Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

(Ordinanza sui ciber-rischi, OCiber)

del 27 maggio 2020

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. alle autorità e ai servizi che, in virtù dell'articolo 2 capoversi 2 e 3 dell'ordinanza del 9 dicembre 2011[4] sull'informatica nell'Amministrazione federale (OIAF), s'impegnano a rispettarla.

RS **120.73**

1 RS **120**
2 RS **172.010**
3 RS **172.010.1**
4 RS **172.010.58**

Art. 3 Definizioni

Nella presente ordinanza s'intende per:

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.

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.

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[5] 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);

5 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[6]), 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;

6 National Cyber Security Centre

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

e. emanare direttive in materia di sicurezza informatica;

f. decidere sulle deroghe alle direttive che ha emanato; se queste deroghe riguardano anche direttive TIC dell'Organo direzione informatica della Confederazione (ODIC), il delegato alla cibersicurezza consulta previamente quest'ultimo.

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;

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 agli articoli 23 e 24 OIAF[7] informano regolarmente il NCSC sulle vulnerabilità scoperte e sui ciberincidenti, nonché sulle misure previste e adottate per porvi rimedio.

3 I dipartimenti e la Cancelleria federale designano ciascuno un incaricato della sicurezza informatica (ISID).

Art. 14 Unità amministrative e i loro fornitori di prestazioni

1 Ogni unità amministrativa designa il proprio incaricato della sicurezza informatica (ISIU). L'ODIC nomina inoltre un incaricato della sicurezza informatica per i servizi standard TIC.

2 Le unità amministrative sono responsabili della protezione dei loro sistemi informatici, delle loro applicazioni e dei loro dati (oggetti da proteggere). Hanno le seguenti funzioni:

a. esaminare regolarmente gli oggetti da proteggere e adottare le necessarie misure di sicurezza; provvedere segnatamente affinché la documentazione di queste misure sia aggiornata per ogni oggetto da proteggere;

b. garantire il rispetto delle direttive in materia di sicurezza informatica, nonché delle decisioni del Consiglio federale, del 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 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 le direttive in materia di sicurezza informatica siano rispettate dai fornitori esterni.

3 I fornitori di prestazioni garantiscono di disporre delle capacità necessarie per gestire i ciberincidenti che potrebbero verificarsi a essi stessi o ai loro beneficiari di prestazioni.

4 I fornitori di prestazioni comunicano senza indugio ai beneficiari di prestazioni le vulnerabilità scoperte e gli incidenti in relazione alla sicurezza.

5 I beneficiari di prestazioni definiscono in collaborazione con i fornitori di prestazioni un processo di gestione dei ciberincidenti. Questo processo disciplina segnatamente le competenze decisionali per l'adozione di misure urgenti.

6 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.

7 RS **172.010.58**

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

8 Le unità amministrative 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 loro a disposizione esperti del pool di cui all'articolo 12 capoverso 1 lettera g.

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 e i servizi, che prima dell'entrata in vigore della presente ordinanza si sono impegnati mediante un accordo con l'ODIC a rispettare le disposizioni dell'OIAF[8], sottostanno fino al 31 dicembre 2021 agli obblighi previsti dalla presente ordinanza nella misura del regime precedente.

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.

27 maggio 2020 In nome del Consiglio federale svizzero:

La presidente della Confederazione, Simonetta Sommaruga
Il cancelliere della Confederazione, Walter Thurnherr

8 RS **172.010.58**

Allegato
(art. 15)

Modifica di altri atti normativi

Le ordinanze qui appresso sono modificate come segue:

1. Ordinanza del 9 dicembre 2011[9] sull'informatica nell'Amministrazione federale

Art. 2 cpv. 3

3 Le autorità e i servizi, che in virtù del capoverso 2 si impegnano a rispettare la presente ordinanza e le direttive che ne derivano, si impegnano a rispettare anche l'ordinanza del 27 maggio 2020[10] sulla protezione contro i ciber-rischi (OCiber) nell'Amministrazione federale e le direttive che ne derivano.

Art. 3 cpv. 4 lett. d e 8, cap. 3 (art. 10 e 11), nonché 14 lett. e

Abrogati

Art. 16a Centro nazionale per la cibersicurezza

Il Centro nazionale per la cibersicurezza (NCSC[11]) di cui all'articolo 12 dell'OCiber[12] è consultato in merito all'elaborazione di direttive informatiche dell'Amministrazione federale riguardanti la cibersicurezza e nel quadro di progetti informatici rilevanti dal profilo della sicurezza.

Art. 17 cpv. 1 lett. e–i

1 L'ODIC ha segnatamente i seguenti compiti:

e. decidere sulle deroghe alle direttive che ha emanato. Se queste deroghe sono rilevanti dal profilo della sicurezza, l'ODIC consulta previamente il delegato alla cibersicurezza;

f.–g. *abrogate*

h. nominare un incaricato della sicurezza informatica per i servizi standard;

i. *abrogata*

9 RS **172.010.58**
10 RS **120.73**
11 National Cyber Security Centre
12 RS **120.73**

Art. 18 cpv. 1

1 Il consiglio informatico della Confederazione (CIC) si compone del delegato per la direzione TIC (art. 20*a* cpv. 2 dell'ordinanza del 17 febbraio 2010[13] sull'organizzazione del Dipartimento federale delle finanze) e di un rappresentante nominato appositamente per ciascun dipartimento, per la Cancelleria federale e per il NCSC. Esso è presieduto dal delegato.

Art. 19

Abrogato

2. Ordinanza del 17 febbraio 2010[14] sull'organizzazione del Dipartimento federale delle finanze

Art. 20a cpv. 3 lett. c

Abrogata

13 RS **172.215.1**
14 RS **172.215.1**