Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Ufficio federale dei trasporti UFT
Divisioni Infrastruttura e Sicurezza

Riferimento: BAV-041.4-3/11/6/15/1/4/1
Data: 24.06.2024
Versione: V1.1

Direttiva

Cibersicurezza in ambito ferroviario

D CySec-Rail

Sulla base dell'articolo 2 capoverso 1bis dell'ordinanza sulle ferrovie (Oferr; RS 742.141.1) e le relative disposizioni d'esecuzione

Editore: Ufficio federale dei trasporti, 3003 Berna
Divisioni Infrastruttura e Sicurezza

Distribuzione: Pubblicazione sul sito Internet dell'UFT
(https://www.bav.admin.ch)

Lingue: Tedesco (originale)
Francese
Italiano

Entrata in vigore: 1° luglio 2024

Ufficio federale dei trasporti
Divisione Infrastruttura

Remund Zuffi Anna Barbara G0BQTG
04.07.2024

Info: admin.ch/esignature | validator.ch

Anna Barbara Remund
Vicedirettrice

Divisione Sicurezza

Sperlich Rudolf 7OUWIO
04.07.2024

Info: admin.ch/esignature | validator.ch

Dott. Rudolf Sperlich
Vicedirettore

Edizioni / cronologia redazionale

Versione	Data	Autore	Modifiche	Stato
V0.4	15.12.2022	Ufficio federale dei trasporti	Rielaborazione dopo revisione SI/st (UFT)	Revisione nel settore
V0.5	27.03.2023	Ufficio federale dei trasporti	Rielaborazione dopo revisione nel settore	Sostituita
V0.7	20.07.2023	Ufficio federale dei trasporti	Lettura di Redguard AG e adeguamento finale	Sostituita
V1.0	22.09.2023	Ufficio federale dei trasporti	Adeguamenti dopo la traduzione	Sostituita
V1.1	24.06.2024	Ufficio federale dei trasporti	Aggiornamento (v. elenco delle modifiche alla fine del documento)	In vigore

[x] Stati previsti: in elaborazione / in revisione / pubblicata / in vigore (con visto) / (versione) sostituita

Indice

1 Situazione iniziale

La disponibilità e la correttezza dei dati e delle informazioni sono un fattore di successo fondamentale per tutti i processi aziendali nel settore dei trasporti pubblici. L'avanzamento della digitalizzazione fa sì che oggi la maggior parte delle informazioni venga elaborata e salvata elettronicamente. Al contempo ci sono sempre più sistemi diversi tra loro e sempre più interconnessi. I confini tra le applicazioni informatiche, gli impianti di comunicazione, industriali e ferroviari così come si conoscono nei trasporti pubblici vanno via via scomparendo.

Si crea così un'elevata dipendenza dai sistemi e dalle applicazioni che elaborano informazioni. La crescente interconnessione apre sì nuove possibilità e opportunità imprenditoriali, ma la correlata maggiore esposizione agli attacchi cibernetici fa sì che i possibili pericoli cambino in continuazione. Lo stesso vale per la potenziale entità dei danni in caso di attacco. Tuttavia, negli ultimi anni vi è stato un grande cambiamento nella consapevolezza dell'opinione pubblica riguardo alle minacce informatiche. Le ripercussioni di attacchi cibernetici sono infatti sempre più numerose e tangibili.

2 Obiettivo e scopo

Il presente documento precisa la strutturazione minima del sistema di gestione della sicurezza delle informazioni (SGSI) di cui alle disposizioni d'esecuzione dell'Oferr (DE-Oferr) DE 2.1^{bis} numero 1.2[2].

Informazioni, dati e sistemi vanno protetti secondo la rispettiva esigenza di protezione e tenendo conto della specifica situazione di rischio.
Tale approccio basato sul rischio è il fondamento per chi applica la presente direttiva.

Esso indica la necessità di definire misure di riduzione del rischio e possibili lacune tra la riduzione del rischio attuale e il livello di rischio sostenibile, una volta individuati i maggiori rischi imprenditoriali a livello normativo, operativo e finanziario o reputazionale (cfr. p. es. ISO/IEC 27005:2022, cap. 6.4).
Il riconoscimento di minacce e l'individuazione di rischi, così come il loro trattamento, sono pertanto temi centrali in un SGSI e nella presente direttiva.

I rimandi a mezzi ausiliari esistenti (all. 3) servono d'aiuto nell'implementazione di un SGSI.

Se le imprese ferroviarie rispettano le disposizioni della direttiva, l'Ufficio federale dei trasporti (UFT) può accettare sotto il profilo metodologico le basi SGSI elaborate. Sono ammesse deroghe a tali disposizioni, purché l'obiettivo perseguito a livello di legge e di ordinanza sia raggiunto in altro modo.

La direttiva funge inoltre da base per le verifiche nel quadro dell'attività di vigilanza dell'UFT.

Considerato che i criminali cibernetici mutano e professionalizzano i loro mezzi e modalità di procedere, la presente direttiva è in continua evoluzione.

3 Basi legali / Riferimenti

Di seguito sono elencati gli standard, le norme e le basi legali su cui si fonda il presente documento.

[1] Legge federale sulle ferrovie (Lferr; RS *742.101*)[1]

[2] Ordinanza sulle ferrovie (Oferr; RS *742.141.1*)[2] e relative disposizioni d'esecuzione (DE-Oferr, innanzitutto DE 2.1^{bis} n. 1.2; RS *742.141.11*)

[3] REGOLAMENTO DELEGATO (UE) 2018/762 DELLA COMMISSIONE, dell'8 marzo 2018[3], che stabilisce metodi comuni di sicurezza relativi ai requisiti del sistema di gestione della sicurezza a norma della direttiva (UE) 2016/798 del Parlamento europeo e del Consiglio e che abroga i regolamenti della Commissione (UE) n. 1158/2010 e (UE) n. 1169/2010 (CSM sul SGS).

[4] Ordinanza concernente il coordinamento dei trasporti in situazioni eccezionali (OCTSE, cfr. https://www.bav.admin.ch e https://www.fedlex.admin.ch/it)

[5] Legge sulla protezione dei dati (LPD; RS *235.1*)[4]

[6] Legge sulla sicurezza delle informazioni (LSIn)[5] – L'articolo concernente l'obbligo di notifica in caso di attacco cibernetico entrerà in vigore nel 2025.

[7] Ordinanza concernente le inchieste sulla sicurezza in caso di eventi imprevisti nei trasporti (OIET; RS *742.161*)[6]

[8] SN ISO/IEC 27001:2022 (panoramica all. 2, cap. 11)[7]

[9] SN ISO/IEC 27002:2022[8]

[10] NIST Cybersecurity Framework CSF 2.0 (NIST CSF 2.0)[8]

[11] CLC/TS 50701:2023[9]

[12] IEC 62443[10]

[13] Manuale di cybersicurezza per le imprese di trasporti pubblici (Manuale UTP del 2020)[11]

[1] https://www.fedlex.admin.ch/eli/cc/1958/335_341_347/it

[2] https://www.fedlex.admin.ch/eli/cc/1983/1902_1902_1902/it

[3] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32018R0762

[4] https://www.fedlex.admin.ch/eli/cc/2022/491/it

[5] https://www.fedlex.admin.ch/eli/fga/2023/2296/it

[6] https://www.fedlex.admin.ch/eli/cc/2015/26/it

[7] Accessibile sulla piattaforma delle norme dell'UTP, esclusivamente ai collaboratori delle imprese di trasporto svizzere associate (senza FFS), dell'UFT e di ZVV: www.voev.ch/normenplattform

[8] https://www.nist.gov/cyberframework

[9] Accessibile sulla piattaforma delle norme dell'UTP, esclusivamente ai collaboratori delle imprese di trasporto svizzere associate (senza FFS), dell'UFT e di ZVV: www.voev.ch/normenplattform

[10] Parzialmente accessibile sulla piattaforma delle norme dell'UTP, esclusivamente ai collaboratori delle imprese di trasporto svizzere associate (senza FFS), dell'UFT e di ZVV: www.voev.ch/normenplattform

[11] https://www.bwl.admin.ch/bwl/it/home/bereiche/ikt/ikt_minimalstandard/ikt_branchenstandards/oeffentlicher_verkehr.html

[14] SN EN 50159:2010[12]

[15] Whitepaper della BDEW Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (versione 2.0 05/2018; Requisiti per sistemi di controllo e di telecomunicazione sicuri)[13]

[16] Ordinanza sulla videosorveglianza nei trasporti pubblici (OVsor-TP; RS *742.147.2*)[14]

[17] Guida integrativa ISO/IEC 27001:2022 di ISACA[15] (solo in ted.)

[18] D RTE 28100 - Nachweisführung Datennetze (Prova reti di dati; Unione dei trasporti pubblici UTP; solo in ted. e fr.)

Quali norme prediligere?

Per la creazione e il mantenimento di un SGSI si è attestata quale norma riconosciuta a livello internazionale la ISO/IEC 27001. La ISO/IEC 27002 è la guida per le misure (controls) da attuare in funzione dei rischi sulla base dei requisiti della ISO/IEC 27001.

Le norme IEC 62443 si basano su quelle ISO 27000, estendendole con le differenze e le specificazioni dell'automazione industriale. Le CLC/TS 50701 si rifanno alle norme IEC 62443 con specificazioni riguardanti i sistemi e i veicoli ferroviari (cfr. anche fig. 1 al n. [11]).

Nel settore degli impianti elettrici sono ampiamente diffusi il referenziato whitepaper della BDEW [15] e la ISO/IEC 27019.

Adatto per un'introduzione al tema della cibersicurezza nelle ferrovie è invece il Manuale di cybersicurezza per le imprese di trasporti pubblici [13], che contiene altresì un mezzo ausiliario per l'autovalutazione.

Per quanto concerne l'introduzione e l'esercizio di nuove reti di dati presso i gestori dell'infrastruttura (GI) si rimanda alla nuova direttiva «D RTE 28100 - Nachweisführung Datennetze», che l'UTP pubblicherà nel secondo semestre 2024 [18].

[12] Accessibile sulla piattaforma delle norme dell'UTP, esclusivamente ai collaboratori delle imprese di trasporto svizzere associate (senza FFS), dell'UFT e di ZVV: www.voev.ch/normenplattform

[13] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf

[14] https://www.fedlex.admin.ch/eli/cc/2009/736/it

[15] https://www.isaca.de/publikationen/publikationen/leitfaeden.html

4 Struttura

Il **capitolo 5** espone il campo d'applicazione della presente direttiva e fornisce alcune indicazioni sulla delimitazione dei requisiti minimi descritti.

Al **capitolo 6** si sottolinea l'importanza di un'adeguata integrazione dell'SGSI nei processi esistenti e nella cultura della sicurezza delle imprese e si crea il nesso con gli altri sistemi di gestione e le norme e gli standard esistenti.

I requisiti minimi descritti sono suddivisi nei due capitoli 7 e 8.

- **Capitolo 7:** contiene i requisiti dell'SGSI volti a impostare e gestire gli aspetti della sicurezza delle informazioni in maniera sistematica e tenendo conto di tutte le disposizioni e le esigenze. Il capitolo 7 precisa le DE 2.1^{bis} numero 1.2 delle DE-Oferr [2] e definisce i requisiti minimi di un SGSI, focalizzandosi su quelli procedurali del sistema di gestione.

- **Capitolo 8:** comprende misure tecniche e organizzative (i cosiddetti «controls») volte a garantire un livello adeguato di sicurezza delle informazioni per il settore ferroviario, considerato parte delle infrastrutture critiche della Svizzera. Sono incluse sia misure generali, valide per tutti i sistemi e le applicazioni, sia misure specifiche per il settore Tecnologia operativa (OT, dall'ingl. operational technology) e per i veicoli ferroviari.

L'**allegato 1** contiene una breve panoramica del nesso tra un SGSI e gli altri sistemi di gestione come parte di un sistema di gestione integrato (SGI).

L'**allegato 2** riporta una breve panoramica delle norme ISO/IEC 27001 e 27002, d'importanza fondamentale per la creazione e l'ulteriore sviluppo di un SGSI.

All'**allegato 3** sono indicati i mezzi ausiliari per l'implementazione di un SGSI.

L'**allegato 4** contiene il modulo di domanda per l'esonero dall'obbligo di SGSI per ITF e/o GI secondo il campo d'applicazione di cui al capitolo 5.

5 Campo d'applicazione

I requisiti minimi si applicano alle organizzazioni e imprese elencate di seguito.

- **Gestore dell'infrastruttura ferroviaria (GI):** impresa in possesso di una concessione e di un'autorizzazione di sicurezza secondo l'articolo 5 Lferr per la costruzione e l'esercizio di un'infrastruttura ferroviaria. Quest'ultima comprende gli impianti per l'esercizio delle ferrovie, inclusi quelli elettrici.

- **Impresa di trasporto ferroviario (ITF):** impresa in possesso di un certificato di sicurezza secondo l'articolo 8*c* Lferr.

Le disposizioni contenute riguardano tutti i processi, i sistemi di trattamento delle informazioni (HW+SW) e le reti di dati impiegati nel quadro delle succitate attività o che indirettamente ne consentono lo svolgimento.
Esse si applicano anche nel caso in cui singole attività vengono delegate a terzi (p. es. fornitori, fabbricanti, imprese di manutenzione, servizi competenti per la manutenzione, detentori di veicoli ferroviari, fornitori di servizi ed enti appaltanti). Responsabili per il loro rispetto restano i GI e/o le ITF.

Le disposizioni sono valide per tutti i sistemi di trattamento delle informazioni (HW + SW) e le reti di dati nei settori tecnologia dell'informazione (IT, dall'ingl. information technology) e OT degli impianti fissi come pure per i veicoli ferroviari.

ITF e GI poco o per niente esposti a tali attacchi nel settore della sicurezza delle informazioni (p. es. ferrovie storiche) possono richiedere all'UFT un esonero dall'obbligo SGSI. Per farlo è necessario compilare il modulo all'allegato 4 e inviarlo per via elettronica tramite il sito Internet dell'UFT https://www.bav.admin.ch. In casi eccezionali e previo accordo con l'UFT, Sezione Omologazioni e regolamenti, è possibile inoltrare le domande firmate alla casella postale zulassung@bav.admin.ch, alla quale si può altresì scrivere per ricevere informazioni. Non è necessario un invio postale separato.

Le ITF che hanno richiesto congiuntamente il CSic e l'ASic (art. 5*d* cpv. 1 Oferr) possono presentare una sola domanda di esonero.

Gli emolumenti si calcolano sulla base dell'ordinanza sugli emolumenti per i trasporti pubblici (OEm-TP; RS *742.102*).

5.1 Delimitazioni

In funzione del campo d'applicazione, la responsabilità di una protezione adeguata dei propri dati e informazioni è del rispettivo GI e/o della rispettiva ITF. Il presente documento si delimita secondo i seguenti principi:

- le disposizioni prevedono misure per garantire un livello minimo di sicurezza delle informazioni;

- a seconda delle condizioni organizzative specifiche e quale risultato di valutazioni del rischio possono essere necessarie misure più estese;

- l'attuazione delle disposizioni qui riportate non è sufficiente a ottenere una certificazione (p. es. ISO/IEC 27001).

6 Relazione con altri sistemi di gestione

Nello strutturare e attuare il SGSI va considerato che le imprese interessate potrebbero già disporre di altri sistemi di gestione. Il SGSI va pertanto implementato in modo tale da non creare conflitti tra sistemi. Qualora questi fossero inevitabili o probabili, bisogna documentarli. Se possibile e opportuno, sfruttare gli elementi disponibili e le connesse sinergie dei sistemi di gestione esistenti. Occorre puntare a un sistema di gestione integrato (SGI; cfr. all. 1).

7 Requisiti minimi del sistema di gestione della sicurezza delle informazioni (SGSI)

Il presente capitolo comprende i requisiti del SGSI volti a impostare e gestire gli aspetti della sicurezza delle informazioni in maniera sistematica e tenendo conto di tutte le disposizioni e le esigenze. **Inoltre precisa le DE 2.1^{bis} numero 1.2 delle DE-Oferr** [2] **e definisce i requisiti minimi di un SGSI** focalizzandosi su quelli procedurali del sistema di gestione. Al **capitolo 8** sono presentate misure concrete (i cosiddetti controls), **che contribuiscono all'adempimento dei requisiti descritti nel presente capitolo.**

Nella colonna «Rimando» si rinvia a norme, standard e prescrizioni di pertinenza federale esistenti e si indicano le possibili sinergie con gli allegati I e II[16] del regolamento delegato (UE) 2018/762 (reg. 2018/762) [3]. Nella colonna «Misure Capitolo 8» si rimanda alle misure connesse al requisito.

Le imprese ferroviarie hanno l'obbligo di allestire un calendario vincolante per l'attuazione dei requisiti del SGSI di seguito descritti e di presentarlo all'UFT su richiesta.

N.	Requisito	Rimando	Misure Capitolo 8
A-01	**Strategia sulla sicurezza delle informazioni** L'alta dirigenza deve stabilire quali obiettivi debbano essere raggiunti con la sicurezza delle informazioni. Tali obiettivi devono essere conciliabili con l'orientamento dell'impresa e gli interessi delle parti coinvolte. L'alta dirigenza deve garantire la disponibilità delle risorse necessarie al loro raggiungimento. Inoltre occorre definire quali settori commerciali sono coperti dal SGSI e in quali invece quest'ultimo non trova applicazione. Il campo d'applicazione minimo del SGSI è riportato al capitolo 5.	ISO/IEC 27001 Cap. 5.1 NIST CSF 2.0 GV.OC-01 GV.PO-01 GV.PO-02 Manuale UTP Cap. 3.2.1 e 3.2.3 Reg. 2018/762 Cap. 1 Cap. 2.1	B-01 B-04 B-05 B-06 B-08 B-09 B-10 B-18 B-20
A-02	**Ruoli e responsabilità** Le responsabilità e le competenze dei ruoli attinenti alla sicurezza delle informazioni devono essere definite e assegnate chiaramente. Occorre nominare un incaricato all'interno dell'impresa e informarne l'UFT.	ISO/IEC 27001 Cap. 5.3 NIST CSF 2.0 GV.RR-02 Manuale UTP Cap. 3.2.2 Reg. 2018/762 Cap. 2.3	B-01 B-02 B-04 B-06 B-08 B-09 B-10 B-12 B-16 B-22 B-23 B-28

[16] Il contenuto degli allegati I e II del reg. 2018/762 è identico, di conseguenza non si fa distinzione.

A-03	**Direttive e organizzazione** **L'alta dirigenza deve garantire che il SGSI sia integrato nei processi aziendali dell'impresa** (v. es. nella fig. 1 all. 1). A tale fine occorre redigere direttive di sicurezza delle informazioni, farle approvare dall'alta dirigenza o dai responsabili e divulgarle in seno all'impresa e ai servizi esterni interessati.	ISO/IEC 27001 Cap. 5.2 NIST CSF 2.0 GV.OC-03 GV.RM-03 Manuale UTP Cap. 3.2.3 Reg. 2018/762 Cap. 2.1-2.4	B-02 B-03 B-04 B-05 B-06 B-07 B-08 B-09 B-10 B-11 B-12 B-15 B-16 B-17 B-18 B-20 B-21 B-22 B-24 B-25 B-29
A-04	**Verifica periodica della sicurezza delle informazioni / Audit** Mediante audit periodici si individuano gli ambiti nei quali va migliorata la sicurezza delle informazioni, inclusi anche i fornitori e le società di servizi. Gli ambiti tematici da verificare e la periodicità degli audit devono essere stabiliti in un apposito programma. Le relative misure saranno da attuare secondo priorità prestabilite.	ISO/IEC 27001 Cap. 9.1 Cap. 9.2 NIST CSF 2.0 GV.SC-07 PR.PS-04 Reg. 2018/762 Cap. 6.1 Cap. 6.2	B-04 B-05 B-06 B-08 B-09 B-10 B-14 B-20
A-05	**Miglioramento continuo** L'impresa deve migliorare continuamente l'idoneità e l'efficacia del proprio SGSI. La verifica deve essere condotta almeno una volta l'anno.	ISO/IEC 27001 Cap. 5.1 Cap. 9.3 Cap. 10 NIST CSF 2.0 ID.IM-03 Reg. 2018/762 Cap. 6.3 Cap. 7	B-04 B-08 B-14

A-06	**Documentazione** Tutti risultati e le attività rilevanti connessi al SGSI devono essere documentati e verbalizzati. Vale a dire, in particolare: a) la descrizione dei processi e delle attività correlate alla sicurezza delle informazioni dell'esercizio ferroviario, compresi i compiti rilevanti per la sicurezza e le relative responsabilità; b) l'identificazione di appaltatori, partner e fornitori con descrizione di tipo e portata dei servizi forniti; c) l'identificazione degli accordi contrattuali o commerciali di altro tipo, conclusi tra l'impresa e le altre parti di cui alla lettera b, necessari al fine di controllare i rischi per la sicurezza generati dall'impresa e dal ricorso ad appaltatori. La documentazione e i verbali devono essere protetti contro accessi non autorizzati e perdita.	ISO/IEC 27001 Cap. 4.1 Cap. 4.2 Cap. 7.5 NIST CSF 2.0 GV.PO-01 GV.PO-02 GV.OC-03 Reg. 2018/762 Cap. 4.5	La documentazione adeguata per ogni misura di base B v. cap. 8
A-07	**Valutazione e trattamento del rischio** L'impresa deve definire e adottare un processo di valutazione dei rischi per la sicurezza delle informazioni. Devono essere stabiliti criteri per l'accettazione del rischio e la conduzione di valutazioni del rischio. Il processo deve comprendere i punti seguenti. **a) Identificazione dei rischi** Individuare i rischi relativi a integrità, disponibilità e confidenzialità derivanti da sistemi d'informazione guasti o compromessi; designare persone che fungano da responsabili dei rischi. **b) Analisi dei rischi** Stimare le possibili conseguenze e la probabilità d'insorgenza dei rischi identificati. **c) Valutazione dei rischi** Comparare i risultati dell'analisi dei rischi (risk assessment) con i criteri di rischio definiti e stabilire un ordine di priorità del relativo trattamento. **d) Trattamento dei rischi** Selezionare, sulla scorta dei risultati della valutazione, misure adeguate per trattare i rischi e pianificarne e gestirne l'attuazione. Il/la responsabile dei rischi deve approvare tale piano, documentare ed eventualmente accettare i rischi residui e informare i collaboratori e gli esterni coinvolti. Occorre assicurare che tali passi vengano ripetuti in caso di cambiamenti rilevanti o di un inasprirsi della minaccia. I passi a) – d) devono essere ripetuti almeno una volta all'anno al fine di identificare nuovi rischi, eventualmente rivalutare quelli esistenti e verificare l'efficacia delle misure adottate.	DE-Oferr DE 2.1^{bis} n. 1.2 ISO/IEC 27001 Cap. 6.1.2 Cap. 6.1.3 NIST CSF 2.0 GV.RM-01 GV.RM-02 GV.SC-01 Manuale UTP Cap. 3.3 Reg. 2018/762 Cap. 3.1 (inserimento nel SGS di minacce rilevanti scaturite dall'analisi dei rischi per la cibersicurezza) Mezzi ausiliari per la gestione dei rischi v. all. 3	B-04 B-13 B-15 B-16 B-19 B-20 B-26 B-27

8 Misure di base (controls)

Le misure qui presentate contribuiscono a soddisfare i requisiti del capitolo 7 e a raggiungere un livello minimo di sicurezza delle informazioni nel settore ferroviario.

L'attuazione delle misure e della loro priorizzazione deve avvenire in funzione dei rischi, il che significa che in virtù dell'analisi dei rischi e dell'esigenza di protezione dei sistemi potrebbe emergere la necessità di misure supplementari o che alcune delle misure qui riportate non siano adeguate.
È consentito realizzare altre misure di compensazione o reagire a conflitti di obiettivi, sempre che l'obiettivo perseguito a livello di legge e di ordinanza venga raggiunto (v. anche [11]). Le misure di compensazione devono essere definite per iscritto.

8.1 Misure a livello organizzativo, di personale, fisico e tecnologico per IT, OT, reti di dati, veicoli ferroviari inclusi

Il presente capitolo comprende misure a livello organizzativo, di personale, fisico e tecnologico (i cosiddetti «controls») volte a garantire un livello adeguato di sicurezza delle informazioni per il settore ferroviario, considerato parte delle infrastrutture critiche della Svizzera.

In questo capitolo 8.1 sono dunque riportate le misure valide per tutti i sistemi e le applicazioni. Al capitolo 8.2 sono presentate le misure specifiche per il settore OT, al capitolo 8.3 le misure specifiche per i veicoli ferroviari.

Nella colonna «Misura» sono descritte misure concrete che si rifanno anche alla ISO/IEC 27001:2022 [8] e/o alla ISO/IEC 27002:2022 [9]. Nella colonna «Rimando» si rinvia a norme, standard, mezzi ausiliari e prescrizioni di pertinenza federale. Nell'ultima colonna sono indicate le possibili sinergie con il SGS [3].

N.	Misura	Rimando	Sinergia con il reg. 2018/762 [3]
B-01	**Determinazione di ruoli e responsabilità** Occorre definire ruoli e responsabilità per il settore della sicurezza delle informazioni, assegnando le singole sfere di compiti a persone con le adeguate conoscenze specialistiche.	ISO/IEC 27002:2022 Cap. 5.2 NIST CSF 2.0 GV.RR-02	Cap. 2.3 Cap. 4.1 Cap. 4.2
B-02	**Gestione dell'accesso e dell'identità** Occorre verificare e gestire le identità di persone e sistemi che hanno accesso a informazioni o ad altri asset. a) Assegnare un'identità sempre solo a una persona o a un sistema b) Definire a quali identità sono attribuiti quali diritti e accessi c) Applicare i principi della necessità di sapere (need-to-know) e del privilegio minimo (least-privilege) d) Verificare periodicamente i diritti concessi e adeguarli alle nuove circostanze e) Disattivare identità non più attive	ISO/IEC 27002:2022 Cap. 5.3 Cap. 5.15 Cap. 5.16 Cap. 5.17 Cap. 5.18 NIST CSF 2.0 PR.AA-01 PR.AA-02 PR.AA-05 PR.AA-06	

B-03	**Asset management (gestione dei mezzi operativi)** a) Allestire un inventario di dati, informazioni e sistemi di trattamento delle informazioni b) Nominare un responsabile per ogni asset ovvero categoria c) Implementare una procedura che garantisca l'inserimento di nuovi asset e l'aggiornamento dell'inventario d) Classificare l'esigenza di protezione degli asset ovvero delle categorie in quanto a confidenzialità, integrità e disponibilità	ISO/IEC 27002:2022 Cap. 5.9 Cap. 5.11 Cap. 5.12 Cap. 7.8 Cap. 7.14 NIST CSF 2.0 ID.AM-01 ID.AM-02 ID.AM-05 Manuale UTP Cap. 3.3.1 TS50701:2023 Cap. 4.2	Cap. 5.2
B-04	**Gestione dei fornitori** Secondo il campo d'applicazione di cui al capitolo 5 occorre garantire che la sicurezza delle informazioni venga considerata nella collaborazione con i fornitori. a) Registrare e valutare tutti i fornitori e il loro contributo alla sicurezza delle informazioni b) Obbligare i fornitori, in funzione dell'esigenza di protezione (criticità) dei dati trattati, a rispettare le disposizioni rilevanti in materia di sicurezza delle informazioni nell'ambito della loro fornitura di prestazioni (tale obbligo va trasmesso anche ai loro collaboratori ed eventuali subfornitori) c) Informare e formare i collaboratori dei fornitori mediante corsi periodici sulle disposizioni legislative e interne di protezione delle informazioni e sulla gestione sicura di sistemi di trattamento delle informazioni d) Prevedere un diritto di audit per contratto, se i documenti di prova non sono altrimenti sufficienti e) Verificare periodicamente se sono rispettate le disposizioni definite contrattualmente	ISO/IEC 27002:2022 Cap. 5.18 Cap. 5.19 Cap. 5.20 Cap. 5.21 LPD NIST CSF 2.0 GV.OC-04 GV.OC-05 GV.SC-01 GV.SC-03 GV.SC-05 GV.SC-07 Manuale UTP Tab. 6 Cap. 3.6 V. anche all. 3 Mezzi ausiliari	Cap. 2.4 Cap. 5.3

B-05	**Sicurezza delle informazioni in progetti con nesso IT e OT** (anche acquisti incl.) nonché negli sviluppi di processi e organizzazione a) Seguire un metodo gestionale di progetto definito b) Considerare la sicurezza delle informazioni come componente del metodo gestionale di progetto c) Determinare, all'inizio del progetto, l'esigenza di protezione e i requisiti rilevanti riguardanti la sicurezza delle informazioni d) Verificare e documentare il grado di adempimento dei suddetti requisiti durante il progetto e) Divulgare in seno all'impresa i requisiti non attuati o i rischi noti f) Integrare tempestivamente i requisiti di sicurezza delle informazioni nei progetti, documentarne il rispetto e fare rapporto agli importanti gruppi d'interesse	ISO/IEC 27002:2022 Cap. 5.2 Cap. 5.8 NIST CSF 2.0 GV.PO-02 ID.RA-04 OT: TS50701:2023 Fig. 6	
B-06	**Misure nel settore cloud** Bisogna garantire che nell'acquisire servizi cloud vengano considerati i requisiti della sicurezza delle informazioni e attuate misure di protezione. Occorre esaminare periodicamente, nel quadro di un processo di approvazione interno, l'idoneità dei servizi cloud che riguardano processi aziendali critici o dati personali. a) Stilare una panoramica di tutti i servizi cloud utilizzati e assegnare un responsabile a ognuno di essi b) Definire in maniera chiara le responsabilità dei fornitori e degli utenti dei servizi cloud (shared responsibility model) c) Verificare, prima dell'uso di servizi cloud, quali dati vi saranno salvati e trattati; condurre un'analisi dei rischi e valutare se le misure di protezione esistenti ovvero quelle proposte dal fornitore dei servizi cloud sono sufficienti	LPD ISO/IEC 27002:2022 Cap. 5.23 Cap. 8.27 Manuale UTP Cap. 3.6.3 V. anche all. 3 Mezzi ausiliari	
B-07	**Sorveglianza (security monitoring)** I sistemi e le reti devono essere sviluppati e configurati in modo che attacchi e anomalie possano essere riconosciuti e valutati quanto prima.	ISO/IEC 27002:2022 Cap. 8.15 Cap. 8.16 NIST CSF 2.0 ID.AM-03 DE.AE DE.CM Manuale UTP Cap. 3.6.4	

B-08	**Gestione di incidenti riguardanti la sicurezza delle informazioni** a) Stabilire procedure per la gestione di incidenti riguardanti la sicurezza delle informazioni. Descrivere nel processo la procedura in caso di incidenti riguardanti la sicurezza e definire le responsabilità e le vie di comunicazione b) Garantire nel processo che siano adottate e attuate misure appropriate di reazione e ripristino c) Documentare le singole fasi di trattamento di un incidente d) Rispettare gli obblighi di notifica vigenti nei confronti delle autorità e di terzi (p. es. IFPDT[17], NCSC[18]) e) Trarre le conoscenze e i miglioramenti del caso dagli incidenti riguardanti la sicurezza delle informazioni	ISO/IEC 27002:2022 Cap. 5.24 Cap. 5.25 Cap. 5.26 Cap. 5.27 Cap. 5.28 NIST CSF 2.0 PR.AT-01 RS.MA-01 RS.MA-04 RS.CO-02 RS.CO-03 RS.CO-04 RC.RP-01 ID.IM-03 LPD LSI (obbligo di notifica dal 2025) OIET	Cap. 7 Cap. 7.1. Cap. 7.2.
B-09	**Gestione della continuità aziendale (Business Continuity Management)** È necessario creare un processo che garantisca la prosecuzione dell'attività aziendale in caso di guasto a componenti critiche o a un sistema. In questo contesto sono chiamate in causa sia le tecnologie dell'informazione e della comunicazione sia le tecnologie dell'OT e il settore dei veicoli ferroviari. a) Conoscere e valutare le componenti o i sistemi critici b) Allestire un piano d'emergenza e di ripristino per tutte le componenti e i sistemi critici c) Testare e fare pratica con tali piani periodicamente o dopo cambiamenti sostanziali Vedere anche B-27 Disponibilità	OCTSE Art. 11 ISO/IEC 27002:2022 Cap. 5.29 Cap. 5.30 NIST CSF 2.0 ID.RA-04 RS.MA-01 RS.RP-01 Manuale UTP Cap. 3.3.5	Cap. 5.5

[17] https://www.edoeb.admin.ch/edoeb/it/home.html

[18] https://www.ncsc.admin.ch/ncsc/it/home.html

B-10	**Impiego di collaboratori** Prima e durante l'impiego di un nuovo collaboratore nell'impresa devono essere condotte le misure illustrate di seguito. a) In particolare in caso di collaboratori con attività sensibili sotto il profilo della sicurezza: condurre un'adeguata verifica di sicurezza tenendo conto delle disposizioni di legge rilevanti e della funzione prevista b) Informare i collaboratori mediante corsi periodici sulle disposizioni legislative e interne di protezione delle informazioni e sulla gestione sicura di sistemi di trattamento delle informazioni c) Negli accordi contrattuali obbligare i collaboratori a rispettare le disposizioni di legge e interne in materia di sicurezza delle informazioni d) Stabilire contrattualmente l'obbligo di mantenere il segreto per le persone che lavorano con informazioni degne di protezione o vi hanno accesso Modifica e/o risoluzione dell'impiego e) Disattivare tempestivamente gli accessi all'infrastruttura dell'impresa per le persone che si accingono a lasciarla f) Stabilire un processo che regola la restituzione o la distruzione dei relativi dati, informazioni e apparecchi per l'elaborazione di informazioni in caso di modifica dell'impiego (cambio interno e in particolare uscita)	ISO/IEC 27002 Cap. 6.1 Cap. 6.2 Cap. 6.3 Cap. 6.4 Cap. 6.5 Cap. 6.6 NIST CSF 2.0 GV.RR-04 PR.AA-01 PR.AA-05 PR.AT-01 PR.AT-02 Manuale UTP Cap. 3.7	Cap. 4.2 Cap. 4.3 Cap. 4.4
B-11	**Gestione di sistemi e reti di dati** I sistemi e le reti **di dati** devono essere configurati e protetti in modo da evitare compromissioni o guasti. a) Disporre di piani di rete aggiornati al fine di avere una panoramica della rete disponibile b) Segregare le reti in misura appropriata e tenendo conto della loro portata, redigendo a tal fine una concezione di rete che descriva misure specifiche di protezione delle informazioni c) Stabilire un'architettura di sicurezza appropriata, p. es. secondo il principio zero trust (non fidarsi mai, verificare sempre), nel caso in cui l'interconnessione di servizi OT e IT con p. es. applicazioni cloud pubbliche si estenda in maniera tale che i passaggi di rete non sono più sicuri secondo il concetto di zone classico «zones and conduits» d) Mettere a verbale le attività rilevanti per la sicurezza delle informazioni e i cambiamenti ai sistemi secondo il processo di gestione delle modifiche	ISO/IEC 27002:2022 Cap. 5.2 Cap. 7.11 Cap. 8.9 Cap. 8.14 Cap. 8.20 Cap. 8.22 NIST CSF 2.0 ID.RA-07 PR.IR-01 PR.PS-01 PR.AA-06 Manuale UTP Cap. 3.5 Concerne i GI, reti di dati per OT: D RTE 28100 Cap. 5	Cap. 3.1.2

B-12	**Elaborazione di direttive (policies) per l'autentificazione nei sistemi** a) Definire direttive che descrivano il processo d'iscrizione degli utenti ai sistemi b) Descrivere nelle direttive quali procedure di autentificazione devono essere utilizzate (p. es. autenticazione a due fattori) e come utilizzarle correttamente c) Se possibile, imporre a livello tecnico i requisiti di sicurezza per le procedure di autentificazione (p. es. requisiti minimi per password, modifica della password iniziale) d) Applicare, laddove possibile, procedure di autentificazione forti (p. es. autenticazione a due fattori, con token o biometriche)	ISO/IEC 27002:2022 Cap. 5.17 NIST CSF 2.0 PR.AA-01 PR.AA-03 PR.AA-05 Manuale UTP Cap. 3.5 V. anche all. 3 Mezzi ausiliari	
B-13	**Misure di protezione dei terminali** I terminali impiegati nei settori IT, OT o per i veicoli ferroviari devono adempiere i seguenti requisiti di sicurezza: a) essere configurati e impiegati secondo determinate direttive; b) se si tratta di terminali privati usati nel contesto dell'impresa, assicurarsi che rispettino almeno i requisiti della direttiva di cui alla lettera a); c) installare tempestivamente patch rilevanti per la sicurezza sui sistemi e terminali; d) se non è possibile fare in tempi utili quanto previsto alla lettera c), adottare altre misure in funzione dei rischi (p. es. limitazioni degli accessi da remoto, ottimizzazione del monitoraggio della sicurezza, per poter riconoscere quanto prima casi di sfruttamento di un punto debole). Vedere anche B-20 b)	ISO/IEC 27002:2022 Cap. 8.1 NIST CSF 2.0 PR.DS-01 PR.DS-02 PR-DS-10 TS50701:2023 Cap. 10.2 Cap. 10.3 Manuale UTP Cap. 3.5 Tabella 6	
B-14	**Protezione dai software nocivi (malware)** Occorre implementare sui sistemi misure di protezione per prevenire e riconoscere i software nocivi. A seconda delle tecnologie impiegate e dello scopo del sistema, l'implementazione può avvenire con l'impiego di rispettivi software o mediante un rafforzamento del sistema (p. es. protezione del perimetro, difesa in profondità [defence-in-depth]). Per OT: vedere anche B-25	ISO/IEC 27002:2022 Cap. 6.3 Cap. 8.7 NIST CSF 2.0 DE.CM-01 DE.CM-04 DE.AE-02 TS50701:2023 B.4.4, C.3 Manuale UTP Cap. 3.5	

B-15	**Gestione della configurazione e delle modifiche** Nella configurazione di hardware e software, all'interno delle reti così come nel settore OT e per i veicoli ferroviari devono essere adempiuti requisiti di sicurezza delle informazioni. a) Autorizzare e attuare modifiche secondo un processo predefinito b) Garantire che delle impostazioni di configurazione possano occuparsi esclusivamente persone autorizzate allo scopo c) Modificare le password standard prima dell'entrata in servizio	ISO/IEC 27002:2022 Cap. 5.22 Cap. 8.9 Cap. 8.32 NIST CSF 2.0 ID.RA-07 PR.PS-01 Manuale UTP Cap. 3.5	Cap. 5.2 Cap. 5.4
B-16	**Lavoro a distanza (remote work)** Si parla di lavoro a distanza quando i collaboratori o i fornitori di servizi esterni operano al di fuori dei locali e del perimetro dell'impresa e hanno accesso a informazioni mediante dispositivi TIC. Nel caso in cui si ricorra a questa modalità di lavoro occorre: a) definire direttive specifiche in quanto a sicurezza delle informazioni b) stabilire quali meccanismi di autentificazione debbano essere impiegati c) sensibilizzare i collaboratori alla tematica del lavoro a distanza e fornire informazioni in merito (p. es. gestione degli account personali) d) intensificare l'adozione di misure che garantiscano l'accesso alle informazioni tramite Internet solo da parte di persone autorizzate (p. es. tramite VPN)	ISO/IEC 27002:2022 Cap. 6.7 NIST CSF 2.0 PR.AA-03 PR.AA-05 PR.IR-01 PR.AT-01 PR-AT-02	
B-17	**Impiego di procedure crittografiche** Se nelle applicazioni vengono impiegate procedure crittografiche, devono basarsi su algoritmi riconosciuti e verificati e su una generazione di chiavi sicura.	TS50701:2023 SR 4.2 SR 4.3 NIST CSF 2.0 PR.DS-01 PR.DS-02 PR.DS-10 V. anche all. 3 Mezzi ausiliari	
B-18	**Protezione dei dati e delle informazioni** Al fine di adempiere i requisiti di leggi, autorità e contratti è necessario proteggere dati e informazioni. Vi è bisogno di una direttiva che definisca le seguenti regole e procedure per la protezione di dati e informazioni. a) Salvare e trasmettere dati e informazioni proteggendoli secondo la relativa esigenza, documentando le misure e le procedure adottate allo scopo	ISO/IEC 27002:2022 Cap. 5.24 Cap. 5.31 Cap. 8.10 Cap. 8.11 Cap. 8.12 Cap. 8.13 Cap. 8.24	Cap. 4.5

	b) Proteggere mediante misure tecniche (p. es. crittografia) i dati degni di protezione (p. es. dati personali, dati di accesso) c) Implementare nei sistemi, nelle reti e in altri dispositivi misure di protezione contro la perdita di dati (p. es. sorveglianza degli accessi ai dati con elevata esigenza di protezione) d) Effettuare e controllare periodicamente il backup di dati, informazioni, software e sistemi e) Cancellare secondo l'esigenza di protezione i dati e le informazioni non più utilizzati, salvati su dispositivi o supporti di memoria; per la distruzione di dispositivi di memoria si raccomanda di affidarsi a fornitori autorizzati e certificati di servizi sicuri di smaltimento	NIST CSF 2.0 PR.DS-01 PR.DS-02 PR.DS-10 PR.DS-11 SN EN 50159: 2010 LPD Manuale UTP Cap. 3.5	
B-19	**Protezione dell'accesso a edifici e veicoli ferroviari** Edifici, locali e zone con sistemi rilevanti per la sicurezza su impianti, impianti esterni e a bordo di veicoli ferroviari devono essere protetti, per quanto possibile e proporzionale, contro l'accesso di persone non autorizzate.	ISO/IEC 27002:2022 Cap. 5.15 Cap. 7.1 Cap. 7.2 Cap. 7.3 Cap. 7.4 NIST CSF 2.0 PR.AA-06 Manuale UTP Cap. 3.5.5	Cap. 5.2
B-20	**Gestione dei punti deboli** Deve essere allestita una gestione dei punti deboli che consideri tutti i sistemi e adempia i seguenti criteri: a) ripartire chiaramente per ogni sistema le responsabilità in merito all'identificazione e alla notifica di punti deboli tra gestore, integratore di sistema, fabbricante e nei Service level agreements (SLA, accordi sui livelli di servizio); b) in caso d'identificazione di un punto debole, farne valutare il rischio ai servizi responsabili e decidere, su tale base, se e quali misure immediate possono essere adottate e quando o a quali condizioni si debba ricorrere a un patch di sicurezza (è possibile che insorga un rischio temporaneo del quale eventualmente bisogna farsi carico).	ISO/IEC 27002:2022 Cap. 8.8 TS50701:2023 Cap. 10.2 Cap. 10.3 NIST CSF 2.0 ID.RA-01 PR.PS-02	
B-21	**Separazione tra gli ambienti di sviluppo, di test e di produzione** a) Separare l'uno dall'altro i sistemi di sviluppo, di test e di produzione b) Eseguire le modifiche in un ambiente di test, prima di applicarle ai sistemi di produzione	ISO/IEC 27002:2022 Cap. 8.29 Cap. 8.31 NIST CSF 2.0 PR.IR-01	

8.2 Misure specifiche nel settore dell'OT

Le misure descritte nel presente capitolo si riferiscono sia ai sistemi OT di impianti fissi sia ai sistemi OT per veicoli ferroviari.
In ambito OT si può ritenere che centrali siano in particolare disponibilità e integrità dei sistemi, mentre la confidenzialità gioca un ruolo inferiore. Nell'attuare le misure di sicurezza in questo ambito va pertanto sempre verificato che non influenzino o abbiano ripercussioni indirette sulla sicurezza della funzione (safety) o sulla capacità d'esercizio del rispettivo sistema. L'implementazione di misure di sicurezza deve essere sempre decisa e attuata in collaborazione e d'intesa con la gestione della safety, per poter considerare adeguatamente le possibili interdipendenze (assenza di interferenze) e identificare i rischi.

L'assenza di interferenze (ovvero l'assenza di reazioni, il che significa che la funzione non compromette altre funzioni legate alla sicurezza) deve essere provata. Per farlo si deve ricorrere, a seconda del caso, sia a metodi analitici sia a test di regressione.

Per modifiche rilevanti ai sistemi esistenti è richiesta un'autorizzazione secondo l'articolo 8 Oferr [2]; in caso di dubbio va contattato l'UFT.

N.	Misura	Rimando
B-22	**Installazione di software nel settore OT** A causa della criticità (esigenza di protezione) dei sistemi OT, le installazioni di software devono essere sorvegliate e controllate. a) Lasciare installare gli aggiornamenti sui sistemi OT solo da personale qualificato b) Garantire che gli aggiornamenti software del produttore per i sistemi OT vengano messi a disposizione per un periodo preventivamente definito con il produttore stesso c) Per l'installazione di aggiornamenti seguire una procedura di approvazione nella quale è coinvolta anche la gestione della safety d) Testare integralmente il software prima di installare aggiornamenti sui sistemi OT, eseguendo i test mediante appositi protocolli che permettono di documentare le funzioni testate ed eventuali anomalie; in caso di problemi non effettuare installazioni né aggiornamenti e) Definire e testare preventivamente una strategia di rollback, ovvero fare in modo che, in caso di problemi di funzionalità, i sistemi OT possano essere riportati allo stato funzionante iniziale f) Mettere a verbale chi ha installato aggiornamenti o software, con i relativi motivi g) Archiviare le vecchie versioni software assieme alle informazioni e ai parametri necessari	TS50701:2023 Cap. 9 Cap. 10.2 Cap. 10.3 NIST CSF 2.0 ID.AM-08 PR.DS-01 PR.PS-02

B-23	**Identificazione e autentificazione** In merito alla gestione utenti e alle possibilità di autentificazione, spesso i sistemi OT sono fortemente limitati rispetto ai sistemi classici oppure a causa degli elevati requisiti in materia di disponibilità non sono realizzabili conformemente allo stato della tecnica. È pertanto il caso di applicare relative contromisure. a) Adottare in funzione del rischio misure di compensazione per le limitate possibilità di autentificazione che hanno molti sistemi OT, p. es. autenticazione forte al confine delle zone della rete mediante un policy enforcement point (p. es. proxy o punto finale VPN), monitoraggio potenziato degli accessi tramite log di accesso, ecc. b) Proteggere secondo la relativa esigenza i terminali impiegati nell'ambito dei sistemi OT	TS50701:2023 SR 1.4 SR 1.11 SR 1.7 SR 2.3 NIST CSF 2.0 PR.AA-01 PR.AA-03 PR.AA-05 PR.AA-06 PR.IR-01
B-24	**Monitoraggio (security monitoring)** I protocolli di sistema rilevanti per la sicurezza dei sistemi interconnessi devono essere trasmessi a un sistema centrale per l'analisi dei log ed essere lì conservati conformemente alle direttive interne all'impresa o al piano di logging. Vedere anche B-07	TS50701:2023 SR 2.1 SR 2.8 NIST CSF 2.0 PR.PS-04 DE.AE-03 DE.AE-04
B-25	**Integrità di sistema** Spesso sui sistemi non è possibile installare un software di rilevamento per proteggersi contro i malware. Quale contromisura andrebbero implementati meccanismi preventivi tra i quali rientrano, p. es., direttive per la gestione di supporti dati rimovibili e terminali in combinazione con meccanismi di rilevamento preinstallati (p. es. IDS).	TS50701:2023 SR 3.2 NIST CSF 2.0 PR.DS-01 PR.PS-01 DE.CM
B-26	**Limitazione del flusso di dati** Le reti devono essere opportunamente segmentate in funzione del livello di protezione dei sistemi e dell'analisi dei rischi condotta. Nel farlo, va tenuto conto che in caso d'emergenza le zone di rete interessate devono poter essere separate dal resto della rete, al fine di ridurre al minimo i danni. Di conseguenza, occorre verificare per quali servizi centrali (p. es. DHCP, DNS) si debba disporre di una ridondanza in più zone. Per limitare i danni, per quanto possibile e opportuno si dovrebbero poter isolare dalle altre reti in particolare i sistemi rilevanti per la safety.	TS50701:2023 SR 5.1 NIST CSF 2.0 PR.IR-01 RS.MI-01
B-27	**Disponibilità** a) Implementare un'adeguata protezione contro gli attacchi Denial of Service (DoS), affinché non si estendano a più sistemi o ambiti di rete b) Definire e implementare un'idonea procedura di backup per dati e file rilevanti; sviluppare una strategia di ripristino per i backup nonché testare periodicamente il ripristino, al fine di garantire che sia sicuro e conforme c) Trasferire sistemi e applicazioni OT in modo che in caso di guasto la disponibilità sia garantita da un sistema ridondante: l'impresa dovrebbe programmare e attuare procedure per l'attivazione di componenti e dispositivi di elaborazione ridondanti Vedere anche B-09 Gestione della continuità aziendale	TS50701:2023 SR 7.1 SR 7.2 SR 7.3 SR 7.4 SR 7.5 ISO/IEC 27002:2022 Cap. 8.14 NIST CSF 2.0 ID.IM-03 ID.IM-04 PR.DS-11

8.3 Misure specifiche per sistemi TIC su veicoli ferroviari

N.	Misura	Rimando
B-28	**Identificazione e autentificazione** A bordo di veicoli ferroviari le procedure di autentificazione non devono impedire il rapido accesso ai sistemi. I sistemi necessari al macchinista per l'esercizio del veicolo ferroviario non devono essere bloccati automaticamente dopo l'identificazione iniziale avvenuta, p. es., con chiave o badge. La protezione dell'accesso deve inoltre essere garantita mediante misure fisiche (p. es. chiusura delle porte di accesso alla cabina di guida). Per altri lavori non condotti durante l'esercizio regolare, come le modifiche di configurazioni software o di parametri, si deve optare per una gestione rigorosa dell'identificazione e dell'autentificazione.	TS50701:2023 SR 1.4 NIST CSF 2.0 PR.AA-01 PR.AA-05
B-29	**Protezione fisica** a) Garantire mediante misure adeguate (p. es. armadi con chiusura) che componenti degne di protezione siano protette contro manipolazioni materiali b) Prevedere altre misure, quali l'installazione di un sistema di sorveglianza del veicolo ferroviario, nel caso in cui non sia possibile realizzare una protezione fisica efficace c) Configurare sistemi di allarme per la sorveglianza (p. es. tramite videocamere, sorveglianza di strutture che coprono componenti degne di protezione) e tutelarli di conseguenza (cfr. punto successivo) d) Posizionare i sistemi di sorveglianza in un posto irraggiungibile dalla persona che fa scattare l'allarme e) Dotare i sistemi di sorveglianza di meccanismi antimanipolazione e testarli periodicamente	ISO/IEC 27002:2022 Cap. 7.4 NIST CSF 2.0 PR.AA-06 Videosorveglianza OVsor-TP [16]

9 Termini

Termine	Definizione
Accesso da remoto	L'accesso da remoto mira a consentire a collaboratori e fornitori di servizi esterni selezionati un accesso sicuro alla rete di un'impresa ovvero OT (p. es. a fini di manutenzione) in modo che determinate applicazioni possano essere usate anche dall'esterno. Per l'accesso da remoto è a disposizione un rispettivo terminale equipaggiato, che deve essere in grado di stabilire una relazione di comunicazione sicura tramite un accesso alla rete (p. es. DSL, WLAN, radiocomunicazione) e una rete di trasferimento (p. es. Internet).
ASic	L'**autorizzazione di sicurezza** conferma l'adeguatezza del sistema di gestione della sicurezza del gestore dell'infrastruttura e il consenso sui provvedimenti che quest'ultimo ha preso per garantire la sicurezza dell'esercizio sulle sue tratte.
Assenza di interferenze	Prova che gli adeguamenti apportati influiscono esclusivamente sui sistemi, componenti o funzioni interessati, interfacce comprese, secondo la descrizione delle modifiche, ovvero che la funzione non ne comprometta altre riguardanti la sicurezza.
Asset	Un asset è tutto ciò che ha valore per l'organizzazione (denominato anche bene o valore informativo). Esistono diversi tipi di asset: informazioni, software, hardware, servizi, persone con le rispettive qualifiche, competenze ed esperienze così come valori immateriali quali la reputazione o l'immagine. La norma ISO/IEC 27005:2022 fa una distinzione tra asset primari e secondari. I primari, che rappresentano l'effettivo valore di un'organizzazione o di un'impresa, devono essere assolutamente protetti. Si tratta, p. es., di processi o segreti aziendali, dati base, reputazione ecc. Gli asset secondari sono necessari affinché i primari espletino il loro valore aggiunto. Si tratta, p. es., di mezzi d'esercizio TIC (hardware, software), immobili, personale, siti web.
Asset owner	L'asset owner è la persona responsabile dell'amministrazione quotidiana degli asset. Essa comprende non solo informazioni elettroniche e stampate, ma anche hardware, software, servizi e dispositivi.
Attacco cibernetico	Qualsiasi forma di attività appositamente avviata da non autorizzati malintenzionati ai danni della tecnologia dell'informazione o delle persone che la utilizzano.
Autentificazione / autenticazione (ingl. «authentication»)	I termini autentificazione e autenticazione nella lingua corrente sono spesso usati come sinonimi, ma in realtà descrivono due diversi processi parziali, p. es. di una procedura di login. Un utente si AUTENTICA in un sistema mediante informazioni di login univoche (p. es. password o smart card). Il sistema verifica dunque la validità dei dati utilizzati e AUTENTIFICA l'utente.
Autorizzazione	Per autorizzazione nella tecnologia dell'informazione s'intende la prima assegnazione e la verifica sistematica dei diritti d'accesso ai dati e ai servizi mediante metodi speciali. Le due forme più frequenti sono: • l'accesso autorizzato alle risorse (p. es. a inventari o file) in una rete informatica; • l'autorizzazione all'installazione o all'uso di programmi informatici.

BSI	**Bundesamt für Sicherheit in der Informationstechnik (Ufficio federale tedesco per la sicurezza nella tecnica dell'informazione)**
Ciberincidente	Evento durante l'esercizio di mezzi informatici che può compromettere la confidenzialità, l'integrità o la disponibilità di informazioni o la tracciabilità della relativa elaborazione. Cfr. anche CLC TS 50701:2023, cap. 3.1.32 e CLC TS 50501:2021, cap. 3.1.29.
Ciberminaccia	Qualsiasi situazione o evento che può causare un ciberincidente (incidente informatico).
Cibersicurezza	Tecnologie, servizi, strategie, pratiche e direttive a protezione di sistemi o reti di tecnologia dell'informazione da attacchi di attori malintenzionati.
CLC	**CENELEC**: Comitato europeo di normazione elettrotecnica
Confidenzialità	Confidenzialità significa che i dati possono essere consultati o trasmessi solo da personale autorizzato. Va definito chiaramente chi ha accesso e con che modalità. Cfr. anche [5].
CSA	Cloud Security Alliance
CSic	Il **certificato di sicurezza** nel trasporto ferroviario conferma che l'organizzazione dell'impresa le consente di transitare in maniera sicura sull'infrastruttura di terzi, con personale e veicoli adeguati.
CSM	**Common safety method** CSM dell'ERA (European Union Agency for Railways, Agenzia ferroviaria europea)
Disponibilità	Capacità di un sistema, in un determinato momento o durante un determinato intervallo di tempo, di adempiere una funzione richiesta a determinate condizioni, purché siano messi a disposizione i mezzi necessari [5].
Esigenza di protezione (classificazione di un oggetto da proteggere)	L'esigenza di protezione di un oggetto è determinata dalla portata del danno che può risultare da una violazione della sicurezza delle informazioni. Si può trattare di violazioni della confidenzialità, dell'integrità e della disponibilità. Generalmente si considerano almeno le seguenti categorie: • **normale:** gli effetti del danno sono limitati e gestibili; • **alta:** gli effetti del danno possono essere notevoli; • **molto alta:** gli effetti del danno possono minacciare l'esistenza e raggiungere dimensioni catastrofiche.
ENISA	**Agenzia dell'Unione europea per la cibersicurezza**
ERA	**Agenzia ferroviaria europea**
GI	**Gestore dell'infrastruttura** (ferroviaria, ovvero sistemi di terra)
ICS	**Industrial Control System** (sistema di controllo industriale) – Sistemi di gestione in impianti industriali (altro termine per OT)
ICS	**Industrial Control System** (sistema di controllo industriale, nel presente documento utilizzato come sinonimo delle abbreviazioni «OT» e «SCADA»).
IDS	**Intrusion Detection System** (sistema di rilevamento delle intrusioni) Sistemi per il rilevamento di accessi non autorizzati a dati o computer.
Integrità	Garanzia della correttezza e dello stato intatto di dati così come del corretto funzionamento di sistemi.

ISACA	**Information Systems Audit and Control Association**
IT	**Tecnologia dell'informazione** Tutte le tecniche e i relativi hardware e software correlati all'elaborazione elettronica dei dati. Per il confronto tra IT o TIC e OT vedere Manuale UTP, tabella 5 [13].
ITF	**Impresa di trasporto ferroviario** (con una concessione)
Misure	I control sono misure che servono a raggiungere obiettivi e a ridurre significativamente i rischi della sicurezza delle informazioni.
NCSC	**Centro nazionale per la cibersicurezza, dal 1° gennaio 2024: Ufficio federale della cibersicurezza**
OCTSE	Ordinanza concernente il coordinamento dei trasporti in situazioni eccezionali
OT	La **tecnologia operativa (operational technology)** designa hardware e software che sorvegliano e gestiscono la prestazione di dispositivi fisici. In passato l'OT si riferiva prevalentemente a sistemi di sorveglianza e di gestione in imprese di produzione, trasporto e distribuzione. Per il confronto tra IT e OT vedere Manuale UTP, tabella 5 [13].
Principi del least-privilege e del need-to-know	Un sistema o una persona fisica riceve accesso solo alle informazioni di cui ha bisogno per l'adempimento dei suoi compiti. Le differenze di compiti o ruoli generano pertanto diverse informazioni need-to-know e, quindi, diversi profili di accesso.
Principio zero-trust	Approccio per il quale ogni accesso a risorse necessita di un'autentificazione. Ogni singolo flusso di dati è sottoposto alla verifica di attendibilità (cfr. anche la considerazione tecnologica Principio «Zero trust», solo in fr. e ted., all'indirizzo https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/technologiebetrachtung.html).
Reg.	Regolamento (UE)
RS	**Raccolta sistematica** (diritto svizzero)
RTE	**Regelwerk Technik Eisenbahn** (normativa di tecnica ferroviaria) Una normativa dell'UTP (Unione dei trasporti pubblici).
Segregation of Duties (SoD)	Conosciuto anche come «principio di separazione dei ruoli».
SGI	Il **sistema di gestione integrato** raccoglie in una struttura unitaria metodi e strumenti per l'adempimento di requisiti di diversi settori nell'ambito del governo d'impresa (p. es. qualità, sicurezza, sicurezza delle informazioni, manutenzione). Mediante l'utilizzo di sinergie e l'unione di risorse consente, rispetto a singoli sistemi di gestione isolati, una gestione più snella ed efficiente.
SGSI/ISMS	**Sistema di gestione della sicurezza delle informazioni (Information Security Management System)** – Parte del sistema di gestione globale, basato su un approccio del rischio imprenditoriale, per la definizione, l'implementazione, l'esercizio, la sorveglianza, la verifica, il mantenimento e il miglioramento della sicurezza delle informazioni. Il sistema di gestione com-

	prende struttura organizzativa, policies, attività di pianificazione, responsabilità, pratiche, processi e risorse.
Sicurezza delle informazioni	La sicurezza delle informazioni serve a conservare intatte autenticità, confidenzialità, integrità e disponibilità di sistemi di tecnica dell'informazione e della comunicazione e dei dati ivi elaborati e/o salvati.
Sistemi / applicazioni di elaborazione di informazioni	Sistemi e applicazioni nei quali vengono elaborate o salvate informazioni.
SMS/SGS	**Safety Management System**, sistema di gestione della sicurezza secondo [3]
SR	**System Requirement** secondo CLC/TS50701:2023, tabella 6 [11] o IEC 62443-3-3 [12]
SRM	**Entity in Charge of Maintenance (soggetto responsabile della manutenzione)** Servizio competente della manutenzione nel traffico ferroviario
STRIDE	**S**poofing (falsificazione di identità) **T**ampering (alterazione dei dati) **R**epudiation (ripudio di un'azione) **I**nformation disclosure (divulgazione di informazioni) **D**enial of service (diniego di servizio) **E**levation of privilege (elevazione dei privilegi)
TIC	Le **tecnologie dell'informazione e della comunicazione** sono tecnologie impiegate per lo svolgimento di processi di comunicazione quali telecomunicazione, radiocomunicazione, sistemi intelligenti di gestione degli edifici, sistemi audiovisivi di elaborazione e trasmissione nonché funzioni di comando e di sorveglianza basate sulle reti.
UFCS	**Ufficio federale della cibersicurezza**
UFT	**Ufficio federale dei trasporti**
UTP	**Unione dei trasporti pubblici** (www.voev.ch)

Altre spiegazioni di termini riguardanti la cibersicurezza sono disponibili all'indirizzo https://www.ncsc.admin.ch/ncsc/it/home/glossario.html nonché in diverse norme.

10 Allegato 1 – Sistema di gestione integrato e SGSI

Un sistema di gestione integrato (SGI) permette di riunire strumenti esistenti per l'adempimento di requisiti di diversi settori in una struttura unica e più snella. Grazie a una rappresentazione globale è possibile sfruttare le sinergie e unire le risorse.

Di seguito si elencano sistemi di gestione che dispongono di interfacce e, pertanto, di potenziale sinergico:

- sistema di gestione della sicurezza (CSM SGS)
- sistema di gestione della qualità (SGQ)
- sistema di gestione della manutenzione SRM (CSM SRM)
- compliance management system (CMS)
- sistema di gestione dei rischi (SGR)
- sistema di controllo interno (SCI)

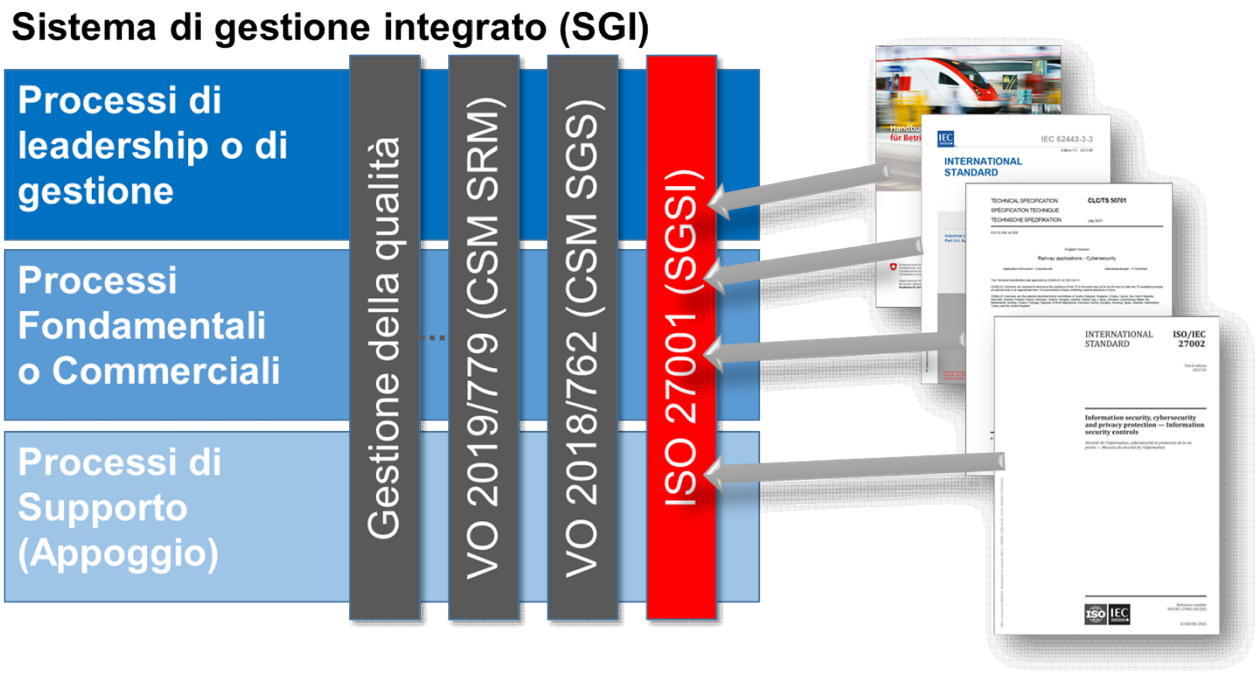
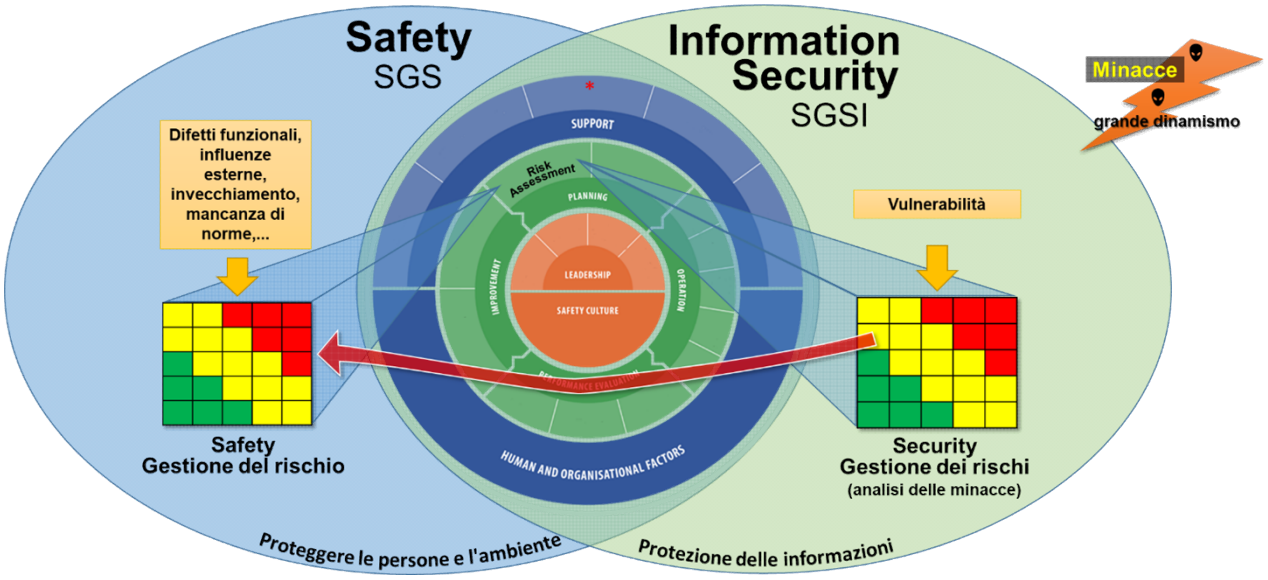


Figura 1 - SGI tipico di un'impresa di trasporto medio-grande con riferimento dei processi aziendali a norme/standard contenenti requisiti di sicurezza

Sotto il profilo della sicurezza, i SGSI e i SGS hanno un'interfaccia comune. Entrambi i sistemi puntano in primo luogo sulla minimizzazione del rischio per migliorare costantemente il livello di sicurezza. A tal fine, è necessario identificare e rendere noti preventivamente gli asset critici e i rischi.

La principale interfaccia tra un SGSI e un SGS è pertanto la gestione dei rischi. I risultati dell'analisi delle minacce di un SGSI devono confluire secondo la figura 2 nella gestione dei rischi del SGS. I rischi ritenuti rilevanti per la safety devono essere inseriti in un registro dei pericoli (cfr. p. es. il registro delle situazioni pericolose di cui alla SN EN 50126:2017).



*Fonte: https://www.era.europa.eu/domains/common-safety-methods/safety-management-system-requirements-csm_en

Figura 2 - Relazione SGSI-SGS (rappresentazione semplificata con la principale interfaccia SGSI-SGS)

11 Allegato 2 – Panoramica su ISO/IEC 27001 e ISO/IEC 27002

La serie di norme ISO/IEC 27000 comprende diverse norme parziali sul tema della gestione della sicurezza delle informazioni.
La norma centrale è la ISO/IEC 27001, costituita da una parte principale con requisiti generali di un SGSI e un vasto allegato A dove sono riportati gli obiettivi specifici delle misure. Nella maggior parte dei casi il campo d'applicazione di un SGSI è l'intera impresa, i suoi compiti principali sono:

- formulazione di obiettivi di sicurezza
- definizione degli asset
- valutazione del rischio
- trattamento del rischio
- miglioramento continuo (p. es. secondo il ciclo PDCA – Plan, Do, Check, Act)

Secondo la ISO/IEC 27001 tutte le informazioni rilevanti di un'impresa nonché i dati e i sistemi che li elaborano devono essere individuati e registrati in un inventario. Informazioni, dati e sistemi di elaborazione con valori e rischi comparabili possono essere riuniti e considerati come valore unico.

L'**allegato A della ISO/IEC 27001:2022** è un catalogo costituito da quattro tematiche riguardanti la sicurezza (control clauses, clausole di controllo) e 93 misure (control). I quattro temi sulla sicurezza sono:

- Organizational Controls - misure organizzative (5.1 - 5.37)
- People Controls - misure concernenti il personale (6.1 - 6.8)
- Physical Controls - misure fisiche (7.1 - 7.14)
- Technological Controls - misure tecnologiche (8.1 - 8.34)

Spiegazioni in merito all'attuazione delle 93 misure ed esempi di misure sono disponibili nella ISO 27002.

L'**allegato A della ISO/IEC 27002:2022** riporta i control con i rispettivi attributi in una rappresentazione a matrice. Quest'ultima consente di raggruppare e filtrare i requisiti di sicurezza che un'impresa dovrebbe adempiere.

Ulteriori informazioni su norme e standard sono disponibili nel Manuale di cybersicurezza per le imprese di trasporti pubblici (cap. 6.2 in [13]) e in numerose pagine web[19].

[19] Per esempio https://en.wikipedia.org/wiki/IT_security_standards

12 Allegato 3 – Mezzi ausiliari per l'attuazione di un SGSI

Mezzo ausiliario	Osservazione
Manuale di cybersicurezza per le imprese di trasporti pubblici (Manuale UTP del 2020) [13]	Il Manuale dell'UTP, basato sullo standard minimo TIC per diversi settori dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE[20]), contiene un'introduzione alla sicurezza delle informazioni nel settore dei TP e consente alle imprese di condurre un'autovalutazione
Implementierungsleitfaden ISO/IEC 27001:2022 von ISACA (**guida all'implementazione di ISACA**, solo in ted., cfr. [17])	Funge da mezzo ausiliario per l'implementazione di un SGSI.
ICS Security Kompendium (**compendio sulla sicurezza**, solo in ted.) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/allgemeine-empfehlungen_node.html	Con l'ICS Security Kompendium il BSI pubblica un'opera basilare per la sicurezza IT nell'ICS.
Gestione dei punti deboli e dei fornitori: ENISA: - Good Practices for Supply Chain Cybersecurity - Threat Landscape for Supply Chain Attacks CISA: - Known Exploited Vulnerabilities Catalog	
Minacce attuali: UFCS: https://www.ncsc.admin.ch/ncsc/it/home.html Internet Storm Center: https://isc.sans.edu/ **Minacce tendenziali:** ENISA: Foresight Cybersecurity Threats For 2030	Una volta registratesi, le imprese possono iscriversi sulla piattaforma multimodale di cibersicurezza, sulla quale l'UFCS (NCSC) informa in merito alle minacce e ai punti deboli più recenti. Su questa piattaforma, gli utenti registrati hanno la possibilità di scambiarsi informazioni attivamente. Per le richieste di registrazione contattare l'UFCS all'indirizzo useraccounts@ncsc.admin.ch.
Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) MITRE ATT&CK è una guida nella quale sono classificati e descritti gli attacchi informatici e gli hacker pubblicata nel 2013, realizzata e sviluppata dalla Mitre Corporation. Cfr. https://attack.mitre.org/ **Indicators of Compromise (IoC) Database:** https://threatfox.abuse.ch/browse/	Le tattiche sono distinte nelle tre matrici Enterprise, Mobile e ICS (industrial control system, sistema di controllo industriale). Il navigatore ATT&CK basato su web può essere utilizzato per commenti e informazioni sulle matrici ATT&CK nonché per visualizzare la copertura difensiva, la pianificazione dei team rosso/blu, la frequenza delle tecniche scoperte e molto più.
Mezzi ausiliari per le analisi dei rischi (risk assessments): - ISO/IEC 27005 - IEC 62443-3-2 - CLC/TS 50701:2023, cap. 6 e 7 - STRIDE	Si veda in proposito anche: https://www.enisa.europa.eu ➔ Risk Management e specifico alla ferrovia: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

[20] www.bwl.admin.ch

Mezzi ausiliari per la segmentazione di reti: - IEC 62443-3-2 e IEC 62443-3-3 - CLC/TS 50701 - Zoning and Conduits for Railways (ENISA, ER-ISAC)	
NIST Cryptography: https://www.nist.gov/cryptography	Informazioni riguardo agli standard di crittografia.
Raccomandazioni BSI su procedure crittografiche e lunghezza delle chiavi (solo in ted.): https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html	
IEEE Cryptography: https://standards.ieee.org/	
Protezione con password e altre informazioni sulla sensibilizzazione dei collaboratori: https://www.passwortcheck.ch/ https://www.s-u-p-e-r.ch/it/consigli/e-per-elaborare/	Diverse informazioni, tra cui preziose indicazioni per la scelta della password.
Mezzo ausiliario per determinare la maturità della cibersicurezza in un'organizzazione: Standard minimo per le TIC – tool di valutazione	RAILplus dispone di un proprio strumento d'ausilio per determinare la maturità della sicurezza delle informazioni.
Mezzo ausiliario sul tema cloud: - Cloud Security Alliance (CSA) - ENISA: Cloud Cybersecurity Market Analysis - BSI: Mindeststandard des BSI zur Nutzung externer Cloud-Dienste - BSI: Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)	
Tabelle di mappatura per diverse norme: - Standard minimo per le TIC – tool di valutazione - Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022 der Bundesnetzagentur - Mapping Tabelle von ENISA für spezifische Sektoren	Le tabelle di mappatura non sono sempre aggiornate.

Per ulteriori mezzi ausiliari consultare la pagina https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen.html.

Molti strumenti d'ausilio per la cibersicurezza sono consultabili su fonti ufficiali e vengono aggiornati per lo più periodicamente. Sempre più ausili sono disponibili anche nel settore.
Il presente allegato è aggiornato sulla pagina Internet dell'UFT.

13 Allegato 4 – Lista di controllo e domanda per l'esonero dall'obbligo di SGSI per ITF e GI

Nome dell'impresa **IDI**[21] ☐ ITF ☐ GI

Persona di contatto (nome e cognome, e-mail, n. di tel., funzione) ☐ CSic/ASic richiesti congiuntamente

N.	Questione	Commento	Spiegazioni / Riferimenti
1	Impieghiamo i seguenti sistemi/veicoli ferroviari nel campo d'applicazione delle DE-Oferr:		
2	Esistono interfacce digitali con i seguenti sistemi operativi e tecnici (in particolare sui sistemi di protezione dei treni e di controllo della marcia dei treni)[22]: **Osservazione:** descrivere anche il tipo di interfaccia (p. es. TCP/IP).		
3	Per l'esercizio secondo i sistemi riportati alla questione 2 ci avvaliamo dei seguenti fornitori di servizi[23]:		
4	I fornitori di servizi (di cui alla questione 3) hanno l'obbligo contrattuale di adempiere i requisiti minimi della cibersicurezza per la vostra parte di forniture?	☐ Sì ☐ No Se sì, quali requisiti minimi? Osservazioni:	
5	Senza i nostri sistemi IT[24] possiamo mantenere l'esercizio per	Numero di ore: Motivazione:	

[21] Numero d'identificazione dell'impresa

[22] Una panoramica è fornita dalla figura 5 nel Manuale UTP [13].

[23] Quali fornitori di servizi vanno considerati innanzitutto quelli nel settore IT e OT, ma anche proprietari di impianti e materiale rotabile affittati.

[24] Tra i sistemi IT rientrano anche gli apparecchi IT aziendali e gli archivi elettronici.

N.	Questione	Commento	Spiegazioni / Riferimenti
	... ore.	Sistemi IT rilevanti per l'esercizio (p. es. sistema per la disposizione):	
6	Affinché le informazioni salvate in forma digitale rilevanti per il nostro esercizio e la manutenzione siano sempre disponibili, abbiamo adottato i seguenti provvedimenti:[25]		
7	Abbiamo previsto le seguenti modifiche/rinnovi che sono o potrebbero essere rilevanti sotto il profilo della cibersicurezza.		
8	Basi disponibili (p. es. analisi dei rischi, descrizioni di sistema) utili per la valutazione della presente domanda (p. f. allegare):		
9	Motivazione del richiedente: perché non ritiene necessaria la creazione e la gestione di un SGSI per la propria impresa?		

Criteri per un esonero dall'obbligo di SGSI

1. Necessità di protezione delle informazioni dei sistemi IT e OT disponibili del richiedente per un esercizio sicuro e affidabile (criticalità)

2. Importanza del richiedente (ITF o GI) per l'approvvigionamento del Paese e in collaborazione con altre imprese di trasporto

3. Possibilità di raggiungere gli obiettivi di sicurezza **senza un SGSI, ma con i sistemi di gestione disponibili** quali p. es. il SGS

Osservazioni: la richiesta di esonero dall'obbligo di SGSI va rinnovata ogni 5 anni, di preferenza in coordinamento con i processi CSic/ASic. Qualora intervengano modifiche rilevanti in merito alla cibersicurezza, il richiedente deve presentare all'UFT una domanda aggiornata al più tardi entro l'entrata in servizio di tale modifica.

Luogo, data:

Nome, cognome e firma[26]:

[25] P. es. backup offline con verifiche periodiche

[26] Il titolare della rispettiva funzione secondo l'articolo 14 capoverso 4 Oferr, RS 742.141.11

14 Elenco delle modifiche

Modifica			Capitolo	Motivazione / Spiegazione
N.	Data	Versione		
1	27.03.2024	1.1	Copertina	Adeguamento a seguito della modifica di Oferr e DE-Oferr (art. 5*c* sostituito con art. 2 cpv. 1bis)
2	27.03.2024	1.1	Pag. 2	Modifiche alla data e alla tabella
3	27.03.2024	1.1	Cap. 2	Adeguamento a seguito della modifica di Oferr e DE-Oferr (art. 5*c* sostituito con DE 2.1^{bis} n. 1.2)
4	27.03.2024 19.06.2024	1.1	Cap. 3	Adeguamento a seguito della modifica di Oferr e DE-Oferr (art. 5*c* sostituito con DE 2.1^{bis} n. 1.2) NIST CSF Versione 1.1 sostituito con Versione 2.0, nonché aggiornamento dei link Rimando alla nuova D RTE 28100
5	27.03.2024	1.1	Cap. 4	Adeguamento a seguito della modifica di Oferr e DE-Oferr (art. 5*c* sostituito con DE 2.1^{bis} n. 1.2)
6	13.02.2024	1.1	Cap. 5	Adeguamento a seguito della modifica di Oferr e DE-Oferr (art. 5*c* sostituito con DE 2.1^{bis} n. 1.2) Integrazioni alla domanda per l'esonero dall'obbligo di SGSI.
7	27.03.2024 19.06.2024	1.1	Cap. 7	Adeguamento a seguito della modifica di Oferr e DE-Oferr (art. 5*c* sostituito con DE 2.1^{bis} n. 1.2) NIST CSF Versione 1.1 sostituito con Versione 2.0 Adeguamento di diversi rimandi nella colonna Misura del cap. 8
8	19.06.2024	1.1	Cap. 7	A-07: NIST CSF GV.SC-01 (nuovo)
9	27.03.2024	1.1	Cap. 8	NIST CSF Versione 1.1 sostituito con Versione 2.0, incl. le misure che sono cambiate con la versione 2.0.
10	19.06.2024	1.1	Cap. 8.1	B-05: NIST CSF: GV.PO-02 (nuovo) B-07: NIST CSF: DE.CM (nuovo) + ID.AM-03 (nuovo) B-08: NIST CSF: ID.IM-03 (nuovo) B-09: NIST CSF: ID.IM-02 (nuovo) B-11: Rimando alla nuova D RTE 28100 B-17: NIST CSF: PR.DS-02 (nuovo) + PR.DS-10 (nuovo)
11	15.05.2024	1.1	Cap. 8.1 B-09	Rimando alla nuova ordinanza OCTSE invece che all'OTPE, abrogata il 1° ago. 2024.
12	15.05.2024	1.1	Cap. 9	Integrazione o adeguamento di diversi termini.
13	27.03.2024	1.1	All. 1	Primo paragrafo dopo la fig. 1: integrazione dell'ultima frase con gli «asset critici» Fig. 2: adeguamento del riferimento
14	27.03.2024	1.1	All. 3	Diverse integrazioni e aggiornamenti
15	13.02.2024	1.1	All. 4	Piccole integrazioni, precisazioni e adeguamento della formattazione
16	24.06.2024	1.1	Diversi	Cambiamento dell'abbreviazione da ISMS a SGSI