Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale

(Ordinanza sui ciber-rischi, OCiber)

del 27 maggio 2020 (Stato 1° aprile 2021)

Il Consiglio federale svizzero,

visto l'articolo 30 della legge federale del 21 marzo 1997[1] sulle misure per la salvaguardia della sicurezza interna;
visti gli articoli 43 capoversi 2 e 3, 47 capoverso 2 e 55 della legge del 21 marzo 1997[2] sull'organizzazione del Governo e dell'Amministrazione,

ordina:

Capitolo 1: Disposizioni generali

Art. 1 Oggetto

La presente ordinanza disciplina l'organizzazione dell'Amministrazione federale volta alla protezione contro i ciber-rischi, nonché i compiti e le competenze dei diversi servizi nel settore della cibersicurezza.

Art. 2 Campo d'applicazione

La presente ordinanza si applica:

a. alle unità amministrative dell'Amministrazione federale centrale di cui all'articolo 7 dell'ordinanza del 25 novembre 1998[3] sull'organizzazione del Governo e dell'Amministrazione;

b.[4] alle autorità, organizzazioni e persone di cui all'articolo 2 capoverso 2 dell'ordinanza del 25 novembre 2020[5] sulla trasformazione digitale e l'informatica (OTDI) che s'impegnano a rispettarla.

Art. 3 Definizioni

Nella presente ordinanza s'intende per:

RU **2020** 2107

1 RS **120**
2 RS **172.010**
3 RS **172.010.1**
4 Nuovo testo giusta l'all. n. 1 dell'O del 25 nov. 2020 sulla trasformazione digitale e l'informatica, in vigore dal 1° gen. 2021 (RU **2020** 5871).
5 RS **172.010.58**

a. *cibersicurezza:* lo stato auspicabile in cui il trattamento dei dati e in particolare lo scambio di dati tra persone e organizzazioni mediante infrastrutture di informazione e comunicazione funziona come previsto;

b. *ciberincidente:* un evento non intenzionale o provocato intenzionalmente da persone non autorizzate, che compromette la confidenzialità, l'integrità, l'accessibilità o la tracciabilità di dati o che può causare disfunzioni;

c. *ciber-rischio:* il pericolo di un ciberincidente, la cui entità corrisponde al prodotto della probabilità che si realizzi e della portata del danno;

d. *resilienza:* la capacità di un sistema, di un'organizzazione o di una società di resistere a perturbazioni di origine interna o esterna e di mantenere il regolare funzionamento o di ripristinarlo il più rapidamente e completamente possibile;

e. *sicurezza informatica:* l'aspetto della cibersicurezza che riguarda i sistemi tecnici;

f. *direttive in materia di sicurezza informatica:* i requisiti di sicurezza che riguardano l'organizzazione, i processi, le prestazioni di servizi e la tecnica;

g. *infrastrutture critiche:* i processi, i sistemi e le installazioni essenziali per il funzionamento dell'economia o il benessere della popolazione;

h.[6] *oggetti informatici da proteggere*: applicazioni, servizi, sistemi, reti, collezioni di dati, infrastrutture e prodotti informatici; più oggetti identici o connessi tra loro possono essere raggruppati in un solo oggetto informatico da proteggere.

Capitolo 2: Principi per la protezione contro i ciber-rischi

Art. 4 Obiettivi

[1] L'Amministrazione federale provvede affinché i suoi organi e i suoi sistemi presentino un'adeguata resilienza ai ciber-rischi.

[2] Essa collabora con i Cantoni, i Comuni, il settore economico, la società, il mondo scientifico e i partner internazionali, nella misura in cui serva a proteggere i suoi interessi in materia di sicurezza, e promuove lo scambio di informazioni.

Art. 5 Strategia nazionale per la protezione della Svizzera contro i ciber-rischi

Nell'ambito della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC), il Consiglio federale definisce il quadro strategico per il miglioramento della prevenzione, dell'individuazione precoce, della reazione e della resilienza.

6 Introdotta dal n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).

Art. 6 Settori

Le misure di protezione contro i ciber-rischi sono suddivise nei tre settori seguenti:

a. settore della cibersicurezza: comprende tutte le misure volte a prevenire e gestire gli incidenti e a migliorare la resilienza ai ciber-rischi, intensificando a tale scopo la collaborazione internazionale;

b. settore della ciberdifesa: comprende tutte le misure militari e del Servizio delle attività informative che servono a proteggere i sistemi critici per la difesa nazionale, a respingere i ciberattacchi, a garantire l'efficienza operativa dell'Esercito in ogni situazione e a creare le capacità e le competenze per fornire un supporto sussidiario alle autorità civili; vi rientrano anche le misure attive volte a individuare le minacce, identificare gli aggressori nonché ostacolare e bloccare gli attacchi;

c. settore del perseguimento penale della cibercriminalità: comprende tutte le misure adottate dalla polizia e dai ministeri pubblici di Confederazione e Cantoni nella lotta contro la cibercriminalità.

Capitolo 3: Organizzazione e competenze

Sezione 1: Collaborazione interdipartimentale

Art. 7 Consiglio federale

Il Consiglio federale svolge le seguenti funzioni:

a. vigilare sull'attuazione della SNPC mediante il controlling strategico e, all'occorrenza, ordinare provvedimenti;

b. definire, nell'ambito delle sue competenze, in quali settori è necessario introdurre o adeguare direttive in materia di protezione contro i ciber-rischi;

c. emanare istruzioni sulla protezione dell'Amministrazione federale contro i ciber-rischi;

d. autorizzare deroghe alle sue direttive.

Art. 8 Comitato ristretto Ciber

1 Il Comitato ristretto Ciber è composto:

a. del delegato alla cibersicurezza (art. 6*a* dell'ordinanza del 17 febbraio 2010[7] sull'organizzazione del Dipartimento federale delle finanze) quale rappresentante del Dipartimento federale delle finanze (DFF);

b. di un rappresentante del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS);

c. di un rappresentante del Dipartimento federale di giustizia e polizia (DFGP);

7 RS **172.215.1**

d. di un rappresentante dei Cantoni designato dalla conferenza dei Governi cantonali competente.

2 Il Comitato ristretto Ciber è presieduto dal delegato alla cibersicurezza.

3 Il Comitato ristretto Ciber informa i rappresentanti delle altre unità amministrative della Confederazione attive nel settore dei ciber-rischi sui punti all'ordine del giorno e può invitarli a singole sedute a scopo consultivo. Per le questioni di politica estera, il Comitato ristretto Ciber coinvolge il Dipartimento federale degli affari esteri (DFAE). Può inoltre ricorrere a esperti attivi nel settore economico e in quello delle scuole universitarie.

4 Il Comitato ristretto Ciber ha segnatamente i seguenti compiti:

a. valutare gli attuali ciber-rischi nonché il loro possibile sviluppo in base a informazioni provenienti dai settori della cibersicurezza, della ciberdifesa e del perseguimento penale della cibercriminalità;

b. valutare costantemente i dispositivi esistenti nei settori della cibersicurezza, della ciberdifesa e del perseguimento penale della cibercriminalità ed esaminare la loro adeguatezza alle minacce;

c. coadiuvare, se necessario con il coinvolgimento di altri servizi, la gestione interdipartimentale degli incidenti;

d. informare il Comitato ristretto Sicurezza della Confederazione sui ciber-incidenti e sugli sviluppi rilevanti per la politica estera e la politica di sicurezza.

5 I tre dipartimenti rappresentati nel Comitato ristretto Ciber mettono a disposizione le informazioni necessarie per la valutazione congiunta della situazione.

6 Il Servizio delle attività informative della Confederazione illustra la situazione generale delle ciberminacce all'attenzione del Comitato ristretto Ciber.

Art. 9 Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi

1 Il Consiglio federale istituisce un Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (CD SNPC).

2 Il CD SNPC si compone del delegato alla cibersicurezza, di rappresentanti dei Cantoni designati dalla conferenza dei Governi cantonali competente, di rappresentanti del settore economico e delle scuole universitarie, nonché di rappresentanti delle unità amministrative a cui spetta la responsabilità principale nell'attuazione di una misura conformemente al piano di attuazione della SNPC. Ogni dipartimento e la Cancelleria federale dispongono di almeno un rappresentante nel CD SNPC.

3 Il CD SNPC è presieduto dal delegato alla cibersicurezza.

4 Il CD SNPC ha i seguenti compiti:

a. assicurare la coerenza strategica nell'attuazione delle misure definite nella SNPC ed esaminarne costantemente l'avanzamento mediante un controlling strategico;

b. proporre misure speciali in caso di attuazione tardiva o incompleta delle misure definite nella SNPC;

c. assicurare lo sviluppo continuo della SNPC; a tal fine, in collaborazione con il Comitato ristretto Ciber, seguire l'evoluzione delle minacce e, se necessario, elaborare proposte per adeguare la SNPC;

d. presentare ogni anno al Consiglio federale e al pubblico un rapporto sull'attuazione della SNPC;

e. assicurare che i servizi coinvolti della Confederazione, dei Cantoni, del settore economico e delle scuole universitarie adottino una procedura coordinata per l'attuazione delle misure definite nella SNPC;

f. garantire che, nell'attuazione delle misure definite nella SNPC, siano considerate la politica della Confederazione in materia di gestione dei rischi, la Strategia nazionale per la protezione delle infrastrutture critiche e le strategie del Consiglio federale nel settore informatico.

Art. 10 Comitato per la sicurezza informatica

1 Il comitato per la sicurezza informatica (C-SI) si compone di un rappresentante del Centro nazionale per la cibersicurezza (NCSC[8]), degli incaricati della sicurezza informatica dei dipartimenti e della Cancelleria federale nonché dell'incaricato della sicurezza informatica dei servizi standard delle tecnologie dell'informazione e della comunicazione (TIC).

2 In casi specifici possono essere coinvolte altre persone con funzione consultiva.

3 Il C-SI è presieduto dal rappresentante del NCSC.

4 Il C-SI è l'organo consultivo del NCSC per tutte le questioni inerenti alla sicurezza informatica nell'Amministrazione federale.

Art. 11 Delegato alla cibersicurezza

1 Il delegato alla cibersicurezza ha i seguenti compiti:

a. dirigere il NCSC;

b. assicurare un coordinamento ottimale dei lavori interdipartimentali nei settori della cibersicurezza, della ciberdifesa e del perseguimento penale della cibercriminalità;

c. assicurare la visibilità delle attività della Confederazione nel settore dei ciber-rischi, contribuire alla creazione di condizioni quadro ottimali per un'economia innovativa della cibersicurezza, fungere da principale persona di riferimento della Confederazione per le questioni inerenti ai ciber-rischi e rappresentare la Confederazione nelle commissioni e nei gruppi di lavoro rilevanti; assicurare un coordinamento ottimale dei lavori dei Cantoni e della Confederazione volto a proteggere la Svizzera dai ciber-rischi;

8 National Cyber Security Centre

d. rappresentare il NCSC negli stati maggiori di crisi della Confederazione;

e. emanare direttive in materia di sicurezza informatica;

f.[9] decidere sulle deroghe alle direttive che ha emanato; se queste deroghe riguardano anche le direttive della Cancelleria federale concernenti la trasformazione digitale e la governance delle TIC, il delegato alla cibersicurezza consulta previamente quest'ultima.

2 Il delegato alla cibersicurezza informa regolarmente il DFF, all'attenzione del Consiglio federale, sullo stato della sicurezza informatica nei dipartimenti e nella Cancelleria federale.

3 Egli può partecipare all'elaborazione di direttive informatiche dell'Amministrazione federale che riguardano la cibersicurezza e a progetti informatici rilevanti dal profilo della sicurezza. Segnatamente può richiedere informazioni, pronunciarsi in merito ed esigere modifiche.

4 Egli può esigere verifiche della sicurezza informatica dopo aver sentito il Controllo federale delle finanze.

Sezione 2: Organi del settore della cibersicurezza

Art. 12 Centro nazionale per la cibersicurezza

1 Il NCSC è il centro di competenza della Confederazione in materia di ciber-rischi che coordina i lavori della Confederazione nel settore della cibersicurezza. Esso ha i seguenti compiti:

a. gestire il servizio nazionale di contatto per le questioni legate ai ciber-rischi; questo servizio riceve e analizza le segnalazioni dell'Amministrazione federale, del settore economico, dei Cantoni e della popolazione e, se necessario, formula raccomandazioni al riguardo;

b. fornire, insieme ai partner competenti dell'Amministrazione federale, supporto sussidiario ai gestori di infrastrutture critiche e promuovere tra questi lo scambio di informazioni sui ciber-rischi;

c. gestire il «Computer Emergency Response Team» (GovCERT); esso costituisce il servizio specializzato nazionale per la gestione tecnica degli incidenti, l'analisi di problematiche tecniche, la valutazione delle minacce dal profilo tecnico e il supporto tecnico del servizio nazionale di contatto;

d. gestire il servizio specializzato per la sicurezza informatica della Confederazione; questo servizio elabora direttive in materia di sicurezza informatica, offre consulenza alle unità amministrative per la rispettiva attuazione e rileva lo stato della sicurezza informatica presso i dipartimenti e la Cancelleria federale;

9 Nuovo testo giusta l'all. n. 1 dell'O del 25 nov. 2020 sulla trasformazione digitale e l'informatica, in vigore dal 1° gen. 2021 (RU **2020** 5871).

e. designare gli incaricati della sicurezza informatica della Confederazione (ISIC);

f. coordinare l'attuazione della SNPC, eseguire il controlling strategico e preparare le sedute del Comitato ristretto Ciber e del CD SNPC;

g. disporre di un pool di esperti incaricati di fornire supporto agli uffici specializzati nell'attuazione delle misure definite nella SNPC nonché nello sviluppo, nell'attuazione e nell'esame di standard e norme in materia di cibersicurezza;

h. contribuire con informazioni mirate a sensibilizzare l'Amministrazione federale e il pubblico sui ciber-rischi, informare sulla situazione attuale ed emanare istruzioni per l'adozione di misure preventive e reattive;

i. gestire un'infrastruttura di analisi e comunicazione resiliente in grado di funzionare indipendentemente dal resto dell'informatica della Confederazione;

j. informare il Comitato ristretto Ciber sui ciberincidenti rilevanti e, se questi ultimi sono d'interesse per la politica estera e la politica di sicurezza, anche il Comitato ristretto Sicurezza della Confederazione.

2 Il NCSC può trattare i dati sui ciberincidenti e sui relativi flussi di comunicazione, qualora ciò serva a proteggere direttamente o indirettamente l'Amministrazione federale dai ciber-rischi. Può comunicare i dati a gruppi statali o privati incaricati della sicurezza, sempre che:

a. il fornitore di dati abbia dato il suo consenso; e

b. non sia violato alcuno obbligo legale di mantenere il segreto.

3 La comunicazione di dati personali all'estero è ammessa soltanto se sono rispettate le pertinenti prescrizioni della legislazione federale sulla protezione dei dati.

4 I dati personali degni di particolare protezione possono essere trattati solo se esiste la necessaria base legale che autorizza il loro trattamento mediante i mezzi informatici della Confederazione.

5 Nel caso di un ciberincidente che minaccia il corretto funzionamento dell'Amministrazione federale, dopo aver consultato i servizi interessati il NCSC assume in seno all'Amministrazione federale la responsabilità principale della sua gestione. A tal fine, gli sono assegnati i compiti e le competenze seguenti:

a. obbligare, se necessario, i fornitori e i beneficiari di prestazioni interessati a fornirgli tutte le informazioni necessarie;

b. ordinare, se necessario, misure urgenti;

c. informare la direzione delle unità amministrative interessate sugli sviluppi della situazione.

6 Se, dopo un ciberincidente, le misure adottate hanno permesso di ridurre sufficientemente la minaccia per la confidenzialità o il funzionamento dell'Amministrazione federale e i necessari lavori successivi nonché il loro finanziamento sono stati definiti, il NCSC trasmette la responsabilità del seguito dei lavori ai servizi interessati.

Art. 13 Dipartimenti e Cancelleria federale

1 Alla fine dell'anno i dipartimenti e la Cancelleria federale riferiscono al NCSC in merito allo stato della sicurezza informatica.

2 I fornitori di prestazioni interni di cui all'articolo 9 OTDI[10] informano regolarmente il NCSC sulle vulnerabilità scoperte e sui ciberincidenti, nonché sulle misure previste e adottate per porvi rimedio.[11]

3 I dipartimenti e la Cancelleria federale designano ciascuno un incaricato della sicurezza informatica (ISID), che opera su incarico diretto della direzione del dipartimento.[12]

4 Gli ISID hanno segnatamente i seguenti compiti:

a. coordinare tutti gli aspetti della sicurezza informatica all'interno del dipartimento o della Cancelleria federale nonché con i servizi preposti al coordinamento e alla collaborazione interdipartimentali;

b. elaborare le basi necessarie per l'attuazione delle direttive in materia di sicurezza informatica e per l'organizzazione a livello di dipartimento o della Cancelleria federale.[13]

5 I dipartimenti e la Cancelleria federale disciplinano il rapporto tra l'ISID e l'incaricato della sicurezza informatica delle unità amministrative (ISIU), segnatamente la responsabilità tecnica per le questioni di sicurezza.[14]

Art. 14[15] Unità amministrative e i loro fornitori di prestazioni

1 Ogni unità amministrativa designa il proprio ISIU, che opera su incarico diretto della direzione dell'unità amministrativa. Il settore Trasformazione digitale e governance delle TIC della Cancelleria federale (settore TDT) designa inoltre un incaricato della sicurezza informatica per i servizi standard.

2 Gli ISIU e l'incaricato della sicurezza informatica per i servizi standard hanno i seguenti compiti:

a. garantire una rapida attuazione delle direttive in materia di sicurezza informatica e l'applicazione delle procedure di sicurezza (cap. 3*a*.);

b. provvedere affinché al momento dell'assunzione, e in seguito periodicamente, i collaboratori vengano sensibilizzati e istruiti sui temi legati alla sicurezza informatica e conoscano le competenze e i processi della sicurezza informatica nel loro ambito lavorativo, a seconda del livello gerarchico e della funzione;

10 RS **172.010.58**
11 Nuovo testo giusta l'all. n. 1 dell'O del 25 nov. 2020 sulla trasformazione digitale e l'informatica, in vigore dal 1° gen. 2021 (RU **2020** 5871).
12 Nuovo testo giusta il n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).
13 Introdotto dal n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).
14 Introdotto dal n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).
15 Nuovo testo giusta il n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).

c. informare il responsabile dell'unità amministrativa almeno ogni sei mesi sullo stato della sicurezza informatica all'interno dell'unità amministrativa.

3 Le unità amministrative sono responsabili della sicurezza dei propri oggetti informatici da proteggere. Hanno le seguenti funzioni:

a. tenere un inventario dei loro oggetti informatici da proteggere e adottare le necessarie misure di sicurezza; provvedere segnatamente affinché la documentazione di queste misure sia aggiornata per ogni oggetto informatico da proteggere;

b. garantire il rispetto e l'attuazione delle direttive in materia di sicurezza informatica, delle procedure di sicurezza nonché delle decisioni del Consiglio federale, dell'NCSC e dei dipartimenti o della Cancelleria federale nel loro settore di competenza;

c. fatto salvo l'articolo 12 capoverso 5, gestire i ciberincidenti che riguardano i loro oggetti informatici da proteggere;

d. in caso di acquisizione di prestazioni presso un fornitore esterno, garantire che le direttive in materia di sicurezza informatica siano parte integrante del rapporto contrattuale con il fornitore;

e. verificare in modo appropriato che i fornitori esterni rispettino le direttive in materia di sicurezza informatica;

f. assicurare che le responsabilità per la sicurezza informatica a livello operativo siano definite negli accordi di progetto e di prestazione tra i fornitori di prestazioni e i beneficiari di prestazioni;

g. provvedere affinché le persone a cui la presente ordinanza non è applicabile possano accedere all'infrastruttura informatica della Confederazione soltanto se si impegnano a rispettare le direttive in materia di sicurezza informatica.

4 I fornitori di prestazioni hanno le seguenti funzioni:

a. su richiesta, mettere a disposizione dei beneficiari di prestazioni in forma adeguata tutte le informazioni necessarie alla protezione degli oggetti informatici da proteggere;

b. garantire di disporre delle capacità necessarie alle analisi tecniche e alla gestione dei ciberincidenti che possono verificarsi ai loro danni o ai danni dei beneficiari di prestazioni;

c. comunicare senza indugio ai beneficiari di prestazioni le vulnerabilità scoperte e gli incidenti legati alla sicurezza riguardanti i loro oggetti informatici da proteggere;

d. definire in collaborazione con i beneficiari di prestazioni un processo di gestione dei ciberincidenti; questo processo disciplina segnatamente le competenze decisionali per l'adozione di misure urgenti.

5 Se un ciberincidente non può essere gestito nell'ambito del processo definito, gli interessati informano il NCSC al fine di determinare l'ulteriore modo di procedere.

6 Le unità amministrative consultano il NCSC in merito a direttive e progetti informatici rilevanti dal profilo della sicurezza.

7 Sono responsabili dello sviluppo, dell'attuazione e dell'esame di standard e norme in materia di cibersicurezza nei loro settori. Per quanto possibile, il NCSC mette a loro disposizione esperti del pool di cui all'articolo 12 capoverso 1 lettera g.

Art. 14*a*[16] Collaboratori

I collaboratori dell'Amministrazione federale che utilizzano mezzi informatici sono responsabili del loro utilizzo conforme alle prescrizioni.

Capitolo 3*a*:[17] Procedura di sicurezza

Art. 14*b* Analisi del bisogno di protezione

1 Le unità amministrative garantiscono che tutti gli oggetti informatici da proteggere siano stati sottoposti a un'analisi recente del bisogno di protezione. Per i progetti IT devono eseguire l'analisi del bisogno di protezione prima dell'avvio del progetto.

2 Nell'ambito dell'analisi del bisogno di protezione valutano gli aspetti della confidenzialità, dell'accessibilità, dell'integrità, della tracciabilità e della minaccia di spionaggio da parte dei servizi di informazione.

Art. 14*c* Protezione di base

Le unità amministrative attuano le direttive per la protezione di base per tutti gli oggetti informatici da proteggere e documentano l'attuazione.

Art. 14*d* Protezione elevata

1 Se dall'analisi del bisogno di protezione risulta un bisogno di protezione elevato, oltre all'attuazione delle direttive in materia di sicurezza per la protezione di base le unità amministrative definiscono, sulla base di un'analisi dei rischi, ulteriori misure di sicurezza, le documentano e le attuano.

2 Le unità amministrative rilevano e documentano i rischi che non possono essere ridotti o possono esserlo soltanto in misura insufficiente (rischi residui). Il committente del progetto, il responsabile dei processi aziendali e la direzione dell'unità amministrativa prendono atto dei rischi residui e ne danno conferma per scritto.

3 Spetta al responsabile dell'unità amministrativa competente decidere se assumere i rischi residui noti.

Art. 14*e* Periodicità

1 Le procedure di sicurezza devono essere eseguite almeno ogni cinque anni.

16 Introdotto dal n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).
17 Introdotto dal n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).

2 Devono essere eseguite senza indugio se l'oggetto informatico da proteggere o la situazione di minaccia subiscono modifiche rilevanti per la sicurezza.

Capitolo 3*b*:[18] Costi sostenuti a livello decentralizzato

Art. 14f

1 I costi sostenuti a livello decentralizzato per la sicurezza informatica fanno parte dei costi dei progetti e di quelli di esercizio.

2 Devono essere debitamente considerati nella pianificazione.

Capitolo 4: Disposizioni finali

Art. 15 Modifica di altri atti normativi

La modifica di altri atti normativi è disciplinata nell'allegato.

Art. 16 Disposizione transitoria dell'articolo 2 lettera b

1 Le autorità, le organizzazioni e le persone di diritto pubblico o privato che, prima dell'entrata in vigore della presente ordinanza, si sono impegnate mediante un accordo con l'Organo direzione informatica della Confederazione (ODIC) a rispettare le disposizioni dell'ordinanza del 9 dicembre 2011[19] sull'informatica nell'Amministrazione federale sottostanno sino al 31 dicembre 2021 agli obblighi della presente ordinanza nella misura del regime precedente.[20]

2 Sottostanno alla presente ordinanza a partire dal 1° gennaio 2022, sempre che l'accordo non sia stato sciolto al più tardi con effetto al 31 dicembre 2021.

Art. 17 Disposizione transitoria dell'articolo 11 capoverso 1 lettera e

1 Le direttive sulla sicurezza TIC emanate dall'ODIC e le deroghe da esso autorizzate prima dell'entrata in vigore della presente ordinanza rimangono applicabili.

2 Il NCSC decide in merito a eventuali modifiche delle direttive e delle deroghe autorizzate.

Art. 18 Entrata in vigore

La presente ordinanza entra in vigore il 1° luglio 2020.

18 Introdotto dal n. I dell'O del 24 feb. 2021, in vigore dal 1° apr. 2021 (RU **2021** 132).
19 RU **2011** 6093; **2015** 4873; **2016** 1783, 3445; **2018** 1093; **2020** 2107
20 Nuovo testo giusta l'all. n. 1 dell'O del 25 nov. 2020 sulla trasformazione digitale e l'informatica, in vigore dal 1° gen. 2021 (RU **2020** 5871).

Allegato
(art. 15)

Modifica di altri atti normativi

Le ordinanze qui appresso sono modificate come segue:

...[21]

21 Le mod. possono essere consultate alla RU **2020** 2107.