Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale delle strade USTRA

ISTRUZIONI

SECURITY GOVERNANCE OT

Sicurezza in ambito di sistemi BSA

Edizione 2022 V1.00
ASTRA 73006

Colophon

Autori

Jolanda Geringer	USTRA DS-DTI, presidenza
Martin Wyss	USTRA I-B
Markus Berger	USTRA I-FU
Manfred Jungo	USTRA DS
Wolfgang Hoffmann	USTRA DS-GOV
Bruno Frey	USTRA DS-GOV
Daniel Gähwiler	CSI Consulting, Zurigo

Assistenza

Bernard Crausaz	USTRA DS-UARS
Mario Pfammatter	USTRA DS-UARS

Traduzione

Servizio linguistico USTRA	fa fede l'originale tedesco

A cura di
Ufficio federale delle strade USTRA
Divisione Reti stradali N
Standard e sicurezza infrastrutture SSI
3003 Berna

Ordinazione
Il documento può essere scaricato gratuitamente dal sito www.ustra.admin.ch.

Prefazione

I progressi tecnici e i requisiti sempre più stringenti in materia di infrastrutture stradali richiedono disposizioni unitarie, e l'ambito della Security non fa eccezione: la sicurezza della rete viaria, con particolare riferimento alle nuove potenziali vulnerabilità, figura tra le priorità dell'Ufficio.

Le presenti istruzioni definiscono la Security Governance applicata ai BSA e alle rispettive funzioni di Operational Technology (tecnologia operativa, OT), illustrando altresì caratteristiche, contesti di impiego e tratti distintivi dei sistemi IT e OT.

Il documento è inteso a fornire un quadro orientativo per favorire il raggiungimento degli obiettivi specifici sul piano strategico, funzionale e operativo.

Ufficio federale delle strade

Jürg Röthlisberger
Direttore

Indice

1 Introduzione

1.1 Scopo

Le presenti istruzioni, volte a regolamentare la Security Governance OT dei sistemi di controllo e comando dell'impiantistica BSA (sistemi OT), trattano i seguenti argomenti:

- Obiettivi della Security Governance OT (vedi cap. 4.1);
- Insieme degli elementi fondanti a supporto di strategia, funzionalità e operatività:
  - Regole: processi, ruoli e organizzazione;
  - Persone: qualifiche e formazione tecnica;
  - Tecnologia: disposizioni tecniche;
- Distinzione tra IT e OT sulle strade nazionali (vedi cap. 3);
- Principali organi delegati all'organizzazione della sicurezza OT (vedi cap. 5.4).

1.2 Campo di applicazione

Le presenti istruzioni si applicano alla pianificazione, alla realizzazione e all'esercizio dell'insieme dei sistemi OT sulle strade nazionali. Il documento ha carattere vincolante e va necessariamente osservato in sede di integrazione degli impianti nella rete IP BSA.

Parte integrante della rete autostradale, i sistemi OT sono soggetti all'ordinanza sulle strade nazionali, motivo per cui non rientrano nel campo di applicazione delle istruzioni W007 del CF (Istruzioni del Consiglio federale concernenti i progetti TIC dell'Amministrazione federale e il portafoglio TIC della Confederazione).

1.3 Normative e standard di riferimento

Realizzazione e gestione degli impianti BSA e della relativa Operational Technology devono rispondere a specifiche disposizioni di legge. Committenti, ingegneri, fornitori e gestori sono tenuti al rispetto delle prescrizioni e delle norme vigenti nel loro ambito (vedi Riferimenti normativi e bibliografici).

1.4 Destinatari

Le presenti istruzioni si rivolgono in prima istanza al personale USTRA e ai gestori dei sistemi OT; in secondo luogo forniscono a committenti, progettisti e addetti alla pianificazione informazioni importanti in materia di organizzazione della sicurezza OT sulle strade nazionali.

1.5 Entrata in vigore e aggiornamenti

Le istruzioni entrano in vigore in data 31.10.2022. La «cronologia redazionale» è riportata a pagina 20.

2 Sicurezza nell'Amministrazione federale

2.1 Riepilogo dei riferimenti normativi della Confederazione

La figura seguente illustra i riferimenti normativi da osservare: per i singoli BSA sono previste deroghe specifiche e mirate rispetto alle disposizioni in materia di sicurezza delle informazioni e protezione dei dati.

Fig. 2.1 Disposizioni in materia di sicurezza delle informazioni e protezione dei dati

2.2 Livelli organizzativi nell'Amministrazione federale

Il Centro nazionale per la cibersicurezza (National Cyber Security Centre – NCSC) è il centro di competenza della Confederazione in ambito di sicurezza informatica. In qualità di servizio specializzato in materia di sicurezza TIC, l'NCSC emana disposizioni di cybersecurity interne alla Confederazione (autoprotezione), monitorandone l'osservanza e presta supporto ai fornitori di servizi nell'eliminazione delle vulnerabilità. La SG DATEC traspone al Dipartimento e ai singoli Uffici tali disposizioni federali, declinandole in base alle aree di competenza. L'USTRA, dal canto suo/stabilisce le prescrizioni specifiche per la rete viaria nazionale in ambito BSA, adottando le norme che risultano applicabili ai sistemi OT.

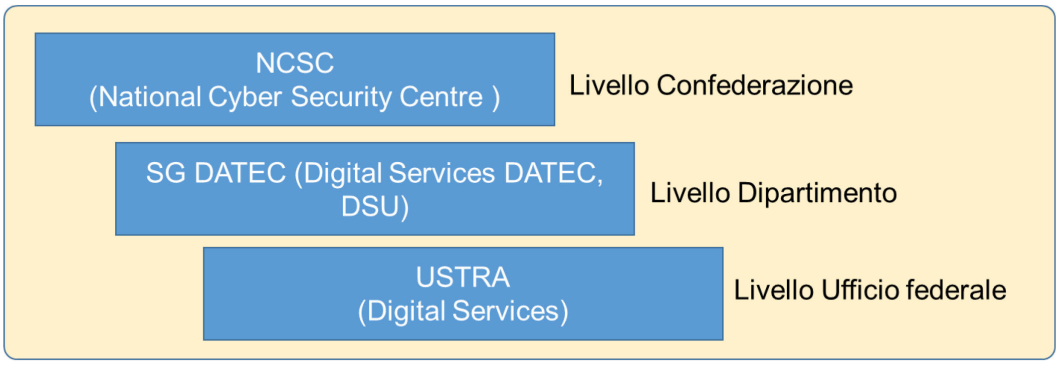

Fig. 2.2 Livelli organizzativi nell'Amministrazione federale

Ai fini della Security OT dell'USTRA assumono particolare rilevanza i seguenti testi normativi:

- Legge federale sulla protezione dei dati e relativa ordinanza (LPD e OLPD) [1], [4];
- Ordinanza sulla protezione delle informazioni della Confederazione (Ordinanza sulla protezione delle informazioni, OPrI) [5];
- Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi, OCiber) [6];
- Ordinanza sulla trasformazione digitale e l'informatica (OTDI) [7];
- Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC) [9];
- Si001 – Protezione IT di base nell'Amministrazione federale (Cancelleria federale CaF, Centro nazionale per la cibersicurezza NCSC) [15].

2.3 Attuazione USTRA in ambito BSA

In ambito di BSA sono previste alcune autorizzazioni speciali volte a garantire la sicurezza sulle strade nazionali e l'applicazione adeguata alle esigenze dei riferimenti normativi, formulati alla luce della distinzione tra IT e OT (vedi capitolo 3).

I prossimi capitoli illustrano le disposizioni specifiche dell'USTRA per le strade nazionali.

3 Distinzione tra Information Technology e Operational Technology

3.1 In breve: la Security OT in relazione ai BSA

L'abbreviazione OT sta per Operational Technology, ossia l'utilizzo di sistemi costituiti da hardware e software destinati al controllo di impianti.

L'impiantistica di esercizio e sicurezza (BSA) comprende dispositivi elettromeccanici e gestionali volti a garantire l'operatività e la sicurezza delle strade nazionali.

Il concetto di OT include dunque i sistemi di controllo e comando dei BSA, l'infrastruttura necessaria (ad es. rete IP BSA), i sistemi OT nonché gli applicativi e i servizi. A loro volta, i sistemi OT e i cosiddetti «aggregati[1]» fanno parte dei BSA.

3.2 Concetti chiave in ambito IT e OT

Lo schema seguente illustra la distinzione tra sfera IT e OT, che ne motiva la gestione e trattazione separata.

Fig. 3.3 Distinzione tra sfera IT e OT

Ambiti d'impiego	**IT**	**OT**
Principali contesti di utilizzo	Comunicazione amministrativa / automazione / applicazioni tecniche senza funzione operativa	Gestione e regolazione affidabili, monitoraggio e controllo di: macchinari, impianti e processi / applicazioni tecniche e applicativi con funzione operativa (ad es. controllo di impianti)
Tipo di attività	Focus sull'interazione transazionale tra persona e applicazione	Interazione basata sugli eventi tra condizioni e sistema di processo
Aspetti legati alla sicurezza	**IT**	**OT**
Obiettivi di Security	Riservatezza Integrità Disponibilità	Sicurezza funzionale Affidabilità Disponibilità
Informazioni e dati critici	Dati operativi (incl. quelli finanziari) Dati personali	Dati dei sistemi di comando (segnali di controllo e sensori)
Integrità	Impatto di livello critico a fronte del contesto.	Impatto di livello critico a fronte del contesto; possibili ripercussioni sull'incolumità personale e sull'ambiente
Disponibilità	Di norma durante gli orari d'ufficio. All'USTRA fanno eccezione le applicazioni tecniche quali SIAC, ETC ecc.	Elevata, in tempo reale (365 giorni l'anno, 24 ore su 24)
Ciclo di vita della tecnologia	3-5 anni; diversi fornitori; estensioni e Lifecycle Management costanti della tecnologia utilizzata	10-20 anni; normalmente un unico fornitore sul lungo periodo; la fine del ciclo di vita del prodotto solleva nuove problematiche relative alla sicurezza
Gestione delle variazioni	Periodica e pianificata in base ai periodi minimi di utilizzo	Pianificazione strategica; processo articolato per via dell'impatto sulla produzione
Sicurezza materiale e ambientale	Da ridotta (sistemi amministrativi) a eccellente (sistemi IT critici)	Di norma eccellente per ambiti critici, maturità variabile in funzione di criticità e cultura

[1] gergo BSA derivato dal tedesco *Aggregat*, equivalente di gruppo o complesso di elementi e componenti di macchinari o dispositivi deputati a una funzione specifica.

4 Security Governance OT

La Security Governance OT (abbreviata in Sec Gov OT) regolamenta la sicurezza dei sistemi OT e garantisce disponibilità, integrità e affidabilità dei sistemi di controllo e comando BSA della rete nazionale. Al contempo si assicura il supporto e l'allineamento tra Security OT e obiettivi dell'Ufficio in ambito di BSA. Mediante l'osservanza delle direttive e i controlli interni, occorre altresì fare in modo che le strategie siano conformi alle leggi e disposizioni vigenti nonché provvedere all'attribuzione delle rispettive responsabilità e competenze: la Governance stabilisce quali soggetti detengono potere decisionale, definisce il quadro per l'obbligo di rendicontazione e garantisce un monitoraggio finalizzato a ridurre adeguatamente i rischi.

4.1 Obiettivi specifici della Security Governance OT

Strutturazione, aggiornamento e monitoraggio del contesto di applicazione della Security Governance OT, con particolare riferimento a:

- Definizione, disposizione e controllo di standard e buone pratiche per la valutazione dei rischi e per tutte le attività attinenti alla fornitura di servizi (attività OT in tutte le fasi progettuali, esercizio OT di applicazioni tecniche e applicativi con funzioni operative), tenendo in considerazione l'equilibrio ottimale tra performance e conformità;
- Definizione, impartizione e verifica dell'osservanza delle prescrizioni; garanzia dell'adeguata assistenza per progetti OT e applicazioni tecniche o applicativi con funzioni operative mediante assunzione del ruolo di lead dell'architettura;
- Verifica da parte dell'ISIU della rilevanza attuativa discrezionale delle disposizioni TIC per le strade nazionali;
- Assicurazione del rispetto delle disposizioni normative, federali e dipartimentali correlate a OT e sistemi di integrazione.

5 Contesto ed elementi fondanti

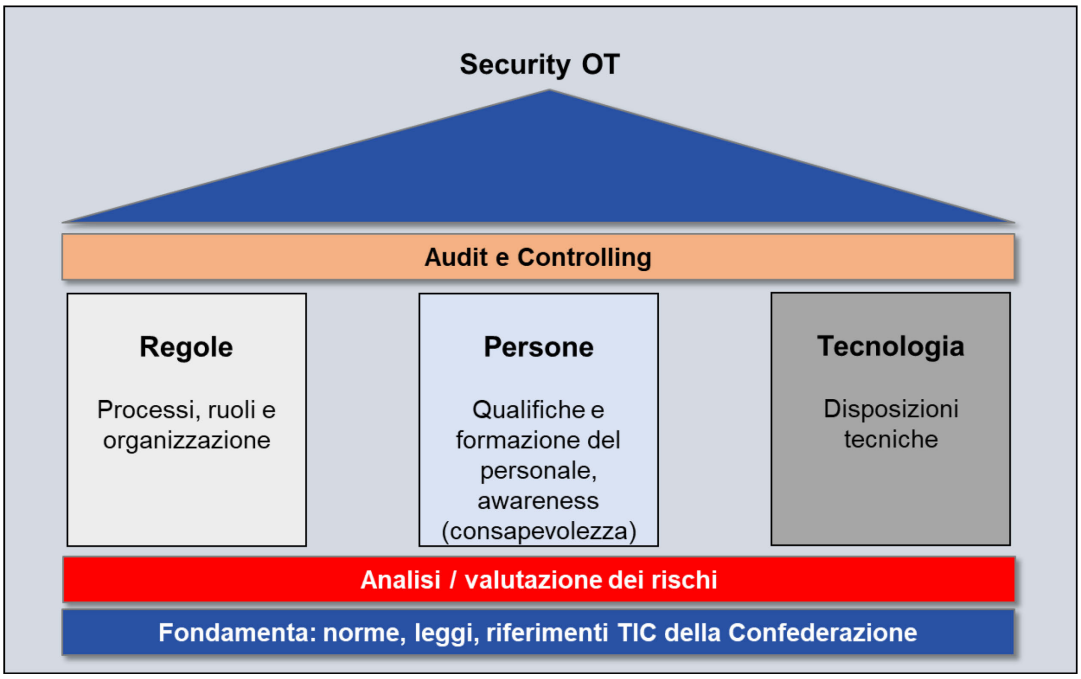

Fig. 5.4 OT Security Management System, gestione della sicurezza informatica (OT-SMS)

5.1 Elementi dell'OT-SMS

Attorno ai tre componenti fondanti (regole, persone e tecnologia) si collocano tre elementi essenziali, illustrati nei successivi sottocapitoli.

5.1.1 Fondamenta: norme, leggi, riferimenti TIC della Confederazione

Disposizioni attuative riguardanti la gestione dei documenti di riferimento, in particolare delle prescrizioni TIC della Confederazione (trasformazione digitale e coordinamento TIC). L'applicabilità all'infrastruttura della rete viaria nazionale è sottoposta a specifico esame.

5.1.2 Audit e controlling

Disposizioni e norme in materia di audit e monitoraggio periodico di OT-SMS e relativa attuazione. Per gli audit, le mansioni di controlling e le attività di garanzia della qualità sono disponibili piani di verifica, checklist e verbali di collaudo.

5.1.3 Analisi / valutazione dei rischi

L'analisi e la valutazione dei rischi stabiliscono i pericoli da contrastare e il relativo ordine di priorità. La gestione del rischio viene eseguita a livello centrale, in funzione del progetto e in ottica operativa.

L'attività di analisi prevede l'esame dei rischi rilevati in diverse fattispecie e situazioni di pericolo durante la fase di individuazione.

Per valutazione si intende lo studio del rischio condotto dal soggetto a esso esposto oppure da terzi.

5.2 Componenti fondanti di OT-SMS

I sottocapitoli seguenti illustrano i componenti fondanti: regole, persone e tecnologie.

5.2.1 Regole: processi, ruoli e organizzazione

Disposizioni e norme in materia di ruoli, mansioni, competenze e responsabilità, ad esempio:

- SPOC (Single Point of Contact);
- Processi di escalation;
- Regolamentazione di entrate e accessi.

5.2.2 Persone: qualifiche e formazione tecnica

Disposizioni e norme in materia di qualifiche e formazione del personale, ad esempio:

- Esercitazioni di sicurezza e attività di sensibilizzazione;
- Garanzia del know-how.

5.2.3 Tecnologia: disposizioni tecniche

Disposizioni e norme in materia di sistemi tecnici e relativa gestione, ad esempio:

- Security Monitoring (raccolta e analisi di informazioni da fonti (log) molto diversificate per individuare eventi di incidenza sulla sicurezza, ossia comportamenti sospetti e variazioni di sistema non autorizzate all'interno della rete);
- IAM BSA (Identity e Access Management dei BSA);
- Log Management (definizione, ricezione, salvataggio ed eliminazione di dati di protocollo trasmessi al Security Monitoring).

5.3 Quadro regolamentare

La regolamentazione è definita all'interno di direttive, standard, schede e manuali tecnici, linee guida e documentazioni.

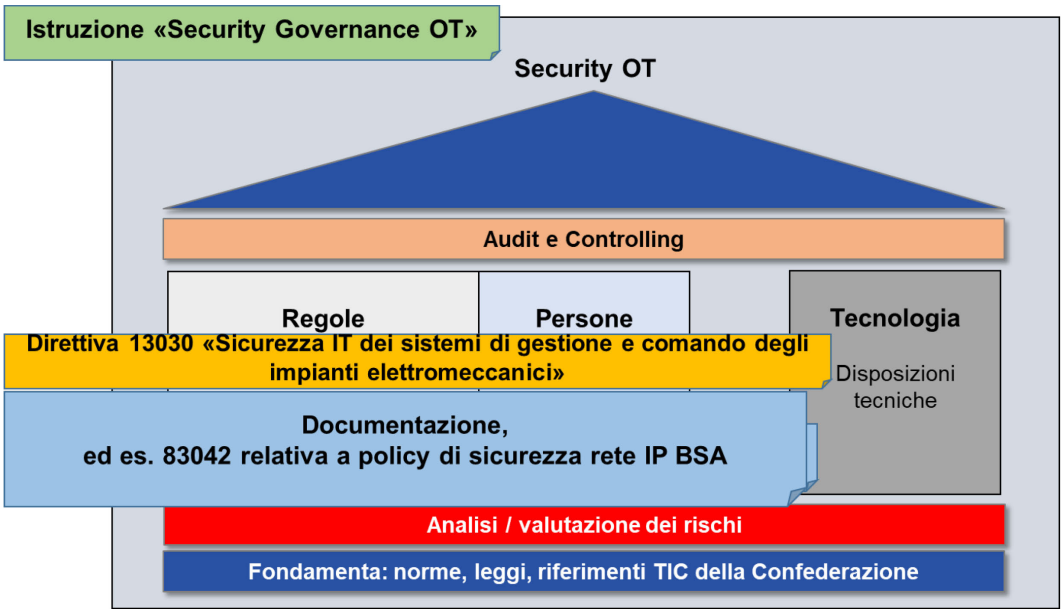

Fig. 5.5 Documenti OT-SMS

La regolamentazione è esposta nei seguenti documenti:

- **Istruzioni 73006 «OT Security Governance»**

  Le istruzioni illustrano il quadro regolamentare della Governance OT per i sistemi di controllo e comando dei BSA.

- **Direttiva 13030 «Sicurezza IT dei sistemi di gestione e comando degli impianti elettromeccanici»**

  La direttiva descrive la materia trattata e i piani di sicurezza fondamentali per minimizzare l'impatto dei rischi individuati.

- **Documentazione**

  La documentazione descrive le modalità d'azione, definendo concretamente misure di attuazione e sistemi di sicurezza, ad esempio IAM BSA oppure la Network Security Policy della rete IP BSA.

5.4 Struttura organizzativa della Security Governance OT (responsabilità)

Le questioni di natura organizzativa sono affrontate in vari ambiti:

- Gestione: adeguamenti, pianificazione e organizzazione;
- Attuazione: strutturazione, reperimento e implementazione;
- Operatività: fornitura, gestione e supporto.

5.4.1 Gestione

L'attività gestionale è affidata al **Change Advisory Board di Security OT (CAB-OT-Sec)**, un team incaricato di valutare le variazioni da implementare in ambiente OT; è composto da tecnici dell'USTRA (Centrale, manager di prodotto Security rete IP BSA, settore Esercizio di Infrastruttura, Filiali) e delle Unità territoriali.

Di seguito si riportano le principali mansioni:

- Redigere, aggiornare (se necessario) e attuare coerentemente istruzioni, direttive e documenti attinenti alla sicurezza;
- Raccordare e integrare dal punto di vista metodico il processo di sicurezza con quello di gestione rischi aziendali nonché garantire il rispetto delle disposizioni procedurali di risk management.

5.4.2 Attuazione

L'attuazione rientra nella competenza di: manager di prodotto, sovrastruttura operativa rete IP BSA, responsabili di progetto delle Filiali e Information Security Officer (BSA) delle Unità territoriali.

Di seguito si riportano le principali mansioni:

- Garantire la gestione tecnica della sicurezza delle informazioni in contesto OT e definire la priorità delle attività in base alla situazione;
- Assicurare l'individuazione, l'analisi e qualora necessario il trattamento di nuove problematiche attinenti alla sicurezza;
- Garantire l'adeguatezza della reportistica rivolta alla Direzione sul piano del contenuto, del livello e delle scadenze.

5.4.3 Esercizio

L'operatività è di competenza delle Unità territoriali e delle sovrastrutture organizzative rete IP BSA e I-B.

Di seguito si riportano le principali mansioni:

- Garantire la reperibilità di risorse e know-how adeguati nell'intera gestione della sicurezza;
- Monitorare lo svolgimento periodico di verifiche, audit e penetration test (analisi della vulnerabilità);
- Adempiere all'obbligo di informazione in caso di eventi di incidenza sulla sicurezza.

Acronimi

Voce	Significato
CAB	Comitato consultivo per le modifiche *Change Advisory Board*
CaF	Cancelleria federale
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
ETC	*Easy Way for Traffic Control* (applicazione tecnica per documentare e analizzare i risultati anonimizzati dei controlli del traffico pesante)
GOV	Governance
I-B	Settore Esercizio della Divisione Infrastruttura
IAM BSA	Gestione delle identità e degli accessi *Identity & Access Management*
IES *BSA*	Impiantistica di esercizio e sicurezza (impianti tecnologici) *Betriebs- und Sicherheitsausrüstungen*
IoT	Internet delle cose *Internet of Things*
IP	Protocollo di rete *Internet Protocol*
ISID	Incaricato della sicurezza informatica del dipartimento
ISIU	Incaricato della sicurezza informatica dell'unità amministrativa
IT	Tecnologia informatica *Information Technology*
LPD e OLPD	Legge federale sulla protezione dei dati e relativa ordinanza
NCSC	Centro nazionale per la cibersicurezza *National Cyber Security Centre*
OCiber	Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale
OLPD	Ordinanza relativa alla legge federale sulla protezione dei dati
OPrI	Ordinanza sulla protezione delle informazioni della Confederazione
OT	Operational Technology *Tecnologia operativa*
OT SMS	Tecnologia operativa di gestione della sicurezza informatica *Operational Technology Security Management System*
OTDI	Ordinanza sulla trasformazione digitale e l'informatica
SG	Segreteria generale del DATEC
SIAC	Sistema d'informazione sull'ammissione alla circolazione
SNPC	Strategia nazionale per la protezione della Svizzera contro i ciber-rischi
SPOC	Punto di contatto centralizzato *Single Point of Contact*
TIC *ICT*	Tecnologie dell'informazione e della comunicazione *Information and communications technology*

Riferimenti normativi e bibliografici

Leggi federali

[1] Confederazione Svizzera (1992), "**Legge federale sulla protezione dei dati (LPD)**", RS *235.1*, www.admin.ch.

[2] Confederazione Svizzera (1960), "**Legge federale sulle strade nazionali (LSN)**", RS *725.11*, www.admin.ch.

[3] Confederazione Svizzera (1958), "**Legge federale sulla circolazione stradale (LCStr)**", RS *741.01*, www.admin.ch.

Ordinanze

[4] Confederazione Svizzera (1993), "**Ordinanza relativa alla legge federale sulla protezione dei dati (OLPD)**", RS *235.11*, www.admin.ch.

[5] Confederazione Svizzera (2007) "**Ordinanza sulla protezione delle informazioni della Confederazione (Ordinanza sulla protezione delle informazioni, OPrI)**", RS *51.411*, www.admin.ch.

[6] Confederazione Svizzera (2020), "**Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi, OCiber)**", RS *120.73*, www.admin.ch.

[7] Confederazione Svizzera (2020), "**Ordinanza sulla trasformazione digitale e l'informatica, (OTDI)**", RS *172.010.58*, www.admin.ch.

[8] Confederazione Svizzera (2007), "**Ordinanza sulle strade nazionali (OSN)**", RS *725.111*, www.admin.ch.

Istruzioni e documenti strategici

[9] Confederazione Svizzera "**Strategia nazionale per la protezione della Svizzera contro i ciber-rischi**" (SNPC 2018-2022).

[10] Confederazione Svizzera "**Strategia relativa alle reti della Confederazione**" del novembre 2018.

[11] Confederazione Svizzera "**Weisung über die Betreiber- und Sourcingentscheide im UVEK**" del 01.01.2022.

[12] Confederazione Svizzera "**Istruzioni sull'uso degli strumenti informatici al DATEC**" del 1.1.2022.

[13] Confederazione Svizzera "**Weisung zur Steuerung, Führung und Kontrolle der Informatik und Digitalisierung im UVEK**" del 01.01.2022.

[14] Confederazione Svizzera "**Weisung Unternehmensarchitektur Management UVEK**" del 1.1.2022.

[15] Confederazione Svizzera "**Si001: Protezione di base delle TIC nell'Amministrazione federale –Versione 5.0**" a cura del NCSC del 23.2.2022.

Cronologia redazionale

Edizione	Versione	Data	Operazione
2022	1.00	31.10.2022	Entrata in vigore edizione 2022 (versione originale in tedesco).