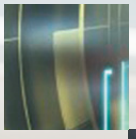
Manuale di cybersicurezza
per le imprese di trasporti pubblici



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'economia,
della formazione e della ricerca DEFR
Ufficio federale per l'approvvigionamento economico del Paese UFAE

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Prefazione

Care lettrici e cari lettori
del manuale di cybersicurezza per le aziende
di trasporti pubblici,

lavorando in un'impresa di trasporti che si annovera tra le infrastrutture critiche del nostro Paese conoscete bene le elevate aspettative in materia di sicurezza, affidabilità e puntualità riposte nel nostro settore. Siete consapevoli dei nuovi rischi che scaturiscono dalla crescente interconnessione dei sistemi e degli impianti e dalla sempre maggiore complessità dei sistemi informatici e sapete che non deve essere ignorato il pericolo di cyberattacchi mirati ai trasporti pubblici. Per garantire, anche in futuro, che queste infrastrutture siano protette nel miglior modo possibile, è necessario trovare un giusto equilibrio tra tecnologie di sicurezza moderne, direttive adeguate, stabilità dei processi e sensibilizzazione dei collaboratori al tema della cybersicurezza.

Il presente manuale intende aiutarvi ad attuare in modo efficace le principali misure di protezione affinché le perturbazioni dovute a cyberincidenti possano essere evitate o risolte in tempi brevi. Si rivolge alle piccole e alle grandi imprese di trasporti. Con l'utilizzo del manuale, che contiene direttive e linee guida note, applicate lo «standard minimo TIC» raccomandato dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) e nel contempo contribuite a migliorare la resilienza delle TIC della vostra azienda e dell'intero settore dei trasporti pubblici.

Questa prima edizione del manuale, cui in futuro saranno regolarmente apportati aggiornamenti e le necessarie aggiunte, è stata realizzata su incarico dell'UTP ed è frutto della collaborazione tra specialisti del settore privato ed esperti dell'UFAE. L'UTP spera così di fornire ai suoi membri raccomandazioni pragmatiche che aiuteranno ad affrontare insieme le sfide poste dalla cybersicurezza.

Vi auguriamo un'interessante lettura, che vi consenta di ottenere i successi sperati.

Ueli Stückelberger
Direttore dell'UTP

Sintesi

Il presente manuale, che si rivolge alle aziende dei trasporti pubblici in Svizzera, formula raccomandazioni per ridurre i cyberrischi a un livello sostenibile. Elaborato da esperti del settore, si prefigge di aiutare i fornitori di trasporti pubblici a migliorare la cybersicurezza[1] nella loro azienda. Le raccomandazioni sono incentrate sull'attuazione di una cosiddetta strategia di difesa in profondità *(defense in depth),* oggi riconosciuta come efficace per fare fronte alle cyberminacce. La strategia comprende raccomandazioni per le tecnologie dell'informazione e della comunicazione (TIC), che devono essere messe in pratica dalle persone in processi efficaci ed efficienti. Inoltre, il manuale rimanda a diversi strumenti e, in particolare, offre un tool di Excel che funge da quadro di riferimento per le imprese, che possono rilevare le proprie capacità, valutarle, confrontarle e svilupparle in modo mirato. Il presente manuale è compatibile con gli standard internazionali, si basa sul Cybersecurity Framework Core del NIST[2] e tiene conto dei risultati e delle misure necessarie derivanti dalle analisi dei rischi e delle vulnerabilità del sottosettore Trasporti e Logistica dell'Ufficio federale dell'approvvigionamento economico del Paese[3].

[1] Il termine «cybersicurezza» designa tutte le misure organizzative e tecniche volte a preservare la disponibilità, l'integrità e la riservatezza delle informazioni sia per le TIC sia per i sistemi di controllo industriale (industrial control system, ICS).
[2] Il Cybersecurity Framework del NIST (NIST CSF), sviluppato dal National Institut of Standards and Technology (autorità federale americana), è un quadro di riferimento in materia di cybersicurezza che si è imposto come standard in numerosi Paesi.
[3] Analisi dei rischi e delle vulnerabilità del sottosettore Trasporti e Logistica. Ufficio federale per l'approvvigionamento economico del Paese UFAE, Berna 2017.

Indice

Situazione iniziale e obiettivi

La Svizzera è fortemente dipendente dalla continuità operativa delle infrastrutture critiche, che assicurano la disponibilità di importanti beni e servizi, tra cui l'energia, le comunicazioni e i trasporti. Perturbazioni totali o parziali delle infrastrutture critiche hanno gravi ripercussioni sull'economia e sulla popolazione e compromettono il funzionamento, la sicurezza e la prosperità della Svizzera. Conformemente all'articolo 2 capoverso 2 della Costituzione federale, la Confederazione è tenuta a promuovere «in modo sostenibile la comune prosperità, la coesione interna e la pluralità culturale del Paese». Ne consegue che la protezione di queste infrastrutture critiche è uno dei principali compiti dello Stato che può essere adempiuto solo con il concorso dell'economia privata.

1.1 Considerazioni generali

La nuova legge sull'approvvigionamento economico del Paese, entrata in vigore il 1° giugno 2017, conferisce all'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) la competenza di attuare misure preventive a titolo sussidiario per migliorare la sicurezza dell'approvvigionamento. Il presente manuale si annovera tra le misure preventive previste dalla legge. Conformemente al principio della sussidiarietà, il manuale è stato concepito come raccomandazione per il settore.

Nel quadro della strategia nazionale per la protezione delle infrastrutture critiche, l'approvvigionamento economico del Paese (AEP), più precisamente l'UFAE, ha verificato le vulnerabilità delle TIC per il settore dei trasporti pubblici. Le analisi dei rischi e delle vulnerabilità nei sottosettori del trasporto stradale (2015) e del trasporto ferroviario (2017) sono state realizzate e verificate congiuntamente dalla Confederazione e dai membri dell'AEP. Esse hanno riguardato, tra l'altro, il rapporto di dipendenza di questi sottosettori dalle risorse TIC e hanno messo in evidenza che la dipendenza del trasporto ferroviario è tendenzialmente più elevata di quella del trasporto stradale.

I trasporti pubblici svizzeri sono unici al mondo. Grazie all'orario cadenzato e alle buone possibilità di coincidenze, offrono ai viaggiatori una catena di trasporto ininterrotta su tutti i mezzi (ferrovia, bus, tram, battello, funivia, come raffigurato nella Figura 1). Oltre a rispondere alle crescenti esigenze di mobilità, i trasporti pubblici rivestono anche una notevole importanza economica e garantiscono l'approvvigionamento dell'intero territorio svizzero.

Figura 1: Mezzi di trasporto pubblico

La sempre maggiore interconnessione dei mezzi di trasporto pubblici agevola gli spostamenti da un punto A a un punto B, ma nel contempo aumenta gli sforzi per conformarsi al crescente numero di prescrizioni legali e mettere in sicurezza i componenti e i sistemi di gestione sempre più complessi verso l'interno e l'esterno.

La figura seguente illustra un possibile scenario di sviluppo e di ampliamento della catena di mobilità nel contesto di una città intelligente *(smart city)* grazie ai cosiddetti hub di mobilità (poli), che integrano mezzi sempre più numerosi (*car sharing,* biciclette elettriche ecc.) nell'offerta dei trasporti pubblici.

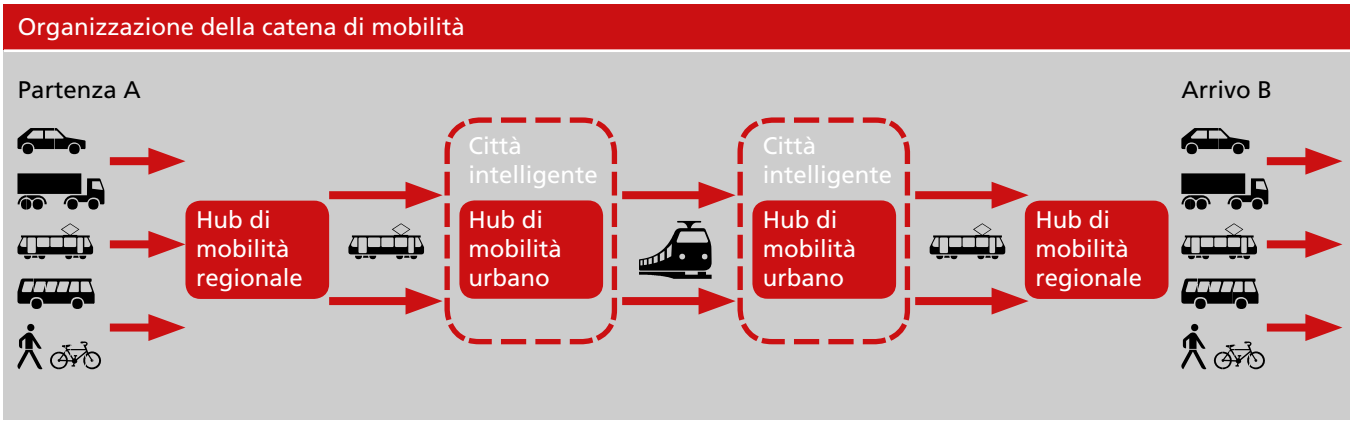


Figura 2: La catena di mobilità del futuro

L'informatizzazione e l'interconnessione crescenti di quasi tutti gli ambiti del quotidiano offrono potenzialità che un Paese industrializzato e altamente sviluppato come la Svizzera deve cogliere. La tecnologizzazione è già molto avanzata nel settore dei trasporti pubblici. Tutti i principali processi sono già supportati da sistemi TIC, indispensabili per mantenere la cadenza molto stretta dei trasporti pubblici. La sempre più accentuata digitalizzazione di tutti gli elementi dei trasporti pubblici accresce progressivamente la dipendenza dai sistemi TIC e, quindi, la necessità di cybersicurezza. Ciò implica nuovi rischi, nuove fonti di vulnerabilità e di errori che possono provocare perturbazioni, con ripercussioni negative sull'attività economica e che, quindi, devono essere affrontati. A causa delle elevate esigenze di sicurezza per i trasporti pubblici, i veicoli con un guasto ai sistemi di sicurezza possono proseguire solo a velocità ridotta oppure devono fermarsi, limitando notevolmente la disponibilità dell'infrastruttura.

1.2 Scopo del manuale

Le aziende dei trasporti pubblici sono interessanti bersagli dei cyberattacchi. Dispongono infatti di interfacce web per un buon numero delle loro piattaforme informatiche e dei loro sistemi e impianti SCADA, dunque rischiano di essere presi facilmente di mira. Versioni ancora sconosciute di ransomware, l'aumento dei vettori di attacco e delle falle aprono la strada a inediti «scenari d'attacco». Per evitare il più possibile che i processi e i sistemi TIC diventino vulnerabili, le aziende dei trasporti pubblici si impegnano per preservare la resilienza dei processi, dei sistemi e degli impianti, che devono essere oggetto di test periodici, affinché possano essere escluse ripercussioni sulla disponibilità e l'integrità dei trasporti pubblici.

Le imprese di trasporti pubblici devono continuare a proteggersi dagli attacchi e migliorare costantemente le misure preventive. A tal fine è essenziale che possano contare su una protezione di base solida e standardizzata. Nonostante ciò, non è possibile coprire adeguatamente tutti i rischi con misure preventive e non sarebbe neppure opportuno in un'ottica economica. In futuro dovrà dunque essere attribuita una maggiore importanza anche alle misure che permettono di identificare gli attacchi o i tentativi di attacco e a una reazione adeguata e rapida. Solo così le imprese di trasporti pubblici riusciranno a gestire i cyberrischi in misura soddisfacente. Ne fanno parte integrante gli scambi e la collaborazione con altre imprese, partner ed esponenti del mondo scientifico.

La sicurezza delle TIC presuppone quindi che ogni operatore assuma le proprie responsabilità adottando un comportamento consapevole dei rischi e utilizzando sistemi sicuri. L'attuazione delle collaudate misure esposte nel presente manuale è già sufficiente a prevenire un numero elevato di perturbazioni e di attacchi alle TIC con un dispendio ragionevole. Il manuale si prefigge di offrire alle aziende e alle organizzazioni uno strumento polivalente con cui migliorare la resilienza della loro infrastruttura TIC. Con il suo approccio fondato sui rischi, consente l'attuazione di diversi livelli di protezione adeguati alle esigenze dell'organismo o dell'impresa.

1.3 Campo di applicazione

Il presente manuale è stato elaborato dall'AEP in collaborazione con esperti esterni. Oggi esistono già diversi standard riconosciuti a livello internazionale per la sicurezza delle TIC, molti dei quali vanno al di là dell'ambito trattato in questa sede (vedi tabella 54). Il manuale non intende in alcun modo sostituirsi agli standard esistenti ed è in linea con essi, seppure la sua portata sia inferiore. Il suo obiettivo è offrire un accesso più semplice alla materia, ma garantire comunque un livello elevato di protezione.

Le raccomandazioni destinate alle imprese del settore rientrano nell'«autodisciplina», quindi la loro attuazione è facoltativa. Il manuale si rivolge sostanzialmente alle imprese e agli organismi che partecipano all'organizzazione dei trasporti pubblici. In futuro potrà essere aggiornato ove necessario.

Il manuale si concentra sui processi interni alle aziende che hanno ripercussioni dirette sulla creazione e sulla fornitura di servizi di trasporto da parte degli attori definiti di seguito.

Gestori dell'infrastruttura ferroviaria (GIF)	Imprese che hanno ottenuto una concessione d'infrastruttura e un'autorizzazione di sicurezza per la costruzione e l'esercizio di un'infrastruttura ferroviaria conformemente all'articolo 5 della legge federale sulle ferrovie (Lferr). Per infrastruttura ferroviaria si intendono gli impianti ferroviari e le linee di trasporto della corrente di trazione.
Imprese di trasporto ferroviario (ITF)	Imprese che forniscono servizi di trasporto ferroviario. Secondo l'articolo 8*c* Lferr, chi intende effettuare trasporti di persone o di merci utilizzando un'infrastruttura ferroviaria deve disporre di un'autorizzazione di accesso alla rete e di un certificato di sicurezza.
Imprese concessionarie di trasporto di persone	Imprese che, conformemente all'articolo 6 della legge sul trasporto di viaggiatori (LTV), dispongono di una concessione per il trasporto regolare e professionale di viaggiatori per ferrovia, mediante tram, impianti a fune, battelli o motoveicoli a propulsione termica o elettrica.

Tabella 1: Attori dei trasporti pubblici

Il livello di protezione deve essere garantito su tutte le linee che hanno una funzione di collegamento ai sensi dell'articolo 5 dell'ordinanza del 4 novembre 2009 sul trasporto di viaggiatori (OTV, RS 745.11). Vi è funzione di collegamento quando ad almeno un'estremità della linea si trova un punto di raccordo con la rete interregionale, nazionale o internazionale dei trasporti pubblici e all'altra estremità o tra le due estremità della linea una località. Sono considerate località gli agglomerati in cui tutto l'anno almeno 100 abitanti risiedono in:

- zone edificabili adiacenti secondo la legge del 22 giugno 1979 sulla pianificazione del territorio, comprese le zone di protezione delle acque, i siti caratteristici, i luoghi storici e i monumenti culturali;
- insediamenti sparsi tradizionali;
- valli nelle regioni di montagna, il cui collegamento è effettuato da un punto comune.

1.4 Guida all'utilizzo del manuale

Il manuale è suddiviso in diversi capitoli: i primi 2 introducono al tema dei trasporti pubblici, il capitolo 3 illustra l'approccio della difesa in profondità, i capitoli 4 e 5 descrivono le misure da attuare e presentano i relativi strumenti.

Per valutare il proprio livello di maturità in materia di cybersicurezza, le imprese e le organizzazioni possono ricorrere al tool di valutazione «Standard minimo TIC». Lo standard minimo TIC è considerato adempiuto se l'«*Overall Cybersecurity Maturity Rating*» corrisponde al valore minimo richiesto.

Processi critici nei trasporti pubblici

Per trattare il tema della cybersicurezza nei trasporti pubblici occorre prima di tutto definire i principali attori del settore, i processi critici e i rapporti di dipendenza dei sistemi di importanza sistemica.

2.1 Principali processi operativi

Il presente manuale intende garantire la cybersicurezza dei principali processi nel settore dei trasporti, focalizzandosi sui settori dei trasporti pubblici ferroviari e stradali. Le prescrizioni e le misure di attuazione qui contenute possono essere tuttavia applicate anche al trasporto di viaggiatori mediante impianti a fune o battelli.

Di seguito sono illustrati i processi operativi informatizzati.

2.1.1 Trasporto ferroviario

Per garantire il funzionamento del trasporto ferroviario sono necessarie tre reti: prima di tutto la *rete di comunicazione* (rete fissa e mobile), che consente lo scambio dei dati necessari alla sicurezza, alla qualità, al mantenimento e al proseguimento del traffico; poi la *rete elettrica,* che costituisce la principale fonte di energia; infine la rete ferroviaria e le relative infrastrutture (incl. gli impianti di sicurezza) che, una volta costruite, devono essere regolarmente manutenute per consentire la circolazione senza incidenti dei treni e dei tram. Nello schema seguente sono riportati i processi informatizzati nel trasporto ferroviario.

Inoltre, gli impianti di manutenzione o di sicurezza ferroviaria si avvicinano sempre più a «sistemi» digitali molto complessi. Gli impianti di sicurezza ferroviaria, che comprendono tra l'altro anche sistemi di segnalazione (p.es ETCS), sono generalmente telecomandati da una centrale operativa mediante sistemi informatizzati (strumentazione di controllo). Le reti di comunicazione digitale collegano e integrano l'insieme degli impianti di tecnica ferroviaria, incluse le applicazioni TIC dell'esercizio ferroviario (sistemi di gestione del traffico ecc.). Esse sono indispensabili per mantenere e proseguire l'esercizio ferroviario.

Le TIC spaziano dalla messa in rete degli impianti fissi alla tecnica dei veicoli, passando per l'esercizio ferroviario. I sistemi e gli impianti possono essere classificati in diverse categorie, in base alla loro funzione principale: informazione, gestione o sicurezza.

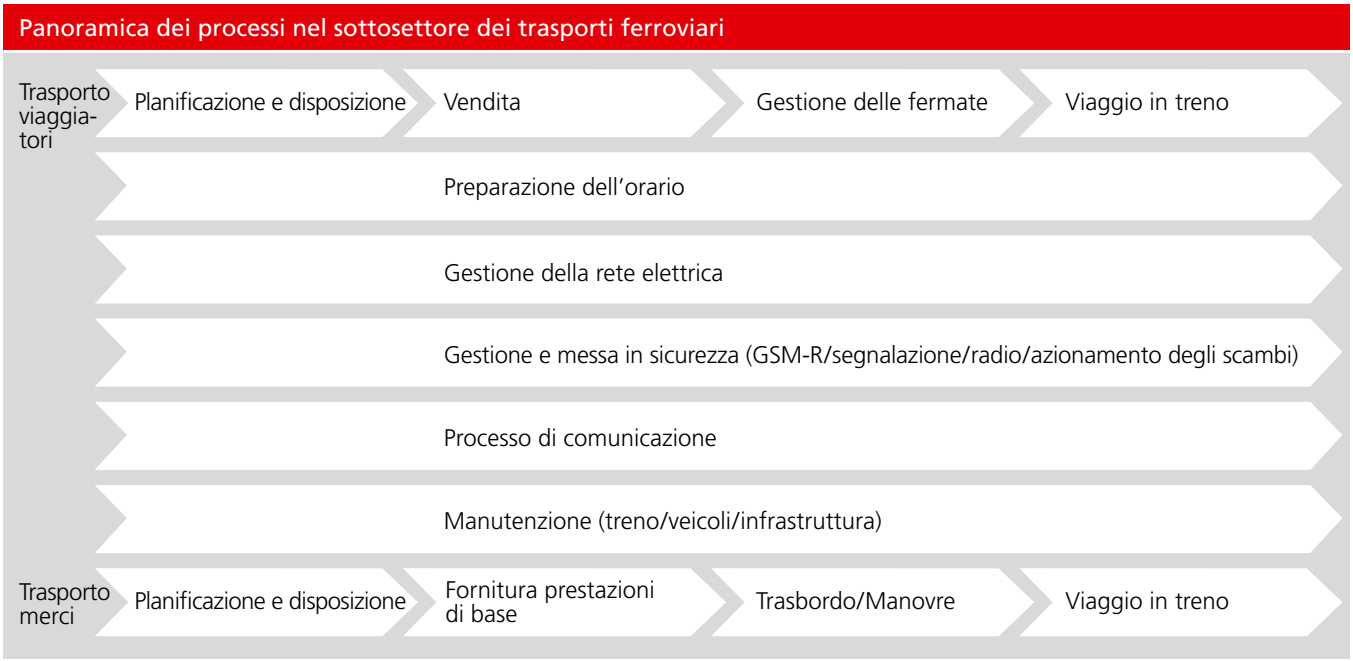


Figura 3: Panoramica dei processi informatizzati nel traffico ferroviario

2.1.2 Traffico stradale

Il traffico stradale pubblico è caratterizzato dall'interazione di diversi attori e si compone di processi complementari che si sovrappongono dal punto di vista temporale e geografico. Le TIC sono utilizzate non solo nella gestione e nel monitoraggio dei diversi elementi dell'infrastruttura (illuminazione stradale, ventilazione delle gallerie ecc.), ma anche per pilotare e sorvegliare il traffico (rilevatori dei flussi di traffico, videocamere, deviazioni, indicatori dinamici dei limiti di velocità) e fornire informazioni agli utenti (segnalazioni di code, dispositivi di navigazione). Inoltre, i veicoli moderni sono sempre più dotati di dispositivi elettronici, la cui gamma è molto ampia: dispositivi di immobilizzazione, elettronica di intrattenimento, controllo delle prestazioni del motore, controllo della trazione o assistenza al mantenimento di corsia ecc.

Come utenti della strada, anche le imprese di bus e di tram ricorrono a questi sistemi. Inoltre dispongono di molteplici sistemi di gestione (p.es sistema di controllo, radio/VoIP, sistemi di localizzazione) e di informazione (a bordo e all'esterno del veicolo, alla fermata, su Internet).

Le imprese di trasporti pubblici sono inoltre collegate ad alcuni sistemi della rete stradale (p.es gestione dei semafori).

Per quanto riguarda le TIC nel trasporto pubblico stradale occorre considerare due tipologie: da un lato, le TIC dei proprietari delle strade (Confederazione, Cantoni, Comuni) sui quali le imprese di trasporto concessionarie hanno un'influenza modesta o non ne hanno alcuna, dall'altra le proprie TIC di cui le imprese di trasporto sono le uniche responsabili.

2.2 Processi critici nei trasporti pubblici

Negli ultimi anni il ricorso ai sistemi informatici o ai sistemi TIC nelle catene dei trasporti e della logistica si è ulteriormente accentuato. Questa evoluzione tecnologica consente di centralizzare la gestione e la regolazione delle informazioni in tempo reale. In tal modo la direzione dell'esercizio della rete diventa molto più agile con la possibilità di reagire in tempi più brevi e in maniera automatizzata agli eventi critici inattesi. Tuttavia, queste trasformazioni verso la tecnologia dell'informazione comportano anche nuovi rischi, che le imprese di trasporto e della logistica sono chiamate a riconoscere, valutare e gestire per essere in grado di adempiere il loro mandato legale.

Processi critici		
Infrastruttura	Traffico, trasporto	Governo d'impresa
• Ciclo di vita dell'infrastruttura	• Ciclo di vita dei veicoli	• Gestione dell'impresa (normativa, strategica, operativa)
• Manutenzione dell'infrastruttura	• Pianificazione dei servizi di trasporto	• Esercizio delle TIC e interfaccia con gli ICS
• Gestione delle vie di comunicazione	• Fornitura dei servizi di trasporto	• Finanze e contabilità
• Direzione del traffico	• Vendita dei servizi di trasporto	• Gestione delle emergenze e delle crisi

Tabella 2: Processi critici nei trasporti pubblici

I diversi processi critici sono sinteticamente descritti di seguito.

2.2.1 Processi legati all'infrastruttura

Ciclo di vita dell'infrastruttura

L'infrastruttura delle imprese di trasporto concessionarie comprende tutte le reti, i sistemi e gli impianti necessari all'esercizio dei trasporti pubblici, tra cui rotaie (sottostruttura), linee aeree di contatto (sovrastruttura), impianti di sicurezza o centrali operative. Il ciclo di vita dell'infrastruttura comprende tutte le fasi: ideazione, sviluppo, realizzazione, messa fuori esercizio e smaltimento.

Manutenzione dell'infrastruttura

La manutenzione delle infrastrutture è pianificata minuziosamente e comprende, tra l'altro, i controlli periodici dello stato degli impianti. Alcune imprese di trasporti pubblici utilizzano sistemi ERP *(enterprise resource planning)* per pianificare i lavori di manutenzione, con la conseguenza che vengono spesso concepite proprie soluzioni.

Gestione delle vie di comunicazione

Le vie di comunicazione sono gestite pianificando le tracce disponibili *(slot)* e attribuendole alle imprese di trasporto concessionarie (ITC). Le tracce attribuite sono archiviate nei sistemi *back-end* (banche dati) delle imprese di trasporti pubblici.

Direzione del traffico

La direzione del traffico consiste nel sorvegliare e gestire i treni, i tram e i bus nonché nell'azionare gli scambi e i segnali. Oggi non sarebbe più concepibile sorvegliare e gestire il trasporto pubblico senza ICS (sistemi industriali di controllo, cfr. cpv. 3.5.1). Un guasto di questi sistemi di controllo, dovuto per esempio a un cyberincidente, comporterebbe perdite di capacità o, addirittura, un'interruzione del traffico sulle tratte interessate.

2.2.2 Processi legati al traffico e al trasporto

Ciclo di vita dei veicoli

L'intero ciclo di vita dei veicoli è pianificato e gestito con i sistemi TIC, senza i quali le imprese di trasporti pubblici si troverebbero di fronte una sfida considerevole, che rischierebbe di compromettere i collegamenti nell'arco di pochi giorni. Solo una parte dei processi del ciclo di vita potrebbe essere assicurata senza ricorrere alle TIC per un periodo prolungato.

Pianificazione dei servizi di trasporto

L'orario, la cui pianificazione è coordinata con almeno un anno di anticipo, non è un documento statico e, grazie alla crescente digitalizzazione, la sua flessibilità aumenta. Oggi sono possibili adattamenti e ottimizzazioni in tempo reale, talvolta addirittura in modo automatizzato. L'orario serve come riferimento per decidere l'impiego dei veicoli e del personale. Un guasto dei sistemi avrebbe conseguenze molto gravi per i trasporti pubblici.

Fornitura dei servizi di trasporto

Lo svolgimento regolare della corsa di un treno, di un tram o di un bus è fortemente dipendente dagli ICS (sistemi di controllo industriali) e dai sistemi TIC (p.es per l'informazione agli utenti). Per esempio, le tratte ferroviarie più recenti possono essere percorse solo da veicoli dotati del sistema ETCS, poiché i segnali sono visualizzati unicamente su uno schermo collocato nella cabina di guida. Nei bus e nei tram, per esempio, il rispetto delle distanze tra diversi veicoli su una determinata linea può essere gestito da un sistema di controllo, senza il quale oggi non sarebbe più possibile garantire la puntualità e l'affidabilità dei trasporti pubblici.

Vendita dei servizi di trasporto

Il processo di vendita può avvenire su diversi canali: allo sportello, su Internet, con un'app o ai distributori automatici di biglietti. I guasti dei sistemi di vendita o delle interfacce con i fornitori esterni di servizi finanziari (Six Payment, banche ecc.) possono provocare perdite alle imprese di trasporto. Anche il conteggio dei passeggeri è importante per garantire le entrate.

2.2.3 Processi legati al governo d'impresa

Gestione d'impresa

Oggi un guasto ai sistemi centrali di informazione che servono alla gestione d'impresa (p.es sistema ERP) comprometterebbe la conduzione di qualunque grande impresa. Nell'ambito dei trasporti pubblici ciò riguarda, tra l'altro, sistemi tra cui i cockpit di gestione, i *software* di gestione finanziaria, di gestione dei progetti o ancora di gestione del personale.

Esercizio delle TIC e interfaccia con gli ICS

Tutti i principali processi del trasporto pubblico sono supportati da sistemi TIC e ICS. Tra questi si annoverano i centri di calcolo, le reti di comunicazione nonché le applicazioni TIC e ICS. Se i sistemi TIC non funzionano, l'operatività dei trasporti pubblici non può essere assicurata nel lungo termine.

Finanze e contabilità

La contabilità finanziaria e la contabilità d'esercizio sono gestite prevalentemente mediante sistemi centralizzati (p.es ERP). Se questi sistemi si guastano (p.es al momento del versamento dei salari) oppure si verificano errori gravi, nel medio termine può risultare compromessa l'esistenza stessa delle imprese di trasporto concessionarie.

Gestione delle crisi

I sistemi di comunicazione sono particolarmente importanti nella gestione delle crisi. A seconda del tipo di crisi, non è tuttavia da escludere che non funzioni affatto o solo parzialmente. Per le imprese di trasporto concessionarie è fondamentale essere ben preparate ad affrontare una crisi, quindi non si può prescindere da una prevenzione delle emergenze a 360°, con piani e sistemi d'emergenza aggiornati e sottoposti a test periodici.

2.3 Dipendenza dei processi critici dai sistemi TIC

I summenzionati processi dipendono dalla stabilità e dalla sicurezza dei necessari sistemi TIC. Di conseguenza, i sistemi e gli impianti si annoverano tra le risorse critiche per il trasporto pubblico. Un processo può dipendere da più sistemi TIC e un sistema TIC può essere una risorsa critica per diversi processi operativi.

È dunque indispensabile che ogni impresa di trasporti pubblici documenti con esattezza e in modo duraturo i propri processi, sistemi e impianti (architettura di sistema). Una protezione contro i rischi non può prescindere dalla conoscenza di ciò che deve essere protetto.

Le seguenti varianti di presentazione illustrano come possano essere visualizzate e documentate le dipendenze dei processi operativi dai principali sistemi informatici o dalle loro funzioni. È possibile optare per diversi livelli di granularità e naturalmente anche combinare diverse forme di documentazione.

La Figura 4 illustra la complessità dei processi critici. Quanto più i collegamenti tra un processo critico e i diversi sistemi sono numerosi, tanto maggiore è la dipendenza dai sistemi TIC e dai sistemi SCADA.

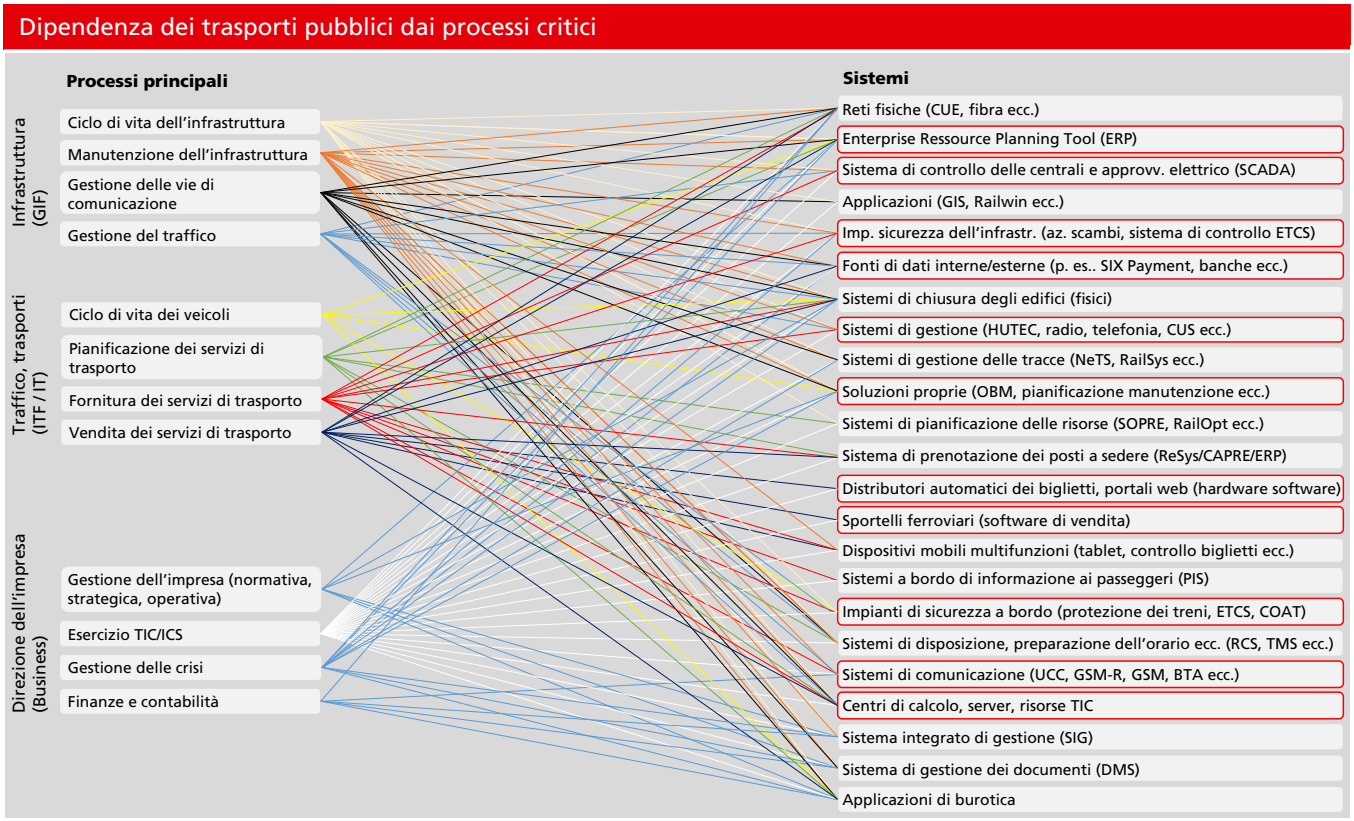


Figura 4: Interconnessione con i sistemi TIC e SCADA

Nella tabella seguente sono illustrate, mediante una matrice, le dipendenze dei processi critici del trasporto pubblico dai sistemi. Ogni impresa dovrà poi verificare se, nel suo caso, la dipendenza in questione è realmente del tipo raffigurato. A tal fine, gli autori del presente manuale propongono analisi concrete da realizzare all'interno dell'impresa sulla base del bilancio d'impatto sull'attività (BIA). In allegato sono riportati alcuni esempi di domande semplici che consentono di delineare un BIA.

Governo d'impresa (Business)					Traffico, trasporto (ITS/AT)				Processi legati all' infrastruttura (GIF)				
Gestione delle crisi	Finanze e contabilità	Esercizio delle TIC/degli ICS	Gestione d'impresa (processo di gestione: normativa, strategica, operativa)		Vendita dei servizi di trasporto	Fornitura dei servizi di trasporto	Pianificazione dei servizi di trasporto	Ciclo di vita dei veicoli	Direzione del traffico	Gestione delle vie di comunicazione	Manutenzione dell'infrastruttura	Ciclo di vita dell'infrastruttura	
×	×	×			×	×	×		×	×	×	×	Reti fisiche (CUE, fibra ecc.)
	×	×	×		×		×	×		×	×	×	Tool di pianificazione delle risorse d'impresa (ERP)
		×				×			×		×	×	Sistema di controllo delle centrali elettriche (SCADA)
		×								×	×	×	Applicazioni (applicazioni geografiche, GIS, Railwin ecc.)
×		×				×			×		×	×	Impianti di sicurezza dell'infrastruttura (azionamento degli scambi, strum. di controllo, ETCS)
	×	×			×				×	×	×		Fonti di dati interne/esterne (p.es Six Payment, banche, fornitori)
	×	×	×		×	×	×	×	×	×	×	×	Sistemi di chiusura degli edifici (fisici)
		×				×			×		×	×	Sistemi di controllo (HUTEC, radio, telefonia, CUS ecc.)
	×	×								×	×	×	Sistemi di gestione delle tracce (NeTS, RailSys ecc.)
	×	×	×					×		×	×	×	Soluzioni proprie (OBM, pianificazione ecc.)
		×					×					×	Sistemi di pianificazione delle risorse (SOPRE, RailOpt ecc.)
		×			×	×	×						Sistema di prenotazione dei posti a sedere (ReSys/CAPRE/ERP)
		×			×								Distributori automatici dei biglietti, portali web (*hardware* e *software*)
		×			×								Sportelli ferroviari (*software* di vendita)
		×			×	×					×		Dispositivi mobili multifunzione (tablet, controllo biglietti ecc.)
		×				×							Sistemi a bordo di informazione ai passeggeri (PIS)
		×				×		×	×			×	Impianti di sicurezza a bordo (protezione dei treni, ETCS, COAT)
		×				×	×		×	×	×		Sistemi di disposizione, preparazione dell'orario ecc. (RCS, TMS ecc.)
×		×				×			×		×		Sistemi di comunicazione (UCC, GSM-R, GSM, BTA ecc.)
		×			×	×	×		×	×	×	×	Centri di calcolo, server, risorse TIC
×	×	×	×								×	×	Sistema integrato di gestione (SIG)
×	×	×	×							×	×	×	Sistema di gestione dei documenti (DMS)
×	×	×	×		×		×	×		×	×	×	Applicazioni di burotica

Dipendenza dai sistemi dei processi critici del trasporto pubblico

Tabella 3: Dipendenza dei processi critici del trasporto pubblico dai sistemi

La seguente tabella indica il grado di dipendenza dai sistemi TIC di ognuno dei processi critici di cui sopra. Il presente capitolo risponde alla seguente domanda: «Il processo può essere eseguito senza TIC (dipendenza dalle TIC)?» Il grado di dipendenza è classificato in tre categorie: basso, medio, elevato. Un grado di dipendenza basso indica che un processo può essere sostanzialmente eseguito anche senza le TIC. Per un processo che necessita di ulteriori risorse (tempo, personale ecc.) per essere eseguito senza le TIC si parla di grado medio. Un processo che non può essere eseguito senza le TIC ha un grado di dipendenza elevata.

Inoltre viene proposto un requisito minimo unitario in termini di maturità (cfr. cpv. 4.3 «Livelli di implementazione»):

Processi critici nei trasporti pubblici		
Processi	Grado di dipendenza dalle TIC	Requisito di maturità
Infrastruttura	(basso/medio/elevato)	(secondo il cap. 4)
Ciclo di vita dell'infrastruttura	medio	2–3
Manutenzione dell'infrastruttura	elevato	2–3
Gestione delle vie di comunicazione	elevato	3–4
Direzione del traffico	elevato	3–4
Traffico, trasporto		
Ciclo di vita dei veicoli	medio	3–4
Pianificazione dei servizi di trasporto	elevato	2–3
Fornitura dei servizi di trasporto	elevato	3–4
Vendita dei servizi di trasporto	medio	2–3
Governo d'impresa		
Gestione dell'impresa (normativa, strategica, operativa)	medio	3–4
Esercizio delle TIC (e interfaccia con gli ICS)	elevato	2–3
Finanze e contabilità	medio	2–3
Gestione delle emergenze e delle crisi	elevato	2–3

Tabella 4: Grado di dipendenza dalle TIC dei processi critici

Questa proposta può essere adattata in funzione dei BIA e delle analisi delle interfacce realizzate nelle imprese. Tuttavia, il livello di maturità non dovrebbe essere inferiore a 2.

2.4 Resilienza dei processi TIC, dei sistemi e degli impianti

In generale il termine «resilienza» designa la capacità dei sistemi di reagire alle perturbazioni. In rapporto con la strategia nazionale per la protezione delle infrastrutture critiche, «resilienza» (o «resilienza delle TIC») indica la capacità dei processi critici valutati di resistere alle perturbazioni dei sistemi informatici.

Tuttavia la resilienza non è limitata alla questione dei sistemi ridondanti e, nel caso dei sistemi TIC, comprende sempre anche gli aspetti organizzativi. Tra le misure organizzative per aumentare la resilienza si annoverano, per esempio, l'elaborazione di direttive concernenti le autorizzazioni e il salvataggio dei dati, una gestione rigorosa degli aggiornamenti correttivi *(patch)*, il rilevamento precoce dei rischi. Inoltre, si pone continuamente la questione della possibilità di realizzare un processo mediante un sistema ridondante non informatizzato. Se uno specifico sistema d'informazione si guasta improvvisamente, le informazioni possono essere comunicate oralmente con il passaparola, per e-mail o per telefono.

Occorre sempre considerare anche la resilienza sistemica. Per esempio, diversi sistemi possono assumere la stessa funzione oppure la velocità di funzionamento di alcuni sistemi può essere aumentata o diminuita per subentrare a un altro sistema che ha subito un guasto. Prendendo come esempio la rete elettrica (p.es una centrale idroelettrica), l'interruzione della fornitura da parte di un produttore può essere affrontata importando elettricità da altre fonti. Questa resilienza sistemica deve essere considerata nella valutazione della resilienza delle TIC.

La resilienza può essere accresciuta concretizzando e attuando i requisiti e le misure esposti nei due capitoli seguenti nonché considerando gli standard di sicurezza rilevanti per le singole imprese.

2.5 Differenza tra *security* e *safety*

Gli addetti ai lavori parlano di *safety* intendendo in particolare la protezione delle persone e dell'ambiente di fronte ai pericoli derivanti da un «sistema». Ciò comprende, per esempio, la prevenzione degli incidenti di cui possono rimanere vittime le persone. Con il termine *security* si intende, invece, la protezione delle persone o dei sistemi nei casi di forza maggiore o di atti illeciti con o senza ricorso alla violenza.

Le analisi e l'attuazione delle misure non devono prescindere dalla considerazione degli aspetti rilevanti ai fini della *safety.* Le imprese di trasporti pubblici mettono a disposizione della popolazione svizzera un servizio (sotto forma di corse in bus, treno, battello ecc.). I beneficiari del servizio sono sempre gli esseri umani.

Di conseguenza le prescrizioni e le misure riguardanti la *safety* devono essere combinate con quelle concernenti la *security* in modo da creare un piano omogeneo per una sicurezza a 360°.

Elementi di una strategia di difesa in profondità

«Difesa in profondità» (in inglese: *defence in depth)* designa un utilizzo coordinato di diverse misure di sicurezza per proteggere i dati e l'elaborazione delle informazioni in un'impresa.

3.1 Panoramica della difesa in profondità

Un'impresa deve orientare la propria strategia di sicurezza delle TIC alla protezione delle risorse critiche TIC che sono indispensabili ai processi operativi. A tal fine occorre un approccio a più livelli noto a livello internazionale come «*defence in depth*», intendendo con ciò un utilizzo coordinato di diverse misure di sicurezza per proteggere gli strumenti operativi TIC *(asset)* di un'impresa. Questo approccio si basa sul principio militare secondo cui un sistema di difesa complesso a più livelli è più difficile da superare per il nemico rispetto a una singola barriera. Parallelamente vengono studiati i metodi e i modi di operare dei potenziali aggressori per approntare opportuni dispositivi di difesa. Nell'ambito della sicurezza delle TIC la difesa in profondità mira a identificare le violazioni della sicurezza informatica, a reagire e ad attenuarne gli effetti (in inglese: *mitigate)*. La difesa in profondità segue un approccio olistico, volto a proteggere tutti gli asset TIC da qualsiasi rischio. Un'impresa deve impegnare le proprie risorse al fine di garantire una protezione efficace contro i rischi noti e un monitoraggio a 360° dei rischi potenziali. Le relative misure devono proteggere la totalità dei sistemi TIC, che comprendono persone, processi, oggetti, dati e dispositivi. Un potenziale aggressore costituisce una minaccia per un sistema TIC solo quando riesce a sfruttare una falla esistente in uno di questi elementi. Gli organismi e le imprese sono tenuti a monitorare costantemente le misure e, all'occorrenza, ad adattarle alle nuove minacce.

L'implementazione dei piani di difesa in profondità può avere diverse sfaccettature. Tra l'informatizzazione degli uffici e una tecnologia operativa (TO, detta anche ICS/SCADA) esistono notevoli differenze già a livello di caratteristiche e di metodi applicati. Tali differenze sono illustrate sulla base dei seguenti esempi di tematiche concernenti la sicurezza (cfr. Tabella 4: Grado di dipendenza dalle TIC dei processi critici):

Tema della sicurezza	TIC (p.es informatizzazione degli uffici)	TO/ICS/SCADA (p.es gestione della produzione)
Direttive di sicurezza	Prescrizioni normative generali, legate al settore (non esistono per tutti i settori).	Direttive normative specifiche, legate al settore (non esistono per tutti i settori).
Ciclo di vita della tecnologia *(Technology support life cycle)*	2–3 anni, più offerenti, sviluppo e aggiornamenti continui *(upgrade)*.	10–20 anni, in genere lo stesso fornitore/operatore per l'intero ciclo di vita; la conclusione del ciclo di vita comporta nuovi rischi per la sicurezza.
Aggiornamenti di sicurezza *(Update management)*	Definiti chiaramente, applicati a livello di tutta l'impresa, automatizzati tramite accesso remoto.	Tempi lunghi di preparazione prima che la *patch* sia installata; sempre specifiche per produttore; può disattivare (temporaneamente) l'ICS; necessità di definire un rischio accettabile.
Metodi di test e audit *(testing and audit method)*	Impiego di metodi aggiornati (ev. automatizzati). I sistemi sono in genere sufficientemente resilienti e affidabili da consentire *assessment* mentre sono operativi.	L'elevato grado di sviluppo individuale, per esempio, rende i metodi di *assessment* automatizzati probabilmente non idonei. Durante un *assessment* la probabilità che un errore si verifichi è più elevata. Gli *assessment* mentre il sistema è in esercizio sono pertanto tendenzialmente più difficili.

Tabella 5: Differenze tra TIC e ICS

Tema della sicurezza	TIC (p.es informatizzazione degli uffici)	TO/ICS/SCADA (p.es gestione della produzione)
Gestione dei cambiamenti *(Change management)*	Pianificata con una cadenza regolare. Adeguata alle esigenze dell'impresa per una durata minima/massima di utilizzo.	Procedura complessa con potenziali conseguenze sull'operatività. Necessità di una pianificazione strategica individuale.
Classificazione degli *asset* *(Asset classification)*	Operazione eseguita abitualmente ogni anno. Le spese e gli investimenti sono pianificati in base ai risultati.	Viene eseguita solo se necessaria o prescritta. Senza inventario, le contromisure sono spesso inadeguate all'importanza dell'elemento del sistema.
Reazione a un evento e sua analisi *(Incident response and forensics)*	Semplice da sviluppare e attuare. A seconda delle circostanze, necessità di attenersi a prescrizioni normative (protezione dei dati).	Si concentra principalmente sul ripristino del sistema. Procedure di analisi poco sviluppate.
Sicurezza fisica *(Physical security)*	Varia da debole (informatizzazione degli uffici) a forte (centri di calcolo con sistemi di protezione rinforzati).	In genere sicurezza fisica molto buona.
Sviluppo sicuro del sistema *(Secure software development)*	Parte integrante del processo di sviluppo.	Storicamente gli ICS sono stati quasi sempre concepiti come sistemi fisici isolati. La sicurezza come parte integrante dello sviluppo del sistema è pertanto poco diffusa. In questo ambito i fornitori di ICS hanno compiuto progressi, per quanto più lenti rispetto all'universo delle TIC. Spesso gli elementi centrali degli ICS non consentono soluzioni di sicurezza a posteriori o queste non sono disponibili.
Antivirus	Diffuso su larga scala. Facile da distribuire e da aggiornare. Gli utenti hanno la possibilità di personalizzarlo. Le protezioni antivirus possono essere configurate su dispositivi o a livello di organismo o impresa.	Il fabbisogno di memoria e i ritardi nello scambio di dati dovuto alla scansione eseguita dal *software* antivirus possono avere un impatto negativo sui sistemi ICS. Il più delle volte gli organismi o le imprese possono proteggere vecchi elementi degli ICS solo con prodotti provenienti dal mercato secondario. Inoltre, le soluzioni antivirus richiedono spesso in un ambiente ICS di escludere alcune cartelle dall'analisi del sistema per evitare la messa in quarantena di file strategici.

Tabella 5: Differenze tra TIC e ICS

I seguenti elementi devono essere considerati in sede di attuazione di un piano di difesa in profondità per un sistema SCI/SCADA:

- i costi per garantire la sicurezza di vecchi sistemi rispetto a nuove esigenze;
- la crescente tendenza a collegare ICS a reti interne all'impresa;
- la possibilità di consentire accessi a distanza agli utenti degli ambienti TIC e ICS;
- la necessità di dover fare affidamento sulla propria catena di fornitura *(supply chain)*;
- le soluzioni moderne di sorveglianza e protezione dei protocolli specifici degli ICS;
- la possibilità di mantenere sempre aggiornate le conoscenze specialistiche in merito alle nuove minacce nei confronti degli ICS.

La strategia della difesa in profondità rende più difficili gli attacchi diretti ai sistemi TIC e aumenta la probabilità di individuare in tempo utile un comportamento sospetto o inconsueto all'interno del sistema. Consente inoltre di costituire zone separate in cui implementare tecnologie in grado di identificare eventuali intrusioni nel sistema *(intrusion detection technology)*. Gli elementi tipici di questa strategia sono riportati nella tabella.

Alcuni dei principali elementi di questa strategia sono riportati nella tabella 6: Elemento di una strategia di difesa in profondità:

Elemento di una strategia di difesa in profondità	
Programma di gestione dei rischi	• Individuazione di rischi per la sicurezza • Profilo del rischio • Gestione accurata della disponibilità degli asset TIC
Architettura della cybersicurezza	• Standard/Raccomandazioni • Direttive • Metodologia
Sicurezza fisica	• Protezione di terminali • Controllo degli accessi al centro di controllo • Videosorveglianza, controllo degli accessi e barriere
Architettura di rete	• Tipiche zone di sicurezza • «Zone demilitarizzate» (DMZ) • Reti locali (LAN) virtuali
Sicurezza del perimetro di rete	• *Firewall* • Accesso remoto e autentificazione • *Jump server/Host*
Sicurezza degli host	• Gestione delle patch e delle vulnerabilità • Terminali • Apparecchi virtuali
Sorveglianza della sicurezza	• Sistemi di rilevamento delle intrusioni (*intrusion detection system,* IDS) • Registrazione degli audit di sicurezza • Sorveglianza degli eventi e degli incidenti di sicurezza
Gestione dei fornitori (Vendor *management*)	• Gestione e sorveglianza delle catene di fornitura • Servizi gestiti ed esternalizzazione *(managed services & outsourcing)* • Utilizzo di servizi *cloud*
Il fattore umano	• Direttive • Metodologia • Formazione e sensibilizzazione

Tabella 6: Elemento di una strategia di difesa in profondità

3.2 Organizzazione, strategia e governance

La definizione, il mantenimento e il monitoraggio di una strategia complessiva della sicurezza delle informazioni consente alla direzione di un'impresa di adottare direttive chiare sia nell'applicazione delle prescrizioni che nella gestione dei rischi.

3.2.1 Governance della sicurezza TIC

La governance della sicurezza è alla base di un'attuazione efficace e duratura della difesa in profondità. Vengono così creati i presupposti affinché sia possibile riconoscere, valutare e affrontare le minacce che incombono sulla strumentazione di controllo dei processi. La governance fornisce una struttura sovraordinata che contribuisce, sul piano strategico, funzionale e operativo, a realizzare gli obiettivi dell'impresa in materia di sicurezza informatica. Il modello di governance descrive

- cosa va fatto;
- come va fatto;
- chi è responsabile;
- come viene valutato.

La governance definisce le regole, i processi, i parametri e le strutture organizzative che servono a una pianificazione e a una gestione efficaci per realizzare le esigenze e gli obiettivi operativi dell'impresa. Questi elementi devono essere contenuti in un documento strategico che, una volta validato dalla direzione, potrà essere divulgato in seno all'azienda. Inoltre, la responsabilità della sicurezza delle informazioni dovrà essere affidata a un membro della direzione, il quale garantirà il necessario supporto da parte del management nell'elaborazione e nell'attuazione della difesa in profondità. La direzione dovrà essere regolarmente informata dall'organo incaricato della sicurezza in merito al grado di maturità raggiunto, agli incidenti verificatisi e agli indicatori chiave di prestazione (*key performance indicators,* KPI) legati alla sicurezza.

In questo ambito è determinante avere il sostegno incondizionato del management e discutere gli oneri, i processi e le risorse necessarie a un'attuazione efficace.

3.2.2 Organizzazione e responsabilità

L'esistenza, all'interno dell'impresa, di un organo incaricato della sicurezza cui sono stati affidati compiti, responsabilità e competenze chiaramente definiti è fondamentale ai fini della governance della sicurezza. Tale organo è chiamato a concepire, attuare e sviluppare la strategia della difesa in profondità. In questo ambito la gestione attiva dei rischi svolge un ruolo fondamentale nell'identificare le possibili minacce alla sicurezza informatica e nell'attuare le misure per farvi fronte. L'organo preposto alla sicurezza deve vedersi riconosciute le necessarie competenze dalla direzione e disporre delle risorse che gli servono per adempiere tutti i propri compiti in modo efficiente. È importante che sia ben integrato e accettato in seno all'impresa. I ruoli e le funzioni all'interno dell'organo preposto alla sicurezza devono essere descritti e documentati con una chiara definizione delle competenze. Occorre inoltre stabilire le interfacce con altri organi interni rilevanti per la sicurezza, chiarendo le competenze in caso di eventuali sovrapposizioni di compiti.

Se le competenze gli sono state conferite dalla direzione, l'organo preposto alla sicurezza può adempiere senza restrizioni i suoi compiti fondamentali in stretta collaborazione con gli altri settori dell'impresa. In particolare deve provvedere affinché:

- sia garantita la direzione specialistica della sicurezza delle informazioni legata alle TIC e agli ICS e le priorità delle attività siano adeguate alla situazione;
- tutti i documenti, le istruzioni e le direttive in materia di sicurezza vengano redatti, se necessario aggiornati e sistematicamente applicati;
- siano identificate, analizzate e, se necessario, trattate nuove tematiche rilevanti ai fini della sicurezza;
- siano messi a disposizione il know-how e le risorse necessarie lungo l'intero processo di gestione della sicurezza;
- verifiche, audit e test di intrusione siano effettuati periodicamente;
- il resoconto all'attenzione della direzione sia corretto dal punto di vista dei contenuti e avvenga sistematicamente nel rispetto dei termini e dei livelli gerarchici;
- il processo di sicurezza sia metodologicamente integrato nel processo di gestione dei rischi di cui devono essere osservate le esigenze.

3.2.3 Istruzioni e direttive

Così come in altri ambiti, anche in quello della sicurezza delle informazioni l'impresa deve stabilire un orientamento strategico. Dove vuole trovarsi fra 3–5 anni? Qual è la sua propensione al rischio? Quali sono le risorse e i mezzi finanziari che intende investire?

Le risposte a queste domande strategiche devono inserirsi nel quadro di una politica della sicurezza che coinvolga tutta l'impresa. La politica della sicurezza deve essere definita dalla direzione e approvata dal consiglio di amministrazione. Generalmente la sua elaborazione spetta all'organo preposto alla sicurezza su incarico della direzione. Tale politica deve definire i seguenti contenuti strategici, che diventano punto di riferimento per qualsiasi attività e prescrizione in materia di sicurezza dell'informazione:

- scopo e campo di applicazione della politica della sicurezza;
- obiettivi in materia di sicurezza;
- principi in materia di sicurezza;
- propensione al rischio;
- collaborazione con gli attori del settore e le autorità;
- applicazione degli standard di sicurezza;
- considerazione degli aspetti economici;
- cultura della sicurezza;
- deroghe alle prescrizioni in materia di sicurezza;
- sicurezza nei progetti;
- ruoli e funzioni dell'organo preposto alla sicurezza.

Oltre alla politica della sicurezza, che regolamenta la sicurezza delle informazioni, possono essere necessari altri documenti con carattere di istruzione in funzione delle dimensioni e della struttura dell'impresa.

È importante creare un insieme di regole che definisca come applicare le istruzioni e le direttive all'interno dell'impresa (responsabile del processo, validazione, comunicazione e formazione, verifica periodica della necessità di aggiornamenti) e quali istruzioni o direttive siano valide o debbano essere appositamente definite anche per i partner e i fornitori esterni.

3.3 Rischio e gestione della continuità operativa

3.3.1 Approntare, valutare e gestire l'inventario degli asset

Per valutare i rischi, occorre prima di tutto determinare quali sono gli asset da proteggere nell'impresa e farne un inventario. Solo così è possibile garantire che l'analisi delle minacce sia corretta e completa.

A tal fine è necessario creare un registro centralizzato degli asset che consente di rappresentare l'intero ciclo di vita di un asset. Oltre alle informazioni necessarie a garantire la piena funzionalità degli asset, il registro deve contenere anche una loro valutazione dal punto di vista dei requisiti in materia di sicurezza che sono: confidenzialità, disponibilità e integrità. Ogni asset deve avere un responsabile cui compete l'attuazione del processo del ciclo di vita.

3.3.2 Programma di gestione dei rischi

L'attuazione di una strategia di difesa in profondità implica la comprensione dei rischi operativi cui un'impresa è esposta in relazione con le minacce informatiche. Tali rischi devono essere gestiti sintonizzandosi sulla propensione al rischio dell'impresa. I responsabili dell'esercizio e della manutenzione dei sistemi TIC devono saper riconoscere i cyberrischi, valutarli e affrontarli. A tal fine occorre avere un quadro chiaro degli scenari di minacce, dei processi tecnici e operativi e delle tecnologie utilizzate. Solo così è possibile integrare nella normale attività quotidiana una strategia di difesa in profondità. È compito della direzione stabilire che la «sicurezza» è un requisito imprescindibile di tutte le attività informatizzate.

Le considerazioni suesposte hanno una validità generale. Varie applicazioni TIC, tuttavia, rivestono un'importanza particolare legata alla loro criticità. Fra queste si annoverano soprattutto i sistemi di controllo industriali (*industrial control systems,* ICS). Un'architettura di sicurezza degli ICS efficace presuppone che i rischi di un organismo o di un'impresa siano posti in relazione con i requisiti funzionali (operativi) dell'ICS. Tale approccio può riguardare anche il contesto fisico (p.es protezione del perimetro situato intorno ai centri di calcolo). I responsabili delle decisioni a qualsiasi livello di un organismo o di un'impresa devono conoscere l'importanza dei cyberrischi e partecipare attivamente al processo di gestione dei rischi. È indispensabile svolgere analisi regolari di selezionati sistemi, applicazioni e processi, incluse le relative reti. Invitiamo pertanto a effettuarle sulla base di severe direttive utilizzando un approccio strutturato e sistematico.

3.3.3 Quadro di riferimento per la gestione dei rischi

Le analisi dei rischi TIC vanno inserite in un quadro di riferimento per la gestione dei rischi ed effettuate regolarmente (di norma ogni anno) per oggetti di indagine chiaramente definiti che possono essere, per esempio, impianti, processi e applicazioni sensibili (anche in fase di sviluppo) e le loro dipendenze da altri sistemi, reti e servizi.

L'obiettivo è attribuire la gestione dei rischi individuati alle persone o ai ruoli responsabili, con l'incarico di monitorarli, valutarli e attuare opportune misure per mantenerli entro limiti accettabili precedentemente definiti secondo la propensione al rischio.

3.3.4 Analisi dei rischi e delle minacce

Nella gestione dei rischi, l'analisi dei rischi di un'impresa riguarda i rischi determinati al momento dell'identificazione dei rischi. Fornisce indicazioni qualitative e quantitative delle perturbazioni e delle minacce che si presentano, ponendo l'accento sui costi e sulle conseguenze per un'impresa di trasporti. L'analisi delle minacce fa parte dell'analisi dei rischi. Mentre quest'ultima considera i rischi inerenti a un sistema TIC o a un sistema di tecnologia operativa, l'analisi delle minacce affronta concretamente le singole minacce. Da quelle identificate e dalla valutazione della situazione di pericolo sono estrapolati i diversi rischi oggetto della gestione dei rischi.

Nel settore dei trasporti pubblici, eventuali cyberincidenti potrebbero causare i seguenti scenari di minaccia:

- estorsione di denaro;
- utilizzo della capacità di calcolo (*cryptomining, botnet, backdoor* per sferrare ulteriori attacchi);
- utilizzo (fortuito o intenzionale) dell'impresa come bersaglio per testare un attacco;
- manipolazione o furto di dati relativi a clienti o processi;
- sabotaggio (perturbazione o interruzione dei collegamenti);
- spionaggio (conoscenza dei processi, dati personali, dati di mercato);
- furto mediante l'emissione o il dirottamento di bonifici.

Il campo di indagine dell'analisi dei rischi deve essere chiaramente definito, descrivendo con la massima precisione i processi operativi coinvolti, i relativi sistemi TIC e TO e i possibili fattori esterni.

3.3.5 Gestione della continuità operativa

La «gestione della continuità operativa» (in inglese: *Business Continuity Management,* BCM), ossia la gestione delle situazioni di emergenza, è un processo volto a individuare tempestivamente i rischi in grado di mettere a repentaglio l'esistenza di un'impresa o di un organismo e ad adottare misure per evitarli. Per assicurare l'operatività e, quindi, la sopravvivenza di un'impresa o di un organismo, devono essere adottate adeguate misure preventive che, da un lato, aumentino la solidità e l'affidabilità dei processi operativi e, dall'altro, consentano reazioni rapide e mirate in caso di emergenza o di crisi.

La gestione della continuità operativa comprende la pianificazione e l'organizzazione delle procedure da seguire per aumentare in modo duraturo la resilienza dei processi operativi critici (eventualmente a carattere urgente), reagire adeguatamente agli eventi avversi e riprendere le attività al più presto possibile.

L'obiettivo è garantire che, anche in situazioni critiche, importanti processi operativi non subiscano interruzioni o le subiscano solo temporaneamente e che la sopravvivenza economica dell'impresa o dell'organismo sia assicurata anche in caso di un evento avverso di vasta portata.

Pertanto è essenziale avere una visione d'insieme, considerando tutti gli aspetti necessari al proseguimento dei processi operativi critici in caso di evento avverso, non solo la risorsa dell'informatica. La gestione della continuità operativa delle TIC fa dunque parte della gestione delle emergenze (p.es ISO 22301 o standard BSI 100-4).

La Business Continuity comprende strategie, piani, misure e processi per ridurre al minimo i danni causati dall'interruzione delle attività in un'azienda o organizzazione. Il suo scopo è sia quello di garantire le attività in condizioni di crisi, sia quello di consentire il riavvio rapido e senza problemi dei processi dopo un guasto. L'obiettivo generale è quello di garantire la continuità dell'azienda e della sua attività economica.

È indispensabile una chiara delimitazione metodologica tra gestione dei rischi, delle crisi e della continuità, che costituisce la base di un'efficace organizzazione di crisi. In tal modo è possibile definire chiaramente le responsabilità e scaglionare correttamente nel tempo i piani delle misure (piani di emergenza, continuità, ripristino).

La norma ISO 22301 definisce la BCM come un processo che identifica le potenziali minacce per un organismo, fornisce un quadro di riferimento per costruire la resilienza operativa e garantisce una reazione adeguata a tutelare i principali portatori di interessi, la reputazione, il marchio e le catene di creazione del valore.

In sostanza è il «piano B» cui un'impresa ricorre per mantenere la capacità operativa quando si verifica un evento che ha un impatto sull'attività (*business impact,* p.es incidente, sabotaggio) e l'impresa non è più in grado di offrire o riprendere la fornitura dei suoi prodotti o servizi.

3.3.6 Analisi dell'impatto sull'attività operativa *(business impact)*

L'analisi dell'impatto sull'attività operativa si prefigge di rilevare gli effetti potenzialmente realistici e quelli potenzialmente peggiori (sull'attività operativa) di un elemento TIC compromesso (incl. persone, dati, processi, servizi, reti) per varie categorie (p.es. in termini finanziari, operativi, giuridici, di reputazione e di salute).

In ultima istanza serve a stabilire quali effetti sulla sua attività l'impresa è disposta a tollerare se le necessarie risorse TIC non sono disponibili come previsto. Vanno pertanto definiti requisiti e livelli di protezione necessari a garantire disponibilità, integrità e confidenzialità delle risorse TIC in funzione del rischio che si intende assumere.

L'analisi dell'impatto sull'attività operativa è un processo di analisi delle attività e degli effetti che le perturbazioni possono avere su di esse.

Il suo obiettivo centrale è comprendere quali processi operativi sono essenziali per proseguire l'attività operativa e quindi importanti per l'impresa o l'organismo e quali siano le conseguenze di una perturbazione. Questi processi operativi «critici» sono oggetto di particolari misure di protezione nell'ambito della gestione della continuità operativa e sono prese misure preventive per le situazioni di crisi.

Nell'ambito della BCM «critico» significa «a carattere urgente», in altri termini l'attività deve essere ripristinata molto rapidamente per evitare che l'impresa o l'organismo rischi di subire un danno notevole, tra cui perdite finanziarie, violazioni di leggi o contratti, danni di immagine o altri scenari avversi. Il fatto che un processo operativo sia classificato come «non critico» dall'analisi dell'impatto non significa che sia di secondaria importanza, ma soltanto che il suo ripristino è meno urgente (norma BSI 100-4/ capitolo 5.1).

Per svolgere un'analisi dell'impatto sull'attività operativa esistono diversi metodi e approcci. Uno di essi è stilare una panoramica dei dati di base e dei processi operativi:

- differenziare le unità organizzative e i processi operativi da includere (limitarsi ai processi operativi rilevanti per la gestione della continuità operativa);
- svolgere un'analisi dei danni (definire una griglia per le categorie di danni e i relativi scenari, stabilire periodi di valutazione e la strategia per trattare particolari disponibilità, valutare i danni che potrebbero verificarsi in caso di perturbazione per ogni singolo processo e ogni periodo di valutazione);
- stabilire i parametri di riavvio (fissare la durata massima tollerabile della perturbazione, i tempi e il livello di riavvio per ogni processo operativo);
- considerare le dipendenze (considerare i parametri di riavvio in funzione delle dipendenze dei processi e degli obiettivi strategici dell'impresa, apportare eventuali correzioni);
- stabilire le priorità e le criticità dei processi operativi (fissare l'ordine di priorità dei processi operativi per il riavvio, definire e delimitare le categorie di criticità);
- identificare le risorse necessarie per l'esercizio normale e di emergenza (identificare le risorse e la capacità necessarie per l'esercizio normale e l'esercizio di emergenza);
- determinare le criticità e i tempi di riavvio (per i processi critici determinare i tempi di riavvio e di ripristino e la criticità delle risorse utilizzate).

La norma BSI 100-4 tratta esaustivamente la gestione della continuità operativa sotto forma di linea guida.

3.3.7 Misure di gestione della continuità operativa

Le misure relative ai rischi descritti nell'analisi dell'impatto sull'attività operativa devono essere determinate, verificate e quindi validate da parte della direzione contestualmente ai piani che indicano l'esatta procedura da seguire.

In proposito occorre provvedere affinché il rischio residuo sia identificato per ogni asset nel suo contesto e gestito in modo adeguato (p.es attenuato, evitato, dislocato o accettato) in funzione della propensione al rischio.

Per ogni singolo asset deve essere così stabilito il rischio massimo tollerabile per calcolare i rischi (cumulati) legati alle TIC.

3.4 Architetture

3.4.1 Architettura della cybersicurezza

L'architettura della cybersicurezza include le misure specifiche e il loro collocamento strategico all'interno della rete per creare un sistema di sicurezza stratificato come quello previsto dalla strategia di difesa in profondità. Il suo obiettivo, inoltre, è consentire di acquisire informazioni sul flusso di dati fra i sistemi e sulle loro connessioni. L'architettura della cybersicurezza deve essere conformata all'inventario fisico degli impianti e degli asset TIC per assicurare una comprensione globale dei flussi di informazioni all'interno dell'organismo o dell'impresa.

Inoltre deve essere in sintonia con il *Cybersecurity Framework Core* del NIST. L'architettura della cybersicurezza tiene conto della protezione della confidenzialità, dell'integrità e della disponibilità di dati, servizi e sistemi. Per realizzarla occorre mettere a punto un piano di implementazione che sia in linea con la cultura dell'impresa e gli obiettivi strategici, ma nel contempo tenga adeguatamente conto delle esigenze di sicurezza ed evidenzi le risorse necessarie. In genere l'architettura della cybersicurezza viene completata da un piano integrato dei compiti che identifica i risultati attesi (indicazioni e spunti per un ulteriore esame e un riorientamento), definisce le tempistiche dei progetti, fornisce stime sulle risorse necessarie e delinea i principali rapporti di dipendenza dei progetti.

3.4.2 Architettura del sistema

Gli ICS devono essere monitorati e controllati in funzione dell'esigenza di proteggerli. Devono beneficiare di una particolare protezione tecnica e fisica soprattutto per garantire i processi rilevanti ai fini dell'approvvigionamento.

Un'architettura di rete sicura e robusta costituisce uno dei pilastri portanti di una protezione efficace da eventuali attacchi. Ogni interfaccia, ogni passaggio e ogni connessione rappresenta un potenziale pericolo, pertanto è indispensabile che tutte le operazioni all'interno delle reti e degli impianti siano conosciute e trattate di conseguenza. Il presupposto è costituito dal corretto raggruppamento e dalla segmentazione dell'architettura di rete.

È importante che la rete sia suddivisa in zone di sicurezza, così come che l'architettura non sia limitata alle infrastrutture fisse (impianti fissi) o mobili (sistemi di veicoli) né che sia osservata isolatamente. È necessario garantire che sia considerata l'intera architettura integrando tutti i suoi elementi, poiché in un'architettura globale è l'anello più debole a rivelare il livello di sicurezza raggiunto.

I gestori di infrastrutture critiche devono dunque imperativamente eseguire analisi dei rischi dell'intera architettura del sistema per dedurne il livello di sicurezza e la maturità da raggiungere.

La figura seguente fornisce un esempio di rappresentazione schematica per un'impresa ferroviaria. Mostra quali componenti (TIC o ICS) e canali di comunicazione sono necessari per la sicurezza dell'esercizio[4].

[4] La raffigurata architettura di rete ICS è un esempio che deve essere adattato alle esigenze dell'impresa.

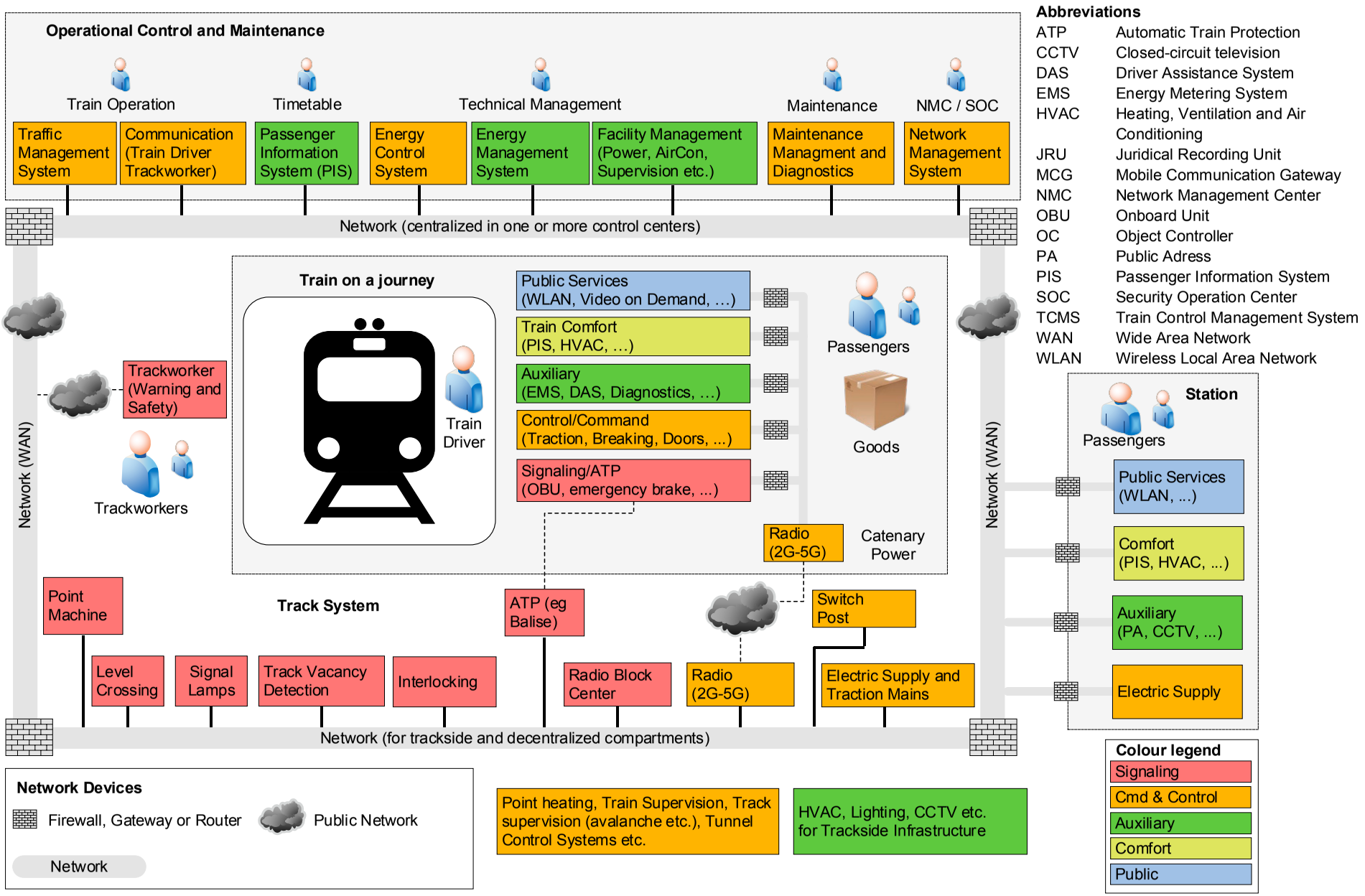


Figura 5: Esempio di un'architettura del sistema (estratto da CENELEC prTS 50701 – D7E6)

3.5 Misure tecniche di sicurezza

3.5.1 Sistemi di controllo industriali

A causa dell'architettura complessa degli ICS o dei sistemi SCADA[5], alcune vulnerabilità possono, nel peggiore dei casi, rimanere inosservate per parecchio tempo e gli *exploit,* ossia i *software* che le sfruttano, rischiano di diventare una minaccia. L'applicazione della summenzionata strategia della difesa in profondità offre una protezione adeguata contro queste minacce.

Di seguito sono riportati alcuni tipici metodi di attacco agli ICS:

- attacchi da Internet che prendono di mira ICS accessibili online con lo scopo di instaurare un accesso remoto duraturo;
- attacchi remoti agli ICS mediante dati di accesso rubati;
- attacchi a sistemi SCADA compiuti sfruttando le falle dell'interfaccia web;
- infezione da malware nell'ICS tramite supporti dati compromessi (p.es chiavette USB, *smartphone* ecc.);
- attacchi alla struttura informatica degli uffici (p.es tramite *e-mail* di *phishing*, infezioni *drive-by* ecc.), con lo scopo di accedere all'ICS attraverso eventuali interfacce.

3.5.2 Sicurezza degli *host*

A livello di *host* e di postazioni di lavoro deve essere aggiunto un ulteriore strato di sicurezza. La maggior parte dei dispositivi è protetta dalle intrusioni esterne mediante i *firewall.* Un modello di sicurezza valido richiede tuttavia diversi livelli di difesa. Per mettere al sicuro l'intera rete occorre proteggere anche tutti gli *host.* Lo strato destinato alla sicurezza degli *host* deve consentire all'utente di utilizzare vari sistemi operativi e applicazioni garantendo nel contempo una protezione adeguata dei dispositivi.

È necessario creare un piano con le regole da applicare alle *password* per tutti gli utenti di un sistema e rinominare gli account noti (p.es amministratore). Gli utenti possono tuttavia eludere rigide direttive conservando le *password* in un luogo non sicuro (p.es. su fogli per appunti) o continuare a utilizzarne di simili. La complessità delle disposizioni sulle *password* deve essere in linea con il livello di autorizzazione degli utenti. Eventualmente possono essere definiti cicli di modifica delle *password.*

Le seguenti raccomandazioni di carattere generale vanno attuate da parte di organismi o imprese per ogni host ICS e ogni dispositivo che abbia accesso alla rete interna (indipendentemente dal sistema operativo):

- installare e configurare un *firewall* specifico per gli *host;*
- impostare per quanto possibile salvaschermo da sbloccare con la richiesta della *password* a intervalli ravvicinati;
- applicare le *patch* ai sistemi operativi e tenere aggiornati i *firmware;*
- attivare la configurazione dei log su tutti i dispositivi;
- disattivare i servizi e gli account che non sono utilizzati;
- sostituire servizi non sicuri come Telnet, *Remote Shell* o FTP con alternative sicure come sTelnet, SSH, sFTP;
- fare in modo che gli utenti non siano in grado di disattivare i servizi;
- eseguire e verificare i *backup* dei sistemi, in particolare se questi ultimi non sono gestiti centralmente;
- attivare i moduli di sicurezza messi a disposizione dai sistemi operativi, come la scansione di protezione, oppure sostituirli con *software* adeguati;
- applicare le stesse direttive anche ai *laptop* e agli altri dispositivi mobili non costantemente collegati con la rete dell'impresa; codificare l'hardisk di tutti i terminali mobili.

3.5.3 Perimetro di sicurezza della rete

Una volta che ha sviluppato e implementato un'architettura di rete robusta, l'impresa deve attuare anche l'architettura di sicurezza per la rete e i sistemi. L'architettura di sicurezza comprende i controlli specifici e il posizionamento strategico di rilevatori e di test all'interno della rete o dei sistemi per instaurare i diversi strati della difesa in profondità. I diagrammi di rete, le matrici di connessione e i diagrammi di flusso delle informazioni, che abbinano tutti i sistemi e i loro collegamenti all'inventario fisico, sono indispensabili per avere una buona comprensione dei flussi di informazioni e delle connessioni necessarie all'interno della rete. Creando aree, zone e settori e sovrapponendo gli strati di sicurezza per ogni sistema o sottosistema che è stato inventariato è possibile determinare quali elementi di gestione e di sorveglianza sono stati realizzati per proteggere il sistema senza limitare la *performance.*

[5] Nel presente documento le espressioni «tecnologia operativa» (TO), «sistema di controllo industriale» (ICS) e «Supervisory Control and Data Acquisition» (SCADA) sono utilizzate come sinonimo.

I responsabili dei sistemi devono eseguire i controlli di sicurezza nella rete, nel sistema, nelle applicazioni e negli strati fisici per garantire la sicurezza delle informazioni. Tra questi compiti rientrano la gestione delle direttive e della sicurezza, la sicurezza delle applicazioni, dei dati, delle piattaforme, della rete e del perimetro nonché la sicurezza fisica e quella degli utenti. L'architettura di sicurezza riunisce tutti i meccanismi e i controlli di difesa che si sovrappongono all'architettura di rete. Definisce dove le misure di difesa in profondità debbano essere applicate. Lo standard NIST 800-82 «*Guide to Industrial Control Systems (ICS) Security*» propone un controllo di sicurezza ICS per tutta l'impresa che si sovrappone agli strati di sicurezza esistenti sulla base dello standard NIST 800-53 «*Security and Privacy Controls for Federal Information Systems and Organizations*».

I costi di un'installazione ICS e il mantenimento di un'infrastruttura di rete omogenea rendono spesso necessario collegare la rete ICS a quella dell'impresa. Questa connessione rappresenta un notevole rischio per la sicurezza e deve pertanto essere tecnicamente protetta. Se le reti vanno collegate, si raccomanda vivamente di autorizzare solo connessioni minime (se possibile uniche) e di ricorrere a un *firewall* e una zona demilitarizzata (DMZ), ossia un segmento di rete isolato. I *server* ICS che contengono dati della rete dell'impresa vanno collocati in una DMZ. Le connessioni esterne devono essere note e limitarsi a un accesso minimo mediante un *firewall.* Lo scambio di dati può essere monitorato e plausibilizzato anche mediante sistemi in grado di individuare anomalie.

3.5.4 Configurazione di dispositivi mobili

Per proteggere i dati da accessi non autorizzati, perdita e furto, i dispositivi mobili (inclusi *laptop, tablet* e *smartphone*) devono disporre sempre di una configurazione standard conforme ai requisiti di sicurezza.

Obiettivo della configurazione standard è garantire la sicurezza dei dati memorizzati o trasferiti sui dispositivi mobili anche in caso di perdita o furto.

3.5.5 Sicurezza fisica

Le misure di sicurezza fisica riducono il rischio di perdite o danni accidentali o intenzionali agli asset TIC dell'organismo o dell'impresa e del suo ambiente. Tra gli asset che vanno protetti rientrano beni patrimoniali fisici come gli strumenti e gli impianti, l'ambiente, il contesto allargato e la proprietà intellettuale, compresi i dati proprietari come le impostazioni dei processi e le informazioni relative ai clienti. I controlli fisici di sicurezza devono adempiere spesso requisiti specifici in materia di ambiente, sicurezza, regolamentazione, diritto e altro. Gli organismi o le imprese devono adattare questi controlli, così come quelli tecnici, alle esigenze di protezione. Per garantire un'ampia protezione si include anche quella delle componenti TIC *(= security*) e dei dati d'ambiente che sono connessi alle TIC. La sicurezza di numerose infrastrutture TIC è strettamente legata alla sicurezza degli impianti *(= safety*), con l'intento di tenere il personale al riparo da situazioni pericolose senza ostacolarlo nel proprio lavoro o nelle procedure di emergenza. I controlli di sicurezza fisici sono costituiti da misure attive o passive, che limitano l'accesso fisico a tutte le componenti dell'infrastruttura TIC. Queste misure di protezione devono impedire fra l'altro:

- l'accesso fisico non autorizzato a luoghi sensibili;
- l'alterazione, la manipolazione, il furto o qualsivoglia asportazione o distruzione di sistemi, infrastrutture, interfacce di comunicazione o ubicazioni;
- la sorveglianza non autorizzata di impianti sensibili tramite l'osservazione visiva, fotografie o qualsiasi altro tipo di registrazione;
- l'introduzione o l'installazione non autorizzata di nuovi sistemi, infrastrutture, interfacce di comunicazione o altro *hardware;*
- l'introduzione non autorizzata di dispositivi (chiavette USB, *wireless access point,* dispositivi bluetooth o mobili) destinati a effettuare manipolazioni su *hardware,* intercettare comunicazioni o avere altri effetti dannosi.

Per soddisfare i requisiti di sicurezza delle informazioni, gli *asset* fisici, inclusi i sistemi e la dotazione di rete, le apparecchiature per uffici (p.es. stampanti in rete e dispositivi multifunzionali) e gli impianti speciali (p.es. sistemi di controllo industriali) devono essere protetti lungo l'intero ciclo di vita, dall'acquisto (o *leasing*) alla manutenzione sino allo smaltimento.

Anche i dispositivi mobili (inclusi *laptop, tablet* e *smartphone*) e i loro dati devono essere protetti da accessi non autorizzati, smarrimento e furto configurando le impostazioni di sicurezza, limitando l'accesso, installando *software* di sicurezza e gestendo i dispositivi in modo centralizzato.

3.6 Gestione dei fornitori, modelli operativi e monitoraggio

3.6.1 Gestione dei fornitori

La gestione dei fornitori consiste nell'identificare e amministrare i rischi legati alle informazioni fornite a operatori esterni (fornitori di *hardware* e *software*, operatori di servizi in *outsourcing* e di servizi *cloud* ecc.). Il disciplinamento in contratto formali di requisiti relativi alla sicurezza delle informazioni consente di ridurre i rischi al minimo.

3.6.2 *Outsourcing,* servizi gestiti

Numerose organizzazioni utilizzano i servizi gestiti e *l'outsourcing* per le funzioni che richiedono tecnologie o abilità altamente specialistiche. Non è insolito che gli organismi e le imprese esternalizzino numerose funzioni legate alla sicurezza informatica (risposta agli incidenti *[incident response]*, analisi tecnica degli incidenti *[forensics]*, valutazioni della vulnerabilità informatica, gestione dei rischi, gestione della catena dell'approvvigionamento e della distribuzione *[supply chain management]*) o altre funzioni che utilizzano raramente o che richiedono un *know-how* specifico solo sporadicamente. L'*outsourcing* ha il vantaggio di implicare un minore impiego di capitali e di essere meno oneroso. Un esperto forense digitale a tempo pieno, per esempio, è molto costoso a causa del notevole *know-how* richiesto, ma è imprescindibile per un'impresa quando deve indagare sugli incidenti verificatisi.

Un *Service Level Agreement* (SLA) è un documento che precisa il livello di servizio convenuto tra un fornitore e l'impresa che esternalizza. Se il fornitore di servizi non soddisfa le aspettative formalizzate nello SLA, il beneficiario della prestazione si riserva il diritto di disdire il contratto. Nel caso in cui i servizi di sicurezza siano affidati a un'entità esterna, è importante che le due parti convengano i ruoli, le responsabilità, la gestione e il *reporting* degli incidenti e la sicurezza delle interfacce, tra cui le direttive e le procedure per l'accesso remoto che un utente può esigere. In aggiunta al *Service Level Agreement*, le imprese dovrebbero definire un memorandum d'intesa/protocollo di accordo (*Memorandum of Understanding/Agreement,* MOU/MOA) e un accordo per la sicurezza di sistemi informatici interconnessi (*Interconnection Security Agreement*) per descrivere le specifiche esigenze di gestione e le esigenze tecniche relative alle prestazioni di servizio.

Quando le valutazioni tecniche sono verificate o controllate da un'entità esterna, tutte le parti coinvolte dovrebbero stabilire e convenire le regole della collaborazione. Le valutazioni della vulnerabilità informatica, per esempio, necessitano solitamente di un certo numero di scansioni passive o attive o test sui sistemi coinvolti, pertanto gli addetti alle valutazioni devono disporre di un accesso personale ai sistemi oppure osservare gli accessi agli asset critici eseguiti da altri all'interno dell'ambiente del sistema di controllo. Il team preposto alla valutazione collabora con il suo omologo all'interno dell'organismo o dell'impresa al fine di garantire che le attività di test non interferiscano con l'attività per gli utenti e siano concordate misure di monitoraggio dei protocolli qualora le attività causassero problemi di qualsiasi tipo all'impresa. Le regole d'ingaggio (*rules of engagement,* RoE) stabiliscono le attività da eseguire sui vari sistemi e le persone abilitate a farlo. Comprendono le decisioni che determinano se i test sono effettuati sul sistema di gestione primario (sistema di produzione attivo) o su un sostituto affidabile, per esempio un sistema di *backup* o di controllo secondario, una rete di test o un sistema autonomo. È opportuno evitare le scansioni attive dei sistemi di produzione poiché possono causare perturbazioni dell'esercizio oppure generare una situazione di negazione del servizio *(denial of service)*. Possono invece rivelarsi opportune le attività passive, tra cui il *network sniffing* (ascolto in rete per raccogliere dati). L'eventuale sistema sostitutivo utilizzato dovrebbe essere confrontato con il sistema attivo per garantire che siano identici in termini di operatività. Il team di valutazione e l'organismo o l'impresa devono convenire la persona che avrà in mano i comandi durante il test, soprattutto se il test riguarda sistemi attivi di gestione (produzione). Il personale locale dovrebbe svolgere tutti i test che concernono i sistemi attivi di gestione.

3.6.3 Utilizzo di servizi *cloud*

Il *cloud computing* non è più una novità ed è entrato a far parte della realtà quotidiana. Si tratta di un modello che consente un accesso generalizzato, comodo e commisurato alle esigenze a un insieme di risorse informatiche configurabili (p.es reti, *server,* memorie, applicazioni e servizi) che possono essere messe rapidamente a disposizione e rilasciate con un minimo di oneri amministrativi o di interazione con il fornitore di servizi. Oltre agli aspetti economici, anche la sicurezza delle informazioni riveste un ruolo centrale certamente anche per le imprese di trasporti pubblici. Proprio sulla scia della digitalizzazione, gli aspetti legati alla sicurezza della *cloud* non hanno solo un impatto sui sistemi TIC, ma sempre di più anche sugli ICS. Tuttavia gli scambi, i treni e gli autobus sono difficili da virtualizzare e containerizzare (ossia disaccoppiare le applicazioni e gli ambienti in cui vengono eseguite senza coinvolgere l'intero sistema operativo), quindi almeno alcuni dei rispettivi sistemi di controllo devono essere gestiti localmente nel medio o persino nel lungo termine.

Ciò comporta quasi sempre un approccio ibrido, che richiede un piano di sicurezza applicabile ai servizi *cloud* così come a quelli locali.

Il *cloud computing* non è esente da rischi. Per i trasporti pubblici i principali sono enunciati di seguito:

- interruzione della connessione *Internet* o di rete che rende impossibile accedere ai dati e alle applicazioni;
- attacchi DoS agli offerenti di servizi *cloud* destinati sicuramente ad aumentare;
- errori nell'amministrazione della *cloud*, che in considerazione dell'elevata complessità può portare a notevoli problemi di sicurezza (interruzione del servizio, perdita di dati ecc.); piccoli errori o guasti che nell'infrastruttura *cloud* possono avere notevoli ripercussioni (non solo sulla sicurezza);
- furto di identità e abuso di account;
- perdita del controllo dei dati e delle applicazioni;
- violazione delle prescrizioni e delle direttive in vigore (p.es requisiti di protezione dei dati);
- sicurezza dei terminali, con i quali sono utilizzati i servizi *cloud;*
- assenza di una strategia di *cloud computing,* quindi gli obiettivi da raggiungere con esso non sono chiari né verificabili;
- forte volontà di utilizzare il *cloud computing* a ogni costo, con la conseguenza di ipotesi fallaci e analisi «abbellite» del rapporto costi/benefici, e conseguenti perdite finanziarie;
- attuazione potenzialmente molto difficile del *cloud computing,* con il rischio di trascurare che deve essere prevista anche una soluzione per uscire dalla *cloud*; in caso contrario si crea una forte dipendenza dall'offerente di servizi *cloud* che può avere conseguenze finanziarie negative;
- ricorso frequente ai servizi del subappaltatore (p.es amministrazione o backup di dati) da parte dell'offerente di servizi *cloud*. Può quindi succedere che, per esempio, dati personali siano trasmessi a organismi non autorizzati (con il rischio di una multa) oppure che un certificato di sicurezza sia compromesso poiché un auditor non è in grado di verificare il subappaltatore;
- frequente assenza di un piano di emergenza, nella convinzione errata da parte degli utenti che la *cloud* sia sempre disponibile.

Il ricorso ai servizi di *cloud computing* implica dunque la necessità di tenere in considerazione gli aspetti approfonditi di seguito.

Definire una strategia di *cloud computing*

A prescindere dalle dimensioni di un progetto di *cloud computing,* è necessario conoscere i requisiti fondamentali e le condizioni quadro da cui ricavare indicazioni operative. Se ciò non avviene, il progetto poggerà su fondamenta poco solide. Le imprese si fidano troppo delle promesse degli offerenti e si scontrano con una dura realtà quando devono constatare di non avere ottenuto il beneficio auspicato, i risparmi previsti né la sicurezza necessaria.

Realizzare studi di fattibilità

Uno studio di fattibilità dovrebbe consentire di rispondere, tra l'altro, agli interrogativi seguenti:

- esame del quadro giuridico (p.es protezione dei dati, protezione del segreto, autorità di vigilanza e direttive emanate dall'impresa stessa o da un'autorità *(compliance)*. Quali tipi di dati è opportuno elaborare nella *cloud*? I dati possono essere trasferiti in una *cloud*? Esistono restrizioni in merito al luogo di archiviazione e di elaborazione (p.es relativamente all'accesso alle informazioni da parte di terzi, allo spionaggio)?
- L'infrastruttura informatica dell'impresa ha raggiunto il grado di maturità necessaria per utilizzare servizi *cloud*? A proposito dell'utilizzo di un'infrastruttura sotto forma di servizio (*Infrastructure as a Service,* IaaS) su vasta scala occorre porsi i seguenti interrogativi: i servizi in questione possono essere virtualizzati? È possibile standardizzarli? Nelle imprese di trasporti pubblici non è sempre così poiché è necessario gestire un numero elevato di applicazioni e di sistemi speciali.
- Definire il modello di servizio e di distribuzione (SaaS, PaaS, IaaS).

Identificare e gestire i rischi della *cloud*

Per definire i requisiti di un servizio di *cloud computing* è essenziale classificare le informazioni da elaborare in termini di confidenzialità, disponibilità e integrità (esigenza di protezione).

Se il dibattito pubblico sulla sicurezza della *cloud* è fortemente incentrato sull'aspetto della confidenzialità (intervento dei servizi delle attività informative, delle autorità di perseguimento penale ecc.), per le imprese di trasporti pubblici sono altrettanto critici gli aspetti della disponibilità e dell'integrità. Se i sistemi non sono disponibili, i veicoli non possono circolare e l'utilizzo di informazioni sbagliate può essere pericoloso per il traffico.

Nell'analisi dei rischi deve dunque essere riservata un'attenzione particolare ai seguenti pericoli:

- accesso ai dati da parte dell'offerente di servizi *cloud;*
- possibilità di accesso da parte delle autorità statali a causa della giurisdizione (ev. straniera) competente per l'offerente di servizi *cloud;*
- mancata disponibilità di dati e servizi;
- autenticazione compromessa;
- perdita di dati;
- manipolazione di dati;
- dipendenza da un solo fornitore *(vendor lock-in)*: spesso è molto oneroso e non sempre possibile sottrarsi alle maglie di un fornitore;
- perdita di know-how *(brain drain)*: con il prolungato ricorso ai servizi *cloud* un'impresa perde progressivamente le capacità tecniche che le consentono di distribuire autonomamente i propri servizi.

Da questa analisi emergono già settori nei quali si rivela necessario adottare particolari misure di sicurezza oppure che presentano rischi difficilmente controllabili. Le imprese di trasporti pubblici devono porre l'accesso sui rischi di indisponibilità di dati e servizi e di manipolazione dei dati poiché, se si concretizzassero, questi rischi potrebbero prima o poi perturbare l'esercizio. Importante: non esiste una soluzione di *cloud computing* che sia sicura in tutti i casi.

Valutazione del rapporto costi/benefici

Una volta chiariti i punti suindicati, occorre procedere a una valutazione di massima del rapporto costi/benefici che consideri almeno i seguenti aspetti:

- costo dell'utilizzo del servizio;
- onere amministrativo interno;
- formazione dei collaboratori e degli amministratori;
- all'occorrenza nuova infrastruttura TIC o nuova connessione di rete;
- costi dell'adattamento dei processi;
- costi della migrazione;
- risparmi interni.

Questa valutazione fornisce una prima indicazione della redditività di un servizio *cloud*. Dopo averli raccolti in un documento, i risultati devono essere presentati ai decisori che si esprimono sull'opportunità di proseguire il progetto.

Definire le esigenze di sicurezza

Se sulla base dello studio di fattibilità, dell'analisi dei rischi e della valutazione del rapporto costi/benefici è stato deciso di utilizzare un servizio *cloud*, si passa alle tappe concrete di realizzazione del progetto.

Oltre ai requisiti funzionali, devono essere definite le esigenze in materia di sicurezza delle informazioni e disponibilità del servizio *cloud* che non riguardano solo i fornitori del servizio *cloud*, ma anche l'impresa stessa. È importante che le esigenze di sicurezza non siano influenzate dalla decisione di hosting né che siano adattate in modo da rendere possibile il ricorso a un servizio *cloud*.

Se l'impresa non stabilisce le proprie esigenze di sicurezza avrà difficoltà a spiegare concretamente all'offerente del servizio *cloud* che cosa si aspetta da lui. Esigere una *cloud* «sicura» e «sempre disponibile», senza formulare esigenze concrete, è destinato a fallire: o il livello di sicurezza è insufficiente o la soluzione proposta è troppo costosa. Se le esigenze di sicurezza sono troppo elevate per una soluzione di *cloud computing,* il processo avviato deve essere fermato.

Elaborare un piano di sicurezza

La documentazione concernente la sicurezza deve essere estesa agli aspetti del *cloud computing.* È importante che le misure descritte nel piano si applichino sia ai sistemi locali sia alla *cloud*. I principali aspetti da considerare sono i seguenti:

- piani trasversali di gestione delle identità e degli accessi (*Identity and Access Management,* IAM): occorre fare in modo che le identità e i ruoli digitali dell'impresa siano gestiti per quanto possibile in maniera centralizzata e con una sola operazione. L'autenticazione può quindi avvenire in maniera decentralizzata, mediante procedure federative (OAuth2, SAML2.0. ecc.);
- sistemi di sicurezza: i sistemi di logging e di monitoraggio (p.es SIEM) devono essere configurati in modo tale da sorvegliare e correlare sia i servizi *cloud* sia quelli locali. Una falla di sicurezza nel perimetro può avere immediate ripercussioni sui servizi *cloud* e viceversa;

- modelli *zero-trust:* dal momento che nella *cloud* mancano alcuni strati del sistema di difesa rispetto all'approccio della difesa in profondità descritto nel capitolo 3 oppure essi non sono più conciliabili con quelli presenti nell'impresa (tipicamente la sicurezza del perimetro), deve essere attribuita un'importanza particolare non solo alla sorveglianza, ma anche alla protezione dell'identità, alla qualità dell'autenticazione e alla gestione degli accessi. In concreto, i sistemi e i processi devono essere configurati in modo tale da poter funzionare sicuramente anche in un ambiente non affidabile (p.es Internet). Disporre di un terminale sicuro e il più possibile rinforzato è essenziale in proposito.

Garantire la protezione dei dati e la compliance

Se nella *cloud* vengono rilevati, elaborati o utilizzati dati personali, la loro protezione deve essere assicurata conformemente alle disposizioni legali in materia.

Oltre alle esigenze in materia di protezione dei dati, gli utenti dei servizi *cloud* devono osservare le disposizioni legali enunciate *(compliance).* In tutti i casi l'elaborazione di questi dati nella *cloud* implica (generalmente) la responsabilità dell'utente, il quale è tenuto a garantire che i dati siano elaborati presso l'offerente dei servizi *cloud* conformemente alle prescrizioni e alle leggi in materia.

3.6.4 Monitoraggio di sicurezza

L'impiego di sistemi di monitoraggio e componenti di rete che riconoscono comportamenti anomali e firme d'attacco rendono ancora più complesso l'ambiente informatico o ICS. Le funzioni di monitoraggio e riconoscimento, tuttavia, sono indispensabili per la strategia di difesa in profondità destinata a proteggere gli *asset* sensibili. Per mettere al riparo gli *asset* critici da accessi non autorizzati, non è sufficiente creare un confine elettronico intorno alla rete ICS. Secondo il modello di difesa in profondità va predisposto un sistema di monitoraggio che allerti precocemente un organismo o un'impresa in caso di incidente. La maggior parte degli organismi o delle imprese dispone di una forma di monitoraggio standard nell'ambiente IT, che tuttavia spesso non utilizza nelle reti ICS.

È pertanto indispensabile:

- effettuare audit approfonditi, indipendenti e periodici delle condizioni di sicurezza (ambienti operativi critici, processi, applicazioni e sistemi/reti di supporto); e
- tenere sotto controllo i rischi legati alla sicurezza delle informazioni, rispettare gli elementi rilevanti ai fini della sicurezza previsti dalle disposizioni legali, regolatorie e contrattuali nonché presentare alla direzione un resoconto periodico sulla sicurezza delle informazioni.

3.6.5 Gestione del ciclo di vita dell'*hardware*

L'acquisto (o il *leasing*) di *hardware* resistenti e affidabili deve avvenire nel rispetto dei requisiti di sicurezza. Eventuali vulnerabilità vanno sempre individuate.

L'obiettivo è garantire che l'*hardware* offra le funzioni necessarie e non pregiudichi la sicurezza di informazioni e sistemi critici o sensibili durante l'intero ciclo di vita.

3.7 Il fattore umano

Le manipolazioni errate causate dall'essere umano sono un aspetto delicato che organismi e imprese devono gestire. Non è mai possibile escludere completamente né quelle intenzionali né quella accidentali malgrado l'adozione di misure tecniche. Le imprese sono tanto più esposte quanto più il personale è inesperto o non qualificato. Anche la lotta agli atti di collaboratori interni malintenzionati costituisce un'ulteriore sfida cui fare fronte. La necessità di confrontarsi con questi aspetti obbliga organismi o imprese a occuparsi delle tematiche esposte di seguito.

3.7.1 Ciclo occupazionale del personale

La sicurezza delle informazioni deve essere considerata parte dell'intero ciclo occupazionale, dall'assunzione sino alla conclusione del rapporto d'impiego. Include misure rilevanti ai fini della sicurezza, come quelle disposte in sede di consegna degli strumenti di lavoro (*hardware*, accesso ai sistemi) o per l'ingresso a edifici/locali e le responsabilità che ne conseguono in materia di protezione. Il relativo programma di formazione per il personale ha il duplice obiettivo di rendere più consapevoli dell'importanza della sicurezza e definire il comportamento da adottare. L'organismo o l'impresa devono documentare lo svolgimento dei corsi per assicurarsi che il personale disponga delle capacità, delle conoscenze e degli strumenti necessari a sostenere i valori veicolati e a rispettare le direttive in materia di sicurezza delle informazioni.

3.7.2 Istruzioni/Direttive

Istruzioni e direttive chiare e attuabili disciplinano il comportamento del personale negli ambiti concernenti la sicurezza. Definiscono un quadro di riferimento e consentono di effettuare controlli allo scopo di proteggere i sistemi e attuare le direttive. Inoltre stabiliscono procedure e specificano le aspettative dell'organismo o dell'impresa nei confronti dei propri collaboratori. Istruzioni e direttive definiscono le regole da rispettare e le sanzioni in caso di violazioni.

3.7.3 Processi

La gestione della sicurezza, che è strutturata in processi, è di competenza dell'unità preposta alla sicurezza informatica. La sua funzione è proteggere le informazioni e i dati dell'impresa, che è tenuta ad applicare anche ai sistemi di controllo industriali i processi di gestione della sicurezza, che includono la definizione di processi, le modalità di attuazione o la configurazione di un determinato sistema. Questi processi devono essere sempre standardizzati e ripetibili al fine di garantire un livello di formazione costante anche al nuovo personale e assicurare che tutte le prescrizioni e le norme necessarie siano note.

3.7.4 Mansioni e responsabilità in ambienti operativi critici

Le mansioni e le responsabilità nell'ambito di processi, applicazioni (inclusi sistemi/reti di supporto), informazioni e ambienti operativi critici devono essere chiaramente definite e assegnate a persone competenti, con l'obiettivo di sensibilizzare il personale alla propria responsabilità individuale. Questa cultura d'impresa contribuisce a fare in modo che ogni collaboratore svolga le proprie mansioni nel rispetto delle esigenze in materia di sicurezza delle informazioni.

3.7.5 Comunicazione/Programma di sensibilizzazione alla sicurezza informatica

Questo programma e le relative misure di comunicazione promuovono nei collaboratori un atteggiamento consapevole e il comportamento auspicato a tutti i livelli gerarchici dell'organismo o dell'impresa.

L'obiettivo è instaurare una cultura d'impresa che favorisca un appropriato comportamento individuale in materia di sicurezza e renda ciascuno capace di prendere decisioni basate sui rischi nel proprio ambito di competenza.

Prescrizioni e quadro di riferimento per la valutazione

4 Quadro di riferimento

A livello internazionale sono state definite numerose norme e fonti di informazione relative alla gestione di rischi TIC. Alcune sono già state riconosciute e vengono utilizzate nell'economia privata. Ove opportuno, possono essere completate da altri standard riconosciuti a livello internazionale.

Il presente manuale rivolto alle imprese di trasporti pubblici si basa sul quadro di riferimento internazionale *Cybersecurity Framework Core* del NIST[6]. Il Framework del NIST e le sue raccomandazioni intendono mettere a disposizione dei gestori di infrastrutture critiche e di altri organismi o imprese dipendenti dalle TIC uno strumento con il quale aumentare autonomamente e sotto la propria responsabilità la resilienza nei confronti dei rischi di sicurezza informatica. Si basa su una selezione di standard, direttive e buone pratiche esistenti e non è vincolato all'uso di una determinata tecnologia.

Il *Framework* del NIST è quindi compatibile anche con gli standard ISO 2700x e ISO/IEC 62443, la cui applicazione costituisce un obiettivo secondo le disposizioni d'esecuzione dell'ordinanza sulle ferrovie (DE-Oferr 2020). Ai fini dell'applicazione dello standard minimo TIC, i diversi standard sono precisati nel capitolo 4.

4.1 Principi

I seguenti principi sono rilevanti ai fini dell'attuazione:

1. Responsabilità propria: i gestori di infrastrutture critiche sono in linea di massima direttamente responsabili di garantire il mantenimento dei loro processi TIC/ICS.
2. Gestione dei rischi: la responsabilità di valutare regolarmente possibili rischi TIC, tra cui violazione della disponibilità, dell'integralità e della confidenzialità, spetta agli utenti del presente manuale. L'organismo o l'impresa devono giudicare quali rischi sono da ridimensionare e quali sono disposti ad assumersi.
3. Gestione della continuità operativa: tutti gli aspetti della sicurezza delle TIC e degli ICS vanno integrati in un sistema sovraordinato di gestione della continuità operativa.
4. Esaustività: il presente manuale raggruppa gli elementi essenziali ai fini dell'attuazione. L'esaustività delle misure di sicurezza da attuare dipende dall'analisi dell'impatto sull'attività operativa e dalle analisi dei rischi. In proposito occorre considerare gli ulteriori standard necessari e le istruzioni operative interne ed esterne.
5. Cultura della sicurezza: al fine di garantire una cybersicurezza duratura è necessario promuovere una cultura della sicurezza interna.

4.2 Visione d'insieme

Il *Cybersecurity Framework Core* del NIST segue un approccio basato sui rischi per affrontare e gestire i rischi di cybersicurezza. Si compone di cinque funzioni:

1. *identificare (identify)*
2. *proteggere (protect)*
3. *intercettare (detect)*
4. *reagire (respond)*
5. *ripristinare (recover)*

4.3 Livelli di implementazione

Il *Cybersecurity Framework* del NIST prevede quattro livelli di implementazione *(implementation tiers)*, che descrivono quelli (in termini di protezione) già realizzati dall'impresa. Essi vanno da nullo (*tier* 1) a dinamico (*tier* 4). Per definire il proprio livello di sicurezza (*tier level*), un organismo o un'impresa deve conoscere esattamente le proprie pratiche di gestione dei rischi, l'ambiente di minaccia, i requisiti giuridici e regolatori, gli obiettivi operativi e le esigenze organizzative.

I livelli di implementazione sono così definiti:

Tier 0: nessuna implementazione

Sebbene l'organismo/l'impresa sia consapevole della necessità di attuare la misura stabilita, non è stato fatto ancora niente.

[6] *https://www.nist.gov/cyberframework/online-learning/components-framework*

Tier 1: parziale

Il livello 1 significa che i processi di gestione dei rischi e le direttive organizzative per la sicurezza delle TIC non sono formalizzate e che i rischi TIC vengono in genere gestiti solo situativamente o in modo reattivo. Un programma di gestione dei rischi integrato a livello organizzativo è stato definito, ma mancano ancora una consapevolezza dei rischi TIC e un approccio organizzativo per affrontarli. L'organismo o l'impresa non dispone generalmente né di processi atti a utilizzare congiuntamente al proprio interno le informazioni sulla cybersicurezza né, spesso, in caso di rischi TIC, di processi standardizzati per lo scambio di informazioni o di una collaborazione coordinata con partner esterni.

Tier 2: informato sui rischi

Gli organismi o le imprese che si collocano nel livello 2 dispongono generalmente di processi di gestione dei rischi TIC, tuttavia non implementati sotto forma di istruzioni operative concrete. Sul piano organizzativo i rischi TIC sono integrati nella gestione globale dei rischi e tutti i livelli gerarchici ne sono consapevoli. Generalmente manca invece un approccio globale volto a gestire e migliorare la consapevolezza *(awareness)* dei rischi TIC attuali e futuri. I processi e le procedure approvati sono definiti e attuati. Il personale dispone di risorse sufficienti per svolgere le proprie mansioni nell'ambito della cybersicurezza. Le informazioni sulla cybersicurezza vengono comunicate all'interno dell'organismo o dell'impresa in modo informale. L'organismo o l'impresa è consapevole del proprio ruolo e comunica con partner esterni sul tema della cybersicurezza (p.es. clienti, fornitori, operatori ecc.). Non esistono tuttavia processi standard per la cooperazione e lo scambio di informazioni con questi partner.

Tier 3: riproducibile

Gli organismi o le imprese del livello 3 dispongono di piani formalmente approvati per la gestione dei rischi e di istruzioni per applicarli al proprio interno. La gestione dei rischi TIC è definita in direttive valide globalmente. I rischi TIC rilevati con criteri standard e le istruzioni per la loro gestione vengono regolarmente aggiornati tenendo conto sia dei cambiamenti delle esigenze operative sia degli sviluppi tecnologici e di un ambiente di minaccia in continuo mutamento a causa della presenza di nuovi soggetti o di un quadro politico in evoluzione.

I processi e le procedure per gestire i nuovi rischi sono definiti per iscritto. Per reagire a questi rischi vengono applicati metodi standard. Il personale dispone delle conoscenze e delle capacità necessarie a svolgere le proprie mansioni.

L'organismo o l'impresa è consapevole del proprio rapporto di dipendenza dai partner esterni e scambia con loro informazioni che consentono alla direzione di adottare decisioni con cui reagire agli incidenti.

Tier 4: dinamico

Il livello 4 indica che un organismo o un'impresa ha soddisfatto pienamente tutti i requisiti dei livelli 1–3 e verifica costantemente, migliorandoli se necessario, i propri processi, metodi e capacità in base a una documentazione completa relativa a tutti gli eventi di cybersicurezza. L'organismo o l'impresa trae le necessarie conclusioni dall'analisi degli eventi passati e adegua in modo dinamico i propri processi e le tecnologie utilizzate in materia di sicurezza in funzione dei più recenti sviluppi tecnologici o dei mutati ambienti di minaccia. La gestione dei rischi TIC è parte integrante della cultura d'impresa. Le conclusioni tratte dagli eventi precedenti, dalle informazioni acquisite da fonti esterne e dal monitoraggio permanente dei propri sistemi e reti vengono integrati continuamente nel processo di gestione dei rischi. L'organismo o l'impresa condivide regolarmente tali informazioni con i partner e dispone di processi standardizzati.

n/a: non applicabile

Questa misura non viene volutamente attuata dall'organismo o dall'impresa dopo aver effettuato la propria valutazione dei rischi.

Profili

Un profilo è il risultato di un adeguamento a norme, direttive e buone pratiche derivate dal *Cybersecurity Framework* con uno scenario individuale di implementazione. I profili possono essere utilizzati per identificare le opzioni che consentono di migliorare la cybersicurezza, confrontando un profilo reale con uno ideale. Per sviluppare il secondo può essere utilizzato il tool di valutazione fornito con il presente manuale. La valutazione delle 106 attività rilevate nel questionario viene rappresentata in base alle 5 funzioni del *Cybersecurity Frameword* del NIST (identificare, proteggere, intercettare, reagire e ripristinare). Il livello minimo è raggiunto quando nell'«*Overall Cybersecurity Maturity Rating*» la situazione attuale corrisponde almeno ai valori minimi (situazione ideale). Il tool contiene una guida che spiega come utilizzarlo.

Esempio di valutazione della sicurezza informatica

Valutazione complessiva di sicurezza informatica	obiettivo	realtà
Identificare *(Identify)*	2.8	2.6
Proteggere *(Protect)*	2.7	2.6
Intercettare *(Detect)*	2.9	2.6
Reagire *(Respond)*	2.0	2.6
Ripristinare *(Recover)*	1.4	2.6

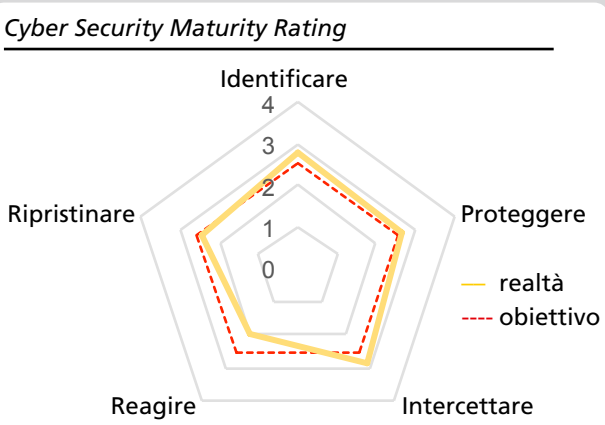


Figura 6: Esempio di valutazione della sicurezza informatica

4.4 Identificare (*Identify* [ID])

Gestione dell'inventario (*Asset Management* [AM])

Dati, persone, apparecchi, sistemi e impianti di un organismo o di un'impresa sono identificati, catalogati e valutati. La valutazione deve corrispondere alla loro criticità in relazione alle procedure operative da attuare e alla strategia di rischio adottata.

Definizione	Mansione
ID.AM-1	Definite una procedura che garantisca la costante presenza di un inventario completo dei vostri strumenti operativi TIC *(asset)*.
ID.AM-2	Inventariate tutte le piattaforme/licenze e applicazioni di *software* all'interno dell'organismo.
ID.AM-3	Catalogate tutti i flussi di comunicazione e di dati interni.
ID.AM-4	Catalogate tutti i sistemi TIC esterni pertinenti per il vostro organismo o la vostra impresa.
ID.AM-5	Definite delle priorità fra le risorse inventariate (apparecchi, applicazioni, dati) in funzione della loro criticità.
ID.AM-6	Stabilite ruoli e responsabilità chiari nel settore della cybersicurezza.

Tabella 7: mansioni ID.AM

Standard	Riferimento
CCS CSC 1	1, 2, 13, 14, 17,19
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO10.04, DSS01.02, APO03.03, APO03.04, APO12.01, BAI04.02, APO01.02, APO07.06, APO13.01, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6, A.12.5.1, A.13.2.1, A.13.2.2
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, PM-5, AC-20, SA-9, CP-2, RA-2, SA-14, SC-6, PS-7, PM-11

Tabella 8: riferimenti ID.AM

Ambiente operativo (*Business Environment* [BE])

Obiettivi, mansioni e attività dell'impresa sono definiti in ordine di priorità e valutati.
Queste informazioni servono da riferimento per l'attribuzione delle responsabilità.

Definizione	Mansione
ID.BE-1	Identificate, documentate e comunicate il ruolo esatto del vostro organismo o della vostra impresa all'interno della catena di approvvigionamento (critica).
ID.BE-2	Il significato dell'organismo o dell'impresa come infrastrutture critiche e la loro posizione all'interno del settore sono identificati e comunicati.
ID.BE-3	Obiettivi, mansioni e attività all'interno dell'impresa sono definiti in ordine di priorità e valutati.
ID.BE-4	Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici.
ID.BE-5	Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio.

Tabella 9: mansioni ID.BE

Standard	Riferimento
CCS CSC 1	1, 2
COBIT 5	APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO02.06, APO03.01, APO02.01, APO10.01, BAI04.02, BAI03.02, DSS04.02, BAI09.02
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	SA-12, CP-2, SA-14, CP-2, PM-11, PM-8, CP-8, PE-9, PE-11, CP-11, SA-13

Tabella 10: riferimenti ID.BE

Direttive (*Governance* [GV])

La governance regola competenze e controlla e garantisce il rispetto dei requisiti regolatori, giuridici e operazionali dell'ambiente operativo.

Definizione	Mansione
ID.GV-1	Definite direttive sulla sicurezza delle informazioni nel vostro organismo o nella vostra impresa.
ID.GV-2	Ruoli e responsabilità nel settore della sicurezza delle informazioni sono coordinati con i ruoli interni (p.es. della gestione dei rischi) e con i partner esterni.
ID.GV-3	Assicuratevi che il vostro organismo o la vostra impresa soddisfi tutte le direttive legali e regolatorie nel settore della cybersicurezza, incluse quelle che riguardano la protezione dei dati.
ID.GV-4	Assicuratevi che i cyberrischi siano parte della gestione dei rischi a livello dell'organismo o dell'impresa.

Tabella 11: mansioni ID.GV

Standard	Riferimento
COBIT 5	APO13.01, APO01.02, APO10.03, DSS05.04, APO13.02, MEA03.01, MEA03.04, DSS04.02, BAI02.01, EDM03.02, APO12.02, APO12.05
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, Clause 6
NIST-SP-800-53 Rev. 4	PM-1, PM-2, PS-7, PM-9, PM-10, PM-11, Rev.4-1 controls from all security control families, SA-2, PM-3, PM-7

Tabella 12: riferimenti ID.GV

Analisi dei rischi (*Risk Assessment* [RA])

L'organismo o l'impresa conosce le conseguenze dei cyberrischi sull'attività, gli strumenti operativi e gli individui, inclusi i rischi legati alla propria reputazione.

Definizione	Mansione
ID.RA-1	Identificate le vulnerabilità (tecniche) dei vostri strumenti operativi e documentatele.
ID.RA-2	Scambiate regolarmente opinioni ed esperienze in forum e comitati per ottenere informazioni aggiornate sulle cyberminacce.
ID.RA-3	Identificate e documentate cyberminacce interne ed esterne.
ID.RA-4	Identificate possibili effetti delle cyberminacce sull'attività operativa e valutate le probabilità che si verifichino.
ID.RA-5	Valutate i rischi per il vostro organismo o la vostra impresa basandovi su minacce, vulnerabilità, conseguenze (sull'attività operativa) e probabilità che si verifichino.
ID.RA-6	Definite possibili misure immediate in presenza di un rischio e classificatele secondo le priorità.

Tabella 13: mansioni ID.RA

Standard	Riferimento
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02, BAI08.01, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2013	A.12.6.1, A.18.2.3, A.6.1.4, Clause 6.1.2, A.16.1.6, Clause 6.1.3
NIST-SP-800-53 Rev. 4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, SI-5, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14, PM-4

Tabella 14: riferimenti ID.RA

Strategia di gestione dei rischi (*Risk Management Strategy* [RM])

Definite priorità, limiti e rischi massimi ammissibili. Valutate in base a questi elementi i rischi operativi.

Definizione	Mansione
ID.RM-1	Definite procedure di gestione dei rischi, applicatele e chiedete riscontro alle persone/ai gruppi di riferimento coinvolti.
ID.RM-2	Definite e comunicate i rischi massimi ammissibili del vostro organismo o della vostra impresa.
ID.RM-3	Assicuratevi che i rischi massimi ammissibili vengano valutati considerando l'importanza del vostro organismo o della vostra impresa come gestori di un'infrastruttura sensibile. Tenete conto anche delle analisi dei rischi specifiche al settore.

Tabella 15: mansioni ID.RM

Standard	Riferimento
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06, APO12.02
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tabella 16: riferimenti ID.RM

Gestione dei rischi della catena di fornitura (*Supply Chain Riskmanagement* [SC])

Definite priorità, limiti e rischi massimi che il vostro organismo o la vostra impresa sono disposti ad assumere in relazione ai fornitori.

Definizione	Mansione
ID.SC-1	Definite procedure chiare per la gestione dei rischi relativi ai fornitori. Fatele verificare da tutti i gruppi di riferimento e chiedete il loro consenso.
ID.SC-2	Identificate fornitori e operatori dei vostri sistemi, componenti e servizi sensibili e stabilite fra loro delle priorità applicando le procedure definite di ID.SC-1.
ID.SC-3	Obbligate per contratto fornitori e operatori a sviluppare e introdurre misure adeguate a rispettare obiettivi e direttive relativi alla procedura di gestione dei rischi nella catena di fornitura.
ID.SC-4	Create un sistema di monitoraggio per garantire che fornitori e operatori si attengano ai loro obblighi secondo le direttive. Chiedete regolarmente riscontro in sede di rapporti su audit o risultati di prove tecniche.
ID.SC-5	Definite con fornitori e operatori procedure di reazione e ripristino susseguenti a cybereventi. Verificatele in sede di test.

Tabella 17: mansioni ID.SC

Standard	Riferimento
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI01.03, BAI02.03, BAI04.02, APO10.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05, DSS04.04
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11
ISO 27001:2013	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.15.2.1, A.15.2.2, A.17.1.3
NIST-SP-800-53 Rev. 4	SA-9, SA-12, PM-9, RA-2, RA-3, SA-14, SA-15, SA-11, AU-2, AU-6, AU-12, AU-16, PS-7, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Tabella 18: riferimenti ID.SC

4.5 Proteggere (Protect [PR])

Gestione e controllo degli accessi (*Access Control* [AC])

Assicuratevi che l'accesso fisico e logico a strumenti e impianti operativi TIC sia possibile solo a persone, procedure e apparecchi autorizzati e unicamente per attività consentite.

Definizione	Mansione
PR.AC-1	Definite una procedura chiaramente definita per attribuire e gestire autorizzazioni e dati di accesso per utenti, apparecchi e procedure.
PR.AC-2	Assicuratevi che unicamente persone autorizzate abbiano accesso agli strumenti operativi TIC. Proteggete con misure (strutturali) gli strumenti operativi TIC da accessi fisici non autorizzati.
PR.AC-3	Definite procedure per gestire gli accessi a distanza.
PR.AC-4	Definite livelli di autorizzazione secondo il principio del privilegio minimo e della separazione delle funzioni.
PR.AC-5	Assicuratevi che l'integrità della vostra rete sia protetta. Separate la vostra rete sul piano fisico e logico qualora utile e necessario.
PR.AC-6	Assicuratevi che le identità digitali siano attribuite chiaramente a persone e procedure verificate.

Tabella 19: mansioni PR.AC

Standard	Riferimento
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS01.05, DSS05.02, DSS05.07, DSS05.10, DSS06.10
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3, SR 1.10
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.6.2.1, A.6.2.2, A13.1.1, A.13.2.1, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.13.1.3, A.14.1.2, A.14.1.3, A.9.3.1, A.18.1.4, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, AC-17, AC-19, AC-20, SC-15, AC-3, AC-5, AC-6,AC-14, AC-16, AC-24, AC-4, AC-10, SC-7, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14

Tabella 20: riferimenti PR.AC

Sensibilizzazione e formazione (*Awareness and Training* [AT])

Assicuratevi che il vostro personale e i partner esterni seguano regolarmente una formazione su tutti gli aspetti legati alla cybersicurezza. Assicuratevi che il vostro personale e i partner esterni svolgano le mansioni pertinenti per la sicurezza secondo le relative procedure e direttive.

Definizione	Mansione
PR.AT-1	Assicuratevi che tutto il personale sia informato e istruito sulla cybersicurezza.
PR.AT-2	Assicuratevi che gli utenti con livelli di autorizzazione elevati siano consapevoli del loro ruolo e delle relative responsabilità.
PR.AT-3	Assicuratevi che tutti i soggetti coinvolti al di fuori dell'impresa (fornitori, clienti, partner) siano consapevoli del loro ruolo e delle relative responsabilità.
PR.AT-4	Assicuratevi che tutti i quadri dirigenti siano consapevoli del loro ruolo e delle relative responsabilità.
PR.AT-5	Assicuratevi che i responsabili della sicurezza fisica e della sicurezza delle informazioni siano consapevoli del loro ruolo e delle loro responsabilità particolari.

Tabella 21: mansioni PR.AT

Standard	Riferimento
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS05.04, DSS06.03, APO07.06, APO10.04, APO10.05, EDM01.01, APO01.02
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.12.2.1, A.6.1.1, A.7.2.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, SA-16, IR-2

Tabella 22: riferimenti PR.AT

Sicurezza dati (*Data Security* [DS])

Assicuratevi che informazioni, dati e supporti dati siano gestiti in modo da proteggere confidenzialità, integrità e disponibilità dei dati secondo la strategia dei rischi del vostro organismo o della vostra impresa.

Definizione	Mansione
PR.DS-1	Assicuratevi che i dati memorizzati siano protetti (da violazioni della confidenzialità, dell'integrità e della disponibilità).
PR.DS-2	Assicuratevi che in sede di trasmissione i dati siano protetti (da violazioni della confidenzialità, dell'integrità e della disponibilità).
PR.DS-3	Assicuratevi che per i vostri strumenti operativi TIC venga definita una procedura formale idonea a proteggere i dati in caso di eliminazione, spostamento o sostituzione di tali strumenti.
PR.DS-4	Assicuratevi che i vostri strumenti operativi TIC dispongano di riserve di capacità sufficienti in relazione alla disponibilità dei dati.
PR.DS-5	Assicuratevi che vengano introdotte misure adeguate conto le fughe di dati *(data leak)*.
PR.DS-6	Definite una procedura per verificare l'integrità di firmware, sistemi operativi, *software* applicativi e dati.
PR.DS-7	Mettete a disposizione un ambiente IT per lo sviluppo e i test completamente indipendente dai sistemi produttivi.
PR.DS-8	Definite una procedura per verificare l'integrità dell'*hardware*.

Tabella 23: mansioni PR.DS

Standard	Riferimento
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06, DSS05.02, BAI09.03, APO13.01, BAI04.04, DSS05.04, DSS05.07, DSS.06.02, BAI03.08, BAI07.04, BAI03.05
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2, SR 3.3
ISO 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.11.2.5, A.12.1.3, A.17.2.1, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.3, A.13.2.1, A.13.2.4, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3A.14.2.4, A.12.1.4, A.11.2.4
NIST-SP-800-53 Rev. 4	MP-8, SC-12, SC-28, SC-8, SC-11, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-13, SC-31, SI-4, SI-7, SC-16, CM-2, SA-10

Tabella 24: riferimenti PR.DS

Protezione di dati (*Information Protection Processes and Procedures* [IP])

Definite direttive per la protezione di sistemi di informazione e strumenti operativi.
Applicate le direttive per proteggere i sistemi di informazione e gli strumenti operativi.

Definizione	Mansione
PR.IP-1	Definite la configurazione standard per l'infrastruttura delle informazioni e della comunicazione e per i sistemi di controllo industriali. Assicuratevi che questa configurazione standard preveda principi di sicurezza tipici (p.es. ridondanza N-1, configurazione minima ecc.).
PR.IP-2	Definite una procedura per il ciclo di vita relativa all'impiego di strumenti operativi TIC.
PR.IP-3	Definite una procedura per il controllo delle modifiche alla configurazione.
PR.IP-4	Assicuratevi che le duplicazioni delle informazioni *(backup)* vengano effettuate, gestite e testate regolarmente (sperimentare il ripristino del *backup*).
PR.IP-5	Assicuratevi di rispettare tutte le disposizioni e le direttive regolatorie in relazione agli strumenti operativi fisici.
PR.IP-6	Assicuratevi che i dati vengano smaltiti secondo le direttive.
PR.IP-7	Assicuratevi che le procedure relative alla sicurezza dell'informazione vengano costantemente aggiornate e migliorate.
PR.IP-8	Scambiate con i vostri partner esperienze sull'efficacia delle tecnologie di protezione.
PR.IP-9	Definite procedure per reagire a cybereventi *(incident response-planning, business continuity management, incident recovery, disaster recovery).*
PR.IP-10	Testate i piani di reazione e ripristino.
PR.IP-11	Definite gli aspetti della cybersicurezza già in sede di iter di assunzione del personale (p.es tramite controlli/verifiche di sicurezza sulle persone).
PR.IP-12	Sviluppate e introducete una procedura per gestire le carenze individuate.

Tabella 25: mansioni PR.IP

Standard	Riferimento
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI03.01, BAI03.02, BAI03.03, BAI06.01, BAI01.06, APO13.01, DSS01.01, DSS04.07, DSS01.04, DSS05.05, BAI09.03, DSS 05.06, APO11.06, APO12.06, DSS04.05, BAI08.04, DSS03.04, DSS04.03, DSS04.04, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, BAI03.10, DSS05.02
ISA 62443-3:2013	SR 7.6, SR 7.3, SR 7.4, SR 4.2, SR 3.3
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, Clause 9, Clause 10, A.16.1.1, A.17.1.1, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4, A.17.1.2, A.17.1.3, A.12.6.1, A.16.1.3, A.18.2.2, A.18.2.3
NIST-SP-800-53 Rev. 4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-11, SA-12, SA-15, SA-17, PL-8, SI-12, SI-13, SI-14, SI-16, SI-17, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, CA-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, SI-4, CP-7, CP-12, CP-13, IR-7, IR-9, PE-17, IR-3, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21, RA-3, RA-5, SI-2

Tabella 26: riferimenti PR.IP

Manutenzione (*Maintenance* [MA])

Assicuratevi che i lavori di riparazione e manutenzione su componenti del sistema TIC e/o dell'ICS vengano effettuati conformemente alle direttive a alle procedure vigenti.

Definizione	Mansione
PR.MA-1	Assicuratevi che il funzionamento, la manutenzione ed eventuali riparazioni agli strumenti operativi vengano registrati e documentati *(logging)*. Assicuratevi che queste operazioni siano effettuate rapidamente e unicamente utilizzando mezzi verificati e autorizzati.
PR.MA-2	Assicuratevi che i lavori di manutenzione a sistemi accessibili a distanza siano registrati e documentati. Assicuratevi che non siano possibili accessi non autorizzati.

Tabella 27: mansioni PR.MA

Standard	Riferimento
COBIT 5	BAI03.10, BAI09.02, BAI09.03, DSS01.05, DSS05.04
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5, MA-6

Tabella 28: riferimenti PR.MA

Impiego di tecnologie di protezione (*Protective Technology* [PT])

Installate soluzioni tecniche per garantire la sicurezza e la resilienza dei sistemi TIC e dei loro dati secondo le direttive e le procedure definite.

Definizione	Mansione
PR.PT-1	Definite le direttive per gli audit e le registrazioni log. Definite e verificate i log regolari secondo le disposizioni e le direttive.
PR.PT-2	Assicuratevi che i supporti rimovibili siano protetti e vengano utilizzati unicamente in base alle direttive.
PR.PT-3	Assicuratevi che il vostro sistema sia configurato in modo da garantirne la funzionalità minima.
PR.PT-4	Assicuratevi che le vostre reti di comunicazione e di controllo siano protette.
PR.PT-5	Assicuratevi che i vostri sistemi funzionino conformemente agli scenari predefiniti. P.es.: funzionalità durante un attacco, nella fase di ripristino e nella fase operativa normale.

Tabella 29: mansioni PR.PT

Standard	Riferimento
COBIT 5	APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01, DSS05.02, DSS05.06, APO13.01, DSS05.05, DSS06.06, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 2.3, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2013	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1, A.14.1.3, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU Family, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Tabella 30: riferimenti PR.PT

4.6 Intercettare (*Detect* [DE])

Anomalie ed eventi (*Anomalies and Events* [AE])

Assicuratevi che le anomalie (comportamenti anormali) e gli eventi pertinenti per la sicurezza vengano individuati in tempo utile e i loro effetti potenziali siano recepiti.

Definizione	Mansione
DE.AE-1	Definite valori standard per operazioni di rete ammesse e relativi flussi di dati per utenti e sistemi. Gestite regolarmente questi valori.
DE.AE-2	Assicuratevi che gli eventi di cybersicurezza individuati siano analizzati in funzione di obiettivi e metodi.
DE.AE-3	Assicuratevi che le informazioni sugli eventi di cybersicurezza provenienti da fonti e sensori diversi siano raggruppate ed elaborate.
DE.AE-4	Definite gli effetti di possibili eventi.
DE.AE-5	Definite i valori soglia a partire dai quali gli eventi di cybersicurezza innescano una situazione di allarme.

Tabella 31: mansioni DE.AE

Standard	Riferimento
COBIT 5	DSS03.01, DSS05.07, APO12.06, BAI08.02
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2013	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2, A.12.4.1, A.16.1.1, A.16.1.4, A.16.1.7
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CM-2, SI-4, AU-6, CA-7, IR-4, IR-5, IR-8, SI-4, CP-2, RA-3

Tabella 32: riferimenti DE.AE

Controllo (*Security Continuous Monitoring* [CM])

Assicuratevi che i sistemi TIC, inclusi tutti gli strumenti operativi, vengano controllati a intervalli regolari per individuare gli eventi di cybersicurezza e verificare l'efficacia delle misure di protezione.

Definizione	Mansione
DE.CM-1	Mettete a punto un sistema di monitoraggio costante della rete per individuare eventi di cybersicurezza.
DE.CM-2	Definite un sistema di monitoraggio/controllo costanti di tutti gli strumenti operativi fisici e degli edifici per individuare eventi di cybersicurezza.
DE.CM-3	Definite un sistema di monitoraggio sull'uso dei TIC da parte del personale per individuare potenziali eventi di cybersicurezza.
DE.CM-4	Assicuratevi che i *software* dannosi vengano identificati.
DE.CM-5	Assicuratevi che i *software* dannosi su apparecchi mobili vengano identificati.
DE.CM-6	Assicuratevi che le attività degli operatori esterni siano sottoposte a controllo in modo da poter individuare eventi di cybersicurezza.
DE.CM-7	Controllate costantemente il vostro sistema per garantire che le attività/gli accessi di persone, apparecchi e *software* non autorizzati possano essere individuati.
DE.CM-8	Effettuate scan di vulnerabilità.

Tabella 33: mansioni DE.CM

Standard	Riferimento
COBIT 5	DSS05.07, DSS05.01, APO07.06, BAI03.10, DSS01.03, DSS03.05, DSS01.04, DSS01.05, APO10.05, DSS05.02, DSS05.05
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.11.1.1, A.11.1.2, A.12.4.1, A.12.4.3, A.12.2.1, A.12.5.1, A.12.6.2, A.14.2.7, A.15.2.1, A.12.6.1
NIST-SP-800-53 Rev. 4	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, AU-13, CM-10, CM-11, SI-3, SI-8, SC-18, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, RA-5

Tabella 34: riferimenti DE.CM

Procedure di intercettazione (*Detection Processes* [DP])

Procedure e istruzioni operative per l'intercettazione di eventi di cybersicurezza vengono gestite, testate e aggiornate.

Definizione	Mansione
DE.DP-1	Definite ruoli e responsabilità in modo che sia chiaro chi svolge quali mansioni e con quali competenze.
DE.DP-2	Assicuratevi che le procedure di intercettazione rispettino tutte le direttive e le condizioni vigenti.
DE.DP-3	Testate le procedure di intercettazione.
DE.DP-4	Segnalate gli eventi intercettati alle persone competenti (p.es fornitori, clienti, partner, autorità ecc.)
DE.DP-5	Migliorate continuamente le vostre procedure di intercettazione.

Tabella 35: mansioni DE.DP

Standard	Riferimento
COBIT 5	APO01.02, DSS05.01, DSS06.03, DSS06.01, MEA03.03, MEA03.04, APO13.02, DSS05.02, APO08.04, APO12.06, DSS02.05, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.7.2.2, A.18.1.4, A.18.2.2, A.18.2.3, A.14.2.8, A.16.1.2, A.16.1.3, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, AC-25, SA-18, SI-3, SI-4, PE-3, PM-14, AU-6, RA-5, PL-2

Tabella 36: riferimenti DE.DP

4.7 Reagire (*Respond* [RS])

Piano di reazione (*Response Planning* [RP])

Definite un piano di reazione per indirizzare gli eventi di cybersicurezza individuati. Assicuratevi che il piano di reazione venga applicato correttamente e tempestivamente nel caso di un evento.

Definizione	Mansione
RS.RP-1	Assicuratevi che il piano di reazione venga applicato correttamente e immediatamente durante o dopo un evento di cybersicurezza intercettato.

Tabella 37: mansioni RS.RP

Standard	Riferimento
COBIT 5	APO12.06, BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8

Tabella 38: riferimenti RS.RP

Comunicazione (*Communications* [CO])

Assicuratevi che le procedure di reazione siano coordinate con i gruppi di riferimento interni ed esterni. Assicuratevi di poter contare in caso di evento, se necessario e opportuno, sull'appoggio di uffici statali.

Definizione	Mansione
RS.CO-1	Assicuratevi che tutte le persone conoscano le proprie mansioni in termini di reazione e priorità in caso di eventi di cybersicurezza.
RS.CO-2	Definite i criteri di segnalazione e assicuratevi che gli eventi di cybersicurezza siano resi noti e gestiti in loro conformità.
RS.CO-3	Attribuite agli eventi di cybersicurezza intercettati informazioni e risultati in base ai criteri definiti.
RS.CO-4	Coordinatevi con tutti i gruppi di riferimento secondo i criteri predefiniti.
RS.CO-5	Create una maggiore sensibilizzazione verso gli eventi di cybersicurezza confrontandovi regolarmente con i vostri partner.

Tabella 39: mansioni RS.CO

Standard	Riferimento
COBIT 5	EDM03.02, APO01.02, APO12.03, DSS01.03, DSS03.04, BAI08.04
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.1, A.7.2.2, A.16.1.1, A.6.1.3, A.16.1.2, Clause 7.4, Clause 16.1.2, A.6.1.4
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, AU-6, IR-6, CA-2, CA-7, IR-4, PE-6, RA-5, SI-4, SI-5, PM-15

Tabella 40: riferimenti RS.CO

Analisi (*Analysis* [AN])

Assicuratevi che vengano effettuate regolarmente analisi tali da consentirvi di reagire adeguatamente a eventi di cybersicurezza.

Definizione	Mansione
RS.AN-1	Assicuratevi che le segnalazioni provenienti dai sistemi di intercettamento vengano prese in considerazione e che siano attivate le relative ricerche.
RS.AN-2	Assicuratevi che le conseguenze di un evento di cybersicurezza siano individuate correttamente.
RS.AN-3	Dopo il verificarsi di un evento effettuate analisi forensi.
RS.AN-4	Classificate gli eventi verificatisi in base alle direttive contenute nel piano di reazione.

Tabella 41: mansioni RS.AN

Standard	Riferimento
COBIT 5	DSS02.04, DSS02.07, DSS02.02, APO12.06, DSS03.02, DSS05.07, EDM03.02
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2013	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
NIST-SP-800-53 Rev. 4	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4, CP-2, AU-7, IR-8, SI-5, PM-15

Tabella 42: riferimenti RS.AN

Diminuzione del danno (*Mitigation* [MI])

Operate in modo da evitare il propagarsi di un evento di cybersicurezza e ridurre possibili danni.

Definizione	Mansione
RS.MI-1	Assicuratevi che gli eventi di cybersicurezza possano essere circoscritti e che ne venga interrotta la diffusione.
RS.MI-2	Assicuratevi che le conseguenze di un evento di cybersicurezza siano individuate correttamente.
RS.MI-3	Assicuratevi che le nuove vulnerabilità individuate vengano ridotte o documentate come rischi accettati.

Tabella 43: mansioni RS.MI

Standard	Riferimento
COBIT 5	APO12.06
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4
ISO 27001:2013	A.12.2.1, A.16.1.5, A.12.6.1
NIST-SP-800-53 Rev. 4	IR-4, CA-7, RA-3, RA-5

Tabella 44: riferimenti RS.MI

Miglioramenti (*Improvements* [IM])

Assicuratevi che la capacità di reazione del vostro organismo o della vostra impresa in caso di eventi di cybersicurezza venga costantemente migliorata basandovi sulle esperienze precedenti.

Definizione	Mansione
RS.IM-1	Assicuratevi che gli elementi e le esperienze raccolti dagli eventi di cybersicurezza vengano recepiti nei vostri piani di reazione.
RS.IM-2	Aggiornate le vostre strategie di reazione.

Tabella 45: mansioni RS.IM

Standard	Riferimento
COBIT 5	BAI01.13, DSS04.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabella 46: riferimenti RS.IM

4.8 Ripristinare (*Recover* [RC])

Piano di ripristino (*Recovery Planning* [RP])

Assicuratevi che le procedure di ripristino siano gestite e svolte in modo tale da garantire la tempestiva riattivazione dei sistemi.

Definizione	Mansione
RC.RP-1	Assicuratevi che il piano di ripristino dopo un evento di cybersicurezza venga effettuato correttamente.

Tabella 47: mansioni RC.RP

Standard	Riferimento
COBIT 5	APO12.06, DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-10, IR-4, IR-8

Tabella 48: riferimenti RC.RP

Miglioramenti (*Improvements* [IM])

Assicuratevi che le vostre procedure di ripristino vengano costantemente migliorate avvalendovi di quanto appreso da precedenti esperienze.

Definizione	Mansione
RC.IM-1	Assicuratevi che gli elementi e le esperienze raccolti dagli eventi di cybersicurezza vengano recepiti nei piani di ripristino.
RC.IM-2	Aggiornate le vostre strategie di ripristino.

Tabella 49: mansioni RC.IM

Standard	Riferimento
COBIT 5	APO12.06, BAI05.07, DSS04.08, BAI07.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabella 50: riferimenti RC.IM

Comunicazione (*Communications* [CO])

Coordinate le attività di ripristino con partner interni ed esterni, p.es internet *service provider*, CERT, autorità, integratori di sistemi ecc.

Definizione	Mansione
RC.CO-1	Confrontatevi attivamente con la vostra immagine pubblica.
RC.CO-2	Assicuratevi che dopo l'evento di cybersicurezza l'immagine del vostro organismo o della vostra impresa torni a essere positiva.
RC.CO-3	Comunicate tutte le attività di ripristino ai gruppi di riferimento interni, in particolare al management/alla direzione.

Tabella 51: mansioni RC.CO

Standard	Riferimento
COBIT 5	EDM03.02, MEA03.02, APO12.06
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tabella 52: riferimenti RC.CO

Conclusioni

La strategia della difesa in profondità privilegia l'approccio proporzionato ai rischi, che consente a ogni organismo o impresa di definire autonomamente la propensione al rischio e stabilire le misure da adottare per ridurre questi rischi. La responsabilità della cybersicurezza rimane nelle mani dell'impresa stessa. Il *Cybersecurity Framework Core* del NIST considerato nel presente manuale consente agli attori dei trasporti pubblici di aumentare la resilienza dei loro processi dipendenti dalle TIC. Sono ipotizzabili numerose altre possibilità di applicazione (analisi comparata, scambio di informazione all'interno del settore, banca dati nazionale, analisi dei gap, audit di terzi ecc.). Emergeranno altre opportunità concrete nell'applicazione pratica e negli scambi con attori, associazioni e Confederazione.

Oltre al presente manuale, l'AEP propone alle imprese di trasporti pubblici uno strumento di valutazione in formato Excel che riprende le raccomandazioni dello standard minimo per le TIC[7]. Tale strumento è particolarmente utile per valutare il livello di maturità dell'impresa o dell'organismo. Il presente manuale è da intendere come documento di accompagnamento che introduce l'argomento e può essere utilizzato come riferimento in caso di domande.

Il manuale non è una direttiva, bensì intende incoraggiare gli attori dei trasporti pubblici a riflettere in materia di cybersicurezza. La sicurezza delle TIC non è uno stato, ma un processo che il presente manuale vuole incoraggiare e aiutare nella sua realizzazione.

[7] *Scaricabile dall'indirizzo: https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html*

Allegato

6.1 Raccomandazioni volte a migliorare la sicurezza delle informazioni

Il quadro di riferimento e il tool di valutazione proposti nella presente raccomandazione per il settore offrono un aiuto prezioso per rilevare e migliorare la sicurezza delle informazioni nell'impresa. La sicurezza delle informazioni comprende tutti i processi, i metodi e le regole che devono garantire la confidenzialità, la correttezza e la disponibilità delle informazioni, siano esse analogiche o digitali. La cybersicurezza è un aspetto della sicurezza delle informazioni. Esistono sovrapposizioni tra i due ambiti. Per esempio, la cybersicurezza comprende anche la protezione dagli incidenti (collisioni di treni), mentre la sicurezza delle informazioni riguarda anche le affermazioni personali dei collabotori.

Le organizzazioni con risorse adeguate e collaboratori formati non avranno difficoltà ad attuare la presente raccomandazione. Non è da escludere che alcune imprese di trasporti pubblici abbiano già messo in pratica il quadro di riferimento proposto nel presente documento oppure un altro.

Tecnica

Le soluzioni tecniche aumentano la complessità e i costi. È opportuno puntare sulla buona prassi e rinunciare a esperimenti costosi.

Esempi:

- due centri di calcolo in ubicazioni diverse; sistemi ridondanti;
- crittografia dei dispositivi mobili;
- *firewall,* filtro web, protezione contro i malware;
- *sandbox;*
- sistema di controllo di accesso alla rete *(Network Access Control System)*;
- *software* di gestione dei dispositivi mobili;
- sistema di accesso elettronico.

Organizzazione

Le misure organizzative sono utilizzate quando le misure tecniche non sono indicate o si rivelano troppo complesse.

Elementi salienti delle misure relative alla sicurezza delle informazioni

Figura 7: Elementi salienti delle misure relative alla sicurezza delle informazioni

Esempi:

- processo di attribuzione dei diritti di accesso (principio del doppio controllo, doppia firma);
- prevenzione delle emergenze (p.es scenari, allerta, organizzazione, misure immediate, decisioni con riserva, esercizio d'emergenza, ritorno all'esercizio normale);
- accordo di segretezza con i collaboratori;
- accordo di riservatezza con i partner esterni;
- classificazione dei documenti;
- piano di smaltimento dei documenti.

Comportamento personale

Ogni collaboratore può identificare nuovi metodi di attacco e introdurre opportuni meccanismi di protezione. Ma il fattore umano costituisce anche una delle principali minacce. Con la sensibilizzazione a una gestione responsabile delle informazioni e l'appello alla responsabilità individuale i collaboratori devono contribuire a migliorare la sicurezza delle informazioni.

Esempi:

- riporre sempre il *notebook* e la valigetta nel baule della macchina;
- utilizzare *password* complesse;
- adottare prudenza con le *e-mail* sconosciute,
- distruggere i documenti cartacei confidenziali (p.es utilizzando il tritacarte) e non limitarsi a gettarli nel cestino;
- non tenere colloqui telefonici confidenziali in luoghi pubblici.

6.2 Principi, documenti e norme

Il presente manuale tiene conto di piani, raccomandazioni e misure che si rifanno a diverse norme e altri documenti normativi (tabella 52).

Titolo	Anno	Editore e descrizione
Misure di protezione dei sistemi di controllo industriali (ICS)	2013	Ed.: **Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI** Basate sui documenti del Dipartimento americano della sicurezza nazionale (DHS), dell'*Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) e del *National Institute of Standards and Technology* (NIST), questa linea guida descrive in nove pagine, in modo sintetico e pragmatico, le undici principali misure da attuare da parte dei gestori di sistemi ICS.
Analisi dei rischi e delle vulnerabilità del sottosettore	2015/ 2017	Ed.: **Ufficio federale per l'approvvigionamento economico del Paese (UFAE)** L'analisi dei rischi e delle vulnerabilità si basa sulla Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) e la Strategia nazionale per la protezione delle infrastrutture critiche (PIC). Il suo obiettivo è esaminare la vulnerabilità di fronte ai guasti o alle perturbazioni delle TIC.
Guida alla protezione delle infrastrutture critiche (Guida PIC)	2015	Ed.: **Ufficio federale della protezione della popolazione (UFPP)** La guida costituisce uno strumento di analisi e, eventualmente, di miglioramento della resilienza delle infrastrutture critiche. In particolare è stata concepita per essere utilizzata nei sottosettori critici da parte di gestori, associazioni di categoria e autorità specializzate. Nella sostanza la guida descrive una possibile procedura in materia di gestione dei rischi: analisi (identificazione delle risorse, vulnerabilità, rischi), valutazione, misure volte a garantire la continuità operativa (attuazione, verifica, miglioramento). La procedura può e dovrebbe essere integrata nei processi di gestione esistenti o essere eseguita basandosi su di essi.
Strategia nazionale per la protezione delle infrastrutture critiche (Strategia PIC)	2012	Ed.: **Ufficio federale della protezione della popolazione (UFPP)** La strategia delinea il campo di applicazione, definisce le infrastrutture critiche e fissa i principi generali per la protezione delle infrastrutture critiche. Si rivolge a tutti gli organi cui competono responsabilità in questo ambito, in particolare alle diverse autorità competenti, ai decisori politici e ai gestori di infrastrutture critiche.
Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)	2018	Ed.: **Organo direzione informatica della Confederazione (ODIC)** Dal momento che la protezione delle infrastrutture TIC dai cyberrischi è di interesse nazionale, il Consiglio federale ha incaricato l'ODIC di elaborare una strategia nazionale per la protezione della Svizzera contro i cyberrischi. La strategia delinea un quadro aggiornato dei cyberrischi, illustra i mezzi di cui la Svizzera dispone, quali sono le lacune e come porvi rimedio nel modo più efficace ed efficiente possibile. La strategia identifica le strutture esistenti, definisce gli obiettivi con le relative misure (p.es le analisi dei rischi e delle vulnerabilità di un sottosettore).

Tabella 53: Documenti pubblicati dalla Confederazione, dai servizi amministrativi e dalle associazioni

Titolo	Anno	Editore e descrizione
Legge federale sull'approvvigionamento economico del Paese (Legge sull'approvvigionamento del Paese, LAP)	2016	Ed.: **Assemblea federale della Confederazione Svizzera** Questa legge disciplina le misure volte a garantire l'approvvigionamento del Paese in beni e servizi d'importanza vitale in situazioni di grave penuria alle quali l'economia non è in grado di far fronte. La Confederazione può promuovere, nei limiti dei mezzi stanziati, misure prese da imprese di diritto privato o pubblico per garantire l'approvvigionamento economico del Paese, se tali misure, nell'ambito dei preparativi in vista di una situazione di grave penuria, contribuiscono a rafforzare considerevolmente i sistemi di approvvigionamento e le infrastrutture d'importanza vitale. Una di queste misure è il presente manuale.

Tabella 53: Documenti pubblicati dalla Confederazione, dai servizi amministrativi e dalle associazioni

Nella seguente tabella è riportata una selezione di norme internazionali considerate (in parte) nel presente documento.

Titolo	Editore e descrizione
ISO 27001 Tecnologia delle informazioni – tecniche di sicurezza Sistema di gestione della sicurezza delle informazioni – Requisiti ISO 27002 Tecnologia delle informazioni – tecniche di sicurezza – linea guida per le misure in materia di sicurezza delle informazioni	Ed.: **Organizzazione internazionale di normazione (*International Standard Organization,* ISO)** La norma precisa le esigenze relative a un sistema di gestione della sicurezza delle informazioni (SGSI). La serie ISO 27000 riguarda una serie di standard in materia di sicurezza delle informazioni. I più interessanti per le tematiche trattate nel presente manuale sono i seguenti: • 27000 Descrizione e vocabolario • 27001 Esigenze: principi basilari con controlli e obiettivi di controllo in allegato • 27002 Linea guida per le misure in materia di sicurezza delle informazioni • 27003 Sistemi di gestione della sicurezza delle informazioni – linee guida per l'attuazione • 27005 Gestione dei rischi • 27019 Misure finalizzate a garantire la sicurezza delle informazioni per l'approvvigionamento energetico Nel frattempo la serie di standard ISO 27000 si è ampiamente diffusa e nei prossimi anni dovrebbe imporsi come il principale quadro di riferimento. Già oggi osservare gli standard di sicurezza ISO è l'approccio giusto. A differenza degli altri standard o quadri di riferimento, sono meno dettagliati, di conseguenza la loro applicazione consente una maggiore flessibilità, e possono essere continuamente migliorati e sviluppati su un lungo periodo. L'SGSI, il contenuto delle misure, deve essere adattato e attuato tenendo conto delle specificità del settore.
ISO 22301 Sicurezza e resilienza – Sistemi di gestione della continuità operativa – Esigenze	Ed.: **Organizzazione internazionale di normazione (*International Standard Organization,* ISO)** La norma precisa i requisiti di un sistema di gestione della continuità operativa.
IEC 62443 Reti di comunicazione industriali – Sicurezza delle reti e dei sistemi	Ed.: **Commissione elettrotecnica internazionale (*International Electrotechnical Commission,* IEC)** Questa serie conta 13 norme di sicurezza e specifiche tecniche applicabili ai sistemi di automazione e di controllo industriali (*Industrial Automation and Control System,* IACS). Lo standard IEC 61508 (norma di base per la sicurezza funzionale dei sistemi di gestione programmabili), cui ora è stato aggiunto l'elemento della sicurezza delle informazioni, copre in modo completo e indipendente la tematica degli IACS per gli impianti industriali. Vengono contemplati quattro diversi aspetti o livelli della sicurezza delle informazioni: • aspetti generali tra cui concetti, terminologia o parametri: IEC 62443-1-x; • gestione della sicurezza informatica: IEC 62443-2-x; • livello del sistema: IEC 62443-3-x; • livello dei componenti: IEC 62443-4-x; Va segnalato in particolare che questa serie di norme copre anche l'architettura di rete e di zona, di cui altri standard non si occupano o non in modo così dettagliato. Questa serie di norme sta diventando una prescrizione normativa fondamentale nel contesto delle norme RAMS (*Reliability, Availability, Maintainability, Safety,* ossia affidabilità, disponibilità, manutenibilità e sicurezza) del CENELEC (EN 50126 e altre).

Tabella 54: Norme nazionali e internazionali relative alla sicurezza informatica

Titolo	Editore e descrizione
(pr)TS 50701 Applicazioni ferroviarie – Cybersicurezza	Ed.: **Comitato europeo di normazione elettrotecnica** Questa specifica tecnica certifica che un sistema ferroviario che la applica è all'avanguardia in materia di cybersicurezza, raggiunge il livello di sicurezza auspicato ed è in grado di garantirlo durante l'esercizio e la manutenzione. Si basa sulle norme IEC 62443. Nella definizione di questa specifica tecnica sono stati perseguiti i seguenti obiettivi: • elaborazione di linee direttrici per i documenti relativi alla cybersicurezza, i risultati da fornire e le tappe del processo; • possibilità di adattarla ai diversi cicli di vita dei sistemi e di supportarli; • possibilità di applicarla ai sistemi ferroviari che sono rilevanti ai fini della sicurezza e anche a quelli non rilevanti (architettura di riferimento); • supporto all'identificazione e alla gestione delle interfacce tra la cybersicurezza e altri compiti nel ciclo di vita del sistema; • compatibilità e coerenza con la norma EN 50126 e altre; • possibilità di operare, ma anche consentire una distinzione tra omologazione di sicurezza *(safety)* e garanzia di sicurezza *(security);* • possibilità di stabilire, in modo armonizzato e standardizzato, esigenze tecniche in materia di sicurezza delle informazioni; • definizione di principi di costruzione per promuovere sistemi semplici e modulari; • possibilità di utilizzare prodotti, per esempio i componenti industriali COTS (*Commercial Off-the-Shelf,* componenti *hardware* e *software* disponibili sul mercato) secondo la norma IEC 62443
IEC 62264 Integrazione del sistema di controllo aziendale	Ed.: **Commissione elettrotecnica internazionale (*International Electrotechnical Commission,* IEC)** Questa serie comprende 4 standard relativi all'integrazione dei sistemi informatici e di controllo-comando aziendali
IEC 62351 Gestione dei sistemi di generazione e trasporto dell'energia e scambio informativo associato – Sicurezza dei dati e delle comunicazioni	**Ed.: Commissione elettrotecnica internazionale (*International Electrotechnical Commission,* IEC)** Questa serie descrive lo standard di sicurezza per i sistemi di gestione dell'energia e lo scambio di dati associato. Descrive le misure volte a soddisfare le quattro esigenze fondamentali in materia di comunicazione ed elaborazione sicure dei dati.
BDEW *Whitepaper* *Anforderungen an sichere Steuerungs- und Telekommunikationssysteme*	Ed.: **BDEW *Bundesverband der Energie- und Wasserwirtschaft e.V., Österreichs E-Wirtschaft*** Il *Whitepaper* (libro bianco) della BDEW è stato sviluppato per delineare le misure di sicurezza fondamentali dei sistemi di gestione e di telecomunicazione nel settore dell'energia. L'obiettivo strategico di questo documento è influenzare positivamente lo sviluppo di prodotti destinati ai summenzionati sistemi nell'ottica della sicurezza informatica e promuovere una consapevolezza condivisa tra gli attori del settore dell'importanza di proteggere questi sistemi. Nella regione D-A-CH (Germania, Austria, Svizzera) il *Whitepaper* della BDEW è diventato un documento di riferimento per l'approvvigionamento nel settore della corrente di trazione. Il documento contiene anche raccomandazioni di esecuzione.

Tabella 54: Norme nazionali e internazionali relative alla sicurezza informatica

Titolo	Editore e descrizione
Guide to Industrial Control Systems (ICS) Security SP 800-82	Ed.: ***National Institute of Standards and Technology*** **(NIST)** Questa guida fornisce una visione d'insieme delle topologie e delle architetture dei sistemi SCADA, identifica le minacce e le vulnerabilità e formula raccomandazioni riguardanti le contromisure e la riduzione dei rischi. Inoltre presenta controlli specifici SCADA basati sul *Framework* NIST 800-53.
Framework for Improving Critical Infrastructure Cybersecurity	Ed.: ***National Institute of Standards and Technology*** **(NIST)** Questo quadro di riferimento dà seguito al decreto presidenziale americano del 2013 «*Improving Critical Infrastructure Cybersecurity*» (migliorare la cybersicurezza delle infrastrutture critich). Raggruppa diverse linee guida volte a valutare la situazione di un'impresa nell'ambito della cybersicurezza e a definire una roadmap per migliorare le pratiche in materia con rimandi ad altri quadri di riferimento e standard (ISO27001, ISA 62443, NIST 800-53, Cobit ecc.).
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	Ed.: ***Industrial Control Systems Cyber Emergency Response Team*** **(ICS-CERT) del Dipartimento americano della sicurezza nazionale (DHS)** Introduzione generale alla strategia della difesa in profondità per i sistemi di controllo industriali.
IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit	Ed.: ***Bundesamt für Sicherheit in der Informationstechnik*** **(BSI, Germania)** Questo compendio è la pubblicazione di riferimento in materia di protezione informatica di base. Insieme agli standard emanati dal BSI costituisce la base per approfondire la tematica della sicurezza delle informazioni. Il documento approfondisce i diversi elementi della protezione informatica di base *(IT-Grundschutz)*. Nella prima parte sono presentate le potenziali minacce, dopo di che le esigenze fondamentali in materia di sicurezza. Gli elementi della protezione informatica di base sono suddivisi in dieci diverse sottocategorie che spaziano dalle applicazioni (APP) alla gestione della sicurezza (ISMS) passando per l'informatica industriale (IND). Vengono sistematicamente esaminati diversi livelli di protezione.
Standard BSI	Ed.: ***Bundesamt für Sicherheit in der Informationstechnik*** **(BSI, Germania)** Gli standard BSI sono una componente chiave della metodologia della protezione informatica di base. Contengono raccomandazioni in merito a metodi, processi e procedure nonché ai modi di operare e alle misure concernenti diversi aspetti della sicurezza informatica. Esempi di standard BSI: 200-1 (gestione della sicurezza delle informazioni); 200-2 (modi di operare per la protezione informatica di base); 200-3 (analisi dei rischi sulla base della protezione informatica di base) e 100-4 (linea guida sulla gestione delle emergenze).
BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz	L'attuazione e il controllo del dispositivo di sicurezza possono essere realizzati secondo la metodologia della protezione informatica di base sviluppata dal BSI, ma anche secondo gli standard della serie ISO 27000. I due approcci sono compatibili. Entrambi consentono di attuare e gestire un SGSI, quindi identificare i rischi in materia di sicurezza informatica e ridurli a un livello accettabile grazie a misure adeguate.
Zuordnungstabelle ISO zum modernisierten IT-Grundschutz	Lo standard BSI 200-2 relativo alla protezione informatica di base interpreta le esigenze e le misure degli standard ISO 27001 e 27002. La tabella delle corrispondenze aiuta gli utenti a stabilire i contenuti dei due standard.

Tabella 54: Norme nazionali e internazionali relative alla sicurezza informatica

Titolo	Editore e descrizione
Industrielle Steuerungs- und Automatisierungssysteme (ICS) – Allgemeine Empfehlungen	Ed.: ***Bundesamt für Sicherheit in der Informationstechnik*** **(BSI, Germania)** Il compendio è un'opera di riferimento che consente di addentrarsi facilmente nella sicurezza informatica dei sistemi SCADA. Illustra alcuni principi generali dell'automazione evidenziando le peculiarità e gli standard in questo ambito. Contiene anche una serie di misure e di metodologie per verificare l'attuazione. Nel sito del BSI sono proposti ulteriori strumenti specialistici a disposizione degli utenti.
Tabella delle corrispondenze – *Mapping of Dependencies to International Standards*	Ed.: **Agenzia dell'Unione europea per la cibersicurezza (European Union Agency for Network and Information Security, ENISA)** Il rapporto analizza le dipendenze e i nessi tra i gestori di servizi essenziali (*operators of essential services,* OES) e i fornitori di servizi digitali (*digital service providers,* DSP) e fornisce una serie di indicatori per la loro valutazione. Questi indicatori sono attribuiti a standard e condizioni quadro internazionali (ISO IEC 27002, COBIT 5, misure di sicurezza del gruppo di cooperazione NIS [sicurezza delle reti e dei sistemi informativi] e *Cybersecurity Framework* del NIST).
Communication Network Dependencies for ICS/SCADA Systems	Ed.: **Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Network and Information Security,* ENISA)** Il rapporto è incentrato sui seguenti argomenti: reti di comunicazione, intercomunicazione tra ICS/SCADA, identificazione delle vulnerabilità, rischi e minacce, impatto sulla sicurezza dei sistemi cyber-fisici. Contiene anche una serie di raccomandazioni per ridurre i rischi identificati. Lo studio preliminare ha permesso di redigere un elenco di pratiche e di direttive convalidate che intendono limitare il più possibile la vulnerabilità dei sistemi ICS/SCADA. L'obiettivo principale del documento è far conoscere le interdipendenze delle reti di comunicazione dei sistemi ICS/SCADA e identificare le risorse critiche dal punto di vista della sicurezza nonché scenari di attacco realistici e minacce contro queste reti di comunicazione.
ENISA Threat Landscape/ Taxonomy	Ed.: **Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Network and Information Security,* ENISA)** Il Threat Landscape dell'ENISA è un rapporto che fornisce una visione d'insieme delle minacce e delle tendenze in atto o emergenti. Si basa sui dati accessibili al pubblico e offre una visione indipendente delle minacce identificate, dei loro autori e delle tendenze che si delineano. La tassonomia categorizza le minacce in modo sistematico.
Branchenanforderungen an die IT-Sicherheit (VDV Schrift 400)	Ed.: ***Verband Deutscher Verkehrsunternehmen*** **(VDV)** Il documento descrive le esigenze di sicurezza informativa relativamente alle infrastrutture critiche. Suggerisce approcci possibili nell'attuazione di queste esigenze con metodi, processi e modi di operare adeguati. Con questo documento l'associazione VDV mette a disposizione dei suoi membri uno standard di sicurezza specifico per il settore (B3S) che si basa sulle guide del BSI.

Tabella 54: Norme nazionali e internazionali relative alla sicurezza informatica

6.3 Sviluppo delle norme

Il progresso tecnologico e i continui cambiamenti che interessano il settore dei trasporti pubblici esigono un'evoluzione costante delle norme. Al momento della stesura del presente manuale sono emerse alcune novità:

- De-Oferr 2020 (art. 5c): esigenza di un sistema di gestione della sicurezza delle informazioni (SGSI). È raccomandato l'utilizzo delle norme.
- Direttiva europea sull'interoperabilità: si prevede di inserire l'aspetto della cybersicurezza nelle nuove TSI 2022 (portata e contenuto ancora da definire).
- CENELEC prTS 50701 (vedi tabella 54): ultima revisione della norma a metà del 2020.

6.4 Elenco delle abbreviazioni

Abbreviazione	Descrizione
AC	*Identity Management, Authentification and Access Control*
AE	*Anomalies and Events*
AEP	Approvvigionamento economico del Paese
AM	*Asset Management*
AN	*Analysis*
AT	Azienda di trasporti
AT	*Awareness and Training*
ATC	Azienda di trasporti concessionaria
ATP	*Automatic train protection* (protezione automatica dei treni)
BCM	*Business Continuity Management* (gestione della continuità operativa)
BE	*Business Environment*
BIA	*Business Impact Analyse* (analisi d'impatto sull'attività operativa)
BLS	BLS SA (prima Ferrovia Berna-Lötschberg-Sempione)
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Germania)
CAPRE	*Capacity and Reservation* (sistema di gestione dei posti, ha sostituito PLABE)
CC	Centro di calcolo
CCTV	*Closed-circuit television* (televisione a circuito chiuso)
CENELEC	*Comité Européen de Normalisation Électrotechnique* (Comitato europeo di normazione elettrotecnica)
CM	*Security Continous Monitoring*

Tabella 55: Elenco delle abbreviazioni

Abbreviazione	Descrizione
CO	*Communications*
COAT	*CCS onboard application platform for trackside related functions*
CUE	Cablaggio universale per edifici
DAS	*Driver Assistance System* (sistema di assistenza alla guida)
DE	*Detect*
DMS	*Document Management System* (sistema di gestione dei documenti)
DMZ	*Demilitarised zone* (zona demilitarizzata: rete di computer, che funge da zona cuscinetto tra due reti)
DNS	*Domain Name System* (sistema dei nomi di dominio)
DP	*Detection Processes*
DS	*Data Security*
EDP	*Electronic Data Processing* (elaborazione elettronica dei dati)
EMS	*Energy Metering System* (sistema di misurazione dell'energia)
ENISA	Agenzia dell'Unione europea per la cibersicurezza
ERP	*Enterprise Ressource Planning* (pianificazione delle risorse d'impresa)
ETCS	*European Train Control System* (sistema europeo di controllo dei treni)
FFS	Ferrovie federali svizzere SA
FR	Ferrovia retica SA
FTP	*File Transfer Protocol* (protocollo di trasferimento file)
GIF	Gestori dell'infrastruttura ferroviaria
GIS	*Geographic Information System* (sistema informativo geografico)
GSM	*Global System for Mobile Communications* (sistema di telefonia mobile internazionale)
GSM-R	*Global System for Mobile Communications* (sistema di comunicazione mobile internazionale per le ferrovie)
GV	*Governance*
HIDS	*Host Intrusion Detection System* (sistema di rilevamento delle intrusioni nell'host)
HMI	*Human Maschine Interface* (interfaccia uomo-macchina)
HVAC	*Heating, Ventilation and Air Conditioning* (riscaldamento, ventilazione, condizionamento d'aria)
IaaS	*Infrastructure as a Service* (infrastruttura sotto forma di servizio)
IAM	*Identity and Access Management* (gestione delle identità e degli accessi)
ICS	*Industrial Control Systems* (sistemi di controllo industriale, utilizzato nel presente documento come sinonimo degli acronimi «TO» e «SCADA»)
ICT	*Information and Communication Technology* (tecnologie dell'informazione e della comunicazione)
ID	*Identify*
IDS	*Intrusion Detection System* (sistema di intercettazione delle intrusioni)
IM	*Improvements*

Tabella 55: Elenco delle abbreviazioni

Abbreviazione	Descrizione
IMPT	Impianto tecnico
IP	*Information Protection Processes and Procedures*
IP	*Internet Protocol* (protocollo di internet)
IPS	*Intrusion Prevention System* (sistema di prevenzione delle intrusioni)
ISA	*Interconnection Security Agreement* (accordo per la sicurezza di sistemi informatici interconnessi)
ISA	*International Society of Automation*
ISMS	*Information Security Management System* (sistema di gestione della sicurezza delle informazioni)
ISMS	Sistema di gestione della sicurezza delle informazioni
ISO	Organizzazione internazionale per la normazione
IT	*Information Technology* (tecnologia dell'informazione)
ITS	Impresa di trasporto ferroviario
JRU	*Juridical Recording Unit*
KPI	*Key Performance Indicator*
LAN	*Local Area Network*
Lferr	Legge federale sulle ferrovie
LTV	Legge sul trasporto di viaggiatori
MA	*Maintenance*
MCG	*Mobile Communication Gateway*
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (Organo direzione informatica della Confederazione)
MI	*Mitigation*
MOU/MOA	*Memorandum of Understanding/Agreement*
MPLS	*Multiprotokoll Label Switching* (istradamento di flussi di traffico multiprotocollo tra nodo di origine e nodo di destinazione tramite l'utilizzo di identificativi)
MPLS-TP	*Multiprotokoll Label Switching Transport Profile*
NAC	*Network Access Control* (controllo di accesso alla rete)
NeTS	*Network-wide Track Management System* (sistema di gestione delle linee per l'intera rete ferroviaria)
NIST	*National Institute of Standards and Technology* (Stati Uniti)
NIST CSF	*National Institute of Standards and Technology Cybersecurity Framework*
NMC	*Network Management Center* (centro di gestione della rete)
OBM	*Open-book Management* (gestione a libro aperto)
OBU	*Onboard Unit* (apparecchiatura di bordo)
OC	*Object Controller*
ODIC	Organo direzione informatica della Confederazione
OTV	Ordinanza sul trasporto di viaggiatori

Tabella 55: Elenco delle abbreviazioni

Abbreviazione	Descrizione
PA	*Public Address*
PaaS	*Platform as a Service* (piattaforma sotto forma di servizio)
PC	*Personal Computer*
PIS	*Passenger Information System* (sistema di informazione al passeggero)
PR	*Protect*
PT	*Protective Technology*
RA	*Risk Assessment*
RailOpt	*Software* di pianificazione (tra infrastruttura e pianificazione operativa)
RailSys	*Software* di pianificazione
RC	*Recover*
RCS	*Rail Control System*
ReSys	Sistema di prenotazione dei posti
RM	*Risk Management Strategy*
RoE	*Rules of Engagement* (regole d'ingaggio)
RP	*Recovery Planning*
RP	*Response Planning*
RS	*Respond*
SaaS	*Software as a Service* (*software* sotto forma di servizio)
SC	*Supply Chain Riskmanagement*
SCADA	*Supervisory Control and Data Acquisition* (utilizzato nel presente documento come sinonimo degli acronimi «ICS» e «TO»)
sFTP	*Secure File Transfer Protocol* (protocollo di trasferimento file basato su Secure Shell)
SIEM	*Security Incident and Event Management* (gestione degli eventi e delle informazioni sulla sicurezza)
SIG	Sistema integrato di gestione
SLA	*Service Level Agreement* (contratto di fornitura di prestazioni di servizi)
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
SOB	*Schweizerische Südostbahn AG*
SOC	*Security Operation Center* (centro operativo di sicurezza)
SOPRE	*Software* di pianificazione dell'impiego di personale e materiale rotabile
SSH	*Secure Shell*

Tabella 55: Elenco delle abbreviazioni

Abbreviazione	Descrizione
TCMS	*Train Control and Management System*
TIC	Tecnologie dell'informazione e della comunicazione
tl	*Transports publics de la région lausannoise*
TMS	*Traffic Management System* (sistema di gestione del traffico)
TO	Tecnologia operativa (acronimo utilizzato nel presente documento come sinonimo degli acronimi «SCADA» e «ICS»)
TPF	*Transports publics fribourgeois Holding* (TPF) SA
TSI	*Technical Specifications for Interoperability* (specifiche tecniche per l'interoperabilità)
UCC	*Unified Communications and Collaboration* (collaborazione e comunicazioni unificate)
UFAE	Ufficio federale per l'approvvigionamento economico del Paese UFAE
UFPP	Ufficio federale della protezione della popolazione
UFT	Ufficio federale dei trasporti
UTP	Unione dei trasporti pubblici
VBZ	*Verkehrsbetriebe der Stadt Zürich*
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WLAN	*Wireless Local Area Network*

Tabella 55: Elenco delle abbreviazioni

6.5 Elenco delle illustrazioni

6.6 Elenco delle tabelle

Autori ed esperti che hanno contribuito alla prima edizione

Nome, cognome	Società	Funzione
Hans-Peter Käser	UFAE	Autore principale/Responsabile del progetto
Daniel Caduff	UFAE	Coautore
Nathalie Gratzer	UFAE	Coautrice
Marcus Griesser	AEP/FFS	RP UTP, coautore, esperto
Patrick Favre	UFT	Esperto, assicurazione qualità
Tobias Hubschmid	UFT	Esperto, assicurazione qualità
Ulrich Schär	UFT	Esperto, assicurazione qualità
Andreas Klopfenstein	BLS	Esperto, assicurazione qualità
Daniel Noger	BLS	Esperto, assicurazione qualità
Martin Wyss	BLS	Esperto, assicurazione qualità
Stephan Berger	BLS	Esperto, assicurazione qualità
Urs Hoerler	RhB	Esperto, assicurazione qualità
Jean-Luc Nottaris	FFS	Esperto, assicurazione qualità
Stefan Käser	FFS	Esperto, assicurazione qualità
Olaf Zanger	FFS	Esperto, assicurazione qualità
Peter Häberli	SOB	Esperto, assicurazione qualità
Roland Kressbach	SOB	Esperto, assicurazione qualità
Giorgio Anastopoulos	tl	Esperto, assicurazione qualità
Marc Striffeler	TPF	Esperto, assicurazione qualità
Marcel Gahler	VBZ	Esperto, assicurazione qualità

Cronologia

Data	«Breve descrizione»
Agosto 2019	Avvio dei lavori del gruppo di lavoro sulla sicurezza delle TIC nelle infrastrutture critiche
Settembre 2019 – Giugno 2020	Redazione della prima bozza del documento
Giugno 2020	Validazione da parte del gruppo di lavoro
Giugno – Luglio 2020	Consultazione dell'UTP (commissione infrastruttura)
Agosto 2020	Validazione da parte dell'UTP

Esclusione di responsabilità

Il presente documento, che contiene raccomandazioni volte a migliorare la sicurezza dei sistemi di informazione e comunicazione e dei sistemi di gestione dei trasporti pubblici, è stato redatto secondo scienza e coscienza dalle persone e dagli uffici coinvolti.

L'Ufficio federale per l'approvvigionamento economico del Paese non si assume alcuna garanzia, né esplicita né implicita. Lo stesso vale per gli esperti, le imprese e i collaboratori che hanno partecipato alla stesura del presente documento. La sicurezza nell'esercizio delle TIC incombe esclusivamente all'utente, che si assume la responsabilità di eventuali danni.

Colophon e contatti

Editore
Ufficio federale per l'approvvigionamento economico del Paese UFAE
Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Telefono +41 58 462 21 71

Associazioni consultate
Unione dei trasporti pubblici UTP


Jeremias Gotthelf