Dipartimento delle informazioni per la sicurezza e' costituito, in via permanente, il Nucleo per la sicurezza cibernetica, a supporto del Presidente e del CISR, nella materia della sicurezza dello spazio cibernetico, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo e' presieduto da un vice direttore generale del DIS, designato dal direttore generale, ed e' composto dal Consigliere militare e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo e' integrato da un rappresentante dell'ufficio centrale per la segretezza di cui all'art. 9, della legge n. 124 del 2007.

3. I componenti possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione e, in particolare, per le esigenze di raccordo di cui all'art. 9, comma 2, lettera a).

4. In relazione agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di universita' o di enti e istituti di ricerca, nonche' di operatori privati interessati alla materia della sicurezza cibernetica.

5. Il Nucleo per la sicurezza cibernetica si riunisce almeno una volta al mese, su iniziativa del presidente-vice direttore generale del DIS o su richiesta di almeno un componente del Nucleo.

6. Sulle attivita' svolte, il Nucleo riferisce al direttore generale del DIS, per la successiva informazione al Presidente e al CISR.

Art. 9

Compiti del Nucleo per la sicurezza cibernetica

1. Per le finalita' di cui all'art. 8, comma 1, il Nucleo per la sicurezza cibernetica svolge funzioni di raccordo tra le diverse componenti dell'architettura istituzionale che intervengono a vario titolo nella materia della sicurezza cibernetica, nel rispetto delle competenze attribuite dalla legge a ciascuna di esse.

2. In particolare, nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi cibernetica, il Nucleo:

a) promuove, sulla base delle direttive di cui all'art. 3, comma 1, lettera d), la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, anche nel quadro di quanto previsto ai sensi dell'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015;

b) mantiene attiva, 24 ore su 24, 7 giorni su 7, l'unita' per l'allertamento e la risposta a situazioni di crisi cibernetica;

c) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della sicurezza cibernetica, e tenuto conto di quanto previsto dall'art. 7 riguardo all'attivita' degli organismi di informazione per la sicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

d) acquisisce le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrita' significativi ai fini del corretto funzionamento delle reti e dei servizi dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal CNAIPIC nell'esercizio dei servizi di protezione informatica delle infrastrutture critiche ai sensi dell'art. 7-bis del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, dalle strutture del Ministero della difesa e dai CERT di cui all'art. 10, comma 3;

e) promuove e coordina, in raccordo con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica;

f) costituisce punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE, altre organizzazioni internazionali ed altri Stati, ferme restando le specifiche competenze del Ministero dello sviluppo economico, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa e di altre amministrazioni previste dalla normativa vigente, assicurando comunque in materia ogni necessario raccordo.

3. Ai fini dell'attivazione delle azioni di risposta e ripristino rispetto a situazioni di crisi cibernetica, il Nucleo:

a) riceve, anche dall'estero, le segnalazioni di evento cibernetico e dirama gli allarmi alle amministrazioni e agli operatori privati, ai fini dell'attuazione di quanto previsto nelle pianificazioni di cui al comma 2, lettera a);

b) valuta se l'evento assume dimensioni, intensita' o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richiede l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso, allo svolgimento delle attivita' di raccordo e coordinamento di cui all'art. 10, nella composizione ivi prevista;

c) informa tempestivamente il Presidente, per il tramite del direttore generale del DIS, sulla situazione in atto, ai fini delle determinazioni di cui all'art. 7-bis, comma 5, del richiamato decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015.

4. Il Nucleo per la sicurezza cibernetica elabora appositi rapporti

sullo stato di attuazione delle misure di coordinamento ai fini della preparazione e gestione della crisi previste dal presente decreto e li trasmette, per le finalita' di cui all'art. 5, comma 2, lettera c), all'organismo collegiale di cui all'art. 5.

Art. 10

Gestione delle crisi di natura cibernetica

1. Per la gestione delle crisi di natura cibernetica, il Nucleo si riunisce nella composizione individuata ai sensi del comma 2, nei casi di cui all'art. 9, comma 3, lettera b), ovvero a seguito delle determinazioni di cui all'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015.

2. Ai sensi del comma 1, la composizione del Nucleo e' integrata, in ragione delle necessita', con un rappresentante del Ministero della salute, del Ministero delle infrastrutture e dei trasporti, del Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile (CITDC), dell'ufficio del Consigliere militare del Presidente del Consiglio dei ministri autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, degli operatori privati di cui all'art. 11 e di altri soggetti eventualmente interessati. Il Nucleo puo' essere convocato anche in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati.

3. E' compito del Nucleo, nella composizione per la gestione delle crisi, di cui al comma 2, assicurare che le attivita' di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica, vengano espletate in maniera coordinata secondo quanto previsto dall'art. 9, comma 2, lettera a), avvalendosi, per gli aspetti tecnici di risposta sul piano informatico e telematico, del Computer Emergency Response Team (CERT) nazionale, istituito presso il Ministero dello sviluppo economico, del CERT-PA, istituito presso l'Agenzia per l'Italia digitale, e degli altri CERT istituiti ai sensi della normativa vigente. Nei casi di cui all'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015, il Nucleo opera nel quadro delle procedure individuate ai sensi delle disposizioni ivi previste.

4. Il Nucleo, per l'espletamento delle proprie funzioni e fermo restando quanto previsto ai sensi dell'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015:

a) mantiene costantemente informato il Presidente, per il tramite del direttore generale del DIS, sulla crisi in atto, predisponendo punti aggiornati di situazione;

b) assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente per il superamento della crisi;

c) raccoglie tutti i dati relativi alla crisi;

d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati;

e) assicura i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO, dell'UE o di organizzazioni internazionali di cui l'Italia fa parte.

Art. 11

Operatori privati

1. Gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di

servizi digitali, di cui rispettivamente all'art. 2, comma 1, lettere p) e q), quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento e' condizionato dall'operativita' di sistemi informatici e telematici, ivi comprese quelle individuate ai sensi dell'art. 1, comma 1, lettera d), del decreto del Ministro dell'interno 9 gennaio 2008, secondo quanto previsto dalla normativa vigente, ovvero previa apposita convenzione:

a) comunicano al Nucleo per la sicurezza cibernetica, anche per il tramite dei soggetti istituzionalmente competenti a ricevere le relative comunicazioni ai sensi dell'art. 16-bis, comma 2, lettera b), del decreto legislativo n. 259 del 2003, ogni significativa violazione della sicurezza o dell'integrita' dei propri sistemi informatici, utilizzando canali di trasmissione protetti;

b) adottano le best practices e le misure finalizzate all'obiettivo della sicurezza cibernetica, definite ai sensi dell'art. 16-bis, comma 1, lettera a), del decreto legislativo n. 259 del 2003, e dell'art. 5, comma 2, lettera d), del presente decreto;

c) forniscono informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso ai Security Operations Center aziendali e ad altri eventuali archivi informatici di specifico interesse ai fini della sicurezza cibernetica, di rispettiva pertinenza, nei casi previsti dalla legge n. 124 del 2007, nel quadro delle vigenti procedure d'accesso coordinato definite dal DIS;

d) collaborano alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalita' dei sistemi e delle reti da essi gestiti.

2. Il Ministro dello sviluppo economico, fermo restando quanto previsto dal regolamento di cui all'art. 4, comma 3, lettera l), della legge n. 124 del 2007, promuove l'istituzione di un centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilita' di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, di cui al comma 1, nonche' di ogni altro operatore per cui sussista un interesse nazionale.

3. Ferme restando le conseguenze derivanti dalla violazione di altri specifici obblighi di legge, la mancata comunicazione degli eventi di cui al comma 1, lettera a), e' altresi' valutata ai fini dell'affidabilita' richiesta per il possesso delle abilitazioni di sicurezza di cui al regolamento adottato ai sensi dell'art. 4, comma 3, lettera l), della legge n. 124 del 2007.

Art. 12

Tutela delle informazioni

1. Per lo scambio delle informazioni classificate e a diffusione esclusiva si osservano le disposizioni di cui al regolamento adottato ai sensi dell'art. 4, comma 3, lettera l), della legge n. 124 del 2007.

2. Il DIS, attraverso l'ufficio centrale per la segretezza, assolve, altresi', ai compiti previsti dal regolamento di cui al comma 1, relativi alla tutela dei Communication and Information System (CIS) delle pubbliche amministrazioni e degli operatori privati di cui all'art. 11 del presente decreto, che trattano informazioni classificate e a diffusione esclusiva.

Art. 13

Disposizioni transitorie e finali

1. Dal presente decreto non derivano nuovi oneri a carico del bilancio dello Stato.

2. Al fine di assicurare il funzionamento, senza soluzione di continuita', dell'unita' di allertamento e risposta a crisi cibernetiche, di cui all'art. 9, comma 2, lettera b), durante il passaggio di competenze del Nucleo per la sicurezza cibernetica al DIS, previsto dal presente decreto, le strutture deputate alla gestione di tali attivita' sulla base del decreto del Presidente del

Consiglio dei ministri 24 gennaio 2013 mantengono la loro operativita' ed erogano i relativi servizi a favore del Nucleo, istituito presso il DIS, dalla data di entrata in vigore del presente decreto e fino a cessate esigenze, comunicate a cura del direttore generale del DIS.

3. Il presente decreto e' pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

4. A decorrere dalla data di pubblicazione del presente decreto e' abrogato il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013.

Roma, 17 febbraio 2017

Il Presidente
Gentiloni Silveri

Registrato alla Corte dei conti il 29 marzo 2017
Ufficio controllo atti P.C.M. Ministeri giustizia e affari esteri, reg.ne prev. n. 691