Istruzioni del Consiglio federale sulla sicurezza TIC nell'Amministrazione federale

del 1° luglio 2015

Il Consiglio federale svizzero
emana le seguenti istruzioni:

1 Disposizioni generali

1.1 Oggetto

Le presenti istruzioni, in esecuzione dell'articolo 14 lettera d dell'ordinanza del 9 dicembre 2011[1] concernente l'informatica e la telecomunicazione nell'Amministrazione federale (OIAF), disciplinano le misure organizzative, personali, tecniche ed edilizie, 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;

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;

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

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

f. *dominio (di rete):* unione logica di tutti i collegamenti e componenti di una rete;

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

g. *linea di condotta applicabile al dominio di rete:* regolamento delle condizioni per l'allacciamento e i requisiti per la comunicazione di diverse reti e diversi sistemi.

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;

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

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 costantemente il bisogno di protezione e adeguano in modo corrispondente le misure di sicurezza.

4 Esse provvedono affinché i collaboratori conoscano le competenze e i processi della sicurezza TIC nel loro ambito lavorativo e in funzione delle loro mansioni.

5 I collaboratori dell'Amministrazione federale che utilizzano mezzi TIC, o che ne affidano l'esercizio a terzi, sono responsabili del loro utilizzo sicuro. Le unità amministrative devono istruire e sensibilizzare 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.

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.

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

3 Le responsabilità e il bisogno di protezione a livello aziendale sono definiti negli accordi di progetto e di prestazioni tra i fornitori e i beneficiari di prestazioni.

3 Procedura di sicurezza

3.1 Direttive in materia di sicurezza

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 di base;

d. il piano SIPD.

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

3 RS **172.010.58**

pertinente processo di verifica volto a ridurre lo spionaggio dei servizi di informazione (n. 3.1 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 di base) sono attuati per tutti gli oggetti da proteggere; l'attuazione deve essere documentata.

4 Se dall'analisi del bisogno di protezione risulta un bisogno di protezione elevato, in aggiunta alla protezione di base deve essere definito un piano SIPD. A tal fine si può rinviare a piani di sicurezza già esistenti relativi a tematiche specifiche.

5 Se vengono rilevati 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, le direttive in materia di sicurezza più dettagliate, la documentazione del processo di verifica per ridurre lo spionaggio dei servizi di informazione e i piani SIPD devono essere esaminati per lo meno dall'ISIU ed 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 in un nuovo ambito nuove tecnologie dell'informazione e della comunicazione (hardware e software) o tecnologie esistenti deve sottoporle a un'analisi dei rischi prima del loro impiego. Il risultato della valutazione dei rischi deve essere presentato all'incaricato della sicurezza informatica competente e all'ODIC.

3.3 Standard internazionali

Le misure di sicurezza si orientano agli attuali standard ISO concernenti le procedure di sicurezza TIC.

3.4 Rischi residui

1 I rischi che non possono essere completamente eliminati (rischi residui) devono essere documentati e comunicati per scritto al committente e ai responsabili dei processi aziendali.

2 Spetta al responsabile dell'unità amministrativa competente decidere se prendere in considerazione rischi residui noti.

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 L'ODIC tiene un elenco di tutti i domini di rete gestiti per conto delle unità amministrative. L'elenco contiene in particolare:

a. i nomi dei domini di rete;

b. i titolari dei domini di rete;

c. il rinvio alla linea di condotta applicabile al dominio di rete;

d. gli accordi sui domini di rete con altri domini di rete.

2 Tutti i domini di rete devono disporre di una linea di condotta. Quest'ultima deve essere approvata dall'ODIC.

3 Gli accordi sui domini di rete conclusi tra unità dell'Amministrazione federale o tra unità dell'Amministrazione federale e terzi devono essere approvati dall'ODIC.

4 Qualora terzi vengano collegati direttamente a un dominio di rete della Confederazione, la competente unità amministrativa deve disciplinare e verificare regolarmente l'osservanza delle direttive in materia di sicurezza secondo le presenti istruzioni. Gli accordi devono essere approvati dall'ODIC.

5 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 14 agosto 2013[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 istruzioni del Consiglio federale del 14 agosto 2013[5] sulla sicurezza TIC nell'Amministrazione federale 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 secondo il numero 3.2 capoversi 1, 5, 6 e 7 sono applicabili a tutti i progetti TIC per i quali è stato impartito un mandato per avviare un progetto dopo che sono entrate in vigore le presenti istruzioni. Gli oggetti TIC da proteggere che al momento dell'entrata in vigore delle presenti istruzioni sono già in una fase HERMES[6] o in esercizio devono essere controllati entro cinque anni dalle unità amministrative competenti e dai loro fornitori di prestazioni.

4 FF **2013** 5771
5 FF **2013** 5771
6 www.hermes.admin.ch

5.3 Entrata in vigore

Le presenti istruzioni entrano in vigore il 1° gennaio 2016.

1° luglio 2015

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Simonetta Sommaruga
La cancelliera della Confederazione, Corina Casanova