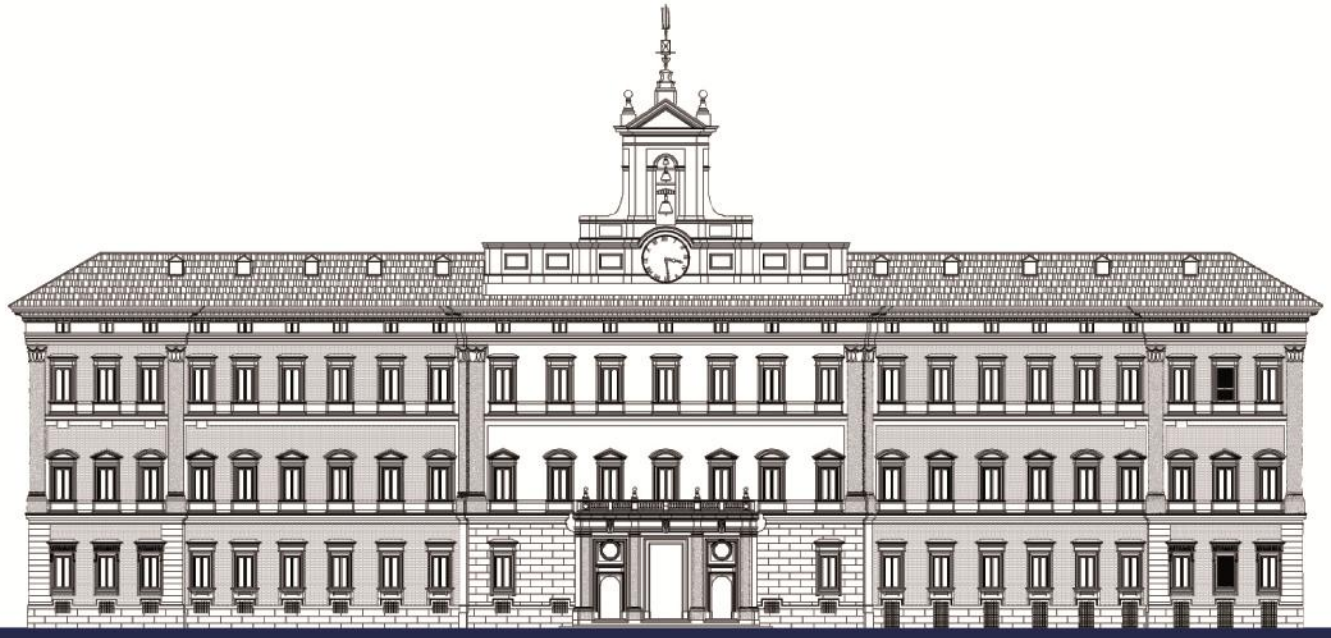
Camera dei deputati

XVII LEGISLATURA

Documentazione e ricerche



Direttiva recante indirizzi per la protezione cibernetica

Testo a fronte tra il DPCM 24 gennaio 2013 e il DPCM 17 febbraio 2017

n. 305

13 giugno 2017

Camera dei deputati

XVII LEGISLATURA

Documentazione e ricerche

Direttiva recante indirizzi per la protezione cibernetica

Testo a fronte tra il DPCM 24 gennaio 2013 e il DPCM 17 febbraio 2017

n. 305

13 giugno 2017

Servizio responsabile:

SERVIZIO STUDI

Dipartimento Difesa

☎ 066760-4939 – ✉ *st_difesa@camera.it*

***File**: DI0587.docx*

I N D I C E

PREMESSA

La nuova direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali D.P.C.M 17 febbraio 2017, pubblicata nella gazzetta ufficiale del 13 aprile del 2017, apporta diverse modifiche alla precedente direttiva D.P.C.M. 24 gennaio 2013, anche al fine di recepire alcune delle prescrizioni contenute nella Direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione e di richiamare l'articolo7-*bis* del decreto legge 174/2015, che ha attribuito al Comitato interministeriale per la sicurezza della Repubblica compiti di consulenza, proposta e deliberazione sugli indirizzi generali della politica di informazione per la sicurezza in caso di situazione di crisi.

TESTO A FRONTE

D.P.C.M. 24 GENNAIO 2013	D.P.C.M. 17 FEBBRAIO 2017
Art. 1 Oggetto	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 della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.	*identico*
2. I soggetti compresi nell'architettura istituzionale di cui al comma 1 operano nel rispetto delle competenze già attribuite dalla legge a ciascuno di essi.	*identico*
3. Il modello organizzativo-funzionale delineato con il presente decreto persegue la piena integrazione con le attività di competenza del Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, nonché con quelle espletate dalle strutture del Ministero della difesa dedicate alla protezione delle proprie reti e sistemi nonché 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	*identico*

difesa civile, e quelle della protezione civile.	
Art. 2 Definizioni	Art. 2 Definizioni
1. Ai fini del presente decreto si intende per:	*1. identico*
a) Presidente: il Presidente del Consiglio dei Ministri	*a) identica*
b) CISR: il Comitato interministeriale per la sicurezza della Repubblica di cui all'art. 5 della legge n. 124/2007;	b) CISR: il Comitato interministeriale per la sicurezza della Repubblica di cui all'art. 5, della legge **3 agosto** 2007, n. 124[1]
	c) CISR tecnico: l'organismo di supporto al CISR di cui all'articolo 5;
c) DIS: il Dipartimento delle informazioni per la sicurezza di cui all'art. 4 della legge n. 124/2007;	*d) Identica alla lettera c) colonna di sinistra*
d) Agenzie: l'Agenzia informazioni e sicurezza esterna e l'Agenzia informazioni e sicurezza interna di cui agli articoli 6 e 7, della legge ~~3 agosto~~ 2007, n. 124;	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;
e) organismi di informazione per la sicurezza: il DIS, l'AISE e l'AISI di cui	*f) identica*

[1] Ai sensi di tale disposizione presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la sicurezza della Repubblica (CISR) con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. Il Comitato elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza, delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze e dal Ministro dello sviluppo economico. Il direttore generale del DIS svolge le funzioni di segretario del Comitato. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, i direttori dell'AISE e dell'AISI, nonché altre autorità civili e militari di cui di volta in volta sia ritenuta necessaria la presenza in relazione alle questioni da trattare.

agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;	
~~f) NISP: Nucleo interministeriale situazione e pianificazione di cui al D.P.C.M. 5 maggio 2010;~~	*Soppressa*
g) Consigliere militare: il Consigliere militare del Presidente del Consiglio dei Ministri di cui all'articolo 11 del D.P.C.M. 1° ottobre 2012;	*Identica*
h) spazio cibernetico: l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi;	*h) identica*
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 od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;	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 od 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 o organizzazioni, statuali e non, pubbliche o private, finalizzate	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 o organizzazioni, statuali e non, pubbliche o private, finalizzate

all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;	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 od accidentale, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;	m) evento cibernetico: avvenimento significativo, di natura volontaria od 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;	*n) Identica*
o) situazione di crisi: situazione in cui l'evento cibernetico assume dimensioni, intensità 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.	o) situazione di crisi **cibernetica**: situazione in cui l'evento cibernetico assume dimensioni, intensità 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	Art. 3 Presidente del Consiglio dei Ministri
1. Il Presidente:	**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[2], 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 modalità stabilite con il regolamento ivi previsto
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 vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei	*b) identica*

[2] Ai sensi di tale disposizione il Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124, e successive modificazioni, può essere convocato dal Presidente del Consiglio dei ministri, con funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, secondo modalità stabilite con apposito regolamento ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124.

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 capacità del Paese di prevenzione e risposta rispetto ad eventi nello spazio cibernetico, anche in un'ottica di diffusione della cultura della sicurezza;	
b) 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;	*c) identica*
c) emana le direttive ed ogni atto d'indirizzo necessari per l'attuazione del Piano di cui alla lettera b);	d) emana le direttive ed ogni atto d'indirizzo necessari per l'attuazione del Piano di cui alla lettera **c);**
d) impartisce, sentito il CISR, le direttive al DIS e alle Agenzie ai sensi dell'art. 1, comma 3-bis, della legge n. 124/2007.	*e) Identica*
Art. 4 Comitato interministeriale per la sicurezza della Repubblica	Art. 4 Comitato interministeriale per la sicurezza della Repubblica
1. Nella materia della sicurezza dello spazio cibernetico, il CISR, ~~nella composizione prevista dall'art. 5, comma 3, della legge n. 124/2007~~:	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, nonché' 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;[3]
a) propone al Presidente l'adozione del quadro strategico nazionale di cui all'art. 3, comma 1, lett. a);	b) propone al Presidente l'adozione del quadro strategico nazionale di cui all'art. 3, comma 1, lettera **b)**;
b) delibera il Piano nazionale per la sicurezza dello spazio cibernetico di cui all'art. 3, comma 1, lett. ~~b),~~ ai fini dell'adozione da parte del Presidente;	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;
c) esprime parere, ai sensi dell'art. 5, comma 2, lett. h), della legge n. 400/1988, sulle direttive del Presidente di cui all'art. 3, comma 1, lett. ~~c)~~**;**	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);**
d) È sentito, ai sensi dell'art. 1, comma 3-bis, della legge 3 agosto 2007, n. 124, ai fini dell'adozione delle direttive del Presidente agli organismi di informazione per la sicurezza;	*e) Identica*
e) esercita l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;	*f) identica*
f)-approva linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di best pratices e di misure rivolte all'obiettivo della sicurezza cibernetica;	*g) identica*
g) elabora, ai sensi dell'art. 5 della legge 3 agosto 2007, n. 124, gli indirizzi generali e gli obiettivi fondamentali in materia di protezione	*h) identica*

[3] La lettera in esame presenta un contenuto analogo alla lettera l) del D.P.C.M. 24 gennaio 2013.

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;	
~~h~~) **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, ~~sia dell~~'UE e ~~della~~ NATO, al fine della definizione e adozione di politiche e strategie comuni di prevenzione e risposta;	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;
i) 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;	*l) identica*
~~l) partecipa, con funzioni di consulenza e di proposta, alle determinazioni del Presidente in caso di crisi.~~	Cfr. lettera a)
~~2. Alle riunioni del CISR aventi ad oggetto la materia della sicurezza cibernetica partecipa, senza diritto di voto, il Consigliere militare.~~.	
3. Si applicano, ~~anche ai fini di cui al comma 2~~, le disposizioni dell'art. 5, commi 4 e 5, della legge ~~3 agosto~~ 2007, n. 124.	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	Art. 5 Organismo di supporto al CISR - «**CISR tecnico**»
1.Alle attività di supporto per lo svolgimento da parte del CISR delle funzioni di cui all'articolo 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 ~~D.P.C.M~~. 26 ottobre 2012, n. 2, recante l'organizzazione ed il funzionamento del Dipartimento delle informazione per la sicurezza.	1. Alle attività 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. Alle riunioni dell'organismo collegiale di coordinamento riguardanti la materia della sicurezza cibernetica partecipa il Consigliere militare.~~	*soppresso*
3. L'organismo collegiale di coordinamento di cui al comma 1:	*2. identica*
a) svolge attività preparatoria delle riunioni del CISR dedicate alla materia della sicurezza cibernetica;	*a) Identica*
b) assicura l'istruttoria per l'adozione degli atti e per l'espletamento delle attività, da parte del CISR, di cui all'articolo 4, comma 1, del presente decreto;	*b) Identica*
c) espleta le attività 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;	*c) Identica*

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, ~~nonché avvalendosi del comitato scientifico di cui all'art. 6~~, la formulazione delle indicazioni necessarie allo svolgimento delle attività di individuazione delle minacce alla sicurezza dello spazio cibernetico, al riconoscimento delle vulnerabilità, nonché per l'adozione di best practices e misure di sicurezza;	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 attività di individuazione delle minacce alla sicurezza dello spazio cibernetico, al riconoscimento delle vulnerabilità, nonché per l'adozione di best practices e misure di sicurezza
4. Per le finalità di cui al comma ~~3~~, l'organismo collegiale di coordinamento compie approfondimenti ed acquisisce ogni utile contributo e valutazione ritenuti necessari.	3. Per le finalità di cui al comma **2**, l'organismo collegiale di coordinamento compie approfondimenti ed acquisisce ogni utile contributo e valutazione ritenuti necessari.
~~Art. 6 Comitato scientifico~~	*Soppresso*
~~1. Presso la Scuola di formazione di cui all'art. 11 della legge n. 124/2007 è istituito un comitato scientifico composto da esperti nel campo delle discipline d'interesse ai fini della sicurezza cibernetica provenienti dalle università, dagli enti di ricerca, dalle pubbliche amministrazioni e dal settore privato, con il compito di predisporre ipotesi di intervento rivolte a migliorare gli standard ed i livelli di sicurezza dei sistemi e delle reti, nel quadro delle azioni finalizzate ad incrementare le condizioni di sicurezza dello spazio cibernetico d'interesse del Paese, al fine di assicurare ogni necessario~~	

~~contributo per lo svolgimento delle attività spettanti rispettivamente all'organismo collegiale di coordinamento di cui all'articolo 5 ed al Nucleo per la sicurezza cibernetica di cui all'articolo 8, nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi.~~ ~~2. Il comitato formula altresì proposte e progetti di promozione e diffusione della cultura della sicurezza nel settore cibernetico.~~	
	Art. 6 **Linee di azione per la sicurezza cibernetica**
	1. Il direttore generale del DIS, per le finalità 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 disponibilità dei più 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 professionalità delle**

	pubbliche amministrazioni, degli enti di ricerca pubblici e privati, delle università e di operatori economici privati. **3. Il direttore generale del DIS, per le finalità di cui al presente articolo, può 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	Art. 7 Organismi di informazione per la sicurezza
1. Il DIS e le Agenzie svolgono la propria attività nel campo della sicurezza cibernetica avvalendosi degli strumenti e secondo le modalità e le procedure stabilite dalla legge n. 124/2007.	*identico*
2. Per le finalità 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. 124/2007 e alla luce degli indirizzi generali e degli obiettivi fondamentali individuati dal CISR, cura, ai sensi dell'art. 4, comma 3, lett. d-bis), della citata legge, il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.	*identico*
3. Il DIS, attraverso i propri uffici, assicura il supporto al Direttore generale per l'espletamento delle attività di coordinamento di cui al	3. Il DIS, attraverso i propri uffici, assicura il supporto al direttore generale per l'espletamento delle attività di coordinamento di cui al

comma 2. Il DIS provvede, altresì, sulla base delle informazioni acquisite ai sensi dell'art. 4, comma 3, lett. c), alla luce delle acquisizioni provenienti dallo scambio informativo di cui all'art. 4, comma 3, lett. e), della legge n. ~~124/2007~~, e dei dati acquisiti ai sensi dell'art. 13, commi 1 e 2, della ~~citata~~ 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 ~~al Nucleo per la sicurezza cibernetica di cui all'art. 8~~, alle pubbliche amministrazioni e agli altri soggetti, anche privati, interessati all'acquisizione di informazioni, ai sensi dell'art. 4, comma 3, lett. f) della legge ~~n. 124/2007~~.	comma 2. Il DIS provvede, altresì, 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, **nonché 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 attività di ricerca informativa stabilite dal Direttore generale del DIS ai sensi del comma 2, le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali.	*identico*
5. Per lo svolgimento delle attività previste dal presente articolo, il DIS e le Agenzie corrispondono con le pubbliche amministrazioni, i soggetti erogatori di servizi di pubblica utilità, le università e con gli enti di ricerca,	5. Per lo svolgimento delle attività 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**,

stipulando a tal fine apposite convenzioni ai sensi dell'art. 13, comma 1, della legge ~~n. 124/2007~~. ~~Per le stesse finalità, le pubbliche amministrazioni ed i soggetti erogatori di servizi di pubblica utilità consentono l'accesso del DIS e delle Agenzie ai propri archivi informatici secondo le modalità e con le procedure previste dal D.P.C.M. n. 4/2009, adottato ai sensi dell'art. 13, comma 2, della predetta legge.~~	corrispondono con le pubbliche amministrazioni, i soggetti erogatori di servizi di pubblica utilità, le università 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 finalità, agli archivi informatici dei soggetti di cui all'art. 13, comma 2, della legge n. 124 del 2007, secondo le modalità e con le procedure indicate dal regolamento ivi previsto.**
6. Il DIS, ai sensi dell'art. 4, comma 3, lett. m), della legge n. 124/2007, 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~~, anche sulla base delle indicazioni del comitato scientifico di cui all'art. 6.~~	6. Il DIS, ai sensi dell'art. 4, comma 3, lett. m), della legge n. 124/2007, 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	Art. 8 Nucleo per la sicurezza cibernetica
1. Presso ~~l'Ufficio del Consigliere militare~~ è costituito, in via permanente, il Nucleo per la sicurezza cibernetica, a supporto del Presidente, 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.	1. Presso **il Dipartimento delle informazioni per la sicurezza** è 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 è presieduto ~~dal Consigliere militare~~ ed è composto da un rappresentante rispettivamente del	2. Il Nucleo è presieduto **da un vice direttore generale del DIS, designato dal direttore generale, ed è**

DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, 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 è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124/2007.	**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 è 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 ed, in particolare, per le esigenze di raccordo di cui all'art. 9, comma 2, lett. a).	*identico*
4. In relazione agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della sicurezza cibernetica.	*identico*
5. Il Nucleo per la sicurezza cibernetica si riunisce almeno una volta al mese, su iniziativa ~~del Consigliere militare~~ o su richiesta di almeno un componente del Nucleo.	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 attività 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	Art. 9 Compiti del Nucleo per la sicurezza
1. Per le finalità di cui all'art. 8, comma 1, ~~del presente decreto~~, 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.	1. Per le finalità 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, il Nucleo ~~per la sicurezza cibernetica~~:	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'articolo 3, comma 1, lett. ~~c)~~, 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;	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 attivo, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica;	*b) Identica*
c) valuta e promuove, in raccordo con le amministrazioni competenti per	*c) Identica*

specifici profili della sicurezza cibernetica, e tenuto conto di quanto previsto dall'art. 7 riguardo all'attività 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, ~~per il tramite del Ministero dello sviluppo economico, degli organismi di informazione per la sicurezza, delle Forze di polizia e delle strutture del Ministero della difesa~~, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi;	d) acquisisce le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità 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;	*e) Identica*
f) costituisce punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE, altre organizzazioni	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, del Ministero dell'interno, del Ministero della difesa e di altre amministrazioni previste dalla normativa vigente, assicurando comunque in materia ogni necessario raccordo.	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:	3. *Identico*
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, lett. a);	*a) Identica*
b) valuta se l'evento assume dimensioni, intensità o natura tali da ~~incidere sulla sicurezza nazionale o non può essere~~ fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richiede l'assunzione di decisioni coordinate in sede interministeriale, provvedendo, ~~ove necessario, a dichiarare la situazione di crisi cibernetica e ad attivare il NISP, quale Tavolo interministeriale di crisi cibernetica, informando tempestivamente il Presidente sulla situazione in atto.~~	b) valuta se l'evento assume dimensioni, intensità 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 attività 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 ~~report~~ 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 finalità di cui all'articolo 5, comma ~~3~~, lett. c), all'organismo collegiale di cui all'articolo 5	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 finalità di cui all'art. 5, comma **2,** lettera c), all'organismo collegiale di cui all'art. 5.[4]
Art. 10 ~~NISP - Tavolo interministeriale di crisi cibernetica~~	Art. 10. **Gestione delle crisi di natura cibernetica**
1. ~~Il NISP, quale Tavolo interministeriale di crisi cibernetica, è attivato dal Nucleo per la sicurezza cibernetica ai sensi dell'articolo 9, comma 3, lett. b).~~	**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. Il Tavolo, presieduto dal Consigliere militare, opera con la presenza di un rappresentante per ciascuna delle amministrazioni indicate dall'art. 5, comma 3, del D.P.C.M. 5 maggio 2010 e di un rappresentante rispettivamente del Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, autorizzati ad assumere decisioni che~~	**2. Ai sensi del comma 1, la composizione del Nucleo è integrata, in ragione delle necessità, 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**

[4] CISR tecnico

~~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 soggetti ed enti di cui all'art. 5, comma 6, del D.P.C.M. 5 maggio 2010, nonché degli operatori privati di cui all'art. 11 del presente decreto, e di altri eventualmente interessati.~~	**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 può essere convocato anche in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati.**
3. È compito ~~del Tavolo interministeriale di crisi cibernetica~~ assicurare che le attività 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 ~~dalle pianificazioni di cui all~~'art. 9, comma 2, lett. 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.	3. E' compito **del Nucleo, nella composizione per la gestione delle crisi, di cui al comma 2**, assicurare che le attività 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 Tavolo altresì~~: .	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 sulla crisi in atto, predisponendo punti aggiornati di situazione;	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;	b) *identica*
c) raccoglie tutti i dati relativi alla crisi;	c) *Identico*
d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati;	d) *Identica;*
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	e) *Identica*
Art. 11 Operatori privati	Art. 11 Operatori privati
1. Gli operatori privati che forniscono	1. Gli operatori privati che forniscono

reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, ivi comprese quelle individuate ai sensi dell'art. 1, comma 1, lett. d), del decreto del Ministro dell'interno 9 gennaio 2008, secondo quanto previsto dalla normativa vigente, ovvero previa apposita convenzione:	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 è condizionato dall'operatività 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, lett. b), del decreto legislativo n. 259/2003, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti;	a) *Identica*
b) adottano le best practices e le misure finalizzate all'obiettivo della sicurezza cibernetica, definite ai sensi dell'art. 16-bis, comma 1, lett. a), del decreto legislativo n. 259/2003, e dell'art. 5, comma ~~3~~, lett. d), del presente decreto;	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 ~~alle banche dati d~~'interesse ai fini della sicurezza cibernetica di	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**

rispettiva pertinenza, nei casi previsti dalla legge n. 124/2007;	**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 funzionalità dei sistemi e delle reti da essi gestiti.	d)*Identica*
	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 vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, di cui al comma 1, nonché 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), è altresì valutata ai fini dell'affidabilità 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	Art. 12 Tutela delle informazioni
1. Per lo scambio delle informazioni classificate si osservano le disposizioni di cui al ~~D.P.C.M. 22 luglio 2011, n. 4, recante disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate.~~	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, altresì, ai compiti ~~di cui al D.P.C.M. 22 luglio 2011, n. 4,~~ relativi alla tutela dei ~~sistemi EAD~~ delle pubbliche amministrazioni e degli operatori privati di cui all'art. 11 del presente decreto, che trattano informazioni classificate.	2. Il DIS, attraverso l'ufficio centrale per la segretezza, assolve, altresì, 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 finali	Art. 13. Disposizioni **transitorie e** finali
1. Dal presente decreto non derivano nuovi oneri a carico del bilancio dello Stato.	1. *Identico*
	2. Al fine di assicurare il funzionamento, senza soluzione di continuità, dell'unità 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 attività sulla base del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013 mantengono la loro operatività 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.
~~2.~~. Il presente decreto è pubblicato nella Gazzetta Ufficiale della Repubblica italiana.	3. *Identico*.
	4. A decorrere dalla data di pubblicazione del presente decreto è abrogato il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013.