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

(Ordinanza sulla sicurezza delle informazioni, OSIn)

avamprogetto del 24 agosto 2022

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 sulla sicurezza delle informazioni del 18 dicembre 2020[1] (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 e 84 cpv. 3 LSIn)

[1] La presente ordinanza si applica:

a. al Consiglio federale;

b. alle unità amministrative dell'Amministrazione federale centrale secondo l'articolo 7 dell'ordinanza del 25 novembre 1998[2] sull'organizzazione del Governo e dell'Amministrazione (OLOGA);

c. all'esercito.

[2] La LSIn e la presente ordinanza si applicano alle unità amministrative dell'Amministrazione federale decentralizzata secondo l'articolo 7*a* OLOGA[3] come segue:

1 RS **128**
2 RS **172.010.1**
3 RS **172.010.1**

a. alle unità amministrative che accedono a mezzi informatici dei fornitori interni di prestazioni TIC secondo l'articolo 9 dell'ordinanza del 25 novembre 2020[4] sulla trasformazione digitale e l'informatica (OTDI), se questi sono assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28: l'intera LSIn e la presente ordinanza;

b. alle unità amministrative che impiegano mezzi informatici assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28: l'intera LSIn e la presente ordinanza;

c. alle unità amministrative che non rientrano tra quelle di cui alla lettera a o b, ma che trattano informazioni classificate della Confederazione: gli articoli 9–15 e 27–73 LSIn nonché le disposizioni della Sezione 4 della presente ordinanza.

3 La Cancelleria federale o i dipartimenti possono chiedere al Consiglio federale di assoggettare le unità amministrative dell'Amministrazione federale decentralizzata che non rientrano tra quelle di cui al capoverso 2 alla LSIn e alla presente ordinanza o a parti di essa.

4 Nell'allegato 1 sono riportate:

a. le unità amministrative di cui al capoverso 2;

b. le unità amministrative di cui al capoverso 3 e la relativa applicabilità della LSIn e della presente ordinanza.

5 Le organizzazioni di cui all'articolo 2 capoverso 4 della legge del 21 marzo 1997[5] sull'organizzazione del Governo e dell'Amministrazione (LOGA) sono escluse dal campo d'applicazione della LSIn e della presente ordinanza.

6 Fatto salvo l'articolo 3 capoverso 2 LSIn, per i Cantoni si applicano:

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.

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 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 partner internazionali contribuiscono a migliorare la sicurezza delle informazioni in Svizzera.

4 RS **172.010.58**
5 RS **172.010**

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 dei Cantoni e dei Comuni.

Art. 4 Responsabilità

1 Le unità amministrative 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 si occupano di tutti i compiti che la presente ordinanza o il 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 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 elabora un sistema di gestione della sicurezza delle informazioni (SGSI).

2 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 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)

1 Le unità amministrative, 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.

2 Le unità amministrative e i dipartimenti consultano il servizio specializzato della Confederazione per la sicurezza delle informazioni riguardo a direttive e a progetti rilevanti sotto il profilo della sicurezza.

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

1 Le unità amministrative compilano un inventario dei loro oggetti da proteggere e lo tengono aggiornato.

2 Sono considerati oggetti da proteggere:

a. le raccolte di informazioni trattate per adempiere un compito della Confederazione;

b. i mezzi informatici di cui all'articolo 5 lettera a LSIn.

3 L'inventario serve a comprovare:

a. la necessità di protezione degli oggetti da proteggere;

b. le responsabilità per gli oggetti da proteggere;

c. eventualmente l'utilizzo condiviso degli oggetti da proteggere;

d. la partecipazione di terzi;

e. il risultato della valutazione dei rischi;

f. l'attuazione delle misure di sicurezza e l'assunzione dei rischi residui;

g. i controlli e gli audit periodici.

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

1 Le unità amministrative valutano costantemente i rischi per i loro oggetti da proteggere e a tale proposito svolgono in particolare i seguenti compiti:

a. analizzare periodicamente minacce e vulnerabilità e valutano 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, le unità amministrative che forniscono prestazioni e gli organi di sicurezza della Confederazione informano le unità amministrative 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 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 non è in grado di adempiere una direttiva per un oggetto da proteggere necessita di un'autorizzazione rilasciata dal servizio che ha deciso la direttiva.

2 Il servizio specializzato della Confederazione per la sicurezza delle informazioni e i dipartimenti possono delegare l'autorizzazione di deroghe.

3 Se una deroga che rientra nell'ambito di competenza del servizio specializzato della Confederazione per la sicurezza delle informazioni riguarda anche direttive della Cancelleria federale sulla trasformazione digitale e la governance delle TIC, il servizio specializzato della Confederazione per la sicurezza delle informazioni sente in via preliminare il delegato TDT di cui all'articolo 4 capoverso 1 OTDI[6].

4 Le unità amministrative, i dipartimenti e il servizio specializzato della Confederazione per la sicurezza delle informazioni tengono ciascuno un registro delle autorizzazioni eccezionali che:

a. hanno rilasciato essi stessi;

b. sono state rilasciate per i loro oggetti da proteggere.

Art. 10 Collaborazione con terzi

(art. 9 LSIn)

1 Secondo le direttive di cui all'articolo 10 le unità amministrative valutano i rischi per i loro oggetti da proteggere che derivano dalla collaborazione con terzi e la loro dipendenza da terzi.

2 I servizi d'acquisto di cui agli articoli 9 e 10 dell'ordinanza del 24 ottobre 2012[7] concernente l'organizzazione degli acquisti pubblici dell'Amministrazione federale (OOAPub) partecipano alla valutazione e mettono a disposizione le informazioni necessarie.

3 Previa consultazione della Conferenza degli acquisti della Confederazione di cui all'articolo 24 OOAPub, il servizio specializzato della Confederazione per la sicurezza delle informazioni raccomanda quali disposizioni in materia di sicurezza delle informazioni devono essere previste nei contratti di acquisto e per prestazioni di servizio della Confederazione.

Art. 11 Formazione e sensibilizzazione

(art. 7 cpv. 1 e 20 cpv. 1 lett. c LSIn)

1 Le unità amministrative 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;

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

6 RS **172.010.58**
7 RS **172.056.15**

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, 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 assicura il coordinamento e 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 stabiliscono come notificare e gestire gli incidenti legati alla sicurezza e le lacune in materia di sicurezza. Stabiliscono chi decide in merito a misure immediate.

2 I fornitori di prestazioni notificano senza indugio alle unità amministrative beneficiarie delle loro prestazioni gli incidenti legati alla sicurezza e le lacune in materia di sicurezza individuati che li riguardano e forniscono loro sostegno nella gestione.

3 Il servizio specializzato della Confederazione per la sicurezza delle informazioni può fornire sostegno alle unità amministrative e ai dipartimenti nella gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza.

4 Quando si tratta di gestire incidenti legati alla sicurezza le unità amministrative verificano se occorre effettuare una notifica all'Incaricato federale della protezione dei dati e della trasparenza secondo la legislazione sulla protezione dei dati.

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 o dell'esercito;

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 il quale o la quale 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 di cui al 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 dell'incidente legato alla sicurezza o di una lacuna in materia di sicurezza. In tale contesto ha i compiti e le competenze seguenti:

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

b. può disporre misure immediate;

c. può impiegare specialisti esterni a scopo di sostegno;

d. informa la direzione delle unità amministrative e dei dipartimenti interessati in merito all'andamento.

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 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 All'interno di un piano annuale dei controlli e degli audit le unità amministrative e i dipartimenti stabiliscono le modalità con cui verificano 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 per la procedura di sicurezza relativa alle aziende di cui all'articolo 51 capoverso 2 LSIn.

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 e lo comunica 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 i dipartimenti e la Cancelleria federale 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.

2 Rilevano le informazioni necessarie a tale scopo presso le unità amministrative e i loro fornitori di prestazioni.

3 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.

4 Stabilisce le modalità per i rapporti dei fornitori interni di prestazioni di cui all'articolo 9 OTDI[8].

5 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 tutti i servizi di cui all'articolo 2 capoversi 1–3 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 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 le informazioni sono riunite in una collezione occorre verificare se quest'ultima deve essere classificata o assegnata a un livello di classificazione più elevato.

3 In presenza di domande di accesso a documenti ufficiali, il servizio competente verifica, indipendentemente da un'eventuale menzione di classificazione, se, conformemente alla legge sulla trasparenza del 17 dicembre 2004[9], l'accesso vada accordato, limitato, differito o negato.

Art. 17 Servizi incaricati della classificazione

(art. 12 LSIn)

1 Le persone e i servizi seguenti sono competenti per la classificazione e la declassificazione di informazioni:

a. i collaboratori della Confederazione nonché i militari: per supporti di informazioni che producono o che fanno produrre, e per informazioni che comunicano a voce;

b. i collaboratori di aziende che dispongono di una dichiarazione di sicurezza aziendale secondo l'articolo 61 LSIn: per supporti di informazioni che producono su incarico della Confederazione;

c. la persona responsabile del compito: per oggetti da proteggere di cui all'articolo 7 capoverso 2 lettera a.

8 RS **172.010.58**
9 RS **152.3**

2 All'interno di un catalogo di classificazione le unità amministrative, la Cancelleria federale e i dipartimenti stabiliscono in che modo classificare le informazioni che vengono trattate di frequente nel rispettivo settore di competenza.

3 Il servizio specializzato della Confederazione per la sicurezza delle informazioni verifica i cataloghi di classificazione di cui al capoverso 2 e in caso di necessità formula una raccomandazione.

4 Previa consultazione della Conferenza degli incaricati della sicurezza delle informazioni, stabilisce in che modo classificare le informazioni che vengono trattate di frequente nell'Amministrazione federale e nell'esercito.

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 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 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 per mesi.

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 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 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 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 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 tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti il trattamento di informazioni classificate e i requisiti organizzativi, tecnici, edili e riguardanti il personale per la loro protezione.

2 Consulta in via preliminare i seguenti servizi:

a. il servizio crittografico dell'esercito;

b. i servizi competenti per l'acquisto di beni nell'ambito della crittologia secondo l'articolo 10 capoverso 1 lettera d OOAPub[10]; e

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

3 Tiene conto degli standard internazionali in materia.

4 La Cancelleria federale disciplina il trattamento degli affari classificati del Consiglio federale.

5 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 le 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 possono decidere prescrizioni per operazioni o impieghi specifici dopo aver consultato il servizio specializzato della Confederazione per la sicurezza delle informazioni:

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 I servizi di cui al capoverso 1 fanno in modo che sia possibile individuare in modo equivocabile se si applicano le prescrizioni relative al trattamento semplificato.

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.

10 RS **172.056.15**

Art. 23 Accreditamento in materia di sicurezza di mezzi informatici
(art. 83 cpv. 1 lett. e LSIn)

1 I mezzi informatici sono soggetti ad accreditamento in materia di sicurezza prima di essere messi in servizio se è soddisfatta una delle condizioni seguenti:

a. vengono impiegati per compiti che riguardano più uffici in cui vengono trattate informazioni classificate «segreto»;

b. vengono impiegati per compiti che riguardano più autorità o dipartimenti in cui vengono trattate informazioni classificate «confidenziale»;

c. l'accreditamento in materia di sicurezza è necessario per la collaborazione a livello internazionale.

2 L'accreditamento in materia di sicurezza dimostra che i mezzi informatici soddisfano i requisiti minimi di sicurezza per il relativo livello di classificazione e che i rischi residui sono sostenibili secondo lo stato della tecnica.

3 In caso di cambiamenti sostanziali riguardo ai rischi o di cambiamenti sostanziali del mezzo informatico l'accreditamento viene ripetuto.

4 Se non è possibile rilasciare l'accreditamento in materia di sicurezza poiché il mezzo informatico non soddisfa i requisiti minimi di sicurezza, è il Consiglio federale a decidere in merito ai rischi residui.

5 Il servizio specializzato della Confederazione per la sicurezza delle informazioni svolge i compiti seguenti:

a. rilascia l'accreditamento in materia di sicurezza dopo aver consultato il servizio crittografico dell'esercito nonché i servizi di cui all'articolo 10 capoverso 1 lettera d OOAPub[11];

b. esclusivamente per sistemi militari può delegare la competenza per l'accreditamento in materia di sicurezza all'Aggruppamento Difesa.

6 Il [dipartimento competente] definisce la procedura di accreditamento in materia di 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 le informazioni classificate sono esposte a pericolo, sono andate perse o sono state usate in modo abusivo oppure che le 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.

11 RS **172.056.15**

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 nonché sempre nei casi in cui le informazioni vengono offerte all'Archivio federale per l'archiviazione.

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 fa in modo che sia garantita la sicurezza delle informazioni secondo la presente ordinanza.

3 Dopo la scadenza del termine di protezione la classificazione degli archivi viene meno. Una proroga del termine di protezione si fonda sull'articolo 14 dell'ordinanza sull'archiviazione dell'8 settembre 1999[12].

Sezione 5: Sicurezza nell'impiego di mezzi informatici

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

1 Le unità amministrative 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 Indicano i rischi che non possono essere adeguatamente ridotti (rischi residui).

4 I responsabili della sicurezza di cui all'articolo 36 decidono se i rischi residui vengono assunti. 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 verificano ogni anno se vi è stato un cambiamento sostanziale secondo il capoverso 5.

12 RS **152.11**

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 considerevole secondo l'articolo 19 o un danno tra 50 e 500 milioni di franchi.

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 almeno 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 applicabili a tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti i requisiti minimi per i relativi livelli di sicurezza secondo l'articolo 17 LSIn.

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, 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 I dipartimenti e la Cancelleria federale 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 assicurano che le responsabilità per la sicurezza informatica 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, della Cancelleria federale, 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 2, 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.

6 Il trattamento di dati personali nel quadro della vigilanza e del monitoraggio secondo il capoverso 4 si fonda sull'ordinanza del 22 febbraio 2012[13] sul trattamento di dati personali 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 emana istruzioni generali e astratte applicabili a tutti i servizi 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[14] 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 e 20 cpv. 1 lett. a e c LSIn)

1 Le unità amministrative assicurano che i collaboratori soggetti a un controllo di sicurezza relativo alle persone secondo l'ordinanza del …[15] 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 I collaboratori di cui al capoverso 1 sono tenuti a comunicare al loro datore di lavoro le circostanze nel loro contesto privato e professionale che compromettono 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, 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.

13 RS **172.010.442**
14 RS **172.010.59**
15 RS **128.xxx**

Art. 34 Misure di protezione fisica
(art. 22 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 emana istruzioni generali e astratte applicabili a tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti le misure minime necessarie 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; e

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

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

1 Le unità amministrative 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 I locali e i settori secondo il capoverso 1 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 tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti i requisiti di sicurezza per le zone di sicurezza e la loro istituzione.

Sezione 7: Organizzazione di sicurezza

Art. 36 Responsabili della sicurezza della Cancelleria federale e delle unità amministrative
(art. 7 cpv. 1 LSIn)

1 Il cancelliere della Confederazione, i segretari generali nonché i direttori delle unità amministrative dell'Amministrazione federale centrale e decentralizzata sono responsabili della sicurezza nel loro settore di competenza.

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

3 I responsabili della sicurezza della Cancelleria federale e delle unità amministrative 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 dell'Amministrazione federale centrale e decentralizzata 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
(art. 7 cpv. 1 LSIn)

1 Le unità amministrative designano un incaricato della sicurezza delle informazioni o diversi incaricati della sicurezza delle informazioni nonché il supplente o i supplenti.

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

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

b. elaborano le necessarie basi decisionali a destinazione dei responsabili della sicurezza e propongono loro la decisione di 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 propongono al responsabile della sicurezza 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 sulla procedura di sicurezza relativa alle aziende del …[16];

h. coordinano la notifica e 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 per l'approvazione;

j. su incarico del responsabile della sicurezza 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;

k. informano il responsabile della sicurezza su base semestrale in merito allo stato della sicurezza delle informazioni.

Art. 38 Sicurezza delle informazioni nei servizi standard
(art. 7 cpv. 1 LSIn)

1 Il delegato TDT è competente per la garanzia della sicurezza delle informazioni nei servizi standard secondo l'articolo 17 capoverso 1 lettera e OTDI[17].

2 Designa un incaricato della sicurezza delle informazioni o diversi incaricati della sicurezza delle informazioni e il supplente o i supplenti.

3 L'incaricato della sicurezza delle informazioni si occupa dei compiti di cui all'articolo 37 capoverso 2 per i servizi standard e informa l'Amministrazione federale e l'esercito in merito ai rischi.

Art. 39 Responsabilità in materia di sicurezza 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 delle unità amministrative;

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

c. vigilano sul SGSI delle unità amministrative e rilevano gli indicatori necessari a tale scopo;

16 RS **128.xxx**
17 RS **172.010.58**

d. stabiliscono ogni anno gli obiettivi in materia di sicurezza per le unità amministrative e verificano se sono stati raggiunti;

e. provvedono a una verifica basata sui rischi della sicurezza delle informazioni;

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 assumere compiti e competenze che la presente ordinanza attribuisce alle unità amministrative.

4 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 o dall'unità amministrativa.

5 Se il capo del dipartimento non decide diversamente, è il segretario generale su suo incarico a essere responsabile della sicurezza 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 a destinazione dei responsabili della sicurezza e propongono loro la decisione di misure;

c. coordinano la notifica e la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza che riguardano più unità amministrative;

d. rappresentano il dipartimento in organi specialistici;

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

f. controllano periodicamente e in caso di cambiamento o di uscita di un membro del Consiglio federale o del cancelliere della Confederazione se i supporti di dati classificati «segreto» sono disponibili e completi;

g. autorizzano l'avvio di controlli di sicurezza relativi alle persone presso terzi (art. 8 cpv. 2 lett. b OCSP[18]);

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

18 RS **128.xxx**

Art. 41 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 seguenti compiti 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.

2 Per valutare e migliorare lo stato della sicurezza delle informazioni della Confederazione può cercare minacce tecniche o vulnerabilità nell'infrastruttura informatica dell'Amministrazione federale e dell'esercito o in Internet; può incaricare altri servizi dell'Amministrazione federale o dell'esercito nonché terzi di tale attività.

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

4 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. può eseguire i controlli previsti dai trattati internazionali o commissionarli;

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 nel contesto internazionale secondo l'articolo 30 OCSP[19].

5 Il servizio specializzato della Confederazione per la sicurezza delle informazioni è attribuito al *[dipartimento competente]*.

Sezione 8: Costi e valutazione

Art. 42 Costi

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

19 RS ...

2 Le unità amministrative assicurano che questi costi vengano considerati in maniera adeguata e riportati in sede di pianificazione.

3 Per il rilascio e il recapito delle attestazioni di sicurezza nel contesto internazionale secondo l'articolo 30 OCSP[20] a persone che non svolgono un'attività sensibile sotto il profilo della sicurezza il servizio specializzato della Confederazione per la sicurezza delle informazioni riscuote un emolumento pari a 100 franchi.

Art. 43 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. 44 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, compresi dati personali, di cui al capoverso 1 nonché con organizzazioni nazionali, internazionali ed estere di diritto pubblico e privato se

a. non vengono violati gli obblighi del segreto legali o contrattuali; e

b. vengono rispettate le direttive della legislazione federale sulla protezione dei dati.

3 Se è necessario per gestire un incidente legato alla sicurezza o una lacuna in materia di sicurezza possono trattare o scambiare tra loro anche dati personali particolarmente degni di protezione concernenti l'identità o gli atti di persone che sono o potrebbero essere coinvolte nell'incidente o interessate dall'incidente.

Art. 45 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 particolarmente degni di protezione di cui all'articolo 44 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.

20 RS **128.xxx**

Art. 46 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 41 capoverso 4 lettera e;

b. per il rilascio e il recapito delle attestazioni di sicurezza nel contesto internazionale secondo l'art. 30 OCSP[21];

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

[2] Con i servizi di modulistica di cui al capoverso 1 possono essere trattati dati personali secondo l'allegato 2. Questi dati possono essere conservati al massimo per 10 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 particolarmente degni di protezione secondo l'articolo 44 capoverso 3 necessari per gestire incidenti legati alla sicurezza e lacune in materia di sicurezza.

[5] I dati di cui al capoverso 4 devono essere cancellati immediatamente dopo l'invio della notifica dal servizio di modulistica. Possono essere salvati temporaneamente per al massimo 24 ore prima dell'invio della notifica.

Sezione 10: Disposizioni finali

Art. 47 Abrogazione e modifica di altri atti normativi

[1] Sono abrogate le seguenti ordinanze:

a. l'ordinanza sui ciber-rischi del 27 maggio 2020[22];

b. l'ordinanza sulla protezione delle informazioni del 4 luglio 2007[23].

[2] La modifica di altri atti normativi è disciplinata nell'allegato 3.

Art. 48 Disposizioni transitorie

[1] Le direttive relative alla sicurezza informatica emanate dal Centro nazionale per la cibersicurezza e le deroghe da esso autorizzate prima dell'entrata in vigore della presente ordinanza rimangono applicabili per al massimo sei anni dopo l'entrata in vigore della presente ordinanza.

21 RS **128.xxx**
22 [RU **2020** 2107, **2020** 5871, **2021** 132]
23 [RU **2007** 3401, **2010** 3207, **2013** 1341, **2014** 3543, **2016** 1785, **2017** 7391, **2020** 6011]

2 Il servizio specializzato della Confederazione per la sicurezza delle informazioni decide in merito a modifiche di direttive e di deroghe autorizzate secondo il capoverso 1.

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 cinque anni al massimo dall'entrata in vigore della presente ordinanza.

4 Le unità amministrative e la Cancelleria federale devono creare il loro SGSI al massimo entro tre anni dall'entrata in vigore della presente ordinanza.

5 L'accreditamento in materia di sicurezza secondo l'articolo 23 non viene svolto per mezzi informatici che:

a. sono in uso prima dell'entrata in vigore della presente ordinanza;

b. sono in fase di sviluppo al momento dell'entrata in vigore della presente ordinanza, qualora comportasse un onere sproporzionato.

Art. 49 Entrata in vigore

La presente ordinanza entra in vigore il … 2023.

… In nome del Consiglio federale svizzero:

Il presidente della Confederazione, …
Il cancelliere della Confederazione, Walter Thurnherr

Allegato 1
(art. 2 cpv. 2 e 3)

Unità amministrative dell'Amministrazione federale decentralizzata alle quali si applicano l'ordinanza sulla sicurezza delle informazioni

1. Le unità amministrative che accedono a mezzi informatici dei fornitori interni di prestazioni TIC di cui all'articolo 9 OTDI[24], se questi sono assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28:

a. …

b. …

c. …

2. Le unità amministrative che impiegano mezzi informatici assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28:

a. …

b. …

c. …

3. Le unità amministrative che non rientrano tra quelle di cui all'articolo 2 capoverso 2 lettera a o b, ma che trattano informazioni classificate della Confederazione:

a. …

b. …

c. …

4. Altre unità amministrative (cfr. art. 2 cpv. 3):

a. …

b. …

c. …

24 RS **172.010.58**

Allegato 2
(art. 46 cpv. 2)

Trattamento dei dati in servizi di modulistica elettronica secondo l'articolo 46

Nei servizi di modulistica secondo l'articolo 46 possono essere trattati i seguenti dati personali:

1. Servizio di modulistica secondo l'articolo 46 capoverso 1 lettera a OSIn
   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. Cittadinanza/e*
      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 (*) vengono comunicate all'autorità di sicurezza estera.

2. Servizio di modulistica secondo l'articolo 46 capoverso 1 lettera b OSIn
   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. Cittadinanza/e
      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'allestimento dell'attestazione.

3. Servizio di modulistica secondo l'articolo 46 capoverso 1 lettera c OSIn
   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 (*) vengono comunicate all'autorità di sicurezza estera.

4. Servizio di modulistica secondo l'articolo 46 capoversi 3–5 OSIn

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 3
(art. 47 cpv. 2)

Modifica di altri atti normativi

I seguenti atti normativi vengono modificati come segue:

1. Ordinanza del 25 novembre 2020[25] sul coordinamento della trasformazione digitale e la governance delle TIC in seno all'Amministrazione federale

Art. 2 cpv. 2, frase introduttiva

2 Fatte salve disposizioni di diverso tenore previste dal diritto federale in materia di organizzazione, possono impegnarsi mediante un accordo con il settore Trasformazione digitale e governance delle TIC della Cancelleria federale (settore TDT della CaF) a rispettare la presente ordinanza, l'ordinanza sulla sicurezza delle informazioni del […][26] e l'ordinanza GEVER del 3 aprile 2019[27] nonché le direttive fondate sulle stesse:

2. Ordinanza del 7 marzo 2003 sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport[28]

Art. 3 cpv. 2

2 Il DDPS emana prescrizioni per garantire l'equipaggiamento dell'esercito.

Art. 6 lett. b

Abrogata

3. Ordinanza del 24 giugno 2009[29] sui contatti militari internazionali

Art. 4 lett. c

I servizi seguenti possono, nel loro settore di compiti, allacciare formalmente contatti militari internazionali senza l'autorizzazione del Protocollo militare:

c. il servizio specializzato della Confederazione per la sicurezza delle informazioni;

Art. 5 cpv. 1

25 RS **172.010.58**
26 RS …
27 RS **172.010.441**
28 RS **172.214.1**
29 RS **510.215**

[1] La consegna di informazioni classificate a persone e organi stranieri nonché l'accesso da parte di visitatori stranieri a informazioni militari classificate, a materiale classificato o a impianti militari in Svizzera si fondano sulle corrispondenti prescrizioni in materia di protezione delle informazioni, segnatamente:

a. il trattato internazionale secondo l'articolo 87 della legge sulla sicurezza delle informazioni del 20 dicembre 2020[30] applicabile nel caso concreto;

b. l'ordinanza del …[31] sui controlli di sicurezza relativi alle persone;

c. l'ordinanza del …[32] sulla sicurezza delle informazioni;

d. l'ordinanza del…[33] sulla procedura di sicurezza relativa alle aziende.

30 RS **128**
31 RS **...**
32 RS **...**
33 RS **...**