Il Presidente del Consiglio dei Ministri

VISTA la legge 23 agosto 1988, n. 400, recante: «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri»;

VISTO il decreto legislativo 30 luglio 1999, n. 300, recante: «Riforma dell'organizzazione del Governo a norma dell'articolo 11 della legge 15 marzo 1997, n. 59»;

VISTO il decreto legislativo 30 marzo 2001, n. 165, recante: «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche»;

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 legislativo 18 maggio 2018, n. 65, recante: «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»;

VISTO il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante: «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»;

VISTO il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale» e, in particolare, l'articolo 2, che attribuisce, in via esclusiva, al Presidente del Consiglio dei ministri, l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, nonché il potere di impartire le direttive per la cybersicurezza, ai fini dell'esercizio di tale competenza;

VISTO il decreto del Presidente del Consiglio dei ministri 17 maggio 2022 con cui è stata adottata la «Strategia nazionale di cybersicurezza» e il relativo «Piano di implementazione»;

SENTITO il Comitato interministeriale per la cybersicurezza;

ADOTTA

la presente direttiva

Premessa

L'intensificazione e la crescente sofisticazione delle minacce informatiche nell'attuale contesto geo-politico, caratterizzato in particolare dalla grave crisi internazionale in atto in Ucraina, richiedono con sempre maggiore urgenza il raggiungimento di un alto livello di cybersicurezza, l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale. Ciò non solo al fine di conseguire una più elevata capacità di protezione e risposta di fronte a emergenze

cibernetiche, ma anche di disporre di un quadro analitico della minaccia funzionale all'esercizio dell'indirizzo politico.

In tale contesto, è affidato dall'ordinamento all'Agenzia per la cybersicurezza nazionale il compito di sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, peculiarmente attribuito alla componente operativa dell'Agenzia (CSIRT Italia), al cui personale, peraltro, viene espressamente riconosciuta, nello svolgimento delle relative funzioni, la qualifica di pubblico ufficiale.

Nell'esercizio di tale compito, e per un immediato ed efficace risultato ai fini del contenimento del rischio e della mitigazione del danno, l'Agenzia può fare ricorso, in attuazione dell'articolo 5, comma 5, del decreto istitutivo (decreto-legge n. 82 del 2021), alla collaborazione di altri organi dello Stato e altre amministrazioni. Ciò nel presupposto che la resilienza cibernetica del Paese non può prescindere da uno sforzo collettivo e sinergico.

Ambito di applicazione, finalità e linee di indirizzo

La presente direttiva si rivolge alle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e fornisce indirizzi di coordinamento e organizzazione volti a promuovere la gestione adeguata e coordinata delle minacce informatiche, degli incidenti e delle situazioni di crisi di natura cibernetica, in coerenza con le finalità espresse in premessa.

Da tale ambito applicativo restano esclusi gli organi dello Stato preposti alla prevenzione, accertamento e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

Appare dunque evidente l'esigenza che l'attività di supporto dell'Agenzia, sviluppata in occasione di eventi e incidenti cibernetici, venga a dispiegarsi con la più ampia collaborazione da parte dei soggetti impattati, nel loro stesso interesse e in quello, più generale, della resilienza cibernetica del Paese, onde ridurre i rischi di possibili propagazioni di conseguenze lesive, ovvero del ripetersi di analoghi attacchi, in danno di ulteriori soggetti pubblici e privati. Rischi, questi, che potrebbero acquisire una rilevanza sistemica sino a determinare un pregiudizio per la sicurezza nazionale.

Si richiamano, pertanto, le amministrazioni destinatarie ad operare garantendo: *i)* che l'Agenzia per la cybersicurezza nazionale nello svolgimento delle sue attività istituzionali e, in particolare, gli operatori del CSIRT Italia anche nel caso di intervento *in situ* a seguito di incidente, dispongano del pieno supporto dei soggetti impattati, anche nel caso in cui si

avvalgano di società *in house* o comunque a controllo pubblico. Ciò anche allo scopo di acquisire una completa ed esaustiva conoscenza situazionale volta a consentire, in corrispondenza, peraltro, agli impegni collaborativi nel quadro unionale, ogni utile operazione di analisi e valutazione della minaccia, funzionali alle attività di prevenzione e gestione degli incidenti di cybersicurezza; *ii)* conseguentemente, per tutto il tempo necessario al pieno esercizio delle proprie competenze, l'accesso ai locali, ai sistemi informativi e alle reti informatiche di pertinenza delle amministrazioni impattate, compatibilmente con i limiti e i vincoli derivanti dalle prerogative dell'autorità giudiziaria.

Si confida nella sensibilità di tutte le amministrazioni, ai fini della piena osservanza delle linee di indirizzo contenute nella presente direttiva.

Roma, 06 LUG 2023

Il Presidente del Consiglio dei ministri

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
SEGRETARIATO GENERALE
UFFICIO DELEGATO PER IL RISCONTRO
DI REGOLARITÀ AMMINISTRATIVO-CONTABILE
VISTO E ANNOTATO AL N. 2563/2023
ROMA 11.07.2023
IL DIRIGENTE

PER COPIA CONFORME ALL'ORIGINALE