«Sicurezza dei prodotti e supply chain risk management nei settori della cibersicurezza e della ciberdifesa»

Rapporto del Consiglio federale
in adempimento dei postulati Dobler 19.3135 «Abbiamo sotto controllo la cibersicurezza nel settore degli acquisti dell'esercito?» e 19.3136 «Infrastrutture critiche. Abbiamo il controllo sui componenti hardware e software?» del 18 marzo 2019

Inhaltsverzeichnis

Management Summary

Oltre a comportare un grande beneficio, l’impiego delle tecnologie dell'informazione e della comunicazione (TIC) è connesso anche a rischi notevoli. Questi cosiddetti ciber-rischi vengono affrontati adottando misure diverse, tra cui la prevenzione di guasti e manipolazioni, il rafforzamento della resilienza o l’allestimento di dispositivi di difesa da ciberattacchi. Agli sforzi intrapresi per la riduzione dei ciber-rischi osta il fatto che finora non si è riusciti a migliorare adeguatamente la sicurezza dei prodotti TIC, che spesso presentano ancora numerose vulnerabilità.

L’applicazione di standard di sicurezza può aiutare a mitigare il problema. Il rapporto espone gli standard esistenti nel settore della sicurezza dei prodotti e del supply chain risk management, illustrando il loro carattere vincolante per la Confederazione e per i gestori di infrastrutture critiche. L’analisi evidenzia l'esistenza di numerosi standard in ambito di sicurezza dei prodotti e della loro applicazione, svariati dei quali trovano anche larga applicazione. Le direttive per il supply chain risk management nel settore della cibersicurezza sono invece decisamente meno sviluppate.

Il rapporto si china altresì sul quadro normativo per l’applicazione degli standard in seno all'Amministrazione federale e alle infrastrutture critiche. Al riguardo, il rapporto giunge alla conclusione che, per la Confederazione, le basi giuridiche per un'applicazione coerente degli standard in ambito di sicurezza dei prodotti TIC e di supply chain risk management sono presenti, mentre per le infrastrutture critiche esistono solo disposizioni isolate che consentono di dedurre il rispetto degli standard per la sicurezza TIC.

Il rapporto espone infine in che misura gli standard vengono effettivamente applicati nell’Amministrazione federale, nell’esercito e alle infrastrutture critiche. In seno all'Amministrazione federale e all’esercito esistono numerose direttive in materia di sicurezza e di applicazione sicura dei prodotti TIC. Riguardo agli standard per la sicurezza dei prodotti, il rapporto giunge alla conclusione che ci si dovrebbe focalizzare maggiormente su un’attuazione continua e su vasta scala delle direttive nonché sul controllo di tale attuazione piuttosto che sull’ulteriore sviluppo delle direttive e degli standard già ampiamente elaborati. Le direttive per il supply chain risk management nel settore della cibersicurezza sono invece decisamente meno sviluppate. Neppure esiste un fondamento giuridico che impone l’implementazione di una gestione sistematica dei rischi. La maggior parte di questi standard si focalizza sui processi e sui metodi, acquisendo così il carattere di istruzioni operative non vincolanti anziché di norme vincolanti.

Rispetto alla situazione vigente nell'Amministrazione federale, per le infrastrutture critiche esistono solo poche direttive vincolanti in materia di sicurezza e di applicazione sicura dei prodotti TIC. L’opzione più ovvia per una maggiore diffusione degli standard consiste nella creazione di nuove direttive giuridicamente vincolanti. Sarebbero concepibili anche dei rinvii agli standard in ambito di sicurezza dei prodotti. Altresì ipotizzabili sarebbero delle direttive per una gestione sicura dei prodotti TIC destinate ai gestori delle infrastrutture critiche. In linea di principio, potrebbero essere introdotte, mediante provvedimenti regolativi, anche direttive per il supply chain risk management.

1 Introduzione

In Svizzera la digitalizzazione procede a ritmo sostenuto. Nelle aziende e in seno alle autorità, l'interconnessione digitale è oggi all'ordine del giorno. Le tecnologie dell'informazione e della comunicazione (TIC) hanno assunto un'importanza tale che, qualora questi strumenti dovessero guastarsi o non funzionare più in modo corretto, nella nostra società non sarebbe praticamente più possibile erogare qualsivoglia prestazione di servizi. Oltre ad apportare grandi vantaggi, l'impiego delle TIC ha comportato anche l'insorgere di notevoli rischi, denominati ciber-rischi, per far fronte ai quali si adottano svariate misure. Con misure preventive di natura tecnica e organizzativa si cerca di impedire che le TIC si guastino o vengano manipolate. Con misure volte a rafforzare la resilienza si dovrebbe inoltre provvedere affinché un'organizzazione possa funzionare anche se le TIC dovessero guastarsi. In aggiunta a ciò, si allestiscono dispositivi di difesa per respingere eventuali ciberattacchi nei confronti delle TIC.
A questi sforzi per ridurre al minimo i ciber-rischi osta però il fatto che finora non si è riusciti a migliorare adeguatamente la sicurezza dei prodotti TIC che, infatti, presentano spesso ancora numerose vulnerabilità. Ciò è dovuto sia a ragioni economiche che politiche. Le ragioni politiche sono state illustrate da vari ricercatori già 20 anni or sono.[1] Anzitutto, il mercato dei prodotti TIC può essere definito come un'economia reticolare nella quale i consumatori acquisteranno un prodotto solo se partono dal presupposto che anche molti altri adotteranno la stessa decisione. Si dovrebbe così evitare il dispendio supplementare nell'ambito della collaborazione con i partner. Per i produttori è pertanto decisivo che il loro prodotto TIC trovi il più rapidamente possibile il maggior numero di utenti possibile, affermandosi come soluzione standard. Di conseguenza, i produttori cercano di introdurre il più rapidamente possibile il loro prodotto sul mercato, risolvendo eventuali problemi – ad esempio quello delle vulnerabilità – solo quando il prodotto si è affermato sul mercato.[2] Secondariamente, l'asimmetria informativa tra offerenti e acquirenti favorisce la carenza di sicurezza dei prodotti TIC. Poiché gli acquirenti non sono in grado di valutare la qualità dei prodotti al momento in cui maturano una decisione d'acquisto, gli offerenti non hanno alcuno stimolo di garantire in ogni caso la qualità. L'assenza di trasparenza in relazione alla sicurezza fa sì che gli offerenti non diano priorità alla sicurezza dei loro prodotti.[3]
Oltre a questi fattori economici, anche i fattori geopolitici acquistano importanza. I mercati per i prodotti TIC sono vieppiù considerati come area di interesse in termini di politica della sicurezza. Al più tardi al momento delle rivelazioni di Edward Snowden, nel 2013, anche il grande pubblico ha acquisito l'inconfutabile consapevolezza che i governi non hanno remore nell'esercitare un'influenza diretta sui fabbricanti di prodotti TIC, così da acquisire l'accesso a determinati dati. Ciò ha ulteriormente minato la fiducia nella sicurezza dei prodotti TIC e reso molti Stati consapevoli del fatto che la dipendenza della loro economia e della loro società dalle TIC, sviluppate soprattutto da produttori di nazioni aventi lo status di superpotenze, è problematica in termini di politica della sicurezza.
Né le caratteristiche del mercato delle TIC, né l'egemonia di pochi produttori di nazioni aventi lo status di superpotenza potranno essere modificate a breve-medio termine e i prodotti TIC non saranno mai assolutamente sicuri. Nonostante ciò, una valutazione delle possibilità di migliorare la sicurezza dei prodotti TIC nei settori critici per la Svizzera è doverosa. L'applicazione di standard di sicurezza può fornire un importante contributo in questo senso. Oggi, gli standard diffusi in materia di sicurezza delle TIC sono già molti e vengono correntemente sviluppati. Definendo criteri chiari e quantificabili per la sicurezza, questi standard incrementano la trasparenza e aiutano a far sì che la sicurezza assurga a criterio di qualità accertabile. Richieste sistematiche di standard da parte di aziende e autorità aumenteranno la pressione sui produttori spingendoli a tenere in maggior considerazione l'aspetto della sicurezza.

[1] GORDON/LOEB: "The economics of information security investment", ACM Transactions on Privacy and Security Volume 5, Issue 4, 2002; ANDERSON/MOORE: "The economics of information security", Science, Vol. 314, 2006, pag. 610-613.
[2] SHAPIRO/VARIAN: "Information Rules. A Strategic Guide to the Network Economy", Boston, Harvard Business School Press, 1998.
[3] GEORGE A. AKERLOF: The market for 'lemons': Quality, uncertainty and the market mechanism. The Quarterly Journal of Economics, Vol. 84, 1970, pag. 488–500;
RAINER BÖHME: A Comparison of Market Approaches to Software Vulnerability disclosure, in: G. Müller (Ed): Emerging Trends in Information and Communication Security, ETRICS 2006, pag. 298-311; part of the Lecture Notes in Computer Science book series (LNCS, volume 3995), Springer, Berlin, Heidelberg

Il presente rapporto si propone di esporre quali sono le misure attuate dalla Confederazione, e in particolare dall'esercito, quando si tratta di effettuare acquisti rilevanti per la sicurezza, quali sono le misure che adottano i gestori di infrastrutture critiche nonché dove sussiste una necessità di intervento.

1.1 Situazione di partenza

La «Strategia nazionale per la protezione della Svizzera contro i ciber-rischi 2018 – 2022» (SNPC)[4] descrive le misure adottate dalla Confederazione e dai Cantoni nonché dall'economia e dalle scuole universitarie per ridurre i ciber-rischi esistenti. Essa comprende misure volte a standardizzare e favorire la resilienza delle infrastrutture critiche nei confronti dei ciber-rischi, senza tuttavia chinarsi esplicitamente sui rischi specifici delle catene di fornitura, il cosiddetto «supply chain risk». Un riferimento concreto alla sicurezza delle catene di fornitura e all'importanza degli standard internazionali è invece insito nella nuova «Strategia Ciber DDPS» del marzo 2021, che illustra il contributo del DDPS alla sovraordinata SNPC.[5]
Anche la «Strategia nazionale per la protezione delle infrastrutture critiche 2018 – 2022» (PIC)[6] affronta la questione dei rischi nelle catene di fornitura e dell'importanza degli standard nel quadro di misure volte a un esame generale delle direttive e all'incentivazione della resilienza.
L'analisi condotta nel presente rapporto e le conoscenze che ne sono emerse vanno a integrare il contesto strategico esistente e dovrebbero contribuire a integrare le strategie in relazione alla gestione dei rischi nel settore «Supply chain».

1.2 Mandato

Il presente rapporto risponde ai postulati Dobler 19.3135 e 19.3136, trasmessi in data 21 giugno 2019. Il testo dei postulati è il seguente:

- **Postulato 19.3135 «Abbiamo sotto controllo la cibersicurezza nel settore degli acquisti dell'esercito?»**
  L'esercizio affidabile dei sistemi d'arma e delle infrastrutture dell'Esercito svizzero è decisivo ai fini della sicurezza nazionale. L'esercito acquista sistemi d'arma e sistemi infrastrutturali da diversi fornitori nazionali e internazionali. La disponibilità, la confidenzialità e l'integrità delle componenti ciberfisiche[7] dei sistemi d'arma e dei sistemi infrastrutturali diventano sempre più il tallone d'Achille per la prontezza all'impiego e la capacità di resistenza delle truppe di terra svizzere e delle Forze aeree. In particolare l'integrità delle forniture digitali (accessi non documentati, malfunzionamenti impiantati) destano preoccupazioni.
  Il Consiglio federale è incaricato di verificare e di elaborare un rapporto sugli standard nazionali e internazionali applicabili (ad. es. NIST Cyber Security Framework, ISO, Common Criteria, NIST 800-161, EU4, EU5, FIPS) al Vendor risk management e alla sicurezza dei prodotti delle componenti tecniche dell'esercito, in particolare delle componenti ciberfisiche in rete. Il rapporto dovrebbe, tra l'altro, incentrarsi sui controlli rilevanti per la sicurezza nel settore degli acquisti. Occorre chiarire se le direttive attuali (OMC compresa) sono sufficienti per ottemperare alle maggiori esigenze in materia di sicurezza a seguito di nuove ciberminacce. In tale contesto si

[4] Il Consiglio federale svizzero, Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC) 2018 – 2022 del 18 aprile 2018, https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf
[5] Dipartimento della difesa, della protezione della popolazione e dello sport, Strategia Ciber DDPS; marzo 2021, https://www.newsd.admin.ch/newsd/message/attachments/66200.pdf
[6] Il Consiglio federale svizzero, Strategia nazionale per la protezione delle infrastrutture critiche 2018-2022 dell'8 dicembre 2017 (PIC, FF 2018 503), https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/nationalestrategie/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/73_1460987489220.download/natstratski2018-2022_de.pdf
[7] Il termine "ciberfisico" designa il collegamento tra il mondo digitale e quello fisico. In un sistema ciberfisico, i componenti meccanici sono collegati fra loro mediante tramite reti e moderni strumenti informatici.

pone in ultima analisi anche la domanda se l'Esercito svizzero, compresi i suoi partner nell'ambito della politica di sicurezza, alla luce delle circostanze (ad es. codice sorgente sconosciuto per prodotti di offerenti stranieri) sia davvero in grado di garantire la sovranità della Svizzera. Sulla base delle analisi il Consiglio federale è chiamato a valutare se le misure attuali siano o meno sufficienti per registrare i rischi, quantificarli e ridurli a un livello accettabile.

- **Postulato 19.3136 «Infrastrutture critiche. Abbiamo il controllo sui componenti hardware e software?»**
  L'affidabilità delle infrastrutture critiche della Svizzera è fondamentale per l'approvvigionamento e la sicurezza a livello nazionale. I gestori delle infrastrutture critiche acquistano sistemi e componenti TIC da diversi fornitori nazionali e internazionali. Le nostre infrastrutture digitali e i loro sottocomponenti provengono quindi da una moltitudine di fornitori.
  La complessità che ne deriva comporta ciber-rischi che mettono a repentaglio la disponibilità, la confidenzialità e l'integrità delle infrastrutture critiche svizzere e la sicurezza dell'approvvigionamento nazionale. In particolare, l'integrità degli oggetti digitali (accessi non documentati, introduzione di vulnerabilità) è motivo di preoccupazione.
  Il Consiglio federale è incaricato di esaminare gli standard nazionali e internazionali (ad es. NIST Cybersecurity Framework, ISO, Common Criteria, NIST 800-161, EU4, EU5, FIPS) applicabili alla gestione del rischio di fornitura e alla sicurezza dei sistemi tecnici, in particolare di quelli interconnessi, e di presentare un rapporto al riguardo. Tale rapporto dovrebbe inoltre descrivere la validità degli standard nonché la loro applicazione e osservanza per tutti gli aspetti relativi alle infrastrutture critiche svizzere e ai mezzi necessari per il loro funzionamento.
  Una volta disponibile tale rapporto, il Consiglio federale dovrà valutare se le misure attuali sono sufficienti per rilevare e misurare i rischi e ridurli a un livello accettabile.

Oltre a rispondere a questi due postulati, il rapporto si occupa anche delle richieste emerse dal working paper «Supply Chain Security»[8] della Commissione per la cibersicurezza di ICTSwitzerland[9] del settembre 2019. Le richieste ivi formulate di condizioni contrattuali orientate specificamente alla problematica della catena di fornitura, di requisiti minimi in ambito di sicurezza dei prodotti e di un centro di controllo per la cibersicurezza sono discusse brevemente nel capitolo conclusivo del rapporto quali possibili misure per la minimizzazione dei rischi nelle catene di fornitura digitali.

Dopo aver introdotto alla tematica, il rapporto descrive, al capitolo 2, i più importanti standard nei settori della sicurezza dei prodotti TIC e del loro Supply Chain Risk Management (SCRM). Il capitolo 3 illustra quali sono le basi giuridiche presenti per l'applicazione di questi standard in Svizzera, distinguendo tra quelle per la Confederazione, per i Cantoni e i comuni e quelle per i soggetti di diritto privato che gestiscono infrastrutture critiche. Il capitolo 4 descrive dove e come si applicano concretamente gli standard. Al capitolo 5 sono infine sintetizzate le conoscenze acquisite, discusse le possibili misure da adottare per una migliore applicazione degli standard in materia di sicurezza dei prodotti e SCRM per prodotti TIC e si volge uno sguardo prospettico all'ulteriore modo di procedere.

1.3 Spiegazione delle definizioni

Qui di seguito, ci proponiamo di spiegare brevemente le definizioni fondamentali per la comprensione del rapporto.

[8] ICTswitzerland: Supply Chain Security, Analyse & Massnahmen zur Sicherung der digitalen Lieferkette (Analisi & misure operative per la messa in sicurezza della catena di fornitura digitale), Gruppo di lavoro Supply Chain Security della Commissione per la cibersicurezza, settembre 2019, https://digitalswitzerland.com/wp-content/uploads/2021/08/White_Paper_Supply_Chain_Security_2019_09_25_DE.pdf
[9] L'associazione mantello ICTswitzerland, in data 01.01.2021, si è fusionata con Digitalswitzerland assumendone anche il nome. La Commissione per la cibersicurezza proseguirà la sua attività anche nella nuova organizzazione frutto della fusione.

1.3.1 Norme e standard

Nell'uso della lingua italiana, la confusione terminologica per quanto riguarda l'impiego di queste due espressioni è andata vieppiù aumentando, cosicché oggi vengono spesso usate praticamente come sinonimi. Il motivo di ciò dovrebbe risiedere, perlomeno parzialmente, nel fatto che in inglese si impiega il termine unitario *standard* sia per *norma* che per *standard.*
Per poter gestire il problema della diversità di utilizzo di questo termine nella lingua, nel settore della tecnica e delle scienze naturali si usa *standard* come termine generale.[10] Poiché nel settore delle TIC trovano prevalentemente applicazione gli standard internazionali e la terminologia in lingua inglese ivi associata, nel presente rapporto si adotterà quest'accezione linguistica utilizzando in linea di massima solo il termine *standard*.

1.3.2 Infrastrutture critiche (IC)

Nella Strategia nazionale PIC, il concetto di IC è definito come segue: Per «infrastrutture critiche» (IC) s'intendono processi, sistemi e installazioni essenziali per il funzionamento dell'economia e per il benessere della popolazione.[11]
Per la Svizzera lo spettro delle IC comprende i seguenti ambiti/settori: autorità ufficiali, energia, smaltimento, finanze, sanità, informazione e comunicazione, alimentazione, sicurezza pubblica, trasporti.

1.3.3 Ciber-rischi, cibersicurezza, ciberdifesa

Nel presente rapporto, le definizioni relative ai ciber-rischi, vengono impiegate conformemente alla terminologia dell'Ordinanza federale sui ciber-rischi[12]. Le definizioni e i settori a cui fare riferimento qui riportati sono i seguenti:

- **ciber-rischio:** il pericolo di un evento (valutato in base al prodotto della probabilità che si realizzi e della portata del danno) che compromette la confidenzialità, l'integrità, l'accessibilità o la tracciabilità di dati o che può causare disfunzioni**;**
- **settore della cibersicurezza:** comprende tutte le misure volte a prevenire e gestire gli incidenti a migliorare la resilienza ai ciber-rischi, intensificando a tale scopo la collaborazione internazionale;
- **settore della ciberdifesa:** comprende tutte le misure militari e del Servizio delle attività informative che servono a proteggere i sistemi critici per la difesa nazionale, a respingere i ciberattacchi, a garantire l'efficienza operativa dell'esercito in ogni situazione e a creare le capacità e le competenze per fornire un supporto sussidiario alle autorità civili; vi rientrano anche le misure attive volte a individuare le minacce, identificare gli aggressori nonché ostacolare e bloccare gli attacchi.

1.3.4 Sicurezza dei prodotti

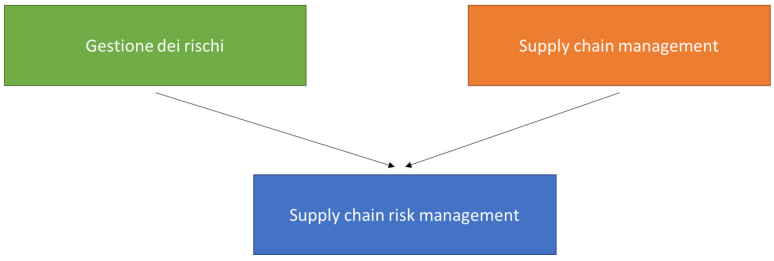
Il concetto di «sicurezza dei prodotti» si riferisce soprattutto a prodotti fisici. In questo ambito, la massima priorità è data alla sicurezza e alla salute degli utenti e dei terzi mentre fanno uso dei prodotti. La legge federale sulla sicurezza dei prodotti (LSPro))[13] esige che i prodotti messi in commercio soddisfino i requisiti di base in materia di sicurezza e salute. havvllmjlLa La concretizzazione tecnica ha luogo mediante rinvio alle norme tecniche. Si presuppone che questi requisiti siano soddisfatti se i prodotti

[10] Con questa premessa, uno standard de jure corrisponderebbe al termine *norma*. Volendo operare una distinzione, per rendere conto al termine *standard*, si potrebbe parlare di standard de facto o quasi-standard.
[11] Strategia nazionale per la protezione delle infrastrutture critiche 2018-2022 dell'8 dicembre 2017 (PIC, FF 2018 503)
[12] Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale del 27 maggio 2020 (Ordinanza sui ciber-rischi; OCiber; RS 120.73)
[13] Legge federale sulla sicurezza dei prodotti (LSPro) del 12 giugno 2009 (RS 930.11)

sono consoni alle norme o agli standard in ambito tecnico e/o organizzativo sviluppati dai comitati specializzati (presunzione di conformità). [14]
Quando si parla di sicurezza dei prodotti TIC ci si riferisce per contro al fatto che l'impiego di tali prodotti non metta a rischio la confidenzialità, l'integrità, l'accessibilità o la tracciabilità di dati. A differenza di quanto avviene per molti prodotti fisici, giudicare come i prodotti TIC debbano essere impiegati per poter risultare sicuri è decisamente più difficile. Di conseguenza, per quanto riguarda la sicurezza dei prodotti TIC, si devono sempre integrare anche le direttive per il loro impiego. In questo ambito, la sicurezza dei prodotti è quindi intesa come termine collettivo che include sia la sicurezza dei prodotti TIC stessi, sia il loro impiego sicuro e la loro integrazione nell'infrastruttura TIC.

1.3.5 Supply chain risk management

Il «vendor risk management» a cui si accenna nei postulati è parte integrante della gestione dei rischi delle catene di fornitura, detta anche «supply chain risk management». Per integrare il rapporto negli attuali dibattiti in materia di SCRM nell'ambito della cibersicurezza, invece di vendor risk management si usa la definizione di più ampia portata SCRM. Alla base di questa definizione ci sono concetti propri della gestione aziendale e delle organizzazioni sviluppati nel corso degli anni:



- **Gestione dei rischi:** la gestione dei rischi designa il processo sistematico di identificazione, analisi, valutazione e gestione dei rischi.[15]
- **Supply chain management (gestione della catena di fornitura):** questo concetto designa l'allestimento e la gestione di catene logistiche integrate (flussi di materiali e di informazioni) lungo l'intero processo di creazione di valore, dall'estrazione della materia prima, ai livelli di finitura fino al consumatore finale.[16]
- **Supply chain risk management (gestione dei rischi della catena di fornitura):** il SCRM combina la gestione dei rischi con la gestione della catena di fornitura. Qui si tratta di identificare, analizzare, valutare e ridurre i rischi intrinseci alla catena di fornitura.[17]
  Definizioni affini e simili a SCRM sono:
  - Vendor risk management: per vendor risk management si intende quella parte di SCRM che si riferisce alla valutazione dei venditori di prodotti e servizi TIC.
  - Third party risk management: anche questa definizione si riferisce a un sottoinsieme facente parte del SCRM, ma non si focalizza solo sui venditori di prodotti e servizi TIC bensì su tutti i terzi aventi rapporti contrattuali con l'organizzazione.

I rischi riferiti ai fornitori, includono anche il fatto che spesso i fornitori di servizi sono società straniere operanti a livello internazionale e soggette al quadro normativo del loro Stato di appartenenza. Poiché negli ultimi anni la concorrenza internazionale per aggiudicarsi influenza in campo digitale si è inasprita notevolmente, i rischi di un'influenza diretta degli Stati su questi fornitori sono aumentati.
Infine, però, si tratta anche di rischi concernenti la qualità e la disponibilità della prestazione stessa del servizio. Non tutti i fornitori di servizi possono garantire in ugual misura il mantenimento a lungo termine della loro prestazione. Soprattutto per i piccoli fornitori di servizi c'è il rischio che la ditta non possa adempiere al suo mandato. Si deve anche tener presente che le società possono dipendere molto dal know-how di singoli collaboratori che occupano posizioni chiave ciò che a sua volta fa aumentare il

[14] Ciò è conforme alla legislazione europea sulla sicurezza dei prodotti: Il "Nuovo approccio" del 1985, aggiornato e integrato nel 2008 dal "Nuovo quadro legislativo", costituisce il quadro normativo per la regolamentazione europea dei prodotti. In questo contesto, per quanto riguarda le direttive per un prodotto, la legislazione europea si limita alla definizione dei requisiti di base. La concretizzazione ha luogo mediante norme armonizzate o altre specifiche tecniche (riferimento normativo). La Svizzera ha per lo più fatto proprie le direttive "Nuovo approccio" dell'Unione europea.
[15] ISO 31000:2018
[16] Gabler Wirtschaftslexikon
[17] NIST Special Publication Supply Chain Risk Management 800-161, p. 2

rischio di una mancata prestazione. Non da ultimo, è anche possibile che i fornitori di servizi siano loro stessi vittime di attacchi all'integrità della loro prestazione di servizio. Per l'aggressore questo può essere un metodo allettante per contaminare i sistemi di molte aziende con un unico intervento mirato.

2 Standard nell'ambito della sicurezza dei prodotti e del SCRM per i prodotti TIC

Nel campo dell'informatica e delle telecomunicazioni, gli standard giocano da sempre un ruolo decisivo poiché consentono la compatibilità dei dispositivi e semplificano notevolmente l'utilizzo di dispositivi di produttori diversi. Molti di questi standard vengono definiti direttamente dai produttori di maggior peso e imposti sul mercato. Parallelamente hanno luogo i processi di standardizzazione propriamente detti, nei quali i produttori, gli utenti ma anche autorità e organizzazioni internazionali si accordano congiuntamente sul rispetto di determinati standard. In un contesto economico globalizzato e dinamico come quello delle TIC, tali processi sono il tentativo di accordarsi sul rispetto di regole in quegli ambiti caratterizzati da un grande interesse comune e da una forte interdipendenza. La sicurezza dei mezzi TIC impiegati è uno di questi ambiti. I dispositivi non sicuri pregiudicano la sicurezza di tutti gli altri dispositivi collegati alla rete comune. Per questo, sono stati presto sviluppati degli standard per valutare la sicurezza dei mezzi informatici. Già nel 1983, il governo americano pubblicò lo standard TCSEC («Trusted Computer System Evaluation Criteria») che, per gran parte, è applicato ancora oggi tramite il cosiddetto standard «Common Criteria». Accanto a questi standard orientati alla sicurezza dei prodotti, sono stati e sono tuttora sviluppati svariati standard per i processi di sicurezza delle TIC. Ciò perché una gran parte dei problemi di sicurezza non sono dovuti in primo luogo a difetti dei prodotti impiegati, ma ad applicazioni errate o a un'attuazione lacunosa delle misure di protezione.
Questi sviluppi hanno fatto sì che per i prodotti e i processi riguardanti la sicurezza delle TIC esista un'ampia gamma di standard. Tuttavia, per l'utente spesso non è facile conoscere quelli più adatti e valutare i futuri sviluppi nel campo della standardizzazione. Inoltre, solo pochi standard hanno potuto imporsi a livello mondiale. Pertanto, l'auspicata quasi obbligatorietà degli standard di sicurezza in forza di un'applicazione globale è stata raramente raggiunta.

2.1 Obbligatorietà degli standard

Per gli standard non c'è un passaggio in giudicato poiché vengono emessi da organizzazioni di diritto privato senza competenze legislative. L'applicazione degli standard è quindi facoltativa o una reazione a una pressione di fatto. Essi diventano vincolanti solo se il loro rispetto è imperativamente prescritto dalla legislazione o se sono oggetto di accordi tra le parti contraenti. Gli standard servono anche alla concretizzazione di concetti giuridici altrimenti imprecisi, come ad esempio il concetto di *stato della tecnica*, e possono così contribuire direttamente alla certezza del diritto nonostante l'assenza di obbligatorietà. In molti casi, sono considerati regole inequivocabili e riconosciute della tecnica e il rispetto di tali regole è un aspetto importante quando si tratta di addurre la prova della regolarità di un comportamento.

2.2 Standard nell'ambito di sicurezza dei prodotti

L'elenco seguente, non esaustivo, riporta alcuni degli standard più frequentemente applicati nell'ambito della cibersicurezza, ciascuno con la specificazione dell'organizzazione che lo emana e una descrizione delle più importanti caratteristiche applicative:

Denominazione	**Applicazione**
NIST Cybersecurity Framework *(National Institute of Standards and Technology, U.S. Department of Commerce)*	Standard generale di cibersicurezza che si riferisce genericamente a tutti i tipi di ciber-rischi.
ISO/IEC 2700x *(International Organization for Standardization / International Electrotechnical Commission)*	L'Organizzazione internazionale per la standardizzazione (ISO) pubblica diversi standard reciprocamente complementari in materia di sicurezza informatica, designati come «famiglia 2700x». Quello maggiormente conosciuto è lo standard ISO 27001. Esso specifica i requisiti per l'allestimento, l'implementazione, il mantenimento e il miglioramento corrente di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) documentato, tenendo conto del contesto di un'organizzazione.
COBIT *(ISACA; Information Systems Audit and Control Association)*	COBIT (Control Objectives for Information and Related Technology) è un framework internazionalmente riconosciuto per la governance e il management dell'IT aziendale. COBIT è stato creato dall'organizzazione non profit ISACA e sviluppato da esperti per soddisfare le esigenze di dirigenti ed esperti di TIC. Il framework abbina governance d'impresa e tecniche di gestione offrendo principi, prassi, modelli e strumenti di analisi in grado di aiutare gli utenti a incrementare coerentemente il valore dei loro sistemi TIC e la fiducia negli stessi.
Common Criteria (CC) *Designazione completa: Common Criteria for Information Technology Security Evaluation* *(Common Criteria Implementation Board)*	Common Criteria è uno standard internazionale che specifica i criteri generali per la valutazione della sicurezza delle tecnologie dell'informazione e che aiuta a valutare e verificare la sicurezza dei prodotti software e hardware sulla base di criteri generali. I CC sono stati sviluppati nell'ambito della cooperazione internazionale e uniformano standard nazionali antecedentemente diversi (CTCPE per il Canada, ITSEC per l'Europa, TCSEC per gli Stati Uniti) creando una base comune per la valutazione della sicurezza dei dati. Con l'adozione della norma ISO/IEC 15408, i CC sono assurti nel 1999 a standard di validità generale riconosciuto in tutto il mondo. I common criteria descrivono diversi requisiti di sicurezza funzionali per raggiungere gli obiettivi di sicurezza precedentemente definiti. Nel contempo, essi definiscono i requisiti di verifica che provvedono a far acquisire la fiducia nella sicurezza del prodotto. Un ulteriore obiettivo della certificazione CC consiste nell'integrazione di questi requisiti negli accordi internazionali, così da poter fare a meno, per i prodotti TIC, di certificazioni multiple sulla base di standard nazionali diversi.
Standard BSI *(Deutsches Bundesamt für Sicherheit in der Informationstechnik – BSI) (Autorità tedesca per la sicurezza nell'ambito della tecnologia dell'informazione)*	Gli standard BSI 200-1, 200-2 e 200-3 sono parti integranti basilari della metodologia di protezione di base TIC del BSI. I contenuti degli standard BSI sono misure, modi di procedere e raccomandazioni vertenti su procedure, metodi e processi relativi a vari aspetti della sicurezza delle informazioni presso aziende e autorità. L'obiettivo di questi standard consiste nel rendere più sicuri i processi aziendali e

	nel proteggere dati introducendo e implementando gradualmente un ISMS. I contenuti sono interamente compatibili con lo standard ISO/IEC 27001 e tengono conto delle raccomandazioni dello standard ISO/IEC 27002. Anche la terminologia è simile a quella degli standard ISO.
Federal Information Processing Standards (FIPS) *(National Institute of Standards and Technology, U.S. Department of Commerce)*	I FIPS sono standard minimi del governo statunitense resi noti pubblicamente, sviluppati per l'applicazione in sistemi di computer di autorità governative e mandatari governativi non militari degli Stati Uniti d'America. Questi standard minimi soddisfano i requisiti di vari campi d'applicazione e saranno applicati finché non esisteranno standard industriali adeguati. I produttori TIC applicano i FIPS su base facoltativa anche al di fuori dell'attività governativa. Molte specifiche FIPS poggiano sulla modifica di standard generalmente applicati (ad es. ANSI, IEEE, ISO).
Direttive ENISA *(European Union Agency for Cybersecurity (ENISA); in precedenza: European Network and Information Security Agency)*	L'ENISA ha pubblicato una serie di diverse direttive in materia di sicurezza delle reti e delle informazioni, come ad esempio: - National Cyber Security Strategy (NCSS) Good Practice Guide - Good Practice Guide on Incident Reporting - Technical Guideline on Security Measures
Standard minimo per il miglioramento della resilienza delle TIC (Standard minimo per le TIC) *(Ufficio federale per l'approvvigionamento economico del Paese, UFAE)*	Standard generale di cibersicurezza che si riferisce genericamente a tutti i tipi di ciber-rischi (basato sul NIST Cybersecurity Framework; vedi sopra).

2.3 Standard in materia di SCRM

In ambito di SCRM, con riferimento alla cibersicurezza, ci sono decisamente meno standard consolidati. Alcuni degli standard in materia di sicurezza delle TIC sottolineano anche l'importanza del SCRM, fornendo tuttavia solo poche direttive concrete. Norme vincolanti per l'applicazione degli standard vengono quindi emanate solo per aspetti parziali del SCRM. Ne sono un esempio gli esami e le certificazioni dei prodotti prescritti in sede di acquisto.[18]

In relazione al SCRM, particolare importanza è attribuita agli standard seguenti:

Denominazione	**Applicazione**
NIST Special Publication 800-161 «Supply Chain Risk Management Practices for Federal Information Systems and Organizations»	Sviluppo e implementazione di strategie, misure e controlli per la gestione dei rischi intrinseci alla catena di fornitura. Questa pubblicazione offre alle autorità federali una guida per l'identificazione, la valutazione e la riduzione dei rischi della catena di fornitura delle TIC, a tutti i livelli della loro organizzazione.

[18] In Svizzera, ad esempio, in base all'Ordinanza sull'approvvigionamento elettrico (OAEl), i sistemi di misurazione intelligenti (smartmeter) devono essere controllati per quanto concerne la sicurezza dei loro dati. Gli stessi vengono certificati dall'Istituto federale di metrologia.

(National Institute of Standards and Technology, U.S. Department of Commerce)	
ISO/IEC 27001 – Annex A.15: Supplier Relationships	L'allegato A.15.1 si occupa della sicurezza delle informazioni nelle relazioni con i fornitori. L'obiettivo consiste nella protezione dei valori patrimoniali importanti dell'organizzazione che sono accessibili ai fornitori o che possono essere da loro influenzati.
ISO/IEC 90003	La ISO/IEC 90003 è una direttiva per l'applicazione della ISO 9001 (requisiti per i sistemi di gestione della qualità) in ambito di acquisti, sviluppo, gestione e manutenzione nello sviluppo di software tra fornitore, mandatario e cliente.
Standardized Information Gathering (Questionnaire) SIG *(The Santa Fe Group / Shared Assessments)*	Questionario standardizzato per giudicare la qualità della relazione con i fornitori e valutare i rischi di fornitura che trova applicazione soprattutto nell'area anglosassone. Il SIG consiste in una raccolta di domande sulla sicurezza delle informazioni e sulla protezione dei dati di terzi che si riferisce a diverse disposizioni e ambiti di controllo. Il SIG è pubblicato da un'organizzazione non profit denominata Shared Assessments. Essa aggiorna il questionario SIG ogni anno, tenendo conto delle nuove sfide in materia di sicurezza e protezione dei dati, delle modifiche delle prescrizioni nonché delle più recenti tendenze e best practices in ambito di gestione dei rischi per i fornitori terzi.

Accanto a questi standard più ricorrenti e consolidati a livello internazionale, esistono svariati altri standard, linee guida e direttive adatte per migliorare la sicurezza delle informazioni in generale e della gestione dei fornitori in particolare. Ne sono un esempio le raccomandazioni delle associazioni di categoria o i lavori di ricerca delle università e delle società specializzate nella sicurezza delle TIC. Tali standard includono, fra l'altro, tematiche come la codificazione, le firme digitali, le funzioni hash, l'autenticazione, gli attestati di comunicazione, i servizi di marcatura temporale, la protezione antincendio, la protezione antieffrazione, la cancellazione sicura dei supporti dati, e così via.

3 Quadro normativo per l'applicazione degli standard

Le basi giuridiche costituiscono il fondamento delle misure volte ad incrementare la sicurezza dei prodotti e di quelle finalizzate alla minimizzazione dei rischi intrinseci alla catena di fornitura. Pur non rinviando direttamente agli standard, esse costituiscono la base per la loro applicazione.
Nell'ambito degli acquisti, lo Stato si muove parallelamente in due sfere giuridiche del tutto diverse. Per poter svolgere i suoi compiti pubblici e quindi giuridici, nella misura in cui non è in grado di farlo con i propri mezzi, esso dipende regolarmente dalla fruizione di prestazioni erogate dall'economia privata. Il diritto in materia di appalti pubblici descrive la procedura che dev'essere applicata al processo decisionale delle autorità. Una volta formata tale volontà e tenuto conto di tutti i vincoli, compresi quelli imposti in materia di sicurezza, si sceglie, nel quadro della procedura di aggiudicazione, l'offerente adatto. Nella documentazione del bando di gara, lo Stato descrive le prestazioni di cui ha bisogno e quali caratteristiche devono avere tali prestazioni. Al riguardo, non ha luogo un'applicazione diretta delle disposizioni

amministrative in vigore. Le autorità, devono piuttosto farsi garantire in via contrattuale il rispetto di tali norme. Ne consegue che anche le violazioni di tali accordi potranno essere sanzionate solo con i mezzi del diritto privato, segnatamente con un risarcimento del danno. Questo vale sia per l'Amministrazione federale stessa (e quindi anche per gli acquisti a favore dell'esercito[19]), sia per le infrastrutture critiche di diritto pubblico e privato, a condizione che queste esercitino in Svizzera delle attività nei settori definiti ai sensi dell'art. 4 cpv. 2 LAPub.
In sede di acquisto di prestazioni sul mercato, il contratto di acquisto, che in primo luogo descrive l'oggetto del contratto o la prestazione da fornire, è quindi l'elemento fondamentale per imporre gli aspetti della sicurezza specifici al caso. Il rispetto degli standard internazionali o il soddisfacimento dei requisiti volti a garantire un certo livello di protezione mediante criteri obbligatori (criteri di idoneità e specifiche tecniche) o mediante criteri ponderati (criteri di aggiudicazione) può essere definito già nel bando di gara, concordato successivamente nel contratto e verificato in occasione della fornitura della prestazione. In ambito di SCRM, al centro dell'interesse vi è la relazione tra mandante/committente/cliente/acquirente e mandatario/produttore/fornitore. Anche questa relazione è di norma descritta e definita in sede contrattuale.

3.1 Basi giuridiche per l'applicazione degli standard nell'Amministrazione federale

Le possibilità e le procedure per l'applicazione degli standard in materia di sicurezza dei prodotti e di SCRM sono disciplinate da diverse leggi federali e ordinanze. Specificamente per il settore della sicurezza dei prodotti TIC e per le informazioni trattate mediante tali prodotti, fino a poco tempo fa non esistevano disposizioni legali federali di rango superiore. Con la nuova Legge federale sulla sicurezza delle informazioni (LSIn) si è provveduto a colmare questa lacuna.

3.1.1 La Legge federale sulla sicurezza delle informazioni (LSIn)[20]

Il 18 dicembre 2020, il Parlamento ha varato la Legge federale sulla sicurezza delle informazioni in seno alla Confederazione (LSIn).[21] La LSIn riunisce in un'unica legge i più importanti aspetti normativi in ambito di cibersicurezza e sicurezza delle informazioni. Questa legge comprende sia prescrizioni in materia di sicurezza dei prodotti, sia prescrizioni in materia di SCRM per i prodotti TIC, in particolare sulla gestione dei rischi, la classificazione delle informazioni, la sicurezza informatica, i controlli di sicurezza relativi alle persone, la protezione fisica, la sicurezza in caso di acquisti sensibili tramite la procedura di sicurezza relative alle aziende nonché sul supporto della Confederazione ai gestori di infrastrutture critiche nell'ambito della sicurezza delle informazioni. La LSIn si applica alle autorità e alle organizzazioni della Confederazione (compreso l'esercito) e definisce i requisiti minimi che le predette sono tenute a soddisfare per proteggere le loro informazioni e infrastrutture informatiche. La legge vincola però anche le autorità cantonali e le aziende di diritto privato che supportano la Confederazione nello svolgimento delle sue mansioni elaborando informazioni classificate della Confederazione o accedendo ai mezzi informatici della Confederazione. La Confederazione cerca così una stretta collaborazione con i Cantoni e l'economia privata onde poter affrontare gli attuali ciber-rischi in continuo aumento.
La LSIn poggia su standard riconosciuti a livello internazionale, in particolare gli standard ISO/IEC 27001 e ISO/IEC 27002. Per migliorare in modo duraturo ed economico la sicurezza delle informazioni in seno alla Confederazione nonché per ottenere un livello di sicurezza che sia il più uniforme possibile tra le autorità federali e altri servizi, l'attenzione è rivolta soprattutto alle informazioni e ai sistemi critici come anche alla standardizzazione delle misure da adottare. Non da ultimo a causa dei rapidi sviluppi

[19] L'esercito stesso non può effettuare acquisti poiché non fa parte dell'Amministrazione federale (ai sensi dell'OLOGA) ed è invece un'istituzione di diritto speciale fondata sulla Legge militare. La sua amministrazione autonoma è possibile solo nel quadro dell'Ordinanza concernente l'amministrazione dell'esercito (OAE, RS 510.301).
[20] Legge federale sulla sicurezza delle informazioni in seno alla Confederazione (Legge sulla sicurezza delle informazioni; LSIn; FF 2020 9975)
[21] La LSIn non è ancora in vigore. Le specifiche ordinanze di esecuzione sono attualmente in fase di elaborazione.

tecnologici, la LSIn si astiene però dallo stabilire misure dettagliate, limitandosi invece a creare un quadro giuridico formale sulla cui base le autorità federali possano concretizzare con la maggiore uniformità possibile, a livello di ordinanze e direttive, la sicurezza delle informazioni.
Il fatto che la Confederazione riunisca i vari aspetti della sicurezza delle informazioni in un'unica legge federale evidenzia la grande importanza attribuita a questo tema.

3.1.2 Standard in ambito di sicurezza dei prodotti TIC

La base giuridica per l'implementazione di standard relativi alla sicurezza dei prodotti (compresi i requisiti per un'applicazione sicura dei prodotti) in seno all'Amministrazione federale è stabilita nell'Ordinanza sui ciber-rischi, nell'Ordinanza sulla protezione delle informazioni e nella Legge sulla protezione dei dati.

Ordinanza sui ciber-rischi (OCiber)[22]**.** Le direttive in materia di sicurezza informatica e applicazione sicura dei mezzi TIC in seno all'Amministrazione federale sono definite nell'OCiber. L'OCiber disciplina la competenza del delegato o della delegata alla cibersicurezza nell'emanare direttive in materia di sicurezza informatica per le unità amministrative dell'Amministrazione federale (art. 11 cpv. 1 lett. e). Il delegato o la delegata può inoltre partecipare all'elaborazione delle direttive informatiche e dei progetti informatici rimanenti che riguardano la cibersicurezza (art. 11 cpv. 3). L'OCiber impone inoltre l'esecuzione di procedure di sicurezza graduate predefinite (art. 14b seg.; vedi capitolo 4.1.1), che possono essere integrate e ampliate attraverso le direttive in materia di sicurezza informatica emanate dalla delegata o dal delegato. Queste procedure di sicurezza costituiscono la base per un'implementazione sicura di tutti i processi aziendali supportati da sistemi informatici, garantendo che vengano coinvolti i servizi giusti al momento giusto. Ciò si applica per l'intero ciclo di vita dei sistemi TIC, vale a dire dall'inizio di un nuovo progetto fino alla messa fuori servizio del sistema. Si garantisce cosicché tutti possano assumere correttamente le proprie responsabilità nelle varie fasi.

Ordinanza sulla protezione delle informazioni (OPrI)[23]**.** L'OPrI disciplina la protezione, nella misura in cui è richiesta nell'interesse del Paese, delle informazioni della Confederazione e dell'esercito. In particolare, essa stabilisce la classificazione (art. 4 seg.) e le conseguenti forme di trattamento di dette informazioni (art. 13 seg.). Nell'allegato all'OPrI, il Consiglio federale ha definito i requisiti tecnici in materia di sicurezza dei prodotti per i sistemi TIC previsti per il trattamento di informazioni classificate. Con l'entrata in vigore della LSIn, l'OPrI è abrogata. Nella misura in cui i contenuti necessari non sono già presenti nella legge, saranno riportati in una nuova ordinanza concernente la sicurezza delle informazioni.

Legge federale sulla protezione dei dati e relativa ordinanza (LPD e OLPD)[24]**.** La legge federale sulla protezione dei dati (LPD) e la relativa ordinanza definiscono quali requisiti tecnici e organizzativi si applicano in sede di trattamento dei dati personali (articoli 7, 11 e 17a LPD, articoli 8-11, 20 e 21 OLPD). Vengono così definiti degli standard minimi di sicurezza per quei prodotti TIC impiegati per il trattamento di tali dati.

3.1.3 Standard per il SCRM

Per l'applicazione degli standard in materia di SCRM si tratta anzitutto di accertare quali possibilità giuridiche si hanno in fase di strutturazione dei processi di acquisto. Le relative basi giuridiche sono

[22] Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi; OCiber; RS 120.73)
[23] Ordinanza sulla protezione delle informazioni della Confederazione, (Ordinanza sulla protezione delle informazioni; OPrI; RS 510.411)
[24] Legge federale sulla protezione dei dati (Legge sulla protezione dei dati; LPD; RS 235.1) e Ordinanza relativa alla legge federale sulla protezione dei dati (OLPD; RS 235.11).

definite nel diritto in materia di appalti pubblici. Inoltre, nell'Ordinanza sulla tutela del segreto e nell'Ordinanza sui controlli di sicurezza relativi alle persone vengono creati requisiti importanti per controllare con maggior precisione i fornitori di servizi e prodotti particolarmente rilevanti per la sicurezza.

Diritto in materia di appalti pubblici – Accordo stipulato nel quadro dell'Organizzazione mondiale del commercio (OMC) e Legge federale sugli appalti pubblici (LAPub)[25]**.** Con l'adesione all'Organizzazione mondiale del commercio (OMC), la Svizzera si è impegnata, nel suo ordinamento giuridico, a liberalizzare il commercio internazionale ed eliminare eventuali ostacoli al commercio. Il diritto internazionale riconosce però che gli Stati, a tutela di interessi di sicurezza preponderanti necessitano di eccezioni al principio del libero commercio. Sia l'Accordo del 15 aprile 1994 che istituisce l'Organizzazione mondiale del commercio,[26] sia l'Accordo riveduto sugli appalti pubblici[27] prevedono quindi che gli Stati firmatari possano adottare le misure necessarie alla tutela di loro interessi fondamentali in materia di sicurezza. Il rilascio di informazioni può inoltre essere rifiutato qualora la loro divulgazione sia contraria a tali interessi. Ciò concerne, in particolare, l'acquisto di armi, munizioni e materiale bellico nonché gli acquisti indispensabili per la sicurezza o la difesa nazionale. Per i contratti nell'ambito della sicurezza e della difesa nazionale, le parti contrattuali possono quindi astenersi dall'applicazione degli obblighi chiave del diritto internazionale in materia di appalti nonché, in particolare, dei principi di non discriminazione e trattamento nazionale[28].

A tutela degli interessi di sicurezza nazionale fondamentali, il legislatore è ricorso alla riserva dell'Accordo riveduto sugli appalti pubblici stabilendo, nell'articolo 10 cpv. 4 lett. a LAPub, che la presente legge non si applica all'aggiudicazione di commesse pubbliche se ciò è ritenuto necessario per la tutela e il mantenimento della sicurezza esterna o interna o dell'ordine pubblico. Questa eccezione è da applicare per tutti i committenti soggetti alla LAPub, quindi non solo per quelli dell'Amministrazione federale centrale, sempre nell'esercizio del loro potere discrezionale (cfr. precedente punto 3). Tuttavia è consentito ricorrere a questa deroga ai principi del libero commercio solo alle condizioni dell'accordo: il servizio di acquisto deve poter dimostrare che non è possibile ridurre il rischio in misura accettabile adottando misure proporzionali e non discriminanti. I criteri costituzionali rimangono applicabili. In particolare, le decisioni vanno adottate in modo fondato e non arbitrario.

Ordinanza sulla tutela del segreto[29]**:** nell'Ordinanza sulla tutela del segreto del 29 agosto 1990 sono definite le misure di sicurezza che trovano applicazione quando mandati con contenuto classificato dal punto di vista militare come SEGRETO e CONFIDENZIALE devono essere eseguiti da terzi. Essa costituisce la base giuridica per l'esecuzione di controlli di sicurezza aziendale per i mandatari della Confederazione e, quindi, per un elemento fondamentale del SCRM. La cosiddetta procedura di sicurezza relativa alle aziende, nella LSIn, è d'ora in poi posta su una base giuridica formale.

Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)[30]**:** basandosi sugli articoli 19-21 della Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI)[31] e sugli articoli 23 cpv. 2, lett. d, 103 cpv. 3 lett. d nonché 113 cpv. 4 lett. d della Legge federale sull'esercito e sull'amministrazione militare (LM)[32], l'Ordinanza del 4 marzo 2011 sui controlli di sicurezza relativi alle persone disciplina le condizioni per l'esecuzione di controlli di sicurezza relativi alle persone. Questa base è essenziale per la gestione dei rischi con riferimento ai collaboratori di fornitori terzi. Con l'entrata in vigore della LSIn, quest'ordinanza viene collocata su una nuova base giuridica formale e totalmente riveduta.

[25] Legge federale sugli appalti pubblici (LAPub; RS 172.056.1)
[26] Accordo che istituisce l'Organizzazione mondiale del commercio (RS 0.632.20)
[27] Accordo riveduto sugli appalti pubblici (RS 0.632.231.422)
[29] Ordinanza sulla procedura di tutela del segreto in occasione di mandati con contenuto classificato dal punto di vista militare (Ordinanza sulla tutela del segreto; RS 510.413)
[29] Ordinanza sulla procedura di tutela del segreto in occasione di mandati con contenuto classificato dal punto di vista militare (Ordinanza sulla tutela del segreto; RS 510.413)
[30] Ordinanza sui controlli di sicurezza relativi alle persone (OCSP; RS 120.4)
[31] Legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI; RS 120)
[32] Legge federale sull'esercito e sull'amministrazione militare (Legge militare; LM; RS 510.10)

3.2 Basi giuridiche per l'applicazione degli standard in ambito di infrastrutture critiche

In Svizzera non c'è nessuna legge che adotti direttive in merito alla sicurezza o all'acquisto dei mezzi TIC valide per tutti i settori delle infrastrutture critiche.[33] Direttive di questo tipo, laddove esistenti, vengono definite in primo luogo negli atti legislativi specifici del settore. Essendo collocati nel loro rispettivo contesto normativo, questi atti presentano forti differenze anche per quanto riguarda le direttive in materia di sicurezza. In generale, si può constatare che per i gestori di infrastrutture critiche vengono imposte direttive poco vincolanti in relazione all'applicazione di standard per la sicurezza dei prodotti o in ambito di SCRM. Diversi atti legislativi rinviano indirettamente agli standard esigendo dai gestori di infrastrutture critiche l'adozione di misure per la sicurezza in conformità allo «stato della tecnica».[34] Questi rinvii indiretti, sono relativamente difficili da interpretare in relazione alla sicurezza delle TIC, poiché è assai complicato accertare quale sia lo stato attuale della tecnica. Resta poco chiaro fino a che punto gli standard internazionali debbano essere applicati affinché questo criterio sia ritenuto soddisfatto.
La tabella seguente riporta quelle basi giuridiche che pongono requisiti diretti in materia di sicurezza e indica inoltre da quali di queste basi risulta un'applicazione vincolante degli standard per l'utilizzo sicuro dei prodotti TIC e per il loro acquisto.

Settori	Direttive
Autorità e sicurezza pubblica	Per l'Amministrazione federale si applicano le basi elencate al capitolo 3.1.
Energia	• L'Ordinanza sull'approvvigionamento elettrico[35] (art. 8b) definisce una verifica dei sistemi di misurazione intelligenti (smartmeter) da parte dell'Istituto federale di metrologia per quanto concerne la sicurezza dei loro dati. La Legge sull'approvvigionamento elettrico[36] (art. 20a) richiede un controllo periodico di sicurezza relativo alle persone per i collaboratori e le persone incaricate presso la società nazionale di rete che possono influenzare la sicurezza della rete di trasporto. • L'Ordinanza sulla corrente forte[37] (art. 4) e l'Ordinanza sulla corrente debole[38] (art. 4), per la sicurezza degli impianti rinviano direttamente alle norme svizzere e internazionali vigenti in materia dichiarandole vincolanti. • La Legge federale sull'energia nucleare[39] e l'Ordinanza sull'energia nucleare[40] contengono varie direttive per la sicurezza nell'ambito dell'esercizio di impianti nucleari. L'Ordinanza sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari[41] stabilisce che tutte le persone che hanno accesso a informazioni classificate in materia di sistemi rilevanti per la sicurezza interna o esterna di impianti nucleari e di materiale nucleare devono essere sottoposte a un controllo di sicurezza relativo alle persone (art. 1). • Ai sensi della Legge federale sugli impianti di accumulazione[42] (art. 5), gli impianti di accumulazione devono essere calcolati, costruiti ed esercitati in modo che la loro sicurezza sia garantita per tutti i casi prevedibili di carico e d'esercizio.
Smaltimento	• L'Ordinanza sulla protezione contro gli incidenti rilevanti[43] (art. 3) impone a determinate aziende di attuare misure di sicurezza aggiornate allo stato della tecnica che tengano

[33] La nuova legge federale sulla sicurezza delle informazioni (cfr. capitolo 3.1) contiene regolamentazioni applicabili anche per i gestori di infrastrutture critiche.
[34] ad es. art. 3 dell'Ordinanza sulla protezione contro gli incidenti rilevanti (OPIR; RS 814.012); art. 3 della Legge federale sulla sicurezza dei prodotti (LSPro; RS 930.11). Il rinvio allo stato della tecnica in relazione al Regolamento generale sulla protezione dei dati (RGPD) nell'Unione europea (UE) è particolarmente dibattuto.
[35] Ordinanza sull'approvvigionamento elettrico (OAEl; RS 734.71)
[36] Legge federale sull'approvvigionamento elettrico (Legge sull'approvvigionamento elettrico; LAEl; RS 734.7)
[37] Ordinanza sugli impianti elettrici a corrente forte (Ordinanza sulla corrente forte; RS 734.2)
[38] Ordinanza concernente gli impianti elettrici a corrente debole (Ordinanza sulla corrente debole; RS 734.1)
[39] Legge federale sull'energia nucleare (LENu; RS 732.1)
[40] Ordinanza sull'energia nucleare (OENu; RS 732.11)
[41] Ordinanza sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari (OCSPN; RS 732.143.3)
[42] Legge federale sugli impianti di accumulazione (Legge sugli impianti di accumulazione; LImA; RS 721.101)
[43] Ordinanza sulla protezione contro gli incidenti rilevanti (OPIR; RS 814.012)

	conto di tutte le cause intrinseche ed estrinseche suscettibili di provocare un incidente rilevante, nonché degli interventi di persone non autorizzate. Nell'ordinanza non si fa però riferimento esplicito alla sicurezza delle TIC e ai relativi standard.
Finanze	• La Legge federale concernente l'Autorità federale di vigilanza sui mercati finanziari[44] conferisce all'Autorità federale di vigilanza sui mercati finanziari (FINMA) la competenza di emanare disposizioni di esecuzione concernenti la sicurezza e la protezione dei dati (art. 13a cpv. 3). L'Ordinanza concernente la legge sulla vigilanza dei mercati finanziari[45] definisce in che modo la FINMA esercita tale competenza e stabilisce che nel farlo deve tenere conto degli standard internazionali (art. 5 e art. 6). • Le circolari della FINMA[46] 2017/01 «Corporate Governance – banche»[47], 2008/07 «Outsourcing - banche»[48] e 2008/21 «Rischi operativi - banche»[49] obbligano le banche all'implementazione di standard che soddisfino i requisiti dello standard NIST.
Sanità	• L'Ordinanza sulla cartella informatizzata del paziente (OCIP)[50] stabilisce che le comunità devono dotarsi di un sistema di gestione della protezione e della sicurezza dei dati adeguato (art. 12). Per quanto concerne le direttive sulla sicurezza degli strumenti d'identificazione, l'OCIP rinvia direttamente alla norma ISO/IEC 29115:2013 (art. 23). Sono inoltre disciplinati l'accreditamento di organismi di certificazione (art. 28) nonché i requisiti, le condizioni e la procedura di certificazione (articoli 30-38).
Informazione e comunicazione	• La Legge sulle telecomunicazioni (LTC)[51] (art. 48a) conferisce al Consiglio federale la competenza di emanare, per i fornitori, disposizioni tecniche e amministrative sulla sicurezza delle infrastrutture di telecomunicazione.
Alimentazione	• Nelle ordinanze non sono stati trovati requisiti di sicurezza in ambito informatico o per i fornitori.
Trasporti	• Nelle ordinanze non sono stati trovati requisiti di sicurezza in ambito informatico o per i fornitori. • L'Ordinanza sulla protezione contro gli incidenti rilevanti include, in parte, anche le vie di comunicazione.

4 Applicazione degli standard

Poiché la regolamentazione delle possibili misure tecniche e organizzative in materia di cibersicurezza è coperta ampiamente dagli standard esistenti, gran parte delle misure tecniche e organizzative per la protezione dai ciber-rischi può essere ricondotta all'applicazione degli standard. In questo capitolo, si espongono le più importanti misure dell'Amministrazione federale e dei gestori di infrastrutture critiche che configurano un'applicazione diretta di quanto prescritto dagli standard sulla sicurezza dei prodotti e sul SCRM dei prodotti TIC.

[44] Legge federale concernente l'Autorità federale di vigilanza sui mercati finanziari (Legge sulla vigilanza dei mercati finanziari; LFINMA; RS 956.1)
[45] Ordinanza concernente la legge sulla vigilanza dei mercati finanziari (RS 956.11)
[46] Con le circolari, la FINMA espone il modo in cui essa applica la legislazione sui mercati finanziari nella propria prassi di vigilanza. Le circolari possono esser consultate al seguente link: https://finma.ch/de/dokumentation/rundschreiben/
[47] Consultabile al seguente link: https://finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-01-20200101.pdf?la=de
[48] Consultabile al seguente link: https://finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-07.pdf?la=de
[49] Consultabile al seguente link: https://finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=de
[51] Legge sulle telecomunicazioni (LTC; RS 784.10)
[51] Legge sulle telecomunicazioni (LTC; RS 784.10)

4.1 Applicazione degli standard nell'Amministrazione federale

La sicurezza dei prodotti TIC ha la massima priorità per l'Amministrazione federale e per l'esercito. Le direttive esistenti in materia di sicurezza dei prodotti e di SCRM vengono correntemente aggiornate. Esse sono fortemente orientate agli standard validi a livello internazionale, ma un rinvio diretto agli standard di cui tenere conto resta l'eccezione.[52]

4.1.1 Applicazione degli standard sulla sicurezza dei prodotti TIC

Nel quadro delle direttive vigenti, l'attuazione delle più importanti misure per la sicurezza delle TIC durante l'intero ciclo di vita di un sistema TIC (pianificazione, acquisto, esercizio, messa fuori servizio) è di fondamentale importanza per la qualità della cibersicurezza. In seno all'Amministrazione federale, il Centro nazionale per la cibersicurezza (NCSC) registra pertanto ogni anno lo stato d'attuazione e lo porta all'attenzione del Consiglio federale. Una sintesi di queste registrazioni è pubblicamente accessibile[53]. Di seguito, si espone quale ruolo svolgono gli standard per la sicurezza dei prodotti TIC in sede di attuazione delle misure.

Le procedure di sicurezza dell'Amministrazione federale
Le procedure di sicurezza definite nell'OCiber sono costituite dai seguenti elementi, graduati gerarchicamente l'uno rispetto all'altro:

- Analisi del bisogno di protezione: per ogni progetto TIC occorre dapprima eseguire un'analisi del bisogno di protezione che sfocerà in una valutazione della classificazione dell'applicazione o del progetto. Tutti gli oggetti informatici da proteggere devono disporre di un'analisi aggiornata del bisogno di protezione. Tale analisi include anche il processo per la riduzione dello spionaggio dei servizi d'informazione (RINA). Questo processo di verifica è stato elaborato per individuare il bisogno di protezione di una fornitura di prestazione informatica con riferimento alla minaccia rappresentata da fornitori di servizi informatici strumentalizzati nonché per adottare eventuali misure di protezione coordinandole con una possibile procedura di acquisto. Oltre a ciò, si identificano i rischi e si stabiliscono le misure da integrare nel concetto di sicurezza dell'informazione e protezione dei dati (concetto SIPD).
- Direttive per la protezione di base: la «protezione di base delle TIC nell'Amministrazione federale» stabilisce in maniera vincolante i requisiti minimi di sicurezza definiti nelle direttive dal punto di vista organizzativo, personale e tecnico nel settore della sicurezza informatica. Per ciascun oggetto informatico da proteggere si deve applicare perlomeno questa protezione di base TIC. L'attuazione deve essere documentata e verificata regolarmente dai responsabili delle unità amministrative.
- Direttive per la protezione elevata: se dall'analisi del bisogno di protezione risulta un bisogno di protezione elevato, oltre all'attuazione delle direttive in materia di sicurezza per la protezione di base le unità amministrative definiscono, sulla base di un'analisi dei rischi, ulteriori misure di sicurezza, le documentano e le attuano. Il concetto di sicurezza dell'informazione e protezione dei dati (concetto SIPD) contiene la descrizione delle misure di sicurezza e della loro attuazione per l'oggetto informatico da proteggere nonché la descrizione dei rischi residui.

Oltre a ciò, in seno alla Confederazione, vengono attuate anche le misure di sicurezza esposte di seguito.

[52] Le Istruzioni sulla sicurezza delle informazioni nel DDPS (WIns VBS) del 16 dicembre 2016 così come le Istruzioni dei responsabili della sicurezza delle informazioni del DDPS sulla sicurezza delle informazioni (WSVIns DDPS) del 26 aprile 2017 contengono regole vincolanti per l'ISMS a livello di DDPS nonché per l'ISMS dei gruppi e degli uffici del DDPS. Si stabilisce esplicitamente che l'ISMS del DDPS si basa sullo standard SN ISO/IEC 27001:2015.
[53] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/informatiksicherheitsberichte-bund.html

- Verifica di prodotti crittografici: i prodotti crittografici[54] servono alla protezione delle informazioni nell'ottica della confidenzialità, dell'integrità, dell'autenticità e/o dell'obbligatorietà. L'acquisto e l'esercizio di tali prodotti è particolarmente delicato poiché il corretto funzionamento crittografico può essere giudicato e verificato solo da esperti del settore certificati. In assenza di un controllo e di una verifica conformi alle regole dell'arte, sussiste il rischio che i prodotti crittografici non soddisfino lo scopo d'applicazione desiderato senza che ciò venga effettivamente notato. Per questo motivo, in ambito crittologico, i prodotti specifici vengono acquistati in linea di principio dall'Ufficio federale dell'armamento (armasuisse) quale organismo specializzato in materia.[55] In questo, armasuisse è supportata dal servizio specializzato in crittologia della Base d'aiuto alla condotta dell'esercito (BAC Critt) i cui esperti eseguono controlli crittologici dettagliati, sia durante il processo di acquisto, sia in caso di modifiche del sistema (ad es. dopo aggiornamenti del firmware o del software), durante l'intero ciclo di vita del sistema.

- Analisi delle vulnerabilità da parte del NCSC: il NCSC è il centro a cui segnalare le vulnerabilità individuate nelle applicazioni dell'Amministrazione federale. Esso verifica la plausibilità delle segnalazioni pervenute, intraprende una valutazione dei rischi che tali vulnerabilità comportano e, in accordo con le unità amministrative e i fornitori di prestazioni interessati, avvia le relative misure correttive. Nel DDPS, gli specialisti del Cyber Defence Campus cercano sistematicamente possibili vulnerabilità e punti a rischio di attacco nei software dei sistemi e delle applicazioni del dipartimento.

- Sistema di gestione della sicurezza delle informazioni (ISMS) in seno al DDPS: un ISMS definisce le regole e i metodi volti a garantire la sicurezza delle informazioni in un'azienda o in un'organizzazione. Esso è preposto all'identificazione ed eliminazione sistematica dei rischi nell'ambito della sicurezza delle informazioni e della cibersicurezza (informazioni, dati e informatica), in sintonia con gli obiettivi superiori dell'organizzazione. Nel DDPS, è stato allestito un ISMS in conformità alla norma ISO/IEC 27001.

4.1.2 Applicazione degli standard in materia di SCRM

Misure in materia di diritto sugli appalti pubblici: ai sensi dell'articolo 20 capoverso 3 LAPub, per l'acquisto di armi, munizioni, materiale bellico o, se sono indispensabili per scopi di difesa e di sicurezza, di altre forniture, prestazioni edili, prestazioni di servizi e prestazioni in materia di ricerca o sviluppo, se il richiedente ne ha il diritto, può ricorrere alla procedura mediante invito. Il servizio di acquisto competente stabilisce quali offerenti intende invitare a presentare un'offerta, senza indire un bando pubblico. In caso di acquisti di sistemi o servizi informatici sensibili in termini di sicurezza, il diritto sugli appalti pubblici lascia quindi libertà di azione per quanto riguarda l'applicazione degli standard in materia di SCRM. Restrizioni nella scelta degli offerenti di prodotti TIC rilevanti per la sicurezza, ad esempio dovute alla nazionalità dell'offerente, sono possibili nell'ambito degli acquisti per scopi di difesa e di sicurezza, e quindi anche per quelli dell'esercito, ai sensi della LAPub.

Conclusione di accordi sulla protezione delle informazioni: per la sua difesa e la sua sicurezza, sia esterna che interna, la Svizzera dipende da una stretta collaborazione con i partner internazionali e la loro base industriale. Poiché, in questi settori vengono spesso conferiti mandati sensibili in termini di

[54] Esempi: apparecchio crittografico, smartcard, hardware security module, random number generator, software di cifratura, libreria crittografica, ecc.
[55] Cfr. art. 10 cpv. 1 lett. d dell'Ordinanza concernente l'organizzazione degli acquisti pubblici dell'Amministrazione federale (OOAPub; RS 172.056.15)

sicurezza, la Svizzera ha concluso con numerosi Stati e organizzazioni internazionali dei cosiddetti accordi sulla protezione di informazioni[56]. Tali accordi disciplinano la protezione reciproca delle informazioni classificate e stabiliscono le misure di sicurezza da adottare in caso di acquisti bilaterali rilevanti per la sicurezza. La conclusione di accordi sulla protezione delle informazioni presuppone che le parti contraenti dispongano, nel loro diritto nazionale, di strumenti di sicurezza che soddisfano gli standard riconosciuti a livello internazionale. In concreto, gli accordi sulla protezione delle informazioni esigono che le aziende e le persone chiamate ad adempiere ai mandati classificati dell'altra parte contraente, vengano sottoposte a una verifica della loro affidabilità nell'ambito di una procedura di certificazione.
Lo standard internazionale per la valutazione dell'affidabilità delle aziende[57] esige, tra l'altro, di verificare se l'azienda è controllata o influenzata da Stati stranieri o da organizzazioni di diritto pubblico o privato («Foreign Ownership, Control and Influence – FOCI»). Se sussiste un rischio troppo alto, si devono adottare misure atte a ridurre tale rischio oppure escludere la ditta dalla procedura di aggiudicazione. Lo stesso vale anche per le persone fisiche.
Di norma, gli accordi sulla protezione delle informazioni non stabiliscono requisiti per la sicurezza dei prodotti. Tuttavia, in tali accordi è sovente stipulato che sistemi destinati a elaborare informazioni dell'altra parte contraente devono essere accreditati da un'autorità di sicurezza nazionale competente. L'accreditamento attesta che il sistema soddisfa i requisiti di sicurezza dell'altra parte contraente, ciò che equivale a una conferma formale della sicurezza dei prodotti.

Applicazione della procedura di tutela del segreto: con la procedura di tutela del segreto, al mandatario vengono imposte dal mandante misure di sicurezza pubbliche.[58] Questa procedura trova tuttavia applicazione solo se si devono trattare informazioni classificate come CONFIDENZIALI o SEGRETE.
Nella procedura di tutela del segreto, il primo passo consiste nella verifica, in collaborazione con il Servizio delle attività informative della Confederazione (SIC), dell'affidabilità della ditta che entra in linea di conto per l'esecuzione del mandato. Successivamente, un servizio specializzato stabilisce ufficialmente in un protocollo di sicurezza le misure concrete che la ditta dovrà attuare durante l'adempimento del mandato. Una volta attuate tutte le misure, la ditta riceve un attestato di sicurezza che equivale a un certificato riconosciuto a livello internazionale e la autorizza a eseguire il mandato classificato. Il servizio specializzato ha la facoltà di ispezionare in qualsiasi momento e senza preavviso una ditta in possesso di un attestato di sicurezza valido, al fine di controllare il rispetto dei vincoli imposti in materia di sicurezza.
In linea di massima, come mandanti, entrano in considerazione le unità amministrative del DDPS e l'Ufficio federale della costruzione e della logistica (UFCL).[59]I mandatari sono organismi pubblici esterni al DDPS e all'UFCL, aziende private o persone addette alla ricezione e al trattamento di informazioni classificate. Se il mandatario è un'azienda con sede in uno Stato terzo, l'esecuzione del mandato in termini di sicurezza e le modalità di collaborazione tra le rispettive autorità di sicurezza nazionali vengono disciplinate nel relativo accordo sulla protezione delle informazioni (vedi sopra). La verifica dell'azienda ha luogo, in questo caso, da parte dei relativi organi di sicurezza dello Stato terzo.
Con la LSIn, la procedura di tutela del segreto è rinominata «procedura di sicurezza relativa alle aziende» ed estesa alle ditte che, nell'ambito di un contratto, devono utilizzare, amministrare, effettuare la manutenzione o verificare sistemi informatici critici della Confederazione (o parti di essi).

Esecuzione di controlli di sicurezza relativi alle persone: a carico delle persone che forniscono servizi TIC o sviluppano prodotti TIC è eseguito un controllo di sicurezza se esse, nello svolgimento

[56] Vedi, ad esempio, l'Accordo fra il Consiglio federale svizzero e il Governo della Repubblica Francese sullo scambio e la reciproca protezione delle informazioni classificate (RS 0.514.134.91) o l'Accordo tra il Dipartimento federale della difesa, della protezione della popolazione e dello sport, in nome del Consiglio federale svizzero e il Ministro federale della difesa della Repubblica d'Austria concernente la protezione delle informazioni militari classificate (RS 0.514.116.31)
[57] Gli standard in ambito di sicurezza industriale internazionale sono elaborati dal Multinational Industrial Security Working Group (MISWG). Essi non sono vincolanti ma fungono da base per il riconoscimento dell'equivalenza delle misure da adottare.
[58] Vedi Ordinanza sulla procedura di tutela del segreto in occasione di mandati con contenuto classificato dal punto di vista militare (Ordinanza sulla tutela del segreto; RS 510.413)
[59] L'attuale limitazione della procedura di tutela del segreto ai mandati con contenuto classificato dal punto di vista militare sarà soppressa con l'entrata in vigore della legge sulla sicurezza delle informazioni.

delle loro attività, devono avere accesso a informazioni classificate come CONFIDENZIALI o SEGRETE. Questa disposizione vale anche per il personale dei fornitori dei prodotti e dei servizi. Gli organismi che eseguono i controlli possono ricorrere in questi casi al casellario giudiziale, al Registro nazionale di polizia e al Sistema d'informazione Sicurezza interna del SIC. In sede di decisione conclusiva, gli organismi di controllo emanano una decisione in cui la persona sottoposta al controllo viene dichiarata innocua oppure tale da rappresentare un rischio per la sicurezza. Una dichiarazione d'assenza di rischio non conferisce però automaticamente il diritto di ricevere un mandato. L'assegnazione del mandato è sempre rimessa alla libertà del mandante. L'esecuzione di tali verifiche è conforme alle direttive dello standard NIST 800-161 per «Third Party Personnel Security» (PS-7).
Con la LSIn, l'esecuzione di controlli di sicurezza relativi alle persone è ora possibile anche per le persone che devono utilizzare, amministrare, provvedere alla manutenzione o controllare sistemi informatici critici della Confederazione (o parti di essi).

Misure in sede di formulazione del contratto: secondo l'OCiber, le unità amministrative della Confederazione garantiscono che, in caso di acquisto di prestazioni da un fornitore esterno, le direttive in materia di sicurezza informatica facciano parte del rapporto contrattuale. In questo contesto, a sostegno delle unità amministrative è stato elaborato il documento «Riferimento alle direttive in materia di sicurezza informatica dell'Amministrazione federale per la documentazione dei bandi»[60]. I blocchi di testo ivi contenuti possono essere integrati nei documenti ufficiali di gara (in particolare per l'acquisto di software TIC) come adeguamenti o aggiunte specifici per la situazione, ad esempio in un modello di capitolato d'oneri.
I contratti della Confederazione contengono sempre le Condizioni generali della Confederazione (CG) corrispondenti al tipo di contratto. Deroghe alle CG sono ammesse solo in casi eccezionali motivati. Tali CG esistono per le prestazioni di servizi, per i mandati di ricerca, per gli acquisti di beni e per svariati negozi giuridici. Di norma esse comprendono anche disposizioni sulla sicurezza. Tuttavia, il tema della sicurezza dipende prevalentemente dalle clausole contrattuali concordate nello specifico rapporto contrattuale.
Per i servizi di acquisto della Confederazione è particolarmente importante riservare un'attenzione accresciuta alla sicurezza delle informazioni presso i partner commerciali dell'Amministrazione federale. La Conferenza degli acquisti della Confederazione (CA) mette a disposizione dei servizi d'acquisto dell'Amministrazione federale un modello di clausola comprendente la protezione dei sistemi TIC contro eventuali attacchi e un corrispondente obbligo di notifica da inserire nei modelli di contratto d'acquisto[61].
Il modello di clausola è una disposizione contrattuale a sé stante che può essere ripresa in un contratto d'acquisto. Essa è finalizzata alla protezione dei dati, delle informazioni e dei sistemi, sia prima che durante i ciberattacchi contro una parte contraente dell'Amministrazione federale. Nell'eventualità di un ciberattacco a un fornitore di prodotti o di servizi dell'Amministrazione federale, l'azienda interessata è chiamata a informare senza indugio e direttamente le sue mandanti in seno alla Confederazione e, d'intesa con le stesse, ad adottare adeguate misure immediate. Il modello di clausola, pertanto, è innanzitutto adatto per gli acquisti che comportano un elevato potenziale di rischio per quanto riguarda i ciberattacchi. L'applicazione della clausola deve essere valutata secondo il bisogno e accordata alle circostanze concrete. Per ogni contratto dev'essere concordata una formulazione individuale e consona ai rischi del caso.

Con un'accurata formulazione del contratto si possono quindi trattare molti aspetti della sicurezza e la Confederazione può riservarsi dei diritti di controllo. In questi casi, la Confederazione non può tuttavia imporre ufficialmente (unilateralmente) le sue esigenze in materia di sicurezza come avviene nella procedura di tutela del segreto ma deve eventualmente adire la via legale in una procedura civile. Per gli acquisti dell'esercito, armasuisse, in quanto servizio d'acquisto competente, disciplina negli accordi contrattuali l'approccio alle informazioni degne di protezione e le direttive relative al loro trattamento.

[60] Vedi Newsletter di settembre 2020 della Conferenza degli acquisti della Confederazione (CA)
[61] Vedi Modello di clausola contrattuale (e relative spiegazioni) della CA concernente i ciber-rischi (PDF, 385 kB, 31.08.2020).

4.2 Applicazione di standard per le infrastrutture critiche

Come esposto al capitolo 3.2, per le infrastrutture critiche esistono poche direttive legali per quanto riguarda l'applicazione degli standard in ambito di sicurezza dei prodotti e di SCRM. Ciononostante, l'importanza di standard per le aziende operanti in settori critici non è da sottovalutare. Gli standard vengono spesso utilizzati come supporti orientativi per l'attuazione delle misure e aiutano le aziende operanti a livello internazionale a coordinare la loro cibersicurezza oltre i confini nazionali.
Nel presente capitolo si affronta innanzitutto l'importanza degli standard nell'ambito delle infrastrutture critiche e si illustra il ruolo che svolgono in ambito di sicurezza dei prodotti e di SCRM, seppur la loro applicazione sia prescritta dalla legge solo in pochi casi. La Confederazione promuove l'applicazione di standard eseguendo sistematiche analisi dei rischi nei settori critici e fornendo supporto specialistico ai settori nell'elaborazione di standard minimi per le TIC. Entrambe le misure vengono anche descritte brevemente.

4.2.1 Valutazione generale dell'applicazione degli standard in ambito di infrastrutture critiche

Anche se l'applicazione degli standard non è vincolante, in sede di attuazione delle misure per la sicurezza informatica molte aziende si orientano agli standard internazionali. Nel quadro dello studio condotto in Germania nel 2019 «TÜV-Cybersicherheitsstudie», ciò è stato confermato dal 64% delle aziende interpellate.[62] È probabile che in Svizzera la situazione sia simile. Secondo uno studio sulla cibersicurezza delle PMI in Svizzera, il 60% delle aziende interpellate afferma di orientarsi agli standard internazionali.[63] Si tratta qui di un approccio pragmatico secondo il quale gli standard vengono applicati come direttive o strumenti ausiliari per il rafforzamento della sicurezza delle TIC senza puntare ad un'implementazione completa e certificata. Per questo motivo, non è facile giudicare in che misura gli standard siano applicati dai gestori di infrastrutture critiche. Per poter valutare meglio questa questione, l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha consultato le sue esperte e i suoi esperti in merito all'importanza degli standard nei loro settori[64]. Questi hanno confermato che la maggior parte delle aziende sono a conoscenza e applicano, a seconda delle necessita, gli standard per l'applicazione sicura dei mezzi TIC. Secondo la valutazione degli interpellati, gli standard più rilevanti per le imprese svizzere sono quelli delle serie ISO. Le esperte e gli esperti constatano che l'applicazione degli standard si limita all'ambito metodologico o procedurale. I test fisici degli hardware o le analisi del codice sorgente del software, stando alle affermazioni unanimi degli esperti consultati, richiederebbero risorse finanziarie e umane di gran lunga superiori a quelle disponibili nelle aziende.
In ambito di SCRM, solo pochissime ditte ricorrono a una gestione sistematica dei fornitori riferita alla sicurezza delle informazioni. Alcune ditte definiscono criteri di valutazione riferiti alla sicurezza e integrano sistematicamente i rischi della gestione dei fornitori nella gestione dei rischi estesa all'intera azienda. Tipicamente, si tratta qui di aziende di maggiori dimensioni, finanziariamente solide e particolarmente esposte.

4.2.2 Analisi dei rischi nei settori critici

I rischi e le vulnerabilità nei settori critici vengono regolarmente analizzati da esperti del settore economico e amministrativo nel quadro dell'implementazione della SNPC e della strategia per la protezione delle infrastrutture critiche (PIC). Qui, l'attenzione è rivolta soprattutto ai ciber-rischi. Le conoscenze acquisite aiutano a categorizzare meglio i ciber-rischi nel contesto della situazione di pericolo complessiva per le infrastrutture critiche, nonché a desumerne misure adeguate e a priorizzarle.
Con il coordinamento dell'Ufficio federale della protezione della popolazione (UFPP), nell'ambito dell'implementazione della seconda SNPC del 2018-2022, tutte le analisi dei rischi e delle vulnerabilità saranno

[62] TÜV Cybersicherheitstudie 2019
[63] Cyberrisiken in Schweizer KMUs, gfs Zurigo, 2017
[64] Il sondaggio ha avuto luogo a giugno 2019.

aggiornate e, all'occorrenza, vengono desunte nuove misure di resilienza. Le misure di resilienza già decise nel quadro del primo periodo della SNPC e quelle attualmente in corso vengono protratte in conformità alle responsabilità concordate.

4.2.3 Standard minimi, manuali e direttive

L'UFAE ha sviluppato uno standard minimo per il miglioramento della resilienza delle TIC.[65] Questo standard minimo si basa sullo standard NIST e dovrebbe fungere per i gestori di infrastrutture critiche da raccomandazione e possibile linea guida per il miglioramento della resilienza delle TIC (SCRM incl.). In stretta collaborazione con i vari settori, l'UFAE sviluppa standard e direttive specifiche al settore desumendoli dallo standard minimo generale.[66]
Gli standard minimi non sono giuridicamente vincolanti, ma hanno il vantaggio di integrarsi nelle strutture consolidate dei vari settori. Le direttive tecniche ivi sviluppate sono applicate e rispettate da molti anni nei vari settori. Integrati con direttive per la sicurezza informatica, questi standard possono influire fortemente sulla sicurezza in seno al settore.

5 Conclusione

Le sfide in ambito di sicurezza dei prodotti e di SCRM concernenti la cibersicurezza e la ciberdifesa sono molto impegnative. Oggigiorno, i rischi riconducibili a difetti di sicurezza dei prodotti stessi e legati ai fornitori possono essere solo ridotti, ma non evitati. Entrambi gli aspetti riguardano elementi chiave nell'ambito di protezione da ciber-rischi. La valutazione delle misure con cui affrontare queste sfide è pertanto molto importante. L'applicazione di standard riconosciuti a livello internazionale può apportare un importante contributo in questo senso.
Le analisi degli standard esistenti hanno dimostrato che nell'ambito della sicurezza dei prodotti e dell'applicazione sicura di tali prodotti esistono molti standard. Questa è una conseguenza del fatto che la carenza di sicurezza dei prodotti TIC è già nota da anni. Diversi di questi standard per la sicurezza dei prodotti trovano anche un'ampia applicazione.
Direttive di SCRM in ambito di cibersicurezza sono invece decisamente meno sviluppate. Da un lato, gli organi per la standardizzazione hanno recepito l'importanza dell'argomento solo negli ultimi anni. I rischi intrinseci alle catene di fornitura sono stati tematizzati solo al momento in cui è stata acquisita la consapevolezza di quanta sia l'influenza dettata da interessi geopolitici esercitata da certi Stati sui fornitori strategicamente importanti. Dall'altro, questo mix di aspetti tecnici, giuridici e politici rende il tema complesso per i progetti di standardizzazione. Poiché è difficile definire quando un rischio intrinseco alle catene di fornitura diventa eccessivo, la maggior parte degli standard in ambito di SCRM si focalizza su processi e metodi, acquistando piuttosto il carattere di istruzioni operative non vincolanti anziché di norme vincolanti.
Il presente rapporto ha analizzato l'approccio della Svizzera agli standard internazionali nei settori presi in esame in riferimento all'Amministrazione federale e all'esercito nonché per quanto concerne le infrastrutture. I risultati di questa analisi sono brevemente riassunti qui di seguito.

5.1 Il ruolo degli standard nell'Amministrazione federale e nell'esercito

In seno all'Amministrazione federale e all'esercito esistono numerose direttive in materia di sicurezza e di applicazione sicura dei prodotti TIC. Il sistema di direttive è fortemente basato sugli standard ISO/IEC

[65] Standard minimo per le TIC (admin.ch)
[66] Standard settoriali (admin.ch)

della serie 2700X e sulla loro esposizione negli standard BSI. Con l'OCiber, entrata in vigore nel 2020, queste direttive sono state poste su una nuova base giuridica. L'analisi relativa al livello di attuazione delle misure di sicurezza delle TIC in seno alla Confederazione, condotta ogni anno dal NCSC all'attenzione del Consiglio federale, evidenzia sempre che la creazione di direttive non è sufficiente. L'implementazione degli standard è impegnativa e richiede un impegno continuo. Volendo tirare le conclusioni riguardo alla situazione in seno all'Amministrazione federale per quanto concerne gli standard per la sicurezza dei prodotti, si può sostenere che l'attenzione deve essere maggiormente focalizzata su un'attuazione continua e globale delle direttive nonché sul controllo di tale attuazione piuttosto che sull'ulteriore sviluppo del regolamento già ampiamente elaborato. Il Consiglio federale prende atto ogni anno dello stato di attuazione delle direttive in materia di sicurezza delle TIC e ne informa dettagliatamente le commissioni parlamentari competenti.
Per quanto riguarda l'applicazione degli standard in ambito di SCRM, questa conclusione non vale in ugual misura per l'Amministrazione federale e per l'esercito. In vari organismi e servizi ci sono singole direttive per l'attuazione di un SCRM, ma non ci sono basi giuridiche che prescrivono l'attuazione di un SCRM sistematico. Ciò è dovuto, da un lato, al fatto che in ambito di SCRM esistono solo pochi standard direttamente attuabili e, dall'altro, alle condizioni giuridiche di base. Le basi per le singole fasi del SCRM erano finora disciplinate in più leggi. Con la Legge sulla sicurezza delle informazioni (LSIn), che tuttavia non è ancora entrata in vigore, è ora creato un quadro giuridico uniforme per le varie misure. In materia di sicurezza delle informazioni, essa segue un approccio integrale comprendente la protezione delle informazioni (protezione dello Stato), la sicurezza informatica, la sicurezza delle persone e la sicurezza relativa alle aziende. Unitamente ai principi di base contenuti nella LAPub e alle eccezioni ai principi del libero commercio, in futuro sarà possibile esercitare un'influenza (ad esempio, esclusione tempestiva di fornitori a rischio) già in una fase precoce del processo di acquisto (Supply Chain), allestendo così in seno alla Confederazione un rigoroso sistema di SCRM.

5.2 Il ruolo degli standard per le infrastrutture critiche

Rispetto alla situazione in seno all'Amministrazione federale, per le infrastrutture critiche esistono solo poche direttive vincolanti per l'applicazione degli standard in relazione alla sicurezza dei prodotti e al SCRM. Negli ultimi anni, si è assistito in molti settori ad un'intensificazione degli sforzi per introdurre tali prescrizioni attraverso accordi settoriali, manuali o direttive. Tuttavia, poiché questi lavori, così come l'attuazione delle prescrizioni, poggiano fondamentalmente sull'impegno volontario delle aziende, l'introduzione di standard per infrastrutture critiche resta incompleta. Data la forte interdipendenza delle infrastrutture critiche dovuta al processo di digitalizzazione, rimane il rischio che i sistemi scarsamente protetti pregiudichino la sicurezza di tutti gli altri gestori di infrastrutture.
L'opzione più palese per ottenere una maggiore diffusione degli standard consiste nella creazione di nuove direttive giuridicamente vincolanti. Siccome nell'ambito di sicurezza dei prodotti esistono già vari standard consolidati ciò sarebbe possibile tramite rinvii a tali standard. Sarebbero ipotizzabili direttive destinate ai gestori di infrastrutture critiche, finalizzate a un trattamento sicuro dei prodotti TIC. Si tratta di verificare quali direttive sono opportune in quale ambito, tenendo conto che i prodotti TIC, in infrastrutture critiche diverse, trovano applicazioni diverse e che le direttive devono quindi essere adeguate al rispettivo contesto. Inoltre, è anche possibile creare direttive per la sicurezza dei prodotti TIC stessi. In questo caso, le certificazioni di prodotti TIC sono solitamente richieste nei settori d'applicazione particolarmente importanti. Attualmente, lo sviluppo di tali schemi di certificazione è fortemente promosso anche in seno all'UE.[67] Lo svantaggio di una normativa di questo tipo risiede nel fatto che sfocia sovente in procedure di certificazione troppo laboriose. L'esecuzione delle certificazioni e i relativi aggiornamenti, data la complessità di molti sistemi TIC e i frequenti update richiesti dai medesimi, comportano un ingente dispendio di tempo e denaro per i produttori e per gli acquirenti. In sede di attuazione della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC), il Consiglio federale verifica

[67] Cfr. in proposito la nuova strategia dell'UE in materia di cibersicurezza: New EU Cybersecurity Strategy (europa.eu)

in quali ambiti sussiste una necessità di regolamentazione, accerta in quali casi tale regolamentazione sia di competenza della Confederazione e, all'occorrenza o qualora sia data tale competenza della Confederazione, propone al Parlamento dei modelli per l'introduzione di direttive vincolanti per l'applicazione degli standard nell'ambito di infrastrutture critiche.[68]

In linea di massima, possono essere introdotte, mediante misure normative, anche direttive per il SCRM. Esempi di possibili direttive in ambito di SCRM si trovano nello standard minimo per le TIC dell'UFAE, al capitolo 2.2.6.[69] In generale, è comunque importante constatare che le prescrizioni per le infrastrutture critiche in merito all'acquisto di servizi e alla formulazione dei rapporti con i fornitori rappresentano un intervento normativo relativamente forte e si deve anzitutto chiarire a quali condizioni queste possono essere emanate dalla Confederazione. Quando si tratta di promuovere l'applicazione di standard in ambito di SCRM, le soluzioni di questo genere non sono quindi poste in primo piano.

In generale, si tratta di verificare come poter migliorare le capacità di analizzare i prodotti e i processi di produzione su cui si basano. Ciò corrisponde a una delle richieste centrali avanzate dal working paper «Supply Chain Security» di ICTswitzerland. La Confederazione accoglie favorevolmente le iniziative private per l'ampliamento di capacità in questo senso o per la creazione di centri di controllo per componenti hardware e software in Svizzera ed è pronta a sostenere tali iniziative con le proprie competenze.

[68] Nell'ambito della Strategia nazionale per la protezione delle infrastrutture critiche 2018 – 2022 (PIC), l'UFPP ha già ricevuto, con la misura 2, il mandato di verificare la creazione o l'adeguamento di basi giuridiche con direttive intersettoriali per i gestori.
[69] Ufficio federale per l'approvvigionamento economico del Paese: Standard minimo per le TIC (admin.ch)