DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81

Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. (21G00089)

(GU n.138 del 11-6-2021)

Vigente al: 26-6-2021

Capo I
Disposizioni generali

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 23 agosto 1988, n. 400;

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 e, in particolare, l'articolo 1, comma 3;

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 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale e, in particolare, l'articolo 29;

Visto il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo e, in particolare, l'articolo 7-bis;

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, di 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 regolamento adottato con decreto del Presidente del Consiglio dei ministri 3 aprile 2020, n. 2, recante l'ordinamento e l'organizzazione del DIS;

Visto il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, ai sensi dell'articolo 1, comma 2, del decreto-legge n. 105 del 2019, in materia di perimetro di sicurezza nazionale cibernetica;

Visto il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, recante direttiva concernente indirizzi per la

protezione cibernetica e la sicurezza informatica nazionali, pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 87 del 13 aprile 2017;

Visto il decreto del Presidente del Consiglio dei ministri 8 agosto 2019, recante disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano, pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 262 dell'8 novembre 2019;

Visto il «Framework nazionale per la cybersecurity e la data protection», edizione 2019 (Framework nazionale), realizzato dal Centro di ricerca di cyber intelligence and information security (CIS) dell'Universita' Sapienza di Roma e dal Cybersecurity national lab del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorita' garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza (DIS), quale strumento di supporto per le organizzazioni pubbliche e private in materia di strategie e processi volti alla protezione dei dati personali, con specifico riferimento alla sicurezza degli stessi a fronte di possibili attacchi informatici, e alla sicurezza cyber, nonche' per il loro continuo monitoraggio;

Considerato di dover tenere conto degli standard definiti a livello internazionale e dell'Unione europea e di assumere, quale base di riferimento per l'individuazione delle misure corrispondenti agli ambiti di cui all'articolo 1, comma 3, lettera b), del decreto-legge n. 105 del 2019, il Framework nazionale, adeguandolo allo specifico contesto operativo delineato dal perimetro di sicurezza nazionale cibernetica e, pertanto, di richiamare, per ciascuna misura individuata, il codice alfanumerico identificativo della relativa sottocategoria del Framework nazionale;

Udito il parere del Consiglio di Stato espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 1° dicembre 2020;

Acquisiti i pareri delle Commissioni I e IX riunite, IV e V della Camera dei deputati e delle Commissioni 1ª, 4ª e 5ª del Senato della Repubblica;

Sulla proposta del Comitato interministeriale per la sicurezza della Repubblica;

Adotta
il seguente regolamento:

Art. 1

Definizioni

1. Ai fini del presente decreto si intende per:

a) decreto-legge, il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

b) perimetro, il perimetro di sicurezza nazionale cibernetica istituito ai sensi dell'articolo 1, comma 1, del decreto-legge;

c) soggetti inclusi nel perimetro, i soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge;

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

e) rete, sistema informativo:

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

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

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

di cui al numero 2);

f) servizio informatico, un servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi informativi, ivi incluso quello di cloud computing di cui all'articolo 3, comma 1, lettera aa), del decreto legislativo n. 65 del 2018;

g) bene ICT (information and communication technology), un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'articolo 1, comma 2, lettera b), del decreto-legge;

h) incidente, ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici;

i) impatto sul bene ICT, limitazione della operativita' del bene ICT, ovvero compromissione della disponibilita', integrita', o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali;

l) DIS, il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri, di cui all'articolo 4 della legge n. 124 del 2007;

m) CISR tecnico, l'organismo tecnico di supporto al CISR, di cui all'articolo 4, comma 5, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 3 aprile 2020, n. 2, che definisce l'ordinamento e l'organizzazione del DIS;

n) CSIRT italiano, il Computer security incident response team istituito presso il DIS ai sensi dell'articolo 8 del decreto legislativo n. 65 del 2018;

o) indicatori di compromissione (IOC), indicatori tecnici impiegati per la rilevazione di una minaccia o compromissione nota e generalmente riconducibili a indirizzi IP, elementi identificativi e moduli software afferenti agli strumenti tecnici impiegati da attori malevoli.

Capo II
Notifiche di incidente

Art. 2

Tassonomia degli incidenti

1. Nelle tabelle n. 1 e n. 2 dell'allegato A al presente regolamento sono classificati, in categorie, gli incidenti aventi impatto sui beni ICT. Nella tabella n. 1 sono indicati gli incidenti meno gravi e nella tabella n. 2 quelli piu' gravi. Tale classificazione e' funzionale alla diversa tempistica necessaria per una risposta efficace.

2. Nelle tabelle di cui al comma 1, per ciascuna tipologia di incidente, sono indicati un codice identificativo e la corrispondente categoria, accompagnata dalla descrizione di ciascuna tipologia di incidente.

Art. 3

Notifica degli incidenti aventi impatto su beni ICT

1. Dal 1° gennaio 2022, i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti avente impatto su un bene ICT di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A, procedono alla notifica al CSIRT italiano secondo le modalita' di cui al presente regolamento.

2. Dalla data di trasmissione degli elenchi dei beni ICT effettuata ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, ovvero, qualora la trasmissione sia avvenuta in una data antecedente

a quella di entrata in vigore del presente regolamento, da quest'ultima data, e sino al 31 dicembre 2021, i soggetti inclusi nel perimetro procedono, in via sperimentale, alle notifiche di cui al comma 1, secondo le modalita' di cui al comma 4.

3. I soggetti inclusi nel perimetro procedono alla notifica di cui ai commi 1 e 2 anche nei casi in cui uno degli incidenti individuati nelle tabelle di cui all'allegato A si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio di cui all'articolo 7, comma 2, del DPCM n. 131 del 2020, condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione.

4. I soggetti inclusi nel perimetro effettuano la notifica di cui ai commi 1, 2 e 3 entro sei ore, qualora si tratti di un incidente individuato nella tabella 1 dell'allegato A, ed entro un'ora, qualora si tratti di un incidente individuato nella tabella 2 del medesimo allegato. I predetti termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza, a seguito delle evidenze ottenute, anche mediante le attivita' di monitoraggio, test e controllo di cui all'articolo 1, comma 3, lettera b), numero 6, del decreto-legge, effettuate sulla base delle misure di sicurezza di cui all'allegato B, di un incidente riconducibile a una delle tipologie individuate nell'allegato A. La notifica e' effettuata tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera a), dell'allegato I, del decreto legislativo n. 65 del 2018, e secondo le modalita' definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano.

5. Qualora il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi, tra cui le specifiche vulnerabilita' sfruttate, la rilevazione di eventi comunque correlati all'incidente oggetto di notifica, ovvero gli indicatori di compromissione (IOC) rilevati, la notifica di cui al comma 1 e' integrata tempestivamente dal momento in cui il soggetto incluso nel perimetro ne e' venuto a conoscenza, salvo che l'autorita' giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

6. Dal 1° gennaio 2022, i soggetti di cui agli articoli 12 e 14 del decreto legislativo n. 65 del 2018, con la notifica di cui al presente articolo comunicano che la stessa, ai sensi dell'articolo 1, comma 8, lettera b), del decreto-legge, costituisce anche adempimento dell'obbligo di notifica di cui, rispettivamente, agli articoli 12, comma 5, indicando a tal fine l'autorita' competente NIS di cui all'articolo 7 del decreto legislativo n. 65 del 2018 alla quale la notifica deve essere inoltrata, e 14, comma 4, del decreto legislativo n. 65 del 2018. I soggetti di cui all'articolo 16-ter, comma 2, del decreto legislativo n. 259 del 2003, con la notifica di cui al presente articolo, comunicano che la stessa, ai sensi dell'articolo 1, comma 8, lettera b), del decreto-legge, costituisce anche adempimento dell'obbligo previsto ai sensi dell'articolo 16-ter del decreto legislativo n. 259 del 2003 e delle correlate disposizioni attuative. Restano fermi, per le notifiche degli incidenti non rientranti nell'ambito di applicazione del decreto-legge, gli obblighi e le procedure di notifica previsti dal decreto legislativo n. 65 del 2018 e dal decreto legislativo n. 259 del 2003.

7. Su richiesta del CSIRT italiano, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi dei commi 1, 2 e 3 provvede, tramite i canali di comunicazione di cui al comma 4 ed entro sei ore dalla richiesta, a effettuare un aggiornamento della notifica, salvo che l'autorita' giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

8. Una volta definiti e avviati i piani di attuazione delle attivita' per il ripristino dei beni ICT impattati dall'incidente

oggetto di notifica, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi dei commi 1, 2 e 3, tramite i canali di comunicazione di cui al comma 4, ne da' tempestiva comunicazione al CSIRT italiano e trasmette, altresi', su richiesta del CSIRT italiano ed entro trenta giorni dalla stessa richiesta, una relazione tecnica che illustra gli elementi significativi dell'incidente, tra cui le conseguenze dell'impatto sui beni ICT derivanti dall'incidente e le azioni intraprese per porvi rimedio, salvo che l'autorita' giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

9. I soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui alla sottocategoria 2.1.4 (ID.AM-6) dell'allegato B, ed in particolare all'incaricato e al referente tecnico di cui alla medesima sottocategoria.

10. Sino al 31 dicembre 2021, restano fermi per i soggetti inclusi nel perimetro, che effettuano, ai sensi del comma 2, le notifiche in via sperimentale, gli obblighi di notifica di cui agli articoli 12, comma 5, e 14, comma 4, del decreto legislativo n. 65 del 2018, nonche' quelli previsti ai sensi dell'articolo 16-ter del decreto legislativo n. 259 del 2003 e delle correlate disposizioni attuative.

Art. 4

Notifica volontaria degli incidenti

1. Al di fuori dei casi di cui all'articolo 3, i soggetti inclusi nel perimetro possono notificare, su base volontaria, gli incidenti, relativi ai beni ICT, non indicati nelle tabelle di cui all'allegato A, ovvero gli incidenti, indicati nelle tabelle di cui all'allegato A, relativi a reti, sistemi informativi e servizi informatici di propria pertinenza diversi dai beni ICT. La notifica e' effettuata tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera a), dell'allegato I, del decreto legislativo n. 65 del 2018, e secondo le modalita' definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano.

2. Le notifiche volontarie sono trattate dal CSIRT italiano in subordine a quelle obbligatorie e qualora tale trattamento non costituisca un onere sproporzionato o eccessivo.

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

4. I soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui alla sottocategoria 2.1.4 (ID.AM-6) dell'allegato B, ed in particolare all'incaricato e al referente tecnico di cui alla medesima sottocategoria.

Art. 5

Trasmissione delle notifiche

1. Il DIS inoltra le notifiche ricevute dal CSIRT italiano:

a) all'organo del Ministero dell'interno per la sicurezza e la regolarita' dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;

b) alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, qualora le notifiche provengano da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, fatta eccezione per quelle concernenti i beni ICT in relazione

ai quali per le attivita' di ispezione e verifica sono competenti le strutture specializzate di cui all'articolo 1, comma 6, lettera c), terzo periodo, del decreto-legge;

c) al Ministero dello sviluppo economico, qualora le notifiche provengano da un soggetto privato.

2. Le notifiche volontarie, di cui all'articolo 4, sono trasmesse solo nel caso in cui siano state trattate.

3. Il CSIRT italiano, ai sensi dell'articolo 1, comma 8, lettera b), del decreto-legge, inoltra le notifiche ricevute dai soggetti inclusi nel perimetro, che siano identificati anche quali soggetti di cui agli articoli 12 e 14 del decreto legislativo n. 65 del 2018, all'autorita' competente NIS indicata ai sensi dell'articolo 3, comma 5.

4. Le modalita' di inoltro delle notifiche previste ai commi 1 e 2 possono essere concordate mediante apposite intese con ciascuna delle amministrazioni interessate e, tenuto anche conto di quanto previsto dall'articolo 8, comma 4, con il Ministero della difesa.

Art. 6

Incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate

1. In materia di notifica degli incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, non inclusi nell'elenco dei beni ICT ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

Capo III
Misure di sicurezza

Art. 7

Misure di sicurezza

1. Le misure di sicurezza, articolate in funzioni, categorie, sottocategorie, punti e lettere, sono individuate nell'allegato B al presente regolamento. La corrispondenza tra le misure di sicurezza e gli ambiti elencati all'articolo 1, comma 3, lettera b), del decreto-legge, e' indicata nella tabella in appendice n. 1 dell'allegato B. Nella tabella in appendice n. 2 del medesimo allegato B e' indicata per ciascuna misura di sicurezza la corrispondente categoria di cui all'articolo 8, comma 1, lettera a), ovvero lettera b).

Art. 8

Modalita' e termini di adozione delle misure di sicurezza

1. I soggetti inclusi nel perimetro adottano, per ciascun bene ICT di rispettiva pertinenza, le misure di sicurezza di cui all'allegato B nei seguenti termini:

a) per le misure di sicurezza appartenenti alla categoria A di cui all'appendice n. 2 dell'allegato B, entro sei mesi dalla data di trasmissione degli elenchi dei beni ICT effettuata ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, ovvero, qualora la trasmissione sia avvenuta in una data antecedente a quella di entrata in vigore del presente regolamento, entro sei mesi da quest'ultima data;

b) per le misure di sicurezza appartenenti alla categoria B di

cui all'appendice n. 2 dell'allegato B, entro trenta mesi dalla data di trasmissione degli elenchi dei beni ICT effettuata ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, ovvero, qualora la trasmissione sia avvenuta in una data antecedente a quella di entrata in vigore del presente regolamento, entro trenta mesi da quest'ultima data.

2. I soggetti di cui al comma 1, dopo l'avvenuta adozione delle misure di sicurezza di cui all'allegato B, ne danno tempestivamente comunicazione al DIS, descrivendo le relative modalita', mediante la piattaforma digitale costituita presso il DIS ai sensi dell'articolo 9, comma 1, del regolamento adottato con DPCM n. 131 del 2020.

3. Ai fini della comunicazione di cui al comma 2, il DIS predispone un apposito modello di cui da' informazione ai soggetti di cui al comma 1.

4. Qualora un soggetto incluso nel perimetro proceda, ai sensi degli articoli 7 e 9 del regolamento adottato con il DPCM n. 131 del 2020, all'aggiornamento dell'elenco dei beni ICT, valuta contestualmente se e' necessario procedere all'adeguamento delle misure di sicurezza adottate ai sensi del presente articolo. Nel caso in cui sia necessario procedere all'adeguamento, vi provvede e ne comunica le relative modalita', con il modello di cui al comma 1, nei seguenti termini:

a) per le misure di sicurezza di cui alla categoria A dell'appendice n. 2 dell'allegato B, entro sei mesi dall'aggiornamento dell'elenco dei beni ICT;

b) per le misure di sicurezza di cui alla categoria B dell'appendice n. 2 dell'allegato B, entro trenta mesi dall'aggiornamento dell'elenco dei beni ICT.

5. In ogni altro caso in cui un soggetto incluso nel perimetro abbia proceduto ad adeguare le misure di sicurezza adottate ai sensi del presente articolo, ne comunica, entro sei mesi, le relative modalita' con il modello di cui al comma 1.

6. Il DIS rende tempestivamente disponibili le comunicazioni ricevute ai sensi dei commi 1, 2 e 3 alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico ai fini dello svolgimento delle rispettive attivita' di verifica e ispezione, fatta eccezione per quelle comunicazioni concernenti i beni ICT in relazione ai quali per le attivita' di ispezione e verifica sono competenti le strutture specializzate di cui all'articolo 1, comma 6, lettera c), terzo periodo, del decreto-legge.

Art. 9

Tutela delle informazioni

1. Le misure minime di sicurezza individuate nell'allegato C al presente regolamento, e corrispondenti agli ambiti di cui all'articolo 1, comma 3, lettera b), numeri 3 e 4, del decreto-legge, si applicano alle informazioni relative:

a) all'elencazione dei soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge;

b) agli elenchi di cui all'articolo 1, comma 2, lettera b), del decreto-legge, comprensivi della descrizione dell'architettura e della componentistica, nonche' dell'analisi del rischio;

c) agli elementi delle notifiche effettuate ai sensi dell'articolo 3, ivi compresa la relazione di cui all'articolo 3, comma 7;

d) al modello di cui all'articolo 8, comma 1, e alla documentazione predisposta in attuazione delle misure di sicurezza di cui all'allegato B.

2. Le misure di sicurezza di cui all'allegato C si applicano entro sessanta giorni dalla data di entrata in vigore del presente regolamento.

3. Resta ferma l'adozione, da parte dei soggetti inclusi nel perimetro, delle misure di sicurezza di livello piu' elevato di cui all'allegato B, entro i termini indicati dall'articolo 8.

4. In caso di attribuzione alle informazioni di cui al comma 1 di una classifica di segretezza, ai sensi dell'articolo 42 della legge n. 124 del 2007, si applicano le misure di sicurezza previste dalla normativa vigente in materia.

Art. 10

Misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate

1. In materia di misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, non inclusi nell'elenco dei beni ICT ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

Capo IV
Disposizioni finali

Art. 11

Disposizioni finali

1. All'attuazione delle disposizioni di cui al presente decreto si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

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

Roma, 14 aprile 2021

Il Presidente: Draghi

Visto, il Guardasigilli: Cartabia

Registrato alla Corte dei conti il 4 giugno 2021
Ufficio di controllo sugli atti della Presidenza del Consiglio, del Ministero della giustizia e del Ministero degli affari esteri, registrazione n. 1450

Allegato A

Parte di provvedimento in formato grafico

Allegato B

Parte di provvedimento in formato grafico

Allegato C

Parte di provvedimento in formato grafico