Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Istruzioni del Consiglio federale sulla sicurezza TIC nell'Amministrazione federale

del 16 gennaio 2019

Il Consiglio federale svizzero
emana le seguenti istruzioni:

1 Disposizioni generali

1.1 Oggetto

Le presenti istruzioni disciplinano, in esecuzione dell'articolo 14 lettera d dell'ordinanza del 9 dicembre 2011[1] concernente l'informatica e la telecomunicazione nell'Amministrazione federale (OIAF), i requisiti e le misure organizzative, in materia di personale e tecniche, al fine di garantire una protezione adeguata della confidenzialità, della disponibilità, dell'integrità e della tracciabilità degli oggetti da proteggere delle tecnologie dell'informazione e della comunicazione (TIC) dell'Amministrazione federale.

1.2 Campo d'applicazione

Il campo d'applicazione delle presenti istruzioni è retto dall'articolo 2 OIAF[2].

1.3 Definizioni

Nelle presenti istruzioni s'intende per:

a. *oggetti TIC da proteggere:* applicazioni, servizi, sistemi, reti, collezioni di dati, infrastrutture e prodotti TIC; più oggetti identici o connessi tra loro possono essere raggruppati in un solo oggetto TIC da proteggere;

b. *procedura di sicurezza:* processi e misure per garantire un'adeguata sicurezza TIC durante l'intero ciclo di vita di un oggetto TIC da proteggere;

c. *analisi del bisogno di protezione:* rilevamento dei requisiti di sicurezza degli oggetti TIC da proteggere;

1 RS **172.010.58**
2 RS **172.010.58**

d. *piano per la sicurezza dell'informazione e la protezione dei dati (piano SIPD):* descrizione delle misure di protezione e della loro attuazione per gli oggetti TIC da proteggere nonché dei rischi residui;

e. *rete:* infrastruttura che permette la comunicazione tra diversi sistemi TIC;

f. *zona:* un insieme logico di sistemi TIC che presentano requisiti di sicurezza simili e sottostanno alla stessa linea di condotta della zona;

g. *linea di condotta della zona:* descrizione, elaborata dal proprietario di una zona, dei requisiti e delle direttive applicabili ai sistemi TIC della zona, alla zona stessa e alla comunicazione interna ed esterna autorizzata per questa zona;

h. *modello di zona Confederazione:* modello generico per la costituzione di zone nell'Amministrazione federale;

i. *portafoglio TIC:* riepilogo uniforme dei progetti TIC previsti o in corso, nonché delle applicazioni in un determinato settore di competenze.

2 Competenze

2.1 Incaricato della sicurezza informatica

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

2 Gli ISID svolgono segnatamente i seguenti compiti:

a. coordinano tutti gli aspetti della sicurezza TIC all'interno dei dipartimenti o della Cancelleria federale nonché con i servizi sovradipartimentali e, nel quadro della sicurezza TIC, sono i principali interlocutori dell'Organo direzione informatica della Confederazione (ODIC);

b. elaborano le basi necessarie per l'attuazione delle direttive in materia di sicurezza TIC e per l'organizzazione a livello di dipartimento o della Cancelleria federale;

3 Ogni unità amministrativa designa il proprio incaricato della sicurezza informatica (ISIU).

4 Gli ISIU svolgono segnatamente i seguenti compiti:

a. coordinano tutti gli aspetti della sicurezza TIC all'interno dell'unità amministrativa nonché con i servizi dipartimentali e sono i principali interlocutori dell'ISID e delle organizzazioni di sicurezza dei fornitori di prestazioni;

b. elaborano le basi necessarie per l'attuazione delle direttive in materia di sicurezza TIC e per l'organizzazione a livello dell'unità amministrativa;

c. informano il responsabile dell'unità amministrativa almeno ogni sei mesi sullo stato attuale della sicurezza TIC all'interno dell'unità amministrativa.

5 I dipartimenti, la Cancelleria federale e le unità amministrative provvedono affinché gli incaricati della sicurezza informatica assumano i loro compiti senza conflitti

d'interessi. Essi disciplinano il rapporto tra l'ISID e l'ISIU, segnatamente la responsabilità tecnica per le questioni di sicurezza.

6 L'ODIC designa un incaricato della sicurezza informatica dei servizi standard (ISI SS). Questi assume i compiti di cui all'articolo 4 per i servizi TIC standard.

2.2 Beneficiari di prestazioni

1 In qualità di beneficiari di prestazioni, le unità amministrative provvedono all'applicazione della procedura di sicurezza.

2 Le persone che nell'unità amministrativa sono responsabili di un'applicazione, di un processo aziendale o di una collezione di dati definiscono in collaborazione con l'ISIU i requisiti di sicurezza per i loro oggetti TIC da proteggere. Le unità amministrative gestiscono il portafoglio TIC con i dati rilevanti per la sicurezza. I requisiti di sicurezza sono convenuti per scritto con i fornitori di prestazioni sia per lo sviluppo e l'esercizio sia per la messa fuori esercizio di mezzi TIC. Le unità amministrative documentano e verificano l'attuazione delle misure di sicurezza nonché la loro efficacia.

3 Le unità amministrative verificano periodicamente il bisogno di protezione degli oggetti TIC da proteggere e adeguano sia la documentazione sulla sicurezza sia le misure di sicurezza.

4 Esse provvedono affinché i collaboratori conoscano le competenze e i processi della sicurezza TIC nel loro ambito lavorativo, a seconda del livello gerarchico e della funzione.

5 I collaboratori dell'Amministrazione federale che utilizzano mezzi TIC sono responsabili del loro utilizzo sicuro. Le unità amministrative devono sensibilizzare e istruire i collaboratori sui temi legati alla sicurezza TIC sia al momento dell'assunzione sia periodicamente.

6 Le unità amministrative provvedono affinché le persone a cui non è applicabile l'OIAF[3] abbiano accesso all'infrastruttura TIC della Confederazione solo se si impegnano a rispettare le direttive in materia di sicurezza TIC.

7 D'intesa con l'ISID e l'ISIU, emanano direttive dettagliate o specifiche per un impiego più sicuro dei mezzi TIC e le aggiornano regolarmente; definiscono in particolare un processo per l'elaborazione degli incidenti riguardanti la sicurezza informatica.

2.3 Fornitori di prestazioni

1 Le direttive definite per i beneficiari di prestazioni di cui al numero 2.2 si applicano per analogia ai fornitori di prestazioni.

3 RS **172.010.58**

2 I fornitori di prestazioni applicano, documentano e verificano le misure necessarie per l'esercizio di mezzi TIC. Comunicano, in forma adeguata, i risultati ai beneficiari di prestazioni interessati.

3 Le responsabilità e il bisogno di protezione a livello aziendale devono essere definiti negli accordi di progetto e di prestazione tra i fornitori di prestazioni e i beneficiari di prestazioni. Occorre in particolare disciplinare le competenze decisionali per l'adozione di misure urgenti in caso di incidente.

4 I fornitori di prestazioni provvedono affinché siano in grado, mediante organizzazioni di sicurezza permanenti o ad hoc, di far fronte rapidamente ed efficacemente agli incidenti riguardanti la sicurezza TIC. Esse sono competenti di effettuare l'analisi tecnica degli incidenti e di coordinarne la risoluzione. Raccolgono informazioni tecniche e le valutano tenendo conto di eventuali eventi simili e informano l'ISID o l'ISIU competente.

3 Procedura di sicurezza

3.1 Direttive in materia di sicurezza

1 A complemento delle presenti istruzioni, l'ODIC emana direttive sulla procedura di sicurezza e sui relativi mezzi ausiliari a livello di Confederazione, segnatamente per quanto concerne:

a. l'analisi del bisogno di protezione;

b. l'elaborazione di un processo di verifica per ridurre lo spionaggio dei servizi di informazione;

c. la protezione TIC di base;

d. il piano SIPD.

2 Definisce il modello di zona Confederazione.

3.2 Analisi del bisogno di protezione, piano SIPD e valutazione dei rischi

1 Per i progetti TIC occorre dapprima eseguire un'analisi del bisogno di protezione. Occorre altresì individuare i casi rilevanti in termini di rischi, conformemente a un pertinente processo di verifica volto a ridurre lo spionaggio dei servizi di informazione (n. 3.1 cpv. 1 lett. b).

2 Gli oggetti TIC da proteggere esistenti devono essere stati sottoposti a un'analisi del bisogno di protezione valida.

3 I requisiti minimi di sicurezza (protezione TIC di base) sono attuati per tutti gli oggetti TIC da proteggere; l'attuazione deve essere documentata.

4 Se dall'analisi del bisogno di protezione risulta un bisogno di protezione elevato, in aggiunta alla documentazione relativa all'attuazione della protezione TIC di base deve essere elaborato un piano SIPD corredato di un'analisi dei rischi. Nell'elabora-

zione del piano SIPD si può rinviare a piani di sicurezza già esistenti relativi a tematiche specifiche.

5 Se vengono individuati casi rilevanti in termini di rischi secondo il processo di verifica per ridurre lo spionaggio dei servizi di informazione, tale processo deve essere svolto integralmente; l'attuazione deve essere documentata.

6 Le analisi del bisogno di protezione, la documentazione relativa all'attuazione della protezione TIC di base, la documentazione del processo di verifica per ridurre lo spionaggio dei servizi di informazione e i piani SIPD devono essere esaminati perlomeno dall'ISIU; per quanto riguarda i servizi standard TIC devono essere esaminati dall'ISI SS. Devono essere approvati dal committente o dai responsabili dei processi aziendali.

7 Se in una fornitura di prestazioni TIC il processo di verifica per ridurre lo spionaggio dei servizi di informazione rileva un'interconnessione con altri sistemi TIC che costituisce una potenziale minaccia, le unità amministrative competenti devono informare l'ODIC.

8 L'unità amministrativa che intende utilizzare nuove tecnologie dell'informazione e della comunicazione (hardware e software) o utilizzare in un nuovo ambito le tecnologie esistenti deve sottoporle a una valutazione dei rischi prima del loro impiego. Il risultato di questa valutazione deve essere presentato all'incaricato della sicurezza informatica competente e all'ODIC.

9 La documentazione sulla sicurezza è valida per cinque anni al massimo. Se l'oggetto TIC da proteggere o la situazione di minaccia subiscono modifiche rilevanti per la sicurezza, essa deve essere immediatamente aggiornata.

3.3 Standard internazionali

Le misure di sicurezza TIC si orientano agli attuali standard internazionali, in particolare agli standard ISO concernenti le procedure di sicurezza TIC.

3.4 Rischi residui

1 I rischi che non possono essere ridotti o possono essere ridotti soltanto in modo insufficiente (rischi residui) devono essere documentati e comunicati per scritto al committente, ai responsabili dei processi aziendali e alla direzione dell'unità amministrativa.

2 Spetta al responsabile dell'unità amministrativa competente decidere se assumere i rischi residui di cui viene a conoscenza.

3.5 Costi

I costi per la sicurezza TIC sono parte dei costi di progetto e di esercizio e devono essere debitamente considerati nella pianificazione.

4 Sicurezza della rete, competenze e direttive in materia di sicurezza

1 Possono essere costituite e gestite soltanto le zone conformi al modello di zona Confederazione e autorizzate dall'ODIC.

2 L'ODIC tiene un elenco di tutte le zone autorizzate. L'elenco contiene segnatamente:

a. il nome della zona;

b. il nome del proprietario della zona;

c. il rinvio alla linea di condotta della zona;

d. il nome del gestore della zona.

3 Tutte le zone devono disporre di una pertinente linea di condotta. Quest'ultima deve essere approvata dall'ODIC.

4 L'ODIC emana le ulteriori direttive sulla sicurezza della rete.

5 Disposizioni finali

5.1 Abrogazione di altre istruzioni

Le istruzioni del Consiglio federale del 1° luglio 2015[4] sulla sicurezza delle TIC nell'Amministrazione federale sono abrogate.

5.2 Disposizioni transitorie

1 Le analisi del bisogno di protezione e i piani SIPD esistenti al momento dell'entrata in vigore delle presenti istruzioni rimangono validi e devono essere aggiornati nell'ambito di verifiche e revisioni.

2 La procedura e il processo di verifica per ridurre lo spionaggio dei servizi di informazione di cui al numero 3.2 capoversi 1, 5, 6 e 7 non sono applicabili ai progetti TIC per i quali è stato conferito un mandato di progetto prima del 1° gennaio 2016. Gli oggetti TIC da proteggere che erano già in una fase HERMES[5] o in esercizio il 1° gennaio 2016 devono essere controllati dalle unità amministrative competenti e dai loro fornitori di prestazioni entro il 1° gennaio 2021.

3 Le zone che al momento dell'entrata in vigore delle presenti istruzioni adempiono le condizioni di cui al numero 4 capoverso 1 e che dispongono di una linea di condotta della zona[6] approvata dall'ODIC secondo il numero 4 capoverso 1 possono continuare ad essere gestite sulla base delle deroghe autorizzate (eccezioni).

4 FF **2015** 4787
5 www.hermes.admin.ch
6 Al riguardo si tratta del dominio di rete blu della *Shared Service Zone* (SSZ), della *Central Access Zone* (CAZ), della rete AVS/AI e dei domini di rete *della Law Enforcement Monitoring Facility* (LEMF).

4 Le reti che al momento dell'entrata in vigore delle presenti istruzioni sono in esercizio e non fanno parte di una zona conforme alle condizioni di cui al numero 4 capoverso 1 possono rimanere in esercizio, ma devono essere trasferite in una zona gestita secondo il numero 4 capoverso 1 in occasione della prossima riorganizzazione, al più tardi tuttavia dieci anni dopo l'entrata in vigore delle presenti istruzioni.

5.3 Entrata in vigore

Le presenti istruzioni entrano in vigore il 15 febbraio 2019.

16 gennaio 2019

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ueli Maurer
Il cancelliere della Confederazione, Walter Thurnherr