Ordinanza sulla sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito

(Ordinanza sulla sicurezza delle informazioni, OSIn)

dell'8 novembre 2023 (Stato 1° maggio 2025)

Il Consiglio federale svizzero,

visti gli articoli 2 capoversi 3 e 4, 12 capoverso 3, 83 capoverso 3, 84 capoverso 1, 85 capoversi 1 e 2 e 86 capoverso 4 della legge del 18 dicembre 2020[1] sulla sicurezza delle informazioni (LSIn),

ordina:

Sezione 1: Disposizioni generali

Art. 1 Oggetto
(art. 1 LSIn)

La presente ordinanza disciplina i compiti, le responsabilità e le competenze nonché le procedure per garantire la sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito.

Art. 2 Campo d'applicazione
(art. 2–3 LSIn)

[1] La presente ordinanza si applica:

a. al Consiglio federale;

b. ai dipartimenti;

c. alla Cancelleria federale (CaF), alle segreterie generali, ai gruppi e agli uffici federali;

d. all'esercito.

[2] Per le unità amministrative dell'Amministrazione federale decentralizzata di cui all'articolo 2 capoverso 3 della legge del 21 marzo 1997[2] sull'organizzazione del Governo e dell'Amministrazione (LOGA) nonché le organizzazioni e le persone di cui all'articolo 2 capoverso 4 LOGA si applicano le disposizioni seguenti della LSIn e della presente ordinanza:[3]

RU **2023** 735

1 RS **128**
2 RS **172.010**
3 Nuovo testo giusta l'all. 2 cifra II n. 1 dell'O del 2 apr. 2025 sulla digitalizzazione, in vigore dal 1° mag. 2025 (RU **2025** 235).

a. se trattano informazioni classificate della Confederazione: gli articoli 5–6, 9–10, 12–15, 20–23 e 27–73 LSIn nonché gli articoli 16, 21, 24, 26 e 32, 34–35 della presente ordinanza;

b.[4] se accedono a mezzi informatici dei fornitori interni di prestazioni TIC secondo l'articolo 10 dell'ordinanza del 2 aprile 2025[5] sulla digitalizzazione (ODigi) oppure fanno gestire i loro mezzi informatici da questi fornitori di prestazioni: gli articoli 5, 6, 9, 10 e 16–73 LSIn nonché gli articoli 10–12, 27 e 29–35 della presente ordinanza.

3 Nel loro ambito di competenza la CaF e i dipartimenti possono assoggettare a tutta la LSIn le unità amministrative dell'Amministrazione federale decentralizzata che svolgono continuamente attività sensibili sotto il profilo della sicurezza.

4 Fatto salvo l'articolo 3 capoverso 2 LSIn, per i Cantoni si applicano le seguenti disposizioni della presente ordinanza:

a. in caso di trattamento di informazioni classificate della Confederazione: le disposizioni della Sezione 4;

b. in caso di accesso a mezzi informatici della Confederazione: gli articoli 28–30 e 34.

5 L'Aggruppamento Difesa si fa carico per l'esercito dei compiti, delle competenze e delle responsabilità che la presente ordinanza attribuisce alle unità amministrative di cui all'articolo 2 capoverso 1 lettera c.

Sezione 2: Principi

Art. 3 Obiettivi in materia di sicurezza
(art. 7 cpv. 2 lett. a LSIn)

1 Le organizzazioni di cui all'articolo 2 capoverso 1 provvedono congiuntamente a una protezione delle loro informazioni e dei loro mezzi informatici basata sui rischi nonché a una resilienza adeguata riguardo ai rischi in materia di sicurezza delle informazioni.

2 Mediante la collaborazione e lo scambio di informazioni con altre autorità federali, i Cantoni, i Comuni, l'economia, la società, la scienza e i partner internazionali contribuiscono a migliorare la sicurezza delle informazioni in Svizzera.

3 Si impegnano a favore di un'armonizzazione delle prescrizioni e dei livelli di sicurezza a livello nazionale e internazionale allo scopo di permettere l'interazione tra autorità federali e altre autorità della Confederazione nonché i Cantoni, i Comuni e i partner internazionali.

4 Nuovo testo giusta l'all. 2 cifra II n. 1 dell'O del 2 apr. 2025 sulla digitalizzazione, in vigore dal 1° mag. 2025 (RU **2025** 235).
5 RS **172.019.1**

Art. 4 Responsabilità

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c sono responsabili della protezione delle informazioni di cui effettuano o commissionano il trattamento nonché della sicurezza dei mezzi informatici che gestiscono direttamente o che fanno gestire da terzi.

2 Nel loro settore di competenza le unità amministrative di cui all'articolo 2 capoverso 1 lettera c si occupano di tutti i compiti che la presente ordinanza o il rimanente diritto federale non attribuiscono a un'altra organizzazione o a un altro servizio.

3 I collaboratori dell'Amministrazione federale nonché i militari che trattano informazioni o utilizzano mezzi informatici della Confederazione sono responsabili del loro trattamento e del loro utilizzo conforme alle prescrizioni.

4 I superiori di tutti i livelli sono responsabili della formazione adeguata ai compiti dei loro collaboratori o dei militari loro subordinati nel settore della sicurezza delle informazioni e sono tenuti a verificare che questi rispettino le prescrizioni.

Sezione 3: Gestione della sicurezza delle informazioni

Art. 5 Sistema di gestione della sicurezza delle informazioni
(art. 7 cpv. 1 LSIn)

1 Ogni unità amministrativa di cui all'articolo 2 capoverso 1 lettera c elabora un sistema di gestione della sicurezza delle informazioni (SGSI).

2 Le unità amministrative definiscono gli obiettivi per il loro SGSI, verificano annualmente se gli obiettivi vengono raggiunti e rilevano gli indicatori necessari a tale scopo.

3 Fanno in modo che il loro SGSI venga verificato almeno ogni tre anni da un servizio indipendente o dal loro dipartimento e si occupano del miglioramento costante del sistema.

4 Si occupano del coordinamento del loro SGSI con la gestione ordinaria dei rischi, la gestione della continuità aziendale e la gestione delle crisi.

Art. 6 Cura delle basi legali e degli obblighi contrattuali
(art. 7 cpv. 1 LSIn)

Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c, i dipartimenti e il Servizio specializzato della Confederazione per la sicurezza delle informazioni tengono un registro ciascuno delle basi legali e degli obblighi contrattuali relativi alla sicurezza delle informazioni determinanti nel loro settore di competenza e lo tengono aggiornato.

Art. 7 Inventariazione degli oggetti da proteggere
(art. 7 cpv. 1 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c compilano un inventario dei loro oggetti da proteggere e lo tengono aggiornato.

2 Sono considerati oggetti da proteggere:

a. singole o più collezioni analoghe o correlate di informazioni che vengono trattate per il disbrigo di un processo operativo della Confederazione;

b. singoli o più mezzi informatici analoghi o correlati secondo l'articolo 5 lettera a LSIn.

3 Nell'inventario occorre riportare:

a. la necessità di protezione degli oggetti da proteggere;

b. le responsabilità per gli oggetti da proteggere;

c. la partecipazione di terzi;

d. il risultato della valutazione dei rischi;

e. l'attuazione delle misure di sicurezza e l'assunzione dei rischi che non possono essere sufficientemente ridotti (rischi residui);

f. i controlli e gli audit periodici;

g. eventualmente: l'utilizzo condiviso degli oggetti da proteggere.

Art. 8 Gestione dei rischi
(art. 7 cpv. 2 lett. b e 8 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c valutano costantemente i rischi per i loro oggetti da proteggere e svolgono in particolare i seguenti compiti:

a. analizzare periodicamente minacce e vulnerabilità e valutare le loro ripercussioni sugli oggetti da proteggere;

b. attuare le misure necessarie e controllare l'efficacia;

c. controllare il rispetto delle direttive;

d. comprovare l'accettazione dei rischi residui.

2 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni, l'Ufficio federale della cibersicurezza (UFCS), le unità amministrative che forniscono prestazioni e gli organi di sicurezza della Confederazione informano le unità amministrative di cui all'articolo 2 capoverso 1 lettera c e i dipartimenti in merito alle minacce e alle vulnerabilità attuali nonché in merito ai rischi che li riguardano. In caso di necessità raccomandano misure volte a ridurre i rischi.

3 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c redigono un rapporto sui loro rischi relativi alla sicurezza delle informazioni nel quadro del processo ordinario di gestione dei rischi secondo le direttive dell'Amministrazione federale delle finanze.

Art. 9 Autorizzazione ed elenco delle deroghe
(art. 7 cpv. 1 LSIn)

1 Se un'unità amministrativa per un oggetto da proteggere non è in grado di adempiere a una direttiva per essa vincolante prevista da un'istruzione generale e astratta secondo

l'articolo 85 LSIn essa necessita di un'autorizzazione eccezionale dell'organo che ha emanato le istruzioni.

2 Se una deroga che rientra nell'ambito di competenza del servizio specializzato della Confederazione per la sicurezza delle informazioni riguarda anche direttive della CaF sulla trasformazione digitale e la governance delle TIC, il servizio specializzato sente in via preliminare il delegato TDT.[6]

3 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c, i dipartimenti e il Servizio specializzato della Confederazione per la sicurezza delle informazioni tengono ciascuno un registro delle autorizzazioni eccezionali valide.

Art. 10 Collaborazione con terzi
(art. 9 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c valutano i rischi per i loro oggetti da proteggere che derivano dalla collaborazione con terzi e la loro dipendenza da terzi.

2 I servizi centrali d'acquisto di cui all'articolo 5 dell'ordinanza del 1° maggio 2024[7] concernente l'organizzazione degli appalti pubblici dell'Amministrazione federale (OOAPub) partecipano alla valutazione e mettono a disposizione le informazioni necessarie.[8]

3 Previa consultazione dell'UFCS e della Conferenza degli acquisti della Confederazione di cui all'articolo 30 OOAPub, il Servizio specializzato della Confederazione per la sicurezza delle informazioni raccomanda quali disposizioni in materia di sicurezza delle informazioni devono essere contemplate in tutti i contratti di acquisto e per prestazioni di servizio della Confederazione.[9]

Art. 11 Formazione e sensibilizzazione
(art. 7 cpv. 1 e 20 cpv. 1 lett. c LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c formano i loro collaboratori quando assumono la loro funzione e poi periodicamente in maniera tale che siano in grado di far fronte alla loro responsabilità in materia di sicurezza delle informazioni. Tengono un registro in merito alle formazioni e alla relativa partecipazione.

2 I contenuti delle formazioni riguardano in particolare:

a. l'identificazione corretta della necessità di protezione delle informazioni;

b. la gestione sicura di informazioni e mezzi informatici;

6 Nuovo testo giusta l'all. 2 cifra II n. 1 dell'O del 2 apr. 2025 sulla digitalizzazione, in vigore dal 1° mag. 2025 (RU **2025** 235).
7 RS **172.056.15**
8 Nuovo testo giusta l'art. 44 cpv. 2 n. 1 dell'O del 1° mag. 2024 concernente l'organizzazione degli appalti pubblici dell'Amministrazione federale, in vigore dal 1° lug. 2024 (RU **2024** 224).
9 Nuovo testo giusta l'art. 44 cpv. 2 n. 1 dell'O del 1° mag. 2024 concernente l'organizzazione degli appalti pubblici dell'Amministrazione federale, in vigore dal 1° lug. 2024 (RU **2024** 224).

c. la reazione corretta in caso di sospetto di un incidente legato alla sicurezza;

d. la conoscenza dell'organizzazione di sicurezza nonché delle persone di contatto in caso di domande relative alla sicurezza delle informazioni;

e. i compiti di controllo dei superiori;

f. l'attuazione della sicurezza delle informazioni nei progetti e nell'attività operativa.

3 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c, i dipartimenti e il Servizio specializzato della Confederazione per la sicurezza delle informazioni provvedono a sensibilizzare periodicamente i collaboratori di tutti i livelli in merito ai rischi legati alla sicurezza delle informazioni.

4 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni realizza ausili per le attività di formazione e di sensibilizzazione.

Art. 12 Gestione degli incidenti
(art. 7 cpv. 1 e 10 cpv. 1 LSIn)

1 D'intesa con i loro fornitori di prestazioni, le unità amministrative di cui all'articolo 2 capoverso 1 lettera c stabiliscono come notificare e gestire o trattare gli incidenti legati alla sicurezza e le lacune in materia di sicurezza. Stabiliscono chi può disporre misure immediate.

2 Se un fornitore di prestazioni individua incidenti legati alla sicurezza o lacune in materia di sicurezza che riguardano una delle unità amministrative che beneficiano delle loro prestazioni, li notifica senza indugio e fornisce sostegno per quanto riguarda la loro gestione o il loro trattamento.

3 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni e l'UFCS possono fornire sostegno alle unità amministrative di cui all'articolo 2 capoverso 1 lettera c e ai dipartimenti nella gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza.

4 Quando gestiscono incidenti legati alla sicurezza, le unità amministrative di cui all'articolo 2 capoverso 1 lettera c verificano se, secondo la legislazione sulla protezione dei dati, occorre effettuare una notifica all'Incaricato federale della protezione dei dati e della trasparenza.

5 Informano senza indugio il loro dipartimento e il Servizio specializzato della Confederazione per la sicurezza delle informazioni in merito all'incidente legato alla sicurezza o alla lacuna in materia di sicurezza se è soddisfatta una delle condizioni seguenti:

a. potrebbe essere compromesso il funzionamento dell'Amministrazione federale;

b. è interessato un mezzo informatico del livello di sicurezza «protezione elevata» o «protezione molto elevata»;

c. potrebbero essere interessati diversi dipartimenti;

d. potrebbe essere minacciata la protezione di informazioni classificate di uno Stato o di un'organizzazione internazionale con cui il Consiglio federale ha concluso un trattato internazionale secondo l'articolo 87 LSIn;

e. l'incidente legato alla sicurezza o la lacuna in materia di sicurezza potrebbe avere un'importanza politica elevata;

f. l'incidente legato alla sicurezza o la lacuna in materia di sicurezza richiede misure che vanno oltre la procedura stabilita secondo il capoverso 1.

6 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni valuta il rischio e la necessità di sostegno insieme all'unità amministrativa interessata.

7 Nei casi di cui al capoverso 5, d'intesa con l'unità amministrativa interessata e il dipartimento interessato, può assumere la direzione della gestione di un incidente legato alla sicurezza o di una lacuna in materia di sicurezza oppure, con il loro consenso, può trasferirla all'UFCS. In tale contesto hanno i compiti e le competenze seguenti:

a. possono obbligare le unità amministrative, i fornitori di prestazioni e i terzi interessati a comunicare loro tutte le informazioni necessarie;

b. possono disporre misure immediate;

c. possono impiegare specialisti esterni a scopo di sostegno;

d. informano la direzione delle unità amministrative e dei dipartimenti interessati in merito all'evoluzione.

8 Se dopo un incidente legato alla sicurezza o una lacuna in materia di sicurezza la sicurezza delle informazioni è stata ripristinata e se i lavori successivi necessari nonché il loro finanziamento sono definiti, il Servizio specializzato della Confederazione per la sicurezza delle informazioni o l'UFCS ritrasferisce la direzione per l'ulteriore trattamento all'unità amministrativa interessata.

Art. 13 Pianificazione dei controlli e degli audit
(art. 7 cpv. 1, 81 cpv. 2 lett. c e 83 cpv. 1 lett. c LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c e i dipartimenti stabiliscono all'interno di un piano annuale dei controlli e degli audit le modalità con cui verificare in base ai rischi il rispetto delle prescrizioni secondo la presente ordinanza e l'efficacia delle misure volte a garantire la sicurezza delle informazioni nel loro settore di competenza nonché presso terzi incaricati.

2 Gli audit presso terzi che dispongono di una dichiarazione di sicurezza aziendale di cui all'articolo 61 LSIn devono essere coordinati con il Servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende.

3 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni rileva il fabbisogno di controlli e di audit per garantire la sicurezza delle informazioni di tutta l'Amministrazione federale e dell'esercito.

4 D'intesa con la CaF o con il dipartimento competente può svolgere audit o delegarne lo svolgimento al Controllo federale delle finanze.

Art. 14 Rapporti
(art. 7 cpv. 1, 81 cpv. 2 lett. c e 83 cpv. 1 lett. h LSIn)

1 Ogni anno la CaF, i dipartimenti, l'UFCS e i fornitori interni di prestazioni TIC secondo l'articolo 10 ODigi[10] redigono un rapporto destinato al servizio specializzato della Confederazione per la sicurezza delle informazioni in merito allo stato della sicurezza delle informazioni nel loro settore di competenza. Rilevano le informazioni necessarie a tale scopo presso le unità amministrative e i loro fornitori di prestazioni.[11]

2 Ogni anno il Servizio specializzato della Confederazione per la sicurezza delle informazioni redige un rapporto destinato al Consiglio federale in merito allo stato della sicurezza delle informazioni in seno alla Confederazione.

3 Coordina i rapporti con le autorità assoggettate di cui all'articolo 2 capoverso 1 LSIn.

Art. 15 Direttive concernenti la gestione della sicurezza delle informazioni
(art. 85 LSIn)

Il Servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte valide per tutte le organizzazioni di cui all'articolo 2 capoversi 1 e 3 concernenti i requisiti minimi per la gestione della sicurezza delle informazioni secondo gli articoli 5–14.

Sezione 4: Informazioni classificate

Art. 16 Principi
(art. 11 e 14 LSIn)

1 La comunicazione e il conferimento dell'accesso a informazioni classificate nonché la produzione di supporti di dati classificati devono essere limitati al minimo indispensabile.

2 Se informazioni vengono raccolte in una collezione, la classificazione deve essere sottoposta a una nuova valutazione.

Art. 17 Servizi incaricati della classificazione
(art. 12 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c e i dipartimenti stabiliscono in un catalogo di classificazione il modo in cui classificare le informazioni che vengono trattate di frequente nel rispettivo settore di competenza e la durata della classificazione.

2 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni verifica i cataloghi di classificazione e in caso di necessità formula una raccomandazione.

10 RS **172.019.1**
11 Nuovo testo giusta l'all. 2 cifra II n. 1 dell'O del 2 apr. 2025 sulla digitalizzazione, in vigore dal 1° mag. 2025 (RU **2025** 235).

3 Previa consultazione della Conferenza degli incaricati della sicurezza delle informazioni, all'interno di istruzioni generali e astratte valide per tutte le organizzazioni di cui all'articolo 2 capoversi 1–3 stabilisce il modo in cui classificare le informazioni che vengono trattate di frequente a livello interdipartimentale e la durata della classificazione.

4 Le persone e i servizi seguenti sono competenti per la classificazione e la declassificazione di informazioni che non sono indicate nei cataloghi di classificazione:

a. i collaboratori della Confederazione nonché i militari;

b. i mandanti se informazioni della Confederazione vengono trattate da terzi.

5 I collaboratori della Confederazione, i militari e i terzi hanno la responsabilità di apporre un contrassegno formale ai supporti di dati che producono o alle informazioni che comunicano a voce.

Art. 18 Livello di classificazione «ad uso interno»
(art. 13 cpv. 1 LSIn)

1 Sono classificate «ad uso interno» le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare gli interessi di cui all'articolo 1 capoverso 2 lettere a–d LSIn come segue:

a. un importante processo operativo del Consiglio federale o dell'Amministrazione federale o un importante processo di condotta dell'esercito è reso più difficoltoso;

b. l'esecuzione di impieghi delle autorità di perseguimento penale, del Servizio delle attività informative della Confederazione (SIC), dell'esercito o di altri organi di sicurezza della Confederazione è resa più difficoltosa;

c. singole persone vengono ferite fisicamente;

d. la sicurezza nucleare o la sicurezza di impianti nucleari o di materiale nucleare è minacciata indirettamente;

e. la Svizzera subisce svantaggi a livello economico o di politica estera;

f. le relazioni tra la Confederazione e i Cantoni o tra i Cantoni sono intralciate.

2 Sono classificate «ad uso interno» le informazioni la cui conoscenza da parte di persone non autorizzate consente di trarre conclusioni su informazioni classificate «confidenziale» o «segreto».

Art. 19 Livello di classificazione «confidenziale»
(art. 13 cpv. 2 LSIn)

Sono classificate «confidenziale» le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2 lettere a–d LSIn come segue:

a. la capacità decisionale o la capacità d'azione del Consiglio federale, del Parlamento, di diverse unità amministrative o di diversi corpi di truppa dell'esercito è resa più difficoltosa per più giorni;

b. l'esecuzione conforme agli obiettivi di operazioni delle autorità di perseguimento penale, del SIC, dell'esercito o di altri organi di sicurezza della Confederazione è minacciata;

c. i mezzi e i metodi operativi dei servizi informazioni e delle autorità di perseguimento penale della Confederazione nonché l'identità delle fonti e delle persone esposte sono resi noti;

d. la sicurezza della popolazione è minacciata per più giorni oppure singole persone o gruppi di persone muoiono;

e. la sicurezza nucleare o la sicurezza di impianti nucleari o di materiale nucleare è minacciata;

f. l'approvvigionamento economico del Paese o l'esercizio delle infrastrutture critiche sono resi più difficoltosi;

g. la Svizzera subisce svantaggi considerevoli a livello economico o di politica estera o le relazioni diplomatiche con uno Stato o un'organizzazione internazionale vengono interrotte;

h. la posizione negoziale della Svizzera in importanti affari di politica estera è temporaneamente indebolita considerevolmente.

Art. 20 Livello di classificazione «segreto»
(art. 13 cpv. 3 LSIn)

Sono classificate «segreto» le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2 lettere a–d LSIn come segue:

a. il Consiglio federale, il Parlamento, diverse unità amministrative o diversi corpi di truppa dell'esercito per giorni sono incapaci di decidere o di agire oppure la loro capacità decisionale o la loro capacità d'azione è resa più difficoltosa per settimane;

b. l'esecuzione di operazioni importanti a livello strategico delle autorità di perseguimento penale, del SIC, dell'esercito o di altri organi di sicurezza della Confederazione è minacciata oppure resa più difficoltosa in misura particolarmente elevata per giorni;

c. le fonti strategiche, l'identità di persone particolarmente esposte oppure i mezzi e i metodi strategici dei servizi informazioni e delle autorità di perseguimento penale della Confederazione sono resi noti;

d. la sicurezza della popolazione è esposta a una minaccia particolarmente grave per settimane oppure un numero elevato di persone muore;

e. la sicurezza nucleare o la sicurezza di impianti nucleari o di materiale nucleare è minacciata in misura particolarmente elevata;

f. l'approvvigionamento economico del Paese o l'esercizio delle infrastrutture critiche non funzionano per giorni;

g. la Svizzera soffre per settimane di conseguenze particolarmente gravi a livello di politica estera o a livello economico come misure d'embargo o sanzioni;

h. la posizione negoziale della Svizzera in affari strategici di politica estera è indebolita per anni.

Art. 21 Direttive concernenti il trattamento
(art. 6 cpv. 2, 84 cpv. 1 e 85 LSIn)

1 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte valide per tutte le organizzazioni di cui all'articolo 2 capoversi 1–3 concernenti il trattamento di informazioni classificate e i requisiti minimi organizzativi, tecnici, edili e riguardanti il personale per la loro protezione. In tale contesto tiene conto degli standard internazionali in materia.

2 Consulta in via preliminare i seguenti servizi:

a. l'UFCS;

b. il servizio crittografico dell'esercito;

c.[12] l'Ufficio federale dell'armamento (armasuisse);

d. i servizi competenti per la sicurezza degli oggetti dell'Amministrazione federale e dell'esercito.

3 La CaF disciplina il trattamento di affari del Consiglio federale classificati.

4 Il trattamento di informazioni classificate provenienti dall'estero avviene secondo le prescrizioni che corrispondono al livello di classificazione estero. Sono fatte salve prescrizioni divergenti di un trattato internazionale secondo l'articolo 87 LSIn.

Art. 22 Misure di sicurezza specifiche all'impiego
(art. 6 cpv. 2 e 85 LSIn)

1 Se informazioni classificate vengono trattate nel quadro di un impiego o di un'operazione e sono accessibili soltanto a una cerchia di utenti chiusa e determinabile in maniera inequivocabile, le seguenti persone, dopo aver consultato il Servizio specializzato della Confederazione per la sicurezza delle informazioni, possono decidere prescrizioni specifiche per operazioni o impieghi per il trattamento semplificato:

a. il direttore dell'Ufficio federale di polizia;

b. il direttore del SIC;

c. il capo dell'esercito;

d. il capo del Comando Operazioni;

e. il direttore dell'Ufficio federale della dogana e della sicurezza dei confini.

2 Le persone di cui al capoverso 1 provvedono affinché sui supporti di informazioni sia chiaramente indicato che si applicano le prescrizioni per il trattamento semplificato.

12 Nuovo testo giusta l'art. 44 cpv. 2 n. 1 dell'O del 1° mag. 2024 concernente l'organizzazione degli appalti pubblici dell'Amministrazione federale, in vigore dal 1° lug. 2024 (RU **2024** 224).

3 Al di fuori della cerchia di utenti nonché per la conservazione in vista dell'archiviazione si applicano le direttive concernenti il trattamento secondo l'articolo 21.

Art. 23 Certificazione della sicurezza di mezzi informatici
(art. 83 cpv. 1 lett. e LSIn)

1 I mezzi informatici sono certificati per quanto riguarda la sicurezza prima di essere messi in servizio, se ciò è necessario per la collaborazione a livello nazionale o internazionale.

2 La certificazione della sicurezza è effettuata dal Servizio specializzato della Confederazione per la sicurezza delle informazioni dopo aver consultato il servizio crittografico dell'esercito e armasuisse.[13]

3 Dimostra che i mezzi informatici soddisfano i requisiti minimi per il relativo livello di classificazione e che i rischi residui sono sostenibili secondo lo stato della tecnica.

4 In caso di cambiamenti sostanziali riguardo ai rischi o di cambiamenti sostanziali del mezzo informatico la certificazione viene ripetuta.

5 Il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) definisce la procedura di certificazione della sicurezza e tiene conto degli standard internazionali in materia.

Art. 24 Protezione in caso di pericolo per le informazioni classificate
(art. 10 cpv. 1 e 11 cpv. 1 LSIn)

1 Chiunque constata che informazioni classificate sono esposte a pericolo, sono andate perse o sono state usate in modo abusivo oppure che informazioni sono state manifestamente classificate in modo errato o che, per errore, non sono state classificate, è tenuto ad adottare le necessarie misure di protezione.

2 Avvisa senza indugio il servizio incaricato della classificazione e gli organi di sicurezza competenti.

Art. 25 Verifica della necessità di protezione e cerchia delle persone autorizzate
(art. 11 cpv. 2 LSIn)

I servizi incaricati della classificazione verificano la necessità di protezione delle loro informazioni classificate e la cerchia delle persone autorizzate almeno ogni cinque anni e sempre nel caso in cui le informazioni vengono offerte all'Archivio federale per l'archiviazione.

13 Nuovo testo giusta l'art. 44 cpv. 2 n. 1 dell'O del 1° mag. 2024 concernente l'organizzazione degli appalti pubblici dell'Amministrazione federale, in vigore dal 1° lug. 2024 (RU **2024** 224).

Art. 26 Archiviazione
(art. 12 cpv. 3 LSIn)

1 L'archiviazione di informazioni classificate è retta dalle prescrizioni della legislazione in materia di archiviazione.

2 L'Archivio federale provvede affinché sia garantita la sicurezza delle informazioni secondo la presente ordinanza.

3 Allo scadere del termine di protezione la classificazione degli archivi viene meno. Proroghe dei termini di protezione si fondano sull'articolo 14 dell'ordinanza dell'8 settembre 1999[14] sull'archiviazione.

Sezione 5: Sicurezza nell'impiego di mezzi informatici

Art. 27 Procedura di sicurezza
(art. 16 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c devono essere in grado di comprovare la necessità di protezione dei loro oggetti da proteggere e la rilevanza di questi ultimi per la gestione della continuità aziendale.

2 Attuano le direttive minime del relativo livello di sicurezza e verificano se sono necessarie misure di sicurezza supplementari.

3 Specificano i rischi residui.

4 I responsabili della sicurezza delle informazioni (art. 36) decidono se i rischi residui sono sostenibili. Possono delegare questa decisione ad altri membri della direzione.

5 La procedura di sicurezza viene ripetuta in caso di cambiamenti sostanziali della minaccia, della tecnologia, dei compiti o della situazione organizzativa.

6 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c verificano ogni anno se vi è stato un cambiamento sostanziale.

7 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte applicabili a tutte le organizzazioni di cui all'articolo 2 capoversi 1–3 concernenti la procedura di sicurezza secondo l'articolo 16 LSIn.

Art. 28 Assegnazione ai livelli di sicurezza «protezione elevata» e «protezione molto elevata»
(art. 17 LSIn)

1 Il livello di sicurezza «protezione elevata» viene assegnato a un mezzo informatico se una violazione della sicurezza delle informazioni può comportare un pregiudizio secondo l'articolo 19 o un danno tra 50 e 500 milioni di franchi.

14 RS **152.11**

2 Il livello di sicurezza «protezione molto elevata» viene assegnato a un mezzo informatico se una violazione della sicurezza delle informazioni può comportare un pregiudizio secondo l'articolo 20 o un danno di oltre 500 milioni di franchi.

Art. 29 Misure di sicurezza
(art. 6 cpv. 3, 18 e 85 LSIn)

1 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte concernenti i requisiti minimi per i relativi livelli di sicurezza secondo l'articolo 17 LSIn applicabili a tutte le organizzazioni di cui all'articolo 2 capoversi 1–3.

2 Tiene conto dei requisiti per la sicurezza dei dati personali secondo la legislazione sulla protezione dei dati nonché di altre informazioni che la Confederazione è tenuta a proteggere in virtù di un obbligo legale o contrattuale.

3 Per i mezzi informatici seguenti, l'efficacia delle misure di sicurezza deve essere verificata prima della messa in servizio, e in caso di cambiamenti sostanziali dei rischi durante l'esercizio, però almeno ogni cinque anni:

a. mezzi informatici assegnati al livello di sicurezza «protezione elevata» che vengono impiegati per adempiere compiti che riguardano più autorità o dipartimenti;

b. mezzi informatici assegnati al livello di sicurezza «protezione molto elevata».

4 La CaF e i dipartimenti inseriscono i loro mezzi informatici assegnati al livello di sicurezza «protezione molto elevata» nella loro gestione della continuità.

Art. 30 Sicurezza durante l'esercizio
(art. 19 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c assicurano che le responsabilità per la sicurezza delle informazioni a livello operativo siano definite negli accordi di progetto e di prestazione stipulati con i fornitori interni di prestazioni.

2 I fornitori interni di prestazioni mettono a disposizione delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c, dei dipartimenti e del Servizio specializzato della Confederazione per la sicurezza delle informazioni le informazioni di cui necessitano per garantire la sicurezza delle informazioni.

3 Garantiscono di disporre delle capacità necessarie in termini finanziari e di personale per l'individuazione tempestiva, l'analisi tecnica e la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza che riguardano loro o, nel quadro degli accordi di cui al capoverso 1, i loro beneficiari di prestazioni.

4 Vigilano sull'utilizzo della loro infrastruttura informatica e la monitorano regolarmente alla ricerca di minacce e vulnerabilità tecniche. Possono incaricare terzi del monitoraggio.

5 Il trattamento di dati personali nel quadro della vigilanza e del monitoraggio secondo il capoverso 4 si fonda sull'ordinanza del 22 febbraio 2012[15] sul trattamento di dati personali e di dati di persone giuridiche derivanti dall'utilizzazione dell'infrastruttura elettronica della Confederazione.

Sezione 6: Misure relative alle persone e protezione fisica

Art. 31 Verifica dell'identità di persone e macchine
(art. 20 e 85 LSIn)

1 Dopo aver consultato il delegato TDT, il Servizio specializzato della Confederazione per la sicurezza delle informazioni può emanare istruzioni generali e astratte applicabili a tutte le organizzazioni di cui all'articolo 2 capoversi 1–3 concernenti i requisiti tecnici minimi per la verifica basata sui rischi dell'identità di persone e macchine che necessitano di avere accesso a informazioni, mezzi informatici, locali e altre infrastrutture della Confederazione.

2 Il trattamento di dati personali in sede di verifica dell'identità in sistemi di gestione delle identità secondo l'articolo 24 LSIn si fonda sulle disposizioni dell'ordinanza del 19 ottobre 2016[16] sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione.

Art. 32 Sicurezza delle persone
(art. 6 cpv. 2 e 3, 8 nonché 20 cpv. 1 lett. a e c LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c assicurano che i collaboratori soggetti a un controllo di sicurezza relativo alle persone secondo l'ordinanza dell'8 novembre 2023[17] sui controlli di sicurezza relativi alle persone (OCSP) vengano sensibilizzati ogni anno in merito all'attività determinante sensibile sotto il profilo della sicurezza e ai relativi rischi.

2 Questi collaboratori sono tenuti a comunicare al loro datore di lavoro le circostanze nel loro contesto privato e professionale che possono compromettere l'esercizio conforme alle prescrizioni dell'attività sensibile sotto il profilo della sicurezza.

Art. 33 Sospetto di reato
(art. 7 cpv. 2 lett. c LSIn)

1 Se in presenza di una violazione delle prescrizioni relative alla sicurezza delle informazioni al contempo è ipotizzabile un reato, la CaF e i dipartimenti inoltrano gli atti con i verbali d'interrogatorio al Ministero pubblico della Confederazione o all'uditore in capo dell'Esercito svizzero.

2 Mettono in sicurezza gli oggetti idonei a fungere da mezzi di prova in un procedimento.

15 RS **172.010.442**
16 RS **172.010.59**
17 RS **128.31**

Art. 34 Misure di protezione fisica
(art. 22 e 85 LSIn)

1 Previa consultazione dei servizi dell'Amministrazione federale e dell'esercito competenti per la sicurezza degli oggetti, il Servizio specializzato della Confederazione per la sicurezza delle informazioni può emanare istruzioni generali e astratte applicabili a tutte le organizzazioni di cui all'articolo 2 capoversi 1–3 concernenti i requisiti minimi per la protezione fisica di informazioni e mezzi informatici.

2 In tale contesto tiene conto:

a. dell'intero ciclo di vita delle informazioni e dei mezzi informatici;

b. dei requisiti specifici per il posto di lavoro;

c. delle strategie direttrici e degli schemi direttori dell'Amministrazione federale e dell'esercito.

Art. 35 Zone di sicurezza
(art. 23 e 85 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c possono istituire le seguenti zone di sicurezza:

a. zona di sicurezza 1: i locali e i settori in cui sono trattate frequentemente informazioni classificate «confidenziale» o sono impiegati mezzi informatici del livello di sicurezza «protezione elevata»;

b. zona di sicurezza 2: i locali e i settori in cui sono trattate frequentemente informazioni classificate «segreto» o sono impiegati mezzi informatici del livello di sicurezza «protezione molto elevata».

2 Questi locali e settori sono considerati come zona di sicurezza soltanto se il servizio competente per la sicurezza degli oggetti dell'Amministrazione federale o dell'esercito prima della messa in servizio e successivamente almeno ogni cinque anni conferma che i requisiti di sicurezza sono soddisfatti.

3 Dopo aver consultato i servizi competenti per la sicurezza degli oggetti dell'Amministrazione federale e dell'esercito, il Servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte applicabili a tutte le organizzazioni di cui all'articolo 2 capoversi 1–3 concernenti i requisiti di sicurezza per le zone di sicurezza e la loro istituzione.

4 Nei dintorni di zone di sicurezza le unità amministrative di cui all'articolo 2 capoverso 1 lettera c possono adottare misure per individuare attività di spionaggio elettromagnetico e per proteggersi da esse.

Sezione 7: Organizzazione di sicurezza

Art. 36 Responsabili della sicurezza delle informazioni delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c
(art. 7 cpv. 1 LSIn)

1 Il cancelliere della Confederazione, i segretari generali nonché i direttori delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c sono responsabili della sicurezza delle informazioni nel loro settore di competenza.

2 Possono delegare la responsabilità della sicurezza delle informazioni a un membro della direzione a condizione che questo disponga dei poteri necessari per predisporre, controllare e correggere misure.

3 I responsabili della sicurezza delle informazioni delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c svolgono in particolare i seguenti compiti:

a. garantiscono lo sviluppo, l'esercizio, la verifica e il miglioramento continuo del SGSI nel loro settore di competenza ed emanano le direttive necessarie a tale scopo;

b. adottano tutte le decisioni che influiscono in misura determinante sulla sicurezza delle informazioni nel loro settore di competenza, in particolare per quanto concerne l'organizzazione, i processi, l'accettazione dei rischi e gli obiettivi di sicurezza;

c. decidono in merito alle misure necessarie, in particolare allo svolgimento di misure di formazione e di sensibilizzazione;

d. approvano il piano annuale di controllo e di audit e mettono a disposizione le risorse necessarie a tale scopo.

4 Il cancelliere della Confederazione, i segretari generali nonché i direttori delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c danno incarico ai loro incaricati della sicurezza delle informazioni secondo l'articolo 37 e provvedono affinché:

a. dispongano di competenze e di risorse adeguate; e

b. non vengano loro assegnati compiti che possono comportare un conflitto d'interessi con i compiti secondo l'articolo 37.

Art. 37 Incaricati della sicurezza delle informazioni delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c
(art. 7 cpv. 1 LSIn)

1 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c designano uno o diversi incaricati della sicurezza delle informazioni nonché il o i sostituti.

2 Gli incaricati della sicurezza delle informazioni hanno in particolare i compiti e le competenze seguenti:

a. su incarico del responsabile della sicurezza delle informazioni gestiscono il SGSI dell'unità amministrativa;

b. elaborano le necessarie basi decisionali all'attenzione dei responsabili della sicurezza delle informazioni e li incaricano di decidere le misure;

c. fungono da organo centrale di contatto dell'unità amministrativa per questioni relative alla sicurezza delle informazioni e forniscono consulenza e sostegno alle persone e ai servizi competenti nell'adempimento dei loro compiti e doveri nel settore della sicurezza delle informazioni;

d. provvedono all'attuazione delle direttive in materia di sicurezza delle informazioni e all'applicazione della procedura di sicurezza di cui all'articolo 27;

e. vigilano sul registro delle basi legali, sull'inventario degli oggetti da proteggere e sul registro delle autorizzazioni eccezionali;

f. vigilano sulla pianificazione della formazione e della sensibilizzazione secondo l'articolo 11 e incaricano il responsabile della sicurezza delle informazioni di svolgere misure supplementari di formazione e di sensibilizzazione;

g. fanno domanda per avviare la procedura di sicurezza relativa alle aziende di cui all'articolo 4 dell'ordinanza dell'8 novembre 2023[18] sulla procedura di sicurezza relativa alle aziende (OPSAz);

h. coordinano la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza nell'unità amministrativa nonché presso terzi incaricati;

i. redigono il piano annuale di controllo e di audit e lo presentano al responsabile della sicurezza delle informazioni per l'approvazione;

j. verificano periodicamente nel loro ambito di competenza la presenza di supporti di informazioni classificati «segreto» e la loro messa in sicurezza;

k. su incarico del responsabile della sicurezza delle informazioni possono controllare o far controllare la gestione delle informazioni in postazioni di lavoro aperte, condivise o non chiudibili a chiave e nei mezzi informatici dell'unità amministrativa;

l. informano a scadenza semestrale il responsabile della sicurezza delle informazioni in merito allo stato della sicurezza delle informazioni.

Art. 38[19] Sicurezza delle informazioni nei mezzi informatici messi a disposizione a livello centralizzato

1 Il delegato TDT è competente per la garanzia della sicurezza delle informazioni dei mezzi informatici messi a disposizione a livello centralizzato dal settore TDT.

2 Designa un incaricato della sicurezza delle informazioni o diversi incaricati della sicurezza delle informazioni e il sostituto o i sostituti.

3 Gli incaricati della sicurezza delle informazioni si occupano dei compiti di cui all'articolo 37 capoverso 2 per i mezzi informatici messi a disposizione a livello centraliz-

18 RS **128.41**
19 Nuovo testo giusta l'all. 2 cifra II n. 1 dell'O del 2 apr. 2025 sulla digitalizzazione, in vigore dal 1° mag. 2025 (RU **2025** 235).

zato dal settore TDT e informano l'Amministrazione federale e l'esercito in merito ai rischi in materia di sicurezza delle informazioni.

Art. 39 Responsabilità in materia di sicurezza delle informazioni dei dipartimenti
(art. 7 cpv. 1 e 81 LSIn)

1 I dipartimenti sono responsabili della gestione e della vigilanza sulla sicurezza delle informazioni nel loro settore di competenza.

2 In tale contesto si occupano in particolare dei compiti seguenti:

a. determinano la politica in materia di sicurezza delle informazioni e l'organizzazione in materia di sicurezza del dipartimento, compresa la direzione specialistica degli incaricati della sicurezza delle informazioni di cui all'articolo 37;

b. emanano le istruzioni necessarie e vigilano sull'attuazione;

c. vigilano sul SGSI delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c e rilevano gli indicatori necessari a tale scopo;

d. stabiliscono ogni anno gli obiettivi in materia di sicurezza per le unità amministrative di cui all'articolo 2 capoverso 1 lettera c e verificano se sono stati raggiunti;

e. approvano il piano annuale di controllo e di audit del dipartimento e mettono a disposizione le risorse necessarie;

f. incaricano i loro incaricati della sicurezza delle informazioni secondo l'articolo 40 e provvedono affinché:
   1. dispongano di competenze e di risorse adeguate,
   2. non vengano loro assegnati compiti che possono comportare un conflitto d'interessi con i loro compiti di cui all'articolo 40.

3 Possono stabilire requisiti di sicurezza per il loro settore di competenza che vanno oltre i requisiti minimi stabiliti dal Servizio specializzato della Confederazione per la sicurezza delle informazioni.

4 Se il capo del dipartimento non decide diversamente, è il segretario generale su suo incarico a essere responsabile della sicurezza delle informazioni nel dipartimento.

Art. 40 Incaricati della sicurezza delle informazioni dei dipartimenti
(art. 7 cpv. 1 e 81 LSIn)

In aggiunta ai compiti di cui all'articolo 81 capoverso 2 LSIn, gli incaricati della sicurezza delle informazioni dei dipartimenti hanno i seguenti compiti:

a. provvedono al coordinamento interdipartimentale della sicurezza delle informazioni;

b. elaborano le necessarie basi decisionali all'attenzione dei responsabili della sicurezza delle informazioni e li incaricano di decidere le misure;

c. coordinano la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza che riguardano più unità amministrative di cui all'articolo 2 capoverso 1 lettera c;

d. redigono il piano annuale di controllo e di audit del dipartimento e lo presentano al responsabile della sicurezza delle informazioni per l'approvazione;

e. rappresentano il dipartimento in organi specialistici;

f. vengono consultati in sede di nomina degli incaricati della sicurezza delle informazioni delle unità amministrative secondo l'articolo 37;

g. controllano periodicamente e in caso di cambiamento o di uscita di un membro del Consiglio federale o del cancelliere della Confederazione che tutti i supporti di dati classificati «segreto» siano integralmente presenti;

h. informano ogni anno il responsabile della sicurezza delle informazioni del dipartimento in merito allo stato della sicurezza delle informazioni nel dipartimento.

Art. 41 Incaricato della sicurezza delle informazioni del Consiglio federale
(art. 81 cpv. 1 lett. a LSIn)

Il DDPS nomina l'incaricato della sicurezza delle informazioni del Consiglio federale nonché il suo sostituto.

Art. 42 Servizio specializzato della Confederazione per la sicurezza delle informazioni
(art. 7 cpv. 1 e 83 LSIn)

1 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni ha i compiti e le competenze seguenti per l'Amministrazione federale e per l'esercito:

a. elabora strategie relative a temi rilevanti sotto il profilo della sicurezza;

b. può richiedere informazioni riguardo a progetti rilevanti sotto il profilo della sicurezza, prendere posizione al riguardo e richiedere modifiche;

c. partecipa alla formazione dell'organizzazione di sicurezza;

d. mette a disposizione modelli e strumenti ausiliari;

e. assiste gli incaricati della sicurezza delle informazioni per quanto riguarda il controllo dei supporti di informazioni classificati «segreto»;

f. è responsabile di soluzioni di sicurezza certificate che vengono impiegate per l'intera Amministrazione federale e l'esercito.

2 Per adempiere questi compiti nonché i compiti di cui all'articolo 83 capoverso 1 LSIn consulta la Conferenza degli incaricati della sicurezza delle informazioni.

3 Nel contesto internazionale rappresenta la Svizzera in veste di autorità di sicurezza nazionale e svolge i seguenti compiti:

a. elabora i trattati internazionali di cui all'articolo 87 LSIn e vigila sulla loro attuazione;

b. assicura che gli incidenti legati alla sicurezza che riguardano informazioni classificate di Stati partner vengano chiariti in maniera adeguata;

c. esegue i controlli previsti dai trattati internazionali o li commissiona;

d. rappresenta la Svizzera in organi specializzati internazionali;

e. autorizza l'accoglienza di persone dall'estero che si recano in Svizzera per progetti classificati nonché l'invio di persone che si recano all'estero per progetti classificati;

f. rilascia le attestazioni di sicurezza secondo l'articolo 30 OCSP[20].

4 Fa parte della Segreteria di Stato della politica di sicurezza in seno al DDPS.

Art. 43 Compiti e competenze dell'UFCS
(art. 7 cpv. 1 e 84 cpv. 1 LSIn)

1 L'UFCS ha i compiti e le competenze seguenti:

a. fornisce consulenza all'Amministrazione federale e all'esercito nonché agli organi di sicurezza di cui agli articoli 81–83 LSIn riguardo a tutte le questioni legate alla sicurezza tecnica delle informazioni;

b. fa parte della Conferenza degli incaricati della sicurezza delle informazioni di cui all'articolo 82 LSIn;

c. per valutare e migliorare lo stato della sicurezza tecnica delle informazioni della Confederazione può cercare minacce tecniche o vulnerabilità in Internet o, d'intesa con i relativi responsabili della sicurezza delle informazioni e i fornitori di prestazioni, nell'infrastruttura informatica dell'Amministrazione federale e dell'esercito; può incaricare altri servizi dell'Amministrazione federale o dell'esercito nonché terzi di tale attività.

2 Coordina le sue attività con il Servizio specializzato della Confederazione per la sicurezza delle informazioni.

Sezione 8: Costi e valutazione

Art. 44 Costi

1 I costi per la sicurezza delle informazioni sostenuti a livello decentralizzato fanno parte dei costi di progetto e di esercizio.

2 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c assicurano che questi costi vengano considerati e riportati in sede di pianificazione in maniera adeguata.

3 Per il rilascio e il recapito delle attestazioni di sicurezza secondo l'articolo 30 OCSP[21] a persone che non svolgono un'attività sensibile sotto il profilo della sicu-

20 RS **128.31**
21 RS **128.31**

rezza, il Servizio specializzato della Confederazione per la sicurezza delle informazioni riscuote un emolumento pari a 100 franchi.

Art. 45 Valutazione
(art. 88 LSIn)

Sei anni dopo l'entrata in vigore della presente ordinanza e successivamente ogni dieci anni, il Servizio specializzato della Confederazione per la sicurezza delle informazioni richiede al Controllo federale delle finanze una valutazione della legislazione in materia di sicurezza delle informazioni in seno alla Confederazione.

Sezione 9: Trattamento di informazioni e di dati personali

Art. 46 In generale

1 Le organizzazioni di cui all'articolo 2 capoversi 1–3 nonché gli organi di sicurezza della Confederazione possono trattare le informazioni opportune per garantire la sicurezza delle informazioni, compresi i dati personali.

2 Possono scambiare tra loro informazioni di cui al capoverso 1, compresi dati personali, nonché con organizzazioni nazionali, internazionali ed estere di diritto pubblico e privato se:

a. ciò è appropriato per garantire la sicurezza delle informazioni;

b. non vengono violati obblighi di tutela segreto legali o contrattuali;

c. vengono rispettate le direttive della legislazione federale sulla protezione dei dati; e

d. queste organizzazioni svolgono compiti legali nell'ambito della sicurezza delle informazioni che corrispondono a quelli dell'autorità o dell'organizzazione che comunica i dati.

3 Se è necessario per la gestione di un incidente legato alla sicurezza o di una lacuna in materia di sicurezza possono trattare o scambiare tra loro anche dati personali degni di particolare protezione secondo l'articolo 5 lettera c della legge del 25 settembre 2020[22] sulla protezione dei dati di persone che vi hanno partecipato o che vi erano o vi potrebbero essere coinvolte.

4 Se nel caso di un incidente legato alla sicurezza in seno alla Confederazione o presso terzi che collaborano con la Confederazione vengono sottratte e pubblicate in Internet informazioni, possono scaricare e analizzare le informazioni per valutare il grado di coinvolgimento della Confederazione e adottare le misure di protezione necessarie. Non possono trattare dati che non sono rilevanti ai fini della valutazione.

5 Possono applicare queste misure già in presenza di un sospetto concreto.

22 RS **235.1**

Art. 47 Applicazione SGSI

[1] Per la gestione della sicurezza delle informazioni le organizzazioni di cui all'articolo 2 capoversi 1–3 possono utilizzare un sistema d'informazione (applicazione SGSI).

[2] Nell'applicazione SGSI possono trattare tutte le informazioni relative alla gestione della sicurezza delle informazioni secondo la presente ordinanza nonché i dati personali degni di particolare protezione di cui all'articolo 46 capoverso 3.

[3] Possono collegare le loro applicazioni SGSI e scambiare tra loro informazioni rilevanti sotto il profilo della sicurezza delle informazioni tramite interfacce automatizzate.

Art. 48 Servizi di modulistica elettronica

[1] Il Servizio specializzato della Confederazione per la sicurezza delle informazioni può gestire servizi di modulistica elettronica e collegarli con la sua applicazione SGSI per i seguenti scopi:

a. per la gestione dei viaggi secondo l'articolo 42 capoverso 3 lettera e;

b. per il rilascio e il recapito delle attestazioni di sicurezza nel contesto internazionale secondo l'articolo 30 OCSP[23];

c. per il rilascio e il recapito delle attestazioni internazionali di sicurezza aziendale secondo l'articolo 66 LSIn.

[2] Con i servizi di modulistica di cui al capoverso 1 possono essere trattati dati personali secondo l'allegato 1. Questi dati possono essere conservati al massimo per dieci anni.

[3] Le organizzazioni di cui all'articolo 2 capoversi 1–3 possono gestire servizi di modulistica elettronica per notificare incidenti legati alla sicurezza e lacune in materia di sicurezza e collegarli con la loro applicazione SGSI.

[4] Con i servizi di modulistica di cui al capoverso 3 possono trattare dati personali, compresi dati personali degni di particolare protezione secondo l'articolo 46 capoverso 3, se sono necessari per gestire incidenti legati alla sicurezza e lacune in materia di sicurezza. Immediatamente dopo la loro comunicazione tramite il servizio di modulistica devono essere cancellati. Possono essere salvati temporaneamente per al massimo 24 ore prima dell'invio della notifica.

Sezione 10: Disposizioni finali

Art. 49 Disposizioni esecutive particolari

Il DDPS può dichiarare vincolanti per i Cantoni determinate versioni provviste di data delle istruzioni generali e astratte secondo l'articolo 17 capoverso 3, 21 capoverso 1, 29 capoverso 1 e 34 capoverso 1.

23 RS **128.31**

Art. 50 Abrogazione e modifica di altri atti normativi

L'abrogazione e la modifica di altri atti normativi sono disciplinate nell'allegato 2.

Art. 51 Disposizioni transitorie

1 Le direttive relative alla sicurezza informatica emanate dal Centro nazionale per la cibersicurezza (NCSC) e le deroghe da esso autorizzate prima dell'entrata in vigore della presente ordinanza rimangono applicabili per tre anni al massimo dall'entrata in vigore della presente ordinanza.

2 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni o il NCSC decidono in merito a modifiche delle direttive e delle eccezioni autorizzate che sono state emanate dal NCSC prima dell'entrata in vigore della presente ordinanza.

3 Le direttive relative alla protezione delle informazioni emanate dalla Conferenza dei segretari generali o dall'organo di coordinamento per la protezione delle informazioni in seno alla Confederazione prima dell'entrata in vigore della presente ordinanza rimangono applicabili per due anni al massimo dall'entrata in vigore della presente ordinanza.

4 Le unità amministrative di cui all'articolo 2 capoverso 1 lettera c devono realizzare il loro SGSI (art. 5) entro tre anni dall'entrata in vigore della presente ordinanza.

5 I cataloghi di classificazione (art. 17) devono essere realizzati entro un anno dall'entrata in vigore della presente ordinanza.

6 Fino al 30 giugno 2025 l'UFCS si occuperà dei compiti e delle competenze del Servizio specializzato della Confederazione per la sicurezza delle informazioni secondo gli articoli 9 capoversi 2 e 3, 11 capoversi 3 e 4, 12 capoversi 3 e 6–8, 15, 27 capoverso 7, 29 capoverso 1 e 31 capoverso 1.

7 Le istruzioni emanate dall'UFCS in applicazione del capoverso 6 valgono al massimo per due anni dall'entrata in vigore della presente ordinanza.

Art. 52 Entrata in vigore

La presente ordinanza entra in vigore il 1° gennaio 2024.

Allegato 1
(art. 48)

Trattamento dei dati con i servizi di modulistica elettronica

Con i seguenti servizi di modulistica possono essere trattati i dati personali indicati in seguito:

1. Servizio di modulistica per lo scopo di cui all'articolo 48 capoverso 1 lettera a

a. Dati personali:
   1. cognome e nome*
   2. numero AVS
   3. appellativo, titolo e rango*
   4. data di nascita*
   5. luogo di origine e luogo di nascita*
   6. nazionalità*
   7. numero della carta d'identità e del passaporto nonché luogo di rilascio e validità*

b. Indicazioni relative alla funzione professionale o militare della persona:
   1. funzione nell'organizzazione o nell'esercito*
   2. indirizzo di lavoro, indirizzo e-mail, numero di telefono e ulteriori dati di contatto, in particolare elettronici
   3. decisione positiva in merito al controllo di sicurezza relativo alle persone, livello di controllo e validità*

c. Indicazioni relative all'organizzazione richiedente:
   1. denominazione, indirizzo e dati di contatto dell'organizzazione*
   2. cognome e nome della persona di riferimento
   3. funzione della persona di riferimento nell'organizzazione o nell'esercito
   4. indirizzo di lavoro, indirizzo e-mail, numero di telefono e dati di contatto elettronici della persona di riferimento

d. Indicazioni relative alla visita:
   1. nome, indirizzo, indirizzo e-mail e dati di contatto dell'organizzazione estera*
   2. motivo della visita*
   3. livello di sicurezza della visita*
   4. durata della visita*
   5. punti di attraversamento del confine*
   6. mezzi di trasporto*
   7. materiali trasportati, compresi armi, munizioni ed esplosivi, veicoli e altri equipaggiamenti*

Le indicazioni seguite da un asterisco (*) vengono comunicate all'autorità di sicurezza estera.

2. Servizio di modulistica per lo scopo di cui all'articolo 48 capoverso 1 lettera b

a. Dati personali:
   1. cognome e nome
   2. numero AVS
   3. appellativo, titolo e rango
   4. data di nascita
   5. luogo di origine e luogo di nascita
   6. nazionalità
   7. numero della carta d'identità e del passaporto nonché luogo di rilascio e validità

b. Indicazioni relative alla funzione professionale o militare della persona:
   1. funzione nell'organizzazione o nell'esercito
   2. indirizzo di lavoro, indirizzo e-mail, numero di telefono e ulteriori dati di contatto, in particolare elettronici
   3. decisione positiva in merito al controllo di sicurezza relativo alle persone, livello di controllo e validità

c. Indicazioni relative all'organizzazione richiedente:
   1. denominazione, indirizzo, indirizzo e-mail e dati di contatto dell'organizzazione
   2. cognome e nome della persona di riferimento
   3. funzione della persona di riferimento nell'organizzazione o nell'esercito
   4. indirizzo di lavoro, indirizzo e-mail e ulteriori dati di contatto, in particolare elettronici, della persona di riferimento
   5. motivo dell'elaborazione dell'attestazione

3. Servizio di modulistica per lo scopo di cui all'articolo 48 capoverso 1 lettera c

a. Indicazioni concernenti l'azienda:
   1. denominazione completa*
   2. forma giuridica*
   3. numero d'identificazione delle imprese
   4. indirizzo, indirizzo e-mail e ulteriori dati di contatto, in particolare elettronici*
   5. sede*
   6. cognome e nome della persona di riferimento*
   7. funzione della persona di riferimento nell'azienda

8. indirizzo di lavoro, indirizzo e-mail e ulteriori dati di contatto, in particolare elettronici, della persona di riferimento

b. Indicazioni relative alla dichiarazione di sicurezza aziendale:
   1. data del rilascio e validità*
   2. campo di applicazione e condizioni*
   3. livello di classificazione o di sicurezza più alto ammesso*

Le indicazioni seguite da un asterisco (*) vengono comunicate all'autorità di sicurezza estera.

4. Servizio di modulistica secondo l'articolo 48 capoverso 3

a. Indicazioni relative alla persona che presenta la notifica:
   1. cognome e nome
   2. indirizzo, indirizzo e-mail, numero di telefono e ulteriori dati di contatto, in particolare elettronici
   3. funzione nell'organizzazione o nell'esercito

b. Indicazioni relative all'evento dannoso e al calcolo del danno

c. Registrazioni fotografiche, audio o video dell'incidente o della lacuna in materia di sicurezza

d. Documenti o file correlati all'incidente o alla lacuna in materia di sicurezza

e. Indicazioni relative a persone eventualmente coinvolte nell'incidente

f. Primi accertamenti effettuati da periti, comprese le misure già adottate

Allegato 2
(art. 50)

Abrogazione e modifica di altri atti normativi

I

L'ordinanza del 27 maggio 2020[24] sui ciber-rischi è abrogata.

II

Gli atti normativi qui appresso sono modificati come segue:
...[25]

24 [RU **2020** 2107, 5871 all. n. 1; **2021** 132]
25 Le mod. possono essere consultate alla RU **2023** 735.