Istruzioni del Consiglio federale sulla sicurezza TIC nell'Amministrazione federale

del 14 agosto 2013

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 disciplinato dall'articolo 2 OIAF.

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**

g. *linea di condotta applicabile al dominio di rete*: normativa 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 assumono segnatamente i seguenti compiti:

a. coordinano tutti gli aspetti della sicurezza TIC all'interno dei dipartimenti e 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 dipartimentale.

3 Le unità amministrative designano ciascuna un incaricato della sicurezza informatica (ISIU).

4 Gli ISIU assumono 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 beneficiarie 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 stabiliscono 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 devono essere convenuti per iscritto con i fornitori di prestazioni per lo sviluppo e l'esercizio così come 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 Le unità amministrative 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 uso sicuro. Le unità amministrative devono istruire e sensibilizzare i collaboratori sui temi della sicurezza TIC sia al momento dell'assunzione sia periodicamente.

6 Le unità amministrative provvedono affinché le persone a cui non è applicabile l'ordinanza sull'informatica nell'Amministrazione federale 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 progetti e prestazioni tra i fornitori e i beneficiari di prestazioni.

3 Procedura di sicurezza

3.1 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.

2 I progetti TIC esistenti devono essere stati sottoposti a un'analisi del bisogno di protezione valida.

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

4 Se dall'analisi del bisogno di protezione risulta un bisogno elevato, in aggiunta all'attuazione documentata dei requisiti minimi di sicurezza occorre definire un piano SIPD. Nella definizione di quest'ultimo si può rinviare a piani di sicurezza già esistenti relativi a tematiche specifiche.

5 Le analisi del bisogno di protezione, le ampie direttive in materia di sicurezza e i piani SIPD devono essere esaminati per lo meno dall'ISIU e devono essere approvati dal committente o dai responsabili dei processi aziendali.

6 Se un'unità amministrativa 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 al competente incaricato della sicurezza informatica e all'ODIC.

3.2 Direttive in materia di sicurezza

L'ODIC emana ulteriori direttive sulla procedura di sicurezza e i relativi mezzi ausiliari a livello di Confederazione, segnatamente per l'analisi del bisogno di protezione, per la protezione di base e per il piano SIPD.

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 iscritto al committente e ai responsabili dei processi aziendali.

2 La decisione se prendere in considerazione rischi residui noti spetta al responsabile della competente unità amministrativa.

3.5 Costi

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

4 Sicurezza della rete

4.1 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 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 istruzioni previgenti

Le istruzioni del 27 settembre 2004 del CIC sulla sicurezza informatica nell'Amministrazione federale sono abrogate.

5.2 Disposizioni transitorie

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

5.3 Entrata in vigore

Le presenti istruzioni entrano in vigore il 1° gennaio 2014.

14 agosto 2013

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ueli Maurer
La cancelliera della Confederazione, Corina Casanova