Standard minimo per migliorare la resilienza delle TIC

Versione maggio 2023, con aggiornamento NIST SP 800-53 Rev. 5 e ISO 27001:2022

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

Prefazione

La digitalizzazione impone misure protettive

La crescente penetrazione dell'informatica e la connessione in rete di tutti gli ambiti della vita schiude prospettive sia economiche che sociali alle quali un Paese altamente sviluppato e industrializzato come la Svizzera non può rinunciare. L'avanzata della digitalizzazione determina tuttavia nuove situazioni a rischio alle quali occorre reagire sistematicamente. In particolare il pericolo di cyberattacchi all'apparato informatico riguarda sia uffici statali che operatori di infrastrutture sensibili e altri organismi o imprese.

A questi ultimi spetta, di massima, la responsabilità di autoproteggersi. Una responsabilità da parte dello Stato, basata sul mandato conferito dalla Confederazione e sulla legge federale sull'approvvigionamento economico del Paese, subentra ogni qual volta a essere interessato è il funzionamento di infrastrutture sensibili. Questo standard minimo TIC si inserisce nella responsabilità di tutelare cittadini, economia, istituzioni e pubblica amministrazione.

Si applica là dove una società moderna può permettersi molto meno che altrove la presenza di criticità: nei sistemi TIC importanti ai fini del funzionamento di infrastrutture sensibili. Agli operatori di queste infrastrutture si raccomanda pertanto di rispettarlo o di adottare parametri comparabili (p.es. ISO, COBIT ecc.). Il presente documento offre comunque in linea di massima un supporto a ogni impresa o organismo interessati, proponendo concrete modalità operative per migliorare la resilienza dei propri TIC.

Management Summary

Il presente standard funge da raccomandazione e possibile criterio di riferimento per migliorare la resilienza TIC. Si rivolge in particolare a gestori di infrastrutture sensibili, ma in linea di massima ogni impresa o organismo può fruirne liberamente e ispirarvisi.

Gli organi dell'Approvvigionamento economico del Paese definiscono per vari settori (energetico, alimentazione ecc.) standard TIC minimi più dettagliati di quello riportato nel presente documento.

Lo standard minimo è destinato in particolare ai responsabili TIC e ai membri della direzione di gestori di infrastrutture sensibili.

Il documento si divide in tre parti:

1. Riferimenti: costituiscono la parte consultiva e contengono informazioni di base sulla sicurezza TIC.

2. Parte strutturale (framework): propone agli utenti una serie di misure concrete, 106 in tutto, suddivise in cinque temi: «identificare», «proteggere», «intercettare», «reagire» e «ripristinare».

3. Auto-assessment e tool di valutazione (Excel): consentono a organismi o imprese di verificare lo stato di avanzamento delle misure e di farlo analizzare anche da ditte terze (audit). I risultati possono essere utilizzati come riferimento per un benchmarking interorganismi o interimprese.

Indice

1 Prima parte: riferimenti

1.1 Panoramica

La prima parte definisce principi e finalità della sicurezza TIC, circoscrive l'ampia tematica e illustra l'applicazione dello standard minimo TIC.

1.2 Riferimenti normativi

I riferimenti normativi citati nel seguito rappresentano la premessa delle attività dell'Approvvigionamento economico del Paese.[1]

- Legge federale sull'approvvigionamento economico del Paese (Legge sull'approvvigionamento del Paese, LAP; RS 531)
- Ordinanza sull'organizzazione dell'approvvigionamento economico del Paese (RS 531.11)
- Ordinanza sui provvedimenti preparatori in materia di approvvigionamento economico del Paese (RS 531.12)

1.3 Contesto e finalità

La sicurezza TIC presuppone un approccio basato sul rischio e l'impiego di sistemi più sicuri nell'ambito di responsabilità dei gestori. L'attuazione di misure collaudate come quelle illustrate nel quadro dello standard minimo può già consentire di contrastare numerosi attacchi TIC con risorse ragionevoli. Il presente standard punta a offrire a imprese ed enti uno strumento di ampio respiro grazie al quale migliorare la resilienza della propria infrastruttura TIC. Partendo da un approccio basato sul rischio lo standard permette di applicare livelli di protezione di varia intensità in linea con le esigenze di ogni organismo o impresa.

1.4 Definizione

Il presente standard minimo è stato elaborato da Approvvigionamento economico del Paese in collaborazione con esperti esterni del settore sicurezza TIC.

Attualmente esistono già numerosi standard riconosciuti a livello internazionale, generalmente molto più specifici di quello riportato in questo documento (cfr. capitolo 1.4.1). Il presente standard non si pone assolutamente in concorrenza con quelli internazionali, bensì risulta compatibile con essi e, nel contempo, più ridotto nei contenuti. Il suo obiettivo è semplificare l'approccio al tema della sicurezza garantendo ciononostante un elevato livello di protezione.

In aggiunta al presente standard, l'Approvvigionamento economico del Paese ne ha messo a punto altri specificamente settoriali[2] (tecnicamente) molto più dettagliati. I gestori di infrastrutture sensibili sono invitati a orientarsi, oltre che allo standard minimo, anche a questi ultimi, qualora disponibili.

Se in un settore vigono già standard propri o vengono applicati standard internazionali come ISO o NIST, le imprese hanno la possibilità di verificare, sulla base della checklist riportata al capitolo «Terza parte: incarico di verifica», se questi standard soddisfano quello minimo.

1.4.1 Documenti di riferimento e standard

A livello internazionale sono stati definiti numerosi standard e fonti di informazione relativi alla gestione di rischi TIC. Alcuni sono già stati riconosciuti dal settore economico e vengono applicati. Il presente standard minimo si basa sul NIST Cybersecurity Framework Core.[3] Dove opportuno, può essere completato da altri standard riconosciuti a livello internazionale. I più importanti sono (per la lista completa cfr. allegato):

1. NIST Guide to Industrial Control Systems (ICS) Security
   Anche questa guida viene curata e pubblicata dal National Institute of Standards and Technology e completa il NIST Cybersecurity Core Framework con direttive specifiche riguardanti in particolare la gestione di sistemi di controllo industriali (ICS), NIST Special Publication 800-82, revisione 2, maggio 2015.[4]

[1] Tutti i testi di legge si possono consultare nella Raccolta sistematica del diritto federale. Sono inoltre disponibili online su: https://www.admin.ch/gov/de/start/bundesrecht/systematische-sammlung.html

[2] Attualmente sono stati definiti quelli relativi all'approvvigionamento energetico e di generi alimentari. Altri sono in fase di elaborazione e saranno pubblicati non appena pronti.

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

[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

2. ISO 2700x
   La International Organization for Standardization (ISO) pubblica una decina di standard sulla sicurezza informatica che si completano a vicenda e vengono definiti «Famiglia 2700x». Il più importante è lo standard ISO 27001, che definisce i requisiti relativi a istituzione, applicazione, mantenimento e costante miglioramento di un sistema di gestione documentato sulla sicurezza dell'informazione in linea con lo specifico contesto operativo di un organismo.[5]

3. COBIT
   Control Objectives for Information and related Technology (COBIT)[6]

4. ENISA Good Practice Guide on National Cyber Security Strategies.[7]

5. Bundesamt für Sicherheit in der Informationstechnik (Germania), BSI 100-2.[8]

1.4.2 Principi

1. Autoresponsabilità: i gestori di infrastrutture sensibili sono responsabili in linea di massima di garantire l'operatività delle loro procedure TIC.
2. Business continuity management: tutti gli aspetti della sicurezza TIC vanno integrati in un business continuity management generale.
3. Gestione rischi: la responsabilità di valutare regolarmente possibili rischi TIC, tra cui violazione della disponibilità, dell'integralità e della confidenzialità, spetta a chi applica questo standard. L'organismo o l'impresa devono giudicare quali rischi vanno attenuati e quali sono disposti ad assumere.

1.4.3 Misure e rimandi nel presente documento

Per quanto possibile si rinuncia a duplicare le informazioni rimandando ad altri standard TIC. L'utente del presente standard viene invitato a consultare, in caso di necessità, le fonti indicate.

[5] https://www.iso.org/standard/66435.html

[6] http://www.isaca.org/COBIT/Pages/default.aspx

[7] https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[8] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html

1.5 Introduzione allo standard minimo TIC

In questo paragrafo vengono presentati i temi centrali relativi allo standard minimo TIC.

1.5.1 Principi di sicurezza TIC

Prima di rendere operative le proprie misure di sicurezza, un organismo o un'impresa devono definire i principi TIC, analizzando in particolare i seguenti aspetti:

- cosa va fatto?
- come va fatto?
- chi è responsabile?
- come si valuta?

I principi di scurezza TIC definiscono regole, procedure, metriche e strutture organizzative necessarie a un controllo e a una pianificazione concreti.

1.5.2 Organizzazione e responsabilità

Per garantire la sicurezza TIC, l'organismo o l'impresa devono creare una struttura generale che stabilisca chiaramente compiti, responsabilità e competenze. In questo contesto va inoltre definita e applicata la cosiddetta strategia defense-in-depth. I rischi TIC devono essere inseriti in una strategia globale di gestione dei rischi; condizione, questa, per individuare possibili minacce e mettere a punto le rispettive misure. Il reparto deputato alla sicurezza deve consentire alla direzione di decidere sulle risorse necessarie. La direzione deve dotarlo di opportune competenze, in modo da permettergli di svolgere pienamente le proprie mansioni principali in stretta collaborazione con i settori dell'organismo o dell'impresa.

1.5.3 Politica, istruzioni e direttive

Prima di attuare una strategia di sicurezza TIC (p. es. la defense-in-depth) è necessario individuare direttive, procedure e istruzioni di lavoro di un organismo o di un'impresa o eventualmente definirle.

Le esigenze operative delle varie unità dell'organismo o dell'impresa vanno rese note ai responsabili della cybersicurezza e documentate. Possono riguardare aspetti giuridici, finanziari, strategici od operativi.

1.5.4 Gestione rischi

Il miglioramento della resilienza TIC attraverso l'implementazione di una strategia defense-in-depth presuppone una gestione dei rischi attiva che tenga conto della propensione al rischio dell'organismo o dell'impresa. È importante, pertanto, che l'unità organizzativa responsabile dell'operatività e della manutenzione dei sistemi TIC conosca metodi e procedure della gestione dei rischi e sia in grado di applicarli in ambito TIC. La procedura per la gestione dei rischi TIC punta a rilevare e valutare possibili minacce suscettibili di mettere in pericolo sistemi TIC, applicazioni e dati da proteggere e a definire come comportarsi di fronte ai rischi individuati. La procedura si suddivide in tre parti: analisi, valutazione ed eliminazione dei rischi con l'adozione di misure pertinenti. Per verificare l'efficacia delle misure, i rischi vengono sottoposti regolarmente a una nuova valutazione che ne rileva eventuali modifiche. Se necessario le misure definite vengono aggiornate.

Ciononostante è impossibile garantire una sicurezza assoluta. La direzione dell'organismo o dell'impresa deve pertanto stabilire quanti rischi è disposta ad assumere.

1.6 Elementi di una strategia defense-in-depth

1.6.1 Panoramica

La strategia di sicurezza TIC va impostata in modo da proteggere gli strumenti sensibili necessari a realizzare le attività operative. Ciò presuppone un approccio stratificato, noto a livello internazionale come «defense-in-depth». Consiste nell'impiego coordinato di più misure di sicurezza atte a proteggere in un organismo o in un'impresa gli strumenti operativi TIC. La strategia si basa su un principio militare, secondo cui per il nemico è più difficile superare un sistema difensivo complesso e stratificato rispetto a un'unica barriera. Nel contempo analizza metodi e procedure dei potenziali attaccanti per preparare opportuni dispositivi di difesa. Nell'ambito della sicurezza TIC, l'obiettivo della strategia defense-in-depth è riconoscere violazioni della sicurezza TIC e ridurne o attenuarne le conseguenze, adottando un approccio olistico che cerca di proteggere tutti gli strumenti operativi (TIC) da qualsiasi tipo di rischio. Le risorse dell'organismo o dell'impresa vanno utilizzate in modo da garantire una protezione efficace da rischi noti e tenere ampiamente sotto controllo quelli potenziali. Le relative misure devono essere adeguate a proteggere l'integralità dei sistemi TIC, inclusi quindi persone, procedure, oggetti, dati e apparecchiature. Un attaccante rappresenta una minaccia per un sistema TIC nel momento in cui riesce a sfruttare un punto debole di uno di questi elementi. Organismi o imprese sono pertanto tenuti a monitorare costantemente le misure e ad adeguarle, qualora necessario, a nuove minacce.

1.6.2 Sistemi di controllo industriali (Industrial control systems, ICS)

A causa della complessa architettura degli ICS, eventuali vulnerabilità possono, nella peggiore delle ipotesi, non essere individuate per molto tempo e i relativi «exploit» rappresentare una minaccia (cosiddetta advanced persistent threat, APT). L'applicazione della strategia defense-in-depth, menzionata in precedenza, offre una protezione adeguata contro queste minacce.

Nel seguito sono riportati alcuni tipici metodi di attacchi agli ICS:

- attacchi da Internet che prendono di mira ICS accessibili online con lo scopo di accedervi durevolmente a distanza;
- attacchi a distanza a ICS che utilizzano dati di accesso rubati;
- attacchi a ICS che sfruttano punti deboli dell'interfaccia web;
- immissione di malware negli ICS tramite supporti dati compromessi (p. es. USB-stick, smartphone ecc.);
- attacchi alla struttura informatica degli uffici (p. es. tramite phishing mail, infezioni drive-by ecc.), con lo scopo di accedere agli ICS attraverso eventuali interfacce.

In linea di massima, in relazione all'applicazione della strategia defense-in-depth sussistono differenze importanti tra struttura informatica degli uffici e un ICS. La tabella 1 riporta i settori tematici pertinenti per la sicurezza e la loro importanza per TIC e ICS.

Il tema della sicurezza	TIC (p.e s. info degli uffici)	ICS (p.es. controllo centrali nucleari)
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 apparecchi o a livello d'organismo o impresa.	Il fabbisogno di memoria e i ritardi nello scambio di dati dovuto allo scan del 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. Le soluzioni antivirus, inoltre, richiedono spesso in un ambiente ICS cartelle «eccezione» per evitare che dati operativi sensibili vengano posti in quarantena.
Aggiornamenti di sicurezza (Update management)	Definiti chiaramente, applicati a livello d'organismo o impresa, automatizzati tramite accesso a distanza.	Tempi lunghi di preparazione e pianificazione sino all'installazione dei patch; sempre specifici per fabbricante; possono disattivare (temporaneamente) l'ICS. Necessità di definire un rischio accettabile.
Ciclo di vita tecnologico (Technology support lifecycle)	2–3 anni, più operatori, sviluppo e upgrade continui.	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.
Metodi di test e audit (Testing and audit methods)	Impiego di metodi aggiornati (ev. automatizzati). I sistemi sono in genere sufficientemente resilienti e affidabili per consentire assessment mentre sono operativi.	L'elevato grado di sviluppo individuale, per esempio, rende i metodi di assessment automatizzati probabilmente inidonei. Durante un assessment la probabilità che un errore si verifichi è più elevata. Gli assessment durante l'operatività del sistema, pertanto, sono tendenzialmente più difficili.
Change management	Pianificato correntemente e a cadenza regolare. Definito in base alle direttive dell'organismo o dell'impresa, per una durata minima/massima.	Procedura complessa con potenziali conseguenze sulla loro operatività. Necessità di una pianificazione strategica individuale.
Classificazione asset (Asset classification)	Eseguita abitualmente e annualmente. Spese/Investimenti vengono pianificati in base ai risultati.	Viene eseguita solo se necessario/disposto. 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. Secondo le circostanze, necessità di attenersi a norme regolatorie (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 rinforzati).	In genere sicurezza fisica molto buona.
Sviluppo sicuro del sistema (Secure software development)	Parte integrale del processo di sviluppo.	Gli ICS sono stati concepiti storicamente come sistemi fisici isolati. La sicurezza come parte integrale dello sviluppo del sistema è pertanto poco diffusa. In questo ambito gli operatori ICS hanno fatto progressi, più lenti tuttavia rispetto a quello TIC. Gli elementi centrali degli ICS non consentono spesso soluzioni di sicurezza successive o queste non sono disponibili.
Direttive di sicurezza	Direttive regolatorie generali, legate al settore (non esistono per tutti i settori).	Direttive regolatorie specifiche, legate al settore (non esistono per tutti i settori).

Tabella 1: differenze fra IT e ICS

In sede di applicazione di una strategia defense-in-depth vanno considerati in un ICS i seguenti aspetti:

- i costi per garantire la sicurezza di vecchi sistemi rispetto a nuove esigenze;
- la crescente tendenza a collegare ICS con reti di business;
- la possibilità di consentire a utenti attacchi a distanza in ambito sia TIC sia ICS;
- la necessità di dover fare affidamento sulla propria catena di fornitori (supply chain);
- le attuali possibilità di controllare e proteggere procedure specifiche per ICS;
- la possibilità di mantenersi regolarmente aggiornati su nuove minacce nei confronti degli ICS.

La strategia defense-in-depth rende più difficili gli attacchi diretti ai sistemi TIC e aumenta la probabilità di individuare in tempo utile un comportamento sospetto o inabituale all'interno del sistema. Consente inoltre di costituire zone separate in cui implementare tecnologie in grado di individuare intrusioni in un sistema (intrusion detection technology). Gli elementi tipici di questa strategia sono riportati nella tabella 2.

Elementi di una strategia defense-in-depth	
Programma di gestione dei rischi	• Individuazione di rischi per la sicurezza • Profilo del rischio • Gestione accurata della disponibilità di strumenti operativi TIC
Architettura della cybersicurezza	• Standard / Raccomandazioni • Direttive • Modalità
Sicurezza fisica	• Protezione di terminali • Centro di controllo, controllo degli accessi • Videocontrollo, controllo degli accessi e barriere
Architettura di rete	• Tipiche zone di sicurezza • Demilitarized Zones (DMZ) • Virtual LAN
Sicurezza del perimetro di rete	• Firewall • Accesso a distanza e autentificazione • Jump server / Host
Sicurezza host	• Gestione patch e punti deboli • Terminali • Apparecchi virtuali • Indurimento
Controllo sicurezza	• Intrusion detection systems • Registrazione audit di sicurezza • Evento di sicurezza e controllo evento • System Monitoring • EDR/XDR
Vendor management	• Controllo e gestione catene di fornitori • Managed services e outsourcing • Uso di servizi cloud
L'elemento umano	• Direttive • Modalità • Esercizio e percezione

Tabella 2: elementi di una strategia defense-in-depth

1.6.3 Gestione rischi

1.6.3.1 Programma di gestione dei rischi

Per applicare una strategia defense-in-depth è necessario capire i rischi operativi legati a minacce TIC cui un organismo o un'impresa possono essere soggetti. Questi rischi vanno gestiti in relazione alla propensione dell'organismo o dell'impresa ad assumerli. I responsabili dell'esercizio e della manutenzione di sistemi TIC devono essere in grado di riconoscere, valutare e indirizzare i cyberrischi. Devono inoltre capire in che modo questi metodi vanno applicati nel rispettivo ambiente di sistema. Ciò presuppone la capacità di avere un quadro chiaro dei possibili scenari di minacce, delle procedure tecniche e operative e delle tecnologie utilizzate. Solo così è possibile integrare nella normale attività professionale quotidiana una strategia defense-in-depth. È compito della direzione di un organismo o di un'impresa definire la «sicurezza» come condizione per tutte le attività informatizzate.

I principi di gestione dei rischi citati in precedenza hanno validità generale. Varie applicazioni TIC, tuttavia, rivestono un'importanza particolare legata alla loro criticità. Fra queste rientrano soprattutto i sistemi di controllo industriali (industrial control systems, ICS). Un'architettura di sicurezza ICS efficace presuppone che i rischi di un organismo o di un'impresa vengano posti in relazione ai requisiti funzionali (operativi) dell'ICS. Questo approccio può riguardare anche il contesto fisico (p. es. protezione del perimetro situato intorno a centri di calcolo.) I responsabili delle decisioni a qualsiasi livello di un organismo o di un'impresa devono conoscere l'importanza dei cyebrrischi e partecipare attivamente alle procedure che ne regolano la gestione. Analisi regolari su sistemi, applicazioni e procedure selezionati, incluse le relative reti, sono indispensabili. Invitiamo pertanto a effettuarle sulla base di severe direttive utilizzando un approccio strutturato e sistematico.

1.6.3.2 Framework di gestione dei rischi

Le analisi dei rischi TIC vanno inserite in un framework di gestione dei rischi ed effettuate regolarmente per elementi chiaramente definiti, come impianti, procedure e applicazioni sensibili (anche in fase di sviluppo) e loro dipendenze da altri sistemi, reti e servizi.

L'obiettivo è attribuire la gestione dei rischi individuati alle persone/ai titolari competenti, con l'incarico di monitorarli e valutarli e di attuare le opportune misure per mantenerli entro limiti accettabili precedentemente definiti (= propensione al rischio).

1.6.3.3 Analisi dei rischi

L'ambito oggetto dell'analisi dei rischi TIC va definito chiaramente. Devono inoltre essere descritti procedure operative, elementi tecnici e possibili fattori esterni, il che equivale a fissare contenuti e limiti dell'analisi.

1.6.4 Analisi del business impact

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

Serve inoltre a stabilire quali effetti sulla sua operatività l'organismo o l'impresa sono disposti ad assumere 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.

1.6.5 Misure

Le misure descritte in un'analisi di business impact vanno individuate, verificate e approvate. Devono essere autorizzate dalla direzione insieme con i piani che ne definiscono le esatte modalità.

In questo contesto è necessario tenere presente che il rischio rimanente va rilevato per tutte le risorse dell'organismo o dell'impresa nell'ambiente pertinente e gestito in maniera opportuna (p.es. attenuato, evitato, trasferito o accettato) in base alla propensione al rischio.

Per ogni risorsa individuale (asset) viene così stabilito il rischio massimo ammesso, in modo da poter calcolare i rischi TIC (cumulati).

1.6.6 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 defense-in-depth. Il suo obiettivo, inoltre, è consentire di acquisire informazioni sul flusso di dati fra sistemi e loro connessioni. L'architettura della cybersicurezza va coordinata con l'inventario degli impianti e degli strumenti TIC per assicurare che i flussi di informazioni vengano recepiti in modo unitario all'interno dell'organismo o dell'impresa.

Deve inoltre essere in sintonia con il NIST Framework Core. L'architettura della cybersicurezza tiene conto della protezione della confidenzialità, integrità e disponibilità di dati, servizi e sistemi. Per realizzarla deve essere messo a punto un piano di implementazione in linea con la cultura dell'organismo o dell'impresa e gli obiettivi strategici, che integri nel contempo in modo adeguato le esigenze di sicurezza includendo le risorse necessarie. In genere l'architettura della cybersicurezza viene completata da un piano di attività che individua i risultati attesi (indicazioni e spunti per ulteriori verifiche e orientamenti), definisce tempistiche di progetto, fornisce stime sulle risorse necessarie e identifica importanti fattori di dipendenza.

1.6.7 Sicurezza fisica

Le misure di sicurezza fisiche riducono il rischio di perdite involontarie o intenzionali o di danni alle risorse TIC dell'organismo o dell'impresa o del loro ambiente. Fra le risorse che vanno protette rientrano beni fisici come apparecchi e impianti, l'ambiente, il contesto operativo in senso lato e la proprietà intellettuale, compresi dati proprietari come impostazioni di procedure e informazioni dei clienti. I controlli fisici di sicurezza devono rispondere spesso a requisiti specifici in materia di ambiente, sicurezza, regolazione, diritto e altro. Gli organismi o le imprese devono adattare questi controlli, così come quelli tecnici, alle esigenze di protezione. Per garantire una protezione più ampia si include anche quella delle componenti TIC (= security) e dei dati d'ambiente connessi con le TIC. La sicurezza di numerose infrastrutture TIC è strettamente legata alla sicurezza degli impianti (= safety), con lo scopo di tenere il personale al riparo da situazioni pericolose senza ostacolarne l'operatività o intralciarlo durante le procedure di emergenza. I controlli di sicurezza fisici sono costituiti da misure attive o passive che limitano concretamente l'accesso a tutte le componenti dell'infrastruttura TIC. Queste misure devono impedire fra l'altro:

- l'accesso non autorizzato a luoghi sensibili;
- modifiche, manipolazioni, furti o qualsivoglia asportazione o distruzione di sistemi, infrastrutture, interfacce di comunicazione o sedi esistenti;
- sorveglianza non autorizzata di impianti sensibili tramite osservazione visiva, fotografie o qualsiasi altro tipo di registrazione;
- introduzione / installazione di nuovi sistemi, infrastrutture, interfacce di comunicazione o altri hardware;
- introduzione non autorizzata di dispositivi (USB stick, wireless access point, buetooth o terminali mobili) destinati a effet tuare manipolazioni di hardware o avere altri effetti dannosi.

Per soddisfare i requisiti di sicurezza dell'informazione, l'infrastruttura operativa fisica, inclusi sistemi e dotazione di rete, apparecchiature per uffici (p.es. stampanti in rete e dispositivi multifunzionali) e impianti speciali (p.es. sistemi di controllo industriali) va protetta durante l'intero ciclo di vita, dall'acquisto (o leasing) alla manutenzione sino allo smaltimento;

lo stesso vale per terminali mobili (inclusi laptop, tablet e smartphone) e per i loro dati contro accesso non autorizzato, perdita e furto, tramite configurazione delle impostazioni di sicurezza, limitazione d'accesso, installazione di software di sicurezza e gestione centrale delle apparecchiature.

1.6.8 Gestione del ciclo di vita degli hardware

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

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

1.6.9 Configurazione di dispositivi mobili

Per proteggere i dati da accesso non autorizzato, perdita e furto, i terminali 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 d'informazione di dati memorizzati o trasferiti su terminali mobili anche in caso di perdita o furto.

1.6.10 Sistemi di controllo industriali

I sistemi di controllo industriali «industrial control system» (ICS), devono essere monitorati e controllati in funzione della necessità di essere protetti. In particolare per garantire la sicurezza di procedure pertinenti ai fini dell'approvvigionamento, questi sistemi devono essere protetti in modo particolare.

1.6.11 Architettura della rete ICS

Nel definire un'architettura di rete si raccomanda in genere di separare le reti ICS da quelle dell'organismo o dell'impresa. Il traffico di dati su queste due reti presenta infatti alcune differenze. Acceso internet, FTP, e-mail e accesso remoto vengono in genere autorizzati nella rete dell'organismo o dell'impresa, ma non in quella ICS. Se vengono trasferiti sulla rete dell'organismo o dell'impresa, i dati possono essere captati o esposti ad attacchi DDoS o man-in-the-middle. Separare la connessione tra rete dell'organismo o dell'impresa e rete ICS o limitarla considerevolmente può ridurre i problemi di sicurezza o di performance.

1.6.12 Perimetro di sicurezza della rete ICS

I costi di un'installazione ICS e il mantenimento di un'infrastruttura di rete omogenea richiedono spesso la necessità di 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 ridurre al minimo il numero delle connessioni (se possibile solo alcune) e di stabilirle tramite un firewall e una DMZ (segmento di rete separato). I server ICS che contengono dati della rete dell'organismo o dell'impresa vanno collocati in una DMZ. I collegamenti esterni devono essere noti e il loro accesso limitato al minimo tramite firewall. Lo scambio di dati può essere monitorato e plausibilizzato ulteriormente mediante sistemi in grado di individuare anomalie.

1.6.13 Sicurezza host

A livello di stazioni host e di lavoro va aggiunto un ulteriore strato di sicurezza. I firewall proteggono la maggior parte degli apparecchi da intrusioni esterne. Un modello di sicurezza valido richiede tuttavia la presenza di vari strati difensivi. Per essere completa, la sicurezza della rete deve includere anche quella degli host. Lo strato destinato alla sicurezza degli host deve consentire all'utente di utilizzare vari sistemi operativi e applicazioni dell'organismo o dell'impresa garantendo nel contempo la protezione degli apparecchi.

Ciò implica la necessità di mettere a punto un progetto di direttive per le password di tutti gli utenti di un sistema e di rinominare gli account noti (tra cui quello di «amministratore»). Gli utenti possono tuttavia vanificare rigide direttive conservando le password in luogo non sicuro (p.es. su fogli per appunti) o continuare a utilizzarne di simili. La complessità delle disposizioni sulle password deve essere corrispondente al livello di autorizzazione degli utenti. Eventualmente possono anche essere definiti cicli per la modifica delle password.

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

- installazione e configurazione di un firewall basato su host;
- impostazione del salvaschermo con brevi intervalli e inviti a inserire la password;
- i sistemi operativi devono disporre di patch e i firmware essere aggiornati:
- la configurazione dei log deve essere attivata su tutti gli apparecchi;
- servizi e account non utilizzati devono essere disattivati;
- servizi non sicuri come Telnet, Remote Shell o rlogin vanno sostituiti con alternative sicure come SSH;
- gli utenti non devono essere in grado di disattivare i servizi;
- i backup dei sistemi vanno effettuati e verificati, in particolare se non gestiti centralmente;
- i moduli di sicurezza messi a disposizione dai sistemi operativi, come gli scanner di sicurezza, devono essere attivati o sostituiti con software adeguati;
- le medesime direttive si applicano anche a laptop e altri apparecchi mobili non costantemente collegati con la rete dell'impresa; l'hardisk di tutti i terminali mobili, infine, va codificato.

1.6.14 Monitoraggio sicurezza

L'impiego di sistemi di monitoraggio e componenti di rete che riconoscono comportamenti anomali e signature (firme d'attacco) rendono ancora più complesso l'ambiente IT o ICS. Le funzioni di controllo e riconoscimento, tuttavia, sono indispensabili per la strategia defense-in-depth destinata a proteggere gli strumenti operativi sensibili. Per proteggere asset critici da accessi non autorizzati, non è sufficiente creare un confine elettronico intorno alla rete ICS. Secondo la strategia defense-in-depth va predisposto un sistema di monitoraggio in grado di avvisare l'organismo o l'impresa in caso di un evento di sicurezza. La maggior parte degli organismi o delle imprese dispongono di una specie di monitoraggio standard nell'ambiente IT, che tuttavia non utilizzano il più delle volte nelle reti ICS.

È pertanto indispensabile:

- effettuare audit approfonditi, indipendenti e regolari sulle condizioni di sicurezza (ambienti operativi critici, procedure, applicazioni e sistemi / reti di supporto);
- tenere sotto controllo i rischi dell'informazione, rispettare gli elementi di sicurezza pertinenti previsti dal contesto giuridico, regolatorio e contrattuale e presentare sistematicamente alla direzione un resoconto sulla sicurezza dell'informazione.

1.6.15 Strategia di sicurezza dell'informazione

Definire, perseguire e controllare un'ampia strategia di sicurezza dell'informazione consente alla direzione di stabilire direttive chiare e di fruire di un supporto nell'attuazione di norme e nella gestione di rischi.

1.6.16 Gestione fornitori

Include l'individuazione e la gestione dei rischi dell'informazione in relazione a operatori esterni (fornitori di hardware e software, operatori di servizi in outsourcing e di servizi cloud ecc.). L'introduzione in contratti formali di esigenze di sicurezza a livello d'informazione punta a una riduzione dei rischi.

1.6.17 L'elemento umano

Le manipolazioni errate causate dall'essere umano sono un altro delicato aspetto che organismi o imprese devono gestire. Sia quelle intenzionali sia quelle dovute a ingenuità non possono mai essere completamente escluse malgrado l'adozione di misure tecniche. Più il personale è inesperto o non qualificato, più ne si è soggetti. Anche la lotta ad attività di collaboratori interni malintenzionati costituisce una sfida supplementare. La necessità di confrontarsi con questi aspetti obbliga organismi o imprese a confrontarsi con i seguenti temi.

1.6.17.1 Ciclo occupazionale del personale

La sicurezza dell'informazione deve essere considerata parte dell'intero ciclo occupazionale, dall'assunzione sino all'uscita del personale. Include misure pertinenti ai fini della sicurezza, come quelle previste in sede di consegna degli strumenti di lavoro (hardware, accesso ai sistemi) o disposte per l'ingresso a edifici/locali e le responsabilità che ne conseguono a livello di protezione. Il relativo programma di formazione per il personale ha un duplice obiettivo: sensibilizzare maggiormente alla sicurezza e definire il comportamento da adottare. L'organismo o l'impresa devono documentare lo stadio di avanzamento e lo svolgimento dei relativi 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 dell'informazione.

1.6.17.2 Istruzioni / Direttive

Istruzioni e direttive per il personale chiare e attuabili ne regolano il comportamento in relazione ad aspetti pertinenti per la sicurezza. Definiscono condizioni quadro e consentono di effettuare controlli allo scopo di proteggere i sistemi e attuare le direttive in vigore. Stabiliscono inoltre procedure e specificano le attese dell'organismo o dell'impresa nei confronti del suo personale. Istruzioni e direttive definiscono ciò che va rispettato e le sanzioni in caso di violazioni.

1.6.17.3 Procedure

La gestione della sicurezza è di competenza dell'unità IT ed è strutturata in procedure. La sua funzione è proteggere informazioni e dati dell'organismo o dell'impresa. Questi ultimi sono tenuti ad applicare anche ai sistemi di controllo industriali le procedure di gestione della sicurezza, che includono la definizione di processi, le modalità di attuazione o la configurazione di un determinato sistema. Le procedure devono essere standard e ripetibili al fine di garantire la medesima formazione anche al nuovo personale e di assicurare che tutti gli standard e le disposizioni siano noti. Le procedure per riconoscere un cyberevento (intrusion detection) sono particolarmente importanti. Altrettanto dicasi per quelle di sicurezza basate su rete in relazione a protocolli del fabbricante e sistemi di legacy.

1.6.17.4 Mansioni e responsabilità in ambienti operativi critici

Le mansioni e le responsabilità nell'ambito di procedure, applicazioni (inclusi sistemi / reti di supporto), informazioni e ambienti operativi critici dovrebbero essere chiaramente definite e assegnate a persone competenti, con l'obiettivo di sensibilizzare il personale alla propria responsabilità individuale. Questa cultura contribuisce a fare in modo che ciascuno svolga le proprie mansioni tenendo conto della sicurezza dell'informazione.

1.6.17.5 Comunicazione / Programma di security awareness

Questo programma e le relative misure di comunicazione promuovono un atteggiamento consapevole e auspicato dell'intero personale in tutti i livelli gerarchici dell'organismo o dell'impresa.

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

1.7 NIST Framework

Il NIST framework e le sue raccomandazioni puntano a mettere a disposizione dei gestori di infrastrutture critiche e di altri organismi o imprese legati alle TIC uno strumento grazie al quale aumentare in autonomia e sotto la loro responsabilità la resilienza nei confronti dei rischi sulla sicurezza. Si basa su una selezione di standard, direttive e best practice esistenti e non è vincolato all'uso di una determinata tecnologia.

1.7.1 NIST Framework Core

Il NIST Framework Core è basato sui rischi. Si compone di cinque funzioni:

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

1.7.2 Implementation tiers

Il NIST Framework prevede quattro implementation tiers («livelli»), che descrivono quelli (in termini di protezione) già realizzati dall'impresa. Questi livelli vanno da parziale (tier 1) a dinamico (tier 4). Per definire il suo livello di sicurezza (tier level), un organismo o un'impresa devono conoscere esattamente le proprie pratiche di gestione dei rischi, l'ambiente ostile, i requisiti giuridici e regolatori, gli obiettivi di business e le direttive organizzative.

2 Seconda parte: standard minimo TIC

2.1 Panoramica

Questo capitolo descrive le mansioni previste per l'attuazione dello standard minimo TIC, suddivise secondo le cinque funzioni del NIST Framework Core (cfr. 1.7.1): identificare, proteggere, intercettare, reagire e ripristinare. Le denominazioni originali inglesi del NIST Framework Core sono riportate ogni volta. Le mansioni (cfr. tabella sottostante) sono ripartite nelle seguenti categorie:

le prime due lettere (p.es. «ID»=«identify») indicano una delle cinque funzioni; la seconda coppia di lettere indica la categoria (p.es. «AM»=«asset management»); Il numero, invece, contrassegna la singola mansione. All'interno della categoria le mansioni vengono numerate ininterrottamente. Esempio: «ID.AM-1» equivale alla prima mansione della categoria «asset management» della funzione «identify».

A ogni tabella con le mansioni del NIST Framework Core ne viene aggiunta una con i riferimenti ad altri standard TIC internazionali. Le tabelle si riferiscono sempre alla rispettiva categoria, p.es. «asset management». Questa soluzione facilita la classificazione agli utenti che strutturano le mansioni di sicurezza TIC secondo altri standard.

2.2 Identificare (Identify)

2.2.1 Gestione dell'inventario (Asset management)

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	Le risorse (ad esempio, hardware, dispositivi, dati, tempo, personale e software) vengono classificate in base alla loro classificazione, criticità e valore aziendale.
ID.AM-6	Vengono stabiliti i ruoli e le responsabilità in materia di cybersecurity per l'intera forza lavoro e per gli stakeholder terzi (ad esempio, fornitori, clienti, partner).

Tabella 3: mansioni ID.AM

Standard	Riferimento
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2022	A.5.2, A.5.3, A.5.9, A.7.9, A.5.12, A.5.14 A.5.32, Clause 7.1, Clause 7.2
NIST-SP-800-53 Rev. 5	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-20, PS-7, PM-2, PM-5, PM-29, SA-17, SC-6, RA-9
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193

Tabella 4: riferimenti ID.AM

2.2.2 Ambiente operativo (Business environment)

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	Catalogate tutti i sistemi TIC esterni pertinenti per il vostro organismo o la vostra impresa.
ID.BE-5	I requisiti di resilienza per supportare l'erogazione dei servizi critici sono stabiliti per tutti gli stati operativi (ad esempio, in caso di stress/attacco, durante il recupero, durante le normali operazioni).

Tabella 5: mansioni ID.BE

Standard	Riferimento
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2022	A.5.19, A.5.21, A.5.23, A.5.24, A.5.28, A.5.29, A.5.30, A.5.31, A.5.33, A.5.37, A.6.2, A.7.11, A.7.12, A.7.5, A.8.14, A.8.6, A.8.30, Clause 4.1
NIST-SP-800-53 Rev. 5	CP-2, CP-8, PM-8, PM-11, PE-9, PE-11,RA-9, SA-20, SR-1, SR-2, SR-3
BSI 100-2	B 1.11, M 2.256, B 2.2, B 2.12, M 2.214

Tabella 6: riferimenti ID.BE

2.2.3 Direttive (Governance)

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

Definizione	Mansione
ID.GV-1	La politica di cybersecurity dell'organizzazione viene stabilita e comunicata.
ID.GV-2	Ruoli e responsabilità nel settore della sicurezza dell'informazione 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 soddisfino 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 7: mansioni ID.GV

Standard	Riferimento
COBIT 5	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, DSS04.02
ISA 62443-3:2013	
ISO 27001:2022	A.5.1, A.5.19, A.5.30, A5.31, A.6.2, A.6.6, A.8.27, A.8.30 A15.1.1, Clause 6
NIST-SP-800-53 Rev. 5	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PM-2, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, PM-29, RA-1, RA-2, RA-3, SA-2, PS-7, PS-9
BSI 100-2	M 2.192, M 2.193, M 2.336, B 1.16

Tabella 8: riferimenti ID.GV

2.2.4 Analisi dei rischi (Risk assessment)

L'organismo o l'impresa conoscono 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 9: mansioni ID.RA

Standard	Riferimento
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2022	A.5.37, A.5.6, A.5.7, A.6.1, A.8.12, A8.14, A.8.16, A,8.2, A.8.3, A.8.7, A.8.8, Clause 6.1.2, Clause 6.1.3, Clause 8, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	CA-2, CA-5, CA-7, CA-8, CP-2, PM-4, PM-9, PM-11, PM-12, PM-15, PM-16, PM-28, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, SA-5, SA-11, SI-2, SI-4, SI-5
BSI 100-2	M 2.35, M 2.199, M 2.546

Tabella 10: riferimenti ID.RA

2.2.5 Strategia di gestione dei rischi (Risk management strategy)

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 11: mansioni ID.RM

Standard	Riferimento
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2022	A.6.1, A.8.2, A.8.3, Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	PM-8, PM-9, PM-11, SA-14

Tabella 12: riferimenti ID.RM

2.2.6 Gestione dei rischi della catena di fornitori (Supply chain riskmanagement)

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	I fornitori e i partner terzi di sistemi informativi, componenti e servizi vengono identificati, classificati e valutati utilizzando un processo di valutazione del rischio della catena di approvvigionamento informatico.
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 fornitori.
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.

Tabella 13: 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, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
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 7
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-12, SA-14, SA-15, SA-11, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
BSI	B 1.11, B 1.17, M 2.256, B 1.3

Tabella 14: riferimenti ID.SC

2.3 Proteggere (Protect)

2.3.1 Gestione dell'inventario (Asset management)

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.
PR.AC-7	Gli utenti, i dispositivi e le altre risorse sono autenticati (ad esempio, a un solo fattore o a più fattori) in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy degli individui e altri rischi organizzativi).

Tabella 15: mansioni PR.AC

Standard	Riferimento
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03
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
ISO 27001:2022	A.5.14, A.5.15, A.5.16, A.5.17, A.5.18, A.5.21,A.5.22, A.5.23, A.5.3, A.5.34, A.6.1, A.6.7, A.7.1, A.7.2. A.7.3, A.7.4, A.7.5, A.7.6, A.7.9, A.8.1, A.8.5, A.8.11, A.15, A.8.16, A.8.18, A.8.2, A.8.3, A.8.5, A.8.20, A.8.22, A.8.27, A.8.31
NIST-SP-800-53 Rev. 5	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, SC-7, SC-10, SC-20, PS-3
BSI	M 2.30, M 2.220, M 2.11, M 4.15, M 1.79, M 2.17, B 2.2, B 2.12, B 5.8, B 4.1, M 2.393, M 2.5, B 1.18, M 2.220, M 2.8, M 4.135, B 4.1, M 5.77, M 2.393, M 2.5, M 3.33, M 2.31,

Tabella 16: riferimenti PR.AC

2.3.2 Sensibilizzazione e formazione

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 dell'informazione siano consapevoli del loro ruolo e delle loro responsabilità particolari.

Tabella 17: mansioni PR.AT

Standard	Riferimento
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS06.03, APO07.03, APO10.04, APO10.05
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2022	A.5.19, A.5.2, A.5.4, A.6.2, A.6.3, A.6.6, A. 7.2, A.7.3, A.7.6, A.8.18, A.8.2, A.8.3, A.8.30, Clause 5.1, Clause 5.3
NIST-SP-800-53 Rev. 5	AT-2, AT-3, CP-3, IR-2, PM-13, PM-14, PS-7, SA-9
BSI	M 2.193, B 1.13

Tabella 18: riferimenti PR.AT

2.3.3 Sicurezza dati (Data security)

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 19: mansioni PR.DS

Standard	Riferimento
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
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
ISO 27001:2022	A.5.7, A.5.10, A.5.13, A.5.14, A.5.15, A.5.23, A.5.24, A.5.29, A.5.33, A.5.34, A.6.1, A.6.2, A.6.5, A.6.6, A.7.5, A.7.8, A.7.9, A.7.10, A.7.14, A.8.1, A.8.11, A.8.12, A.8.13, A.8.14, A.8.16, A.8.18, A.8.19, A.8.2, A.8.20, A.8.22, A.8.23, A.8.24, A.8.26, A.8.28, A.8.29, A.8.31, A.8.34, A.8.3, A.8.4, A.8.6, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AC-5, AC-6, AU-4, AU-13, CM-2, CM-8, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, CP-2, PE-11, PE-16, PE-19, PE-20, PS-6, SA, 10, SC-5, SC-7, SC-8, SC-11, SC-28, SI-4, SI-7, SI-10
BSI	M 2.217, B 4.1, M 2.393, B 5.3, B 5.4, B 5.21, B 5.24, B 1.7, M 2.3, B 1.15, M 5.23, M 3.33, M 2.226, M 3.2, M 3.6, B 1.18, M 2.220, M 2.8, M 4.135, M 4.494, M 5.77, M 2.393, B 5.3, M 3.55, B 5.4, B 5.21, B 5.24, B 1.7, B 1.6, B 1.9, B 5.4, B 5.21, B 5.24, M 2.62, M 2.4

Tabella 20: riferimenti PR.DS

2.3.4 Protezione di dati (Information protection processes and procedures)

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 dell'informazione 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 21: mansioni PR.IP

Standard	Riferimento
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, DSS01.04, DSS05.05, BAI09.03, APO11.06, DSS04.05, DSS04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISA 62443-3:2013	SR 7.6
ISO 27001:2022	A.5.10, A.5.11, A. 5.19, A.5.24, A.5.26, A.5.27, A.5.29, A.5.30, A.5.31, A.5.33, A. 5.35, A.5.36, A.5.37, A.5.5, A.5.6, A.5.7, A.6.1, A.6.2, A.6.4, A.6.5, A.6.6, A.6.8, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14, A.7.5, A.7.8, A.5.8, A. 8.1, A.8.13, A.8.19, A.8.25, A.8.27, A.8.29, A.8.32, A.8.7, A.8.8, A.8.9, A.8.13, Clause 9, Clause 10
NIST-SP-800-53 Rev. 5	AC-21, CA-2, CA-7, CA-8, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, CP-1, CP-2, CP-4, CP-6, CP-7, CP-9, CP-10, IR-1, IR-3, IR-7, IR-8, IR-9, MP-6, PE-1, PL-2, PM-6, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-3, RA-5, SA-3, SA-4, SA-8, SA-10, SA-11, SA-21, SI-2, SI-4, SR-12
BSI	B 1.4, B 1.3, M 2.217, B 1.14, B 1.9, M 2.62, B 5.27, M 4.78, M 2.9, B 1.0, M 2.80, M 2.546, B 5.27, B 5.21, B 5.24

Tabella 22: riferimenti PR.IP

2.3.5 Manutenzione (Maintenance)

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 23: mansioni PR.MA

Standard	Riferimento
COBIT 5	BAI09.03, DSS05.04, APO11.04, DSS05.02, APO13.01
ISA 62443-3:2013	
ISO 27001:2022	A.5.14, A.5.15, A.5.19, A.5.22, A.6.7, A.7.13, A.8.2, A.8.9, A.8.15, A.8.16
NIST-SP-800-53 Rev. 5	MA-1, MA-2, MA-3, MA-4, MA-5, MA-6
BSI	M 2.17, M 2.4, M 2.218, M 2.4, B 1.11, B 1.17, M 2.256

Tabella 24: riferimenti PR.MA

2.3.6 Impiego di tecnologie di protezione (Protective technology)

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 25: mansioni PR.PT

Standard	Riferimento
COBIT 5	APO11.04, DSS05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.3, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, 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 27001:2022	A.5.14, A.5.15, A.5.18, A.5.29, A.5.30, A.5.34, A.5.37, A.8.11, A.8.13, A.8.14, A.8.15, A.8.16, A.8.20, A.8.21, A.8.22, A.8.2, A.8.3, A.8.34, A.8.5, A.8.6, A.8.9, A.9.2, A.5.10, A.6.7, A.7.10, A.7.14, A.8.13, A.8.24
NIST-SP-800-53 Rev. 5	AC-3, AC-4, AC-17, AC-18, AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16, CM-7, CP-7, CP-8, CP-11, CP-12, CP-13, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, PE-11, PL-8, SC-6, 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
BSI	B 5.22, M 2.500, M 2.220, M 2.64, M 4.227, M 2.64, B 1.18, B 4.1, M 2.393, B 1.3, B 2.4, B 2.9

Tabella 26: riferimenti PR.PT

2.4 Intercettare (Detect)

2.4.1 Anomalie ed eventi (Anomalies and events)

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 27: mansioni DE.AE

Standard	Riferimento
COBIT 5	DSS03.01, APO12.06
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 27001:2022	A.5.24, A.5.25, A.5.27, A.5.28, A.5.37, A.8.1, A.8.12, A.8.15, A.8.16, A.8.20, A.8.21, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AU-6, CA-3, CA-7, CM-2, CP-2, SI-4, AU-6, IR-4, IR-5, IR-8, SC-16, SI-4, RA-3, RA-5
BSI	B 1.8

Tabella 28: riferimenti DE.AE

2.4.2 Controllo (Security continous monitoring)

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	Vengono eseguite scansioni di vulnerabilità.

Tabella 29: mansioni DE.CM

Standard	Riferimento
COBIT 5	DSS05.01, DSS05.07, APO07.06, BAI03.10
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2022	A.5.14, A.5.15, A.5.18, A.5.19, A.5.21, A.5.23, A.5.7, A.6.7, A.7.1, A.7.2, A.7.4, A.7.8, A.7.9, A.8.1, A.8.11, A.8.12, A.8.15, A.8.16, A.8.19, A.8.2, A.8.20, A.8.21, A.8.23, A.8.28, A.8.3, A.8.30, A.8.5, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, PS-7, RA-5, SA-4, SA-9, SC-5, SC-7, SC-18, SC-44, SI-3, SI-4, SI-8
BSI	B 5.22, M 2.500, B 1.6, B 2.9, B 1.9, B 5.25, B 1.11, M 2.256, M 2.35

Tabella 30: riferimenti DE.CM

2.4.3 Procedure di intercettazione (Detection processes)

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 31: mansioni DE.DP

Standard	Riferimento
COBIT 5	DSS05.01, APO13.02, APO12.06, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2022	A.5.2, A.5.26, A. 5.27, A.5.3, A.5.35, A.5.4, A.6.3, A.6.8, A.7.4, A.8.12, A.8.15, A.8.16, A.8.17, A.8.27, A.8.6, A.8.7, A.8.8, A.8.9, Clause 5.3, Clause 7.2, Clause 9.2, Clause 10.1
NIST-SP-800-53 Rev. 5	AC-1, AT-1, AU-1, AU-6, CA-1, CA-2, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-1, PM-14, PS-1, PT-1, RA-1, RA-5, SA-1, SC-1, SI-1, SI-3, SI-4, SR-1, SR-9, SR-10
BSI	M 2.193, M 2.568, B 1.8

Tabella 32: riferimenti DE.DP

2.5 Reagire (Respond)

2.5.1 Piano di reazione (Response planning)

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 33: mansioni RS.RP

Standard	Riferimento
COBIT 5	BAI01.10
ISA 62443-3:2013	
ISO 27001:2022	A.5.26, A.5.28, A.5.29
NIST-SP-800-53 Rev. 5	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Tabella 34: riferimenti RS.RP

2.5.2 Comunicazione (Communications)

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	Il coordinamento con le parti interessate è coerente con i piani di risposta.
RS.CO-5	La condivisione volontaria delle informazioni avviene con gli stakeholder esterni per ottenere una più ampia consapevolezza della situazione della cybersicurezza.

Tabella 35: mansioni RS.CO

Standard	Riferimento
COBIT 5	
ISA 62443-3:2013	
ISO 27001:2022	A.5.2, A.5.24, A.5.26, A.5.3, A.5.30, A.5.37, A.5.5, A.5.6, A.6.3, A.6.8, A.7.4
NIST-SP-800-53 Rev. 5	AU-6, CP-2, CP-3, IR-3, IR-4, IR-6, IR-8, PM-15, SI-5
BSI	B 1.3, B 1.8, M 2.193

Tabella 36: riferimenti RS.CO

2.5.3 Analisi (Analysis)

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.
RS.AN-5	Vengono stabiliti processi per ricevere, analizzare e rispondere alle vulnerabilità divulgate all›organizzazione da fonti interne ed esterne (ad esempio, test interni, bollettini di sicurezza o ricercatori di sicurezza).

Tabella 37: mansioni RS.AN

Standard	Riferimento
COBIT 5	DSS02.07
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 27001:2022	A.5.19, A.5.25, A.5.26, A.5.27, A.5.28, A.5.35, A.5.5, A.5.6, A.6.3, A.8.15, A.8.16, A.10.2
NIST-SP-800-53 Rev. 5	AU-6, AU-7, CA-1, CA-2, CA-7, CP-2, IR-4, IR-5, IR-8, PE-6, PM-4, PM-15, RA-1, RA-3, RA-5, RA-7, SI-4, SI-5, SR-6
BSI	B 5.22, M 2.500, M 2.64, B 1.8

Tabella 38: riferimenti RS.AN

2.5.4 Diminuzione del danno (Mitigation)

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 39: mansioni RS.MI

Standard	Riferimento
COBIT 5	
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4, A.12.2.1, A.16.1.5
ISO 27001:2022	A.5.26, A.8.23, A.8.8
NIST-SP-800-53 Rev. 5	IR-4, CA-2, CA-7, RA-3, RA-5, RA-7
BSI	B 1.6, B 1.8, M 2.35

Tabella 40: riferimenti RS.MI

2.5.5 Miglioramenti (Improvements)

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 41: mansioni RS.IM

Standard	Riferimento
COBIT 5	BAI01.13
ISA 62443-3:2013	
ISO 27001:2022	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8
BSI	B 1.8

Tabella 42: mansioni RS.IM

2.6 Ripristinare (Recover)

2.6.1 Piano di ripristino (Recovery planning)

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 43: mansioni RC.RP

Standard	Riferimento
COBIT 5	DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2022	A.5.29, A.5.30, A.5.37
NIST-SP-800-53 Rev. 5	CP-10, IR-4, IR-8

Tabella 44: riferimenti RC.RP

2.6.2 Miglioramenti (Improvements)

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 45: mansioni RC.IM

Standard	Riferimento
COBIT 5	BAI05.07
ISA 62443-3:2013	
ISO 27001:2022	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8

Tabella 46: mansioni RC.IM

2.6.3 Comunicazione (Communications)

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 47: mansioni RC.CO

Standard	Riferimento
COBIT 5	EDM03.02
ISA 62443-3:2013	
ISO 27001:2022	A.5.24, A.5.26, A.5.5, A.6.3, Clause 7.4
NIST-SP-800-53 Rev. 5	CP-2, IR-4

Tabella 48: riferimenti RC.CO

3 Terza parte: incarico di verifica

3.1 Introduzione

Questo paragrafo descrive le modalità di verifica periodica della completezza e dell'efficacia delle misure adottate. L'esito della verifica deve tradursi in una dichiarazione sul grado di maturità della cybersicurezza, che consenta di effettuare un confronto a livello di settore o intersettoriale.

Le misure qui riportate per migliorare la resilienza TIC (cfr. capitolo 2) rimangono senza effetto se non vengono attuate da parte delle imprese. È importante che i responsabili recepiscano l'importanza del tema cybersicurezza, che collaboratori e partner siano sensibilizzati e che vengano pianificate e approvate sufficienti risorse attuative. Si suggerisce di effettuare la verifica del presente standard minimo almeno con cadenza annuale e di realizzare per quanto possibile rapidamente le misure necessarie a migliorare la resilienza.

La sicurezza non è una condizione che può essere raggiunta, bensì un processo da attuare, valutare, adeguare e migliorare costantemente. La cybersicurezza non può essere ignorata a lungo. Iniziate subito ad adottare opportune misure per migliorare la resilienza delle vostre risorse critiche TIC.

Ognuna delle mansioni riportate al capitolo 2 deve essere valutata fra 0 e 4 secondo lo schema qui sotto (cfr. 3.1.1). Queste valutazioni servono da riferimento per definire il tier level di un organismo o di un'impresa (cfr. capitolo 3.2).

3.1.1 Schema di valutazione delle mansioni

0 = non attuata
1 = parzialmente attuata, non definita e approvata completamente
2 = parzialmente attuata, definita e approvata completamente
3 = attuata, completamente o in gran parte attuata, statica
4 = dinamica, attuata, verificata costantemente, migliorata

3.2 Descrizione del tier level di un organismo o di un'impresa

I tier vanno da parziali (tier 1) a dinamici (tier 4) e descrivono un crescente grado di maturità. Gli organismi o le imprese devono definire il tier level che intendono raggiungere e garantire che sia in grado di concretizzare gli obiettivi organizzativi.

Le descrizioni dettagliate dei quattro tier level vengono illustrate nel prossimo paragrafo.

3.2.1 Tier 1: parziale

Il tier level 1 significa che le procedure di gestione dei rischi e le direttive organizzative per la sicurezza TIC non sono formalizzate e che i rischi TIC vengono abitualmente 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 dispongono in genere né di procedure atte a utilizzare congiuntamente al loro interno le informazioni sulla cybersicurezza né, spesso, in caso di rischi TIC, di procedure standard finalizzate allo scambio di informazioni o a una collaborazione coordinata con partner esterni.

3.2.2 Tier 2: informato sui rischi

Gli organismi o le imprese che si autoinseriscono nel tier level 2 dispongono in genere di procedure di gestione dei rischi TIC, che tuttavia non sono state concretizzate sotto forma di istruzioni operative. Sul piano organizzativo i rischi TIC sono integrati nella gestione aziendale dei rischi e tutti i livelli aziendali ne sono consapevoli. A mancare è invece in genere un approccio volto a gestire e migliorare la consapevolezza (awareness) di rischi TIC attuali e futuri. I processi e le procedure 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. Organismo o impresa sono consapevoli del proprio ruolo e comunicano con partner esterni sul tema della sicurezza (p.es. clienti, fornitori, operatori ecc.). Non esistono tuttavia procedure standard per la cooperazione e lo scambio di informazioni.

3.2.3 Tier 3: riproducibile

Gli organismi o le imprese del tier level 3 dispongono di piani di gestione dei rischi formalmente approvati e di istruzioni per applicarli al proprio interno. La gestione dei rischi TIC è definita in direttive con validità generale. I rischi TIC rilevati con criteri standard e le istruzioni per la loro gestione vengono regolarmente aggiornati tenendo conto sia delle esigenze operative sia dello sviluppo tecnologico e di un contesto delle minacce in continuo mutamento causa la presenza di nuovi soggetti o di un quadro politico in costante evoluzione.

Processi e procedure per la gestione di nuovi rischi sono definiti per iscritto. Per reagire a questi rischi vengono applicati metodi standard. Il personale dispone delle conoscenze e delle capacità necessarie per svolgere le proprie mansioni.

L'organismo o l'impresa sono consapevoli del proprio rapporto di dipendenza con i partner esterni e scambiano informazioni per consentire alla direzione di adottare decisioni con cui reagire agli eventi di cybersicurezza.

3.2.4 Tier 4: dinamico

Il tier level 4 indica che un organismo o un'impresa hanno interamente soddisfatto tutti i requisiti dei tier level 1 – 3 e verificano inoltre, migliorandoli se necessario, i propri metodi, capacità e procedure in base a una documentazione completa relativa a tutti gli eventi di cybersicurezza. L'organismo o l'impresa traggono le necessarie conclusioni dall'analisi degli eventi precedenti e adeguano in modo dinamico le proprie procedure e tecnologie in materia di sicurezza in funzione delle più recenti tecnologie o dei contesti di minacce. La gestione dei rischi TIC è parte integrante della cultura dell'organismo o dell'impresa. Le conclusioni tratte dagli eventi precedenti e le informazioni acquisite da fonti esterne e dal controllo permanente dei propri sistemi e reti vengono integrati continuamente nella procedura di gestione dei rischi. L'organismo o l'impresa comunicano regolarmente tali informazioni ai partner e dispone di procedure standard.

3.3 Valutazione dell'assessment con esempio

L'illustrazione seguente mostra a titolo di esempio una valutazione fittizia di tutte le mansioni descritte. L'assessment può essere svolto con l'aiuto di un file Excel scaricabile dal sito dell'Ufficio federale per l'approvvigionamento economico del Paese.

I diagrammi sottostanti forniscono all'utente informazioni sul grado di maturità della cybersicurezza nel suo organismo o nella sua impresa in ciascuna delle cinque categorie (ID-Identify, PR-Protect, DE-Detect, RS-Response, RC-Recover). Per ognuna tutte le mansioni sono state valutate tra 0 e 4 (linea colorata). La linea tratteggiata indica il valore medio di ciascuna categoria. Il diagramma in alto a sinistra (valutazione del grado di maturità della cybersicurezza) indica la valutazione complessiva costituita dai valori medi delle singole categorie.

Riporta esplicitamente esempi e non valori indicativi o di riferimento. Ogni organismo o impresa devono definire la propria propensione al rischio e stabilire così il rispettivo livello di protezione.

[9] https://www.bwl.admin.ch

Esempio della valutazione di un *assessment*

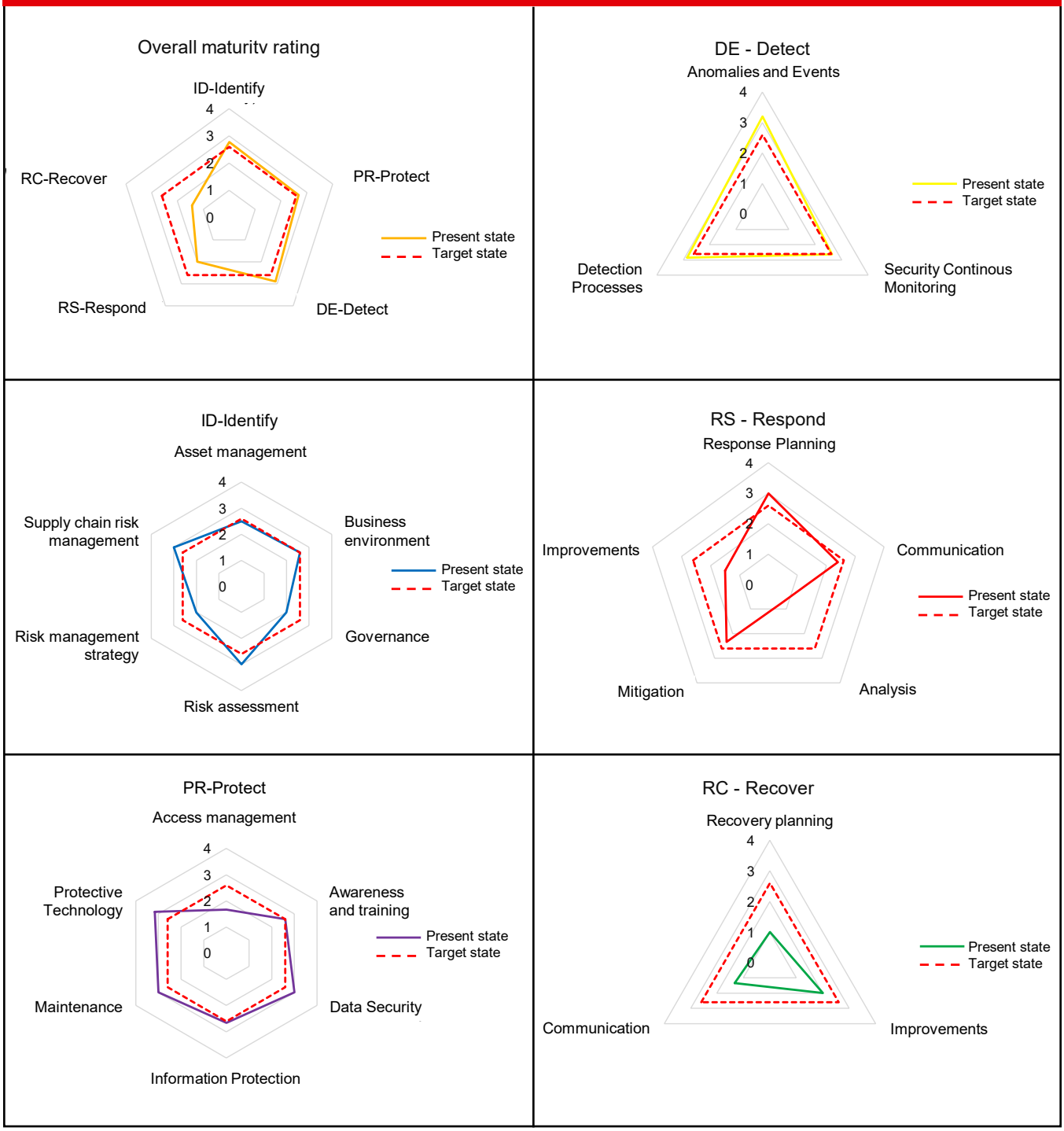

Illustrazione 1: Esempio della valutazione di un assessment

4 Allegato

4.1 Elenco delle illustrazioni

4.2 Elenco delle tabelle

4.3 Glossario

Nel seguito sono riportati termini che nell'ambito del presente documento presentano un significato specifico. Si rinuncia in questa sede a un elenco di termini generali in uso nel contesto TIC (p.es. hardware, software, backup ecc.).

Termine	Significato
Attacchi man-in-the-middle	Per attacco man-in-the-middle (attacco MTM) si intende una forma di attacco condotta in reti TIC. L'attaccante si trova fisicamente o – oggi per lo più – logicamente fra i due partner della comunicazione e tramite il suo sistema ha il controllo completo sul traffico di dati fra due o più utenti della rete e può vedere o addirittura manipolare a piacimento le informazioni.
Benchmarking	Il benchmark è un parametro di confronto. Indica l'analisi comparativa di procedure e risultati. Nel presente documento il confronto è esplicitamente riferito a organismi o imprese che puntano ad avere un livello di protezione simile.
Compromissione	Un sistema, una banca dati o anche un singolo set di dati vengono considerati compromessi qualora i dati potrebbero essere manipolati e il proprietario (o l'amministratore) del sistema non ha più il controllo sul corretto funzionamento o contenuto.
Configurazione di dispositivi mobili	Include tutte le misure e le impostazioni tecniche destinate a proteggere dati su apparecchi mobili (smartphone, laptop ecc.) anche in caso di loro smarrimento fisico.
Cyberattacchi	Comprendono tutte le attività condotte consapevolmente allo scopo di violare disponibilità, integrità o confidenzialità di dati.
Gestione del ciclo di vita degli hardware	Si tratta di un approccio globale per la gestione di hardware TIC per tutta la durata del loro impiego.
Infezione drive-by	Si intende l'infezione di un computer per mezzo di malware (p.es. virus, cavalli di Troia ecc.) per il tramite di una normale visita a una pagina web. Basta aprire una pagina infetta per trasmettere l'infezione sul proprio computer.
Infrastruttura critica	Lo spettro delle infrastrutture critiche (IC) include nove settori, suddivisi in 27 sotto-settori (rami). La panoramica completa è disponibile online su: https://www.babs.admin.ch/it/aufgabenbabs/ski/kritisch.html
Infrastruttura TIC	Tutti gli elementi della struttura informativa e delle telecomunicazioni di cui un organismo o un'impresa hanno bisogno per le loro procedure operative: desktop di pc, cellulari, centri di calcolo ecc.
Monitoraggio sicurezza	Descrive la procedura in base alla quale i flussi di dati e le attività nella propria rete sono sottoposti a costante osservazione con l'obiettivo di individuare in tempo utile comportamenti sospetti. A tale scopo vengono impiegati sistemi di monitoraggio sicurezza dedicati.

Termine	Significato
Perimetro di sicurezza della rete ICS	Riguarda la sicurezza nelle connessioni fra rete dell'organismo o dell'impresa e una rete pubblica come Internet. Il perimetro di sicurezza viene costituito tramite il perimetro dei firewall, che offre una prima protezione strategica contro gli attacchi.
Phishing mail	Questo termine (neologismo per fishing, ingl. per «pescare») indica i tentativi di accedere ai dati personali di un utente, e quindi a rubarne l'identità, attraverso siti, mail o brevi messaggi falsificati.
Programma di security awareness	Un programma di security awareness ha l'obiettivo di accrescere la sensibilità sui temi della sicurezza e di migliorare il rispettivo comportamento di collaboratori, partner, fornitori ecc.
Sicurezza host	Include tutte le misure di sicurezza applicate al terminale, come firewall o programmi antivirus.
Sistema di gestione sulla sicurezza dell'informazione (SGSI)	Un sistema di gestione sulla sicurezza dell'informazione (SGSI) è un sistema operativo in tutta l'impresa che garantisce il rispetto del livello di sicurezza e della continuità delle informazioni in modo efficace e duraturo.
Sistemi di controllo industriali	È un termine generale per indicare tutti gli elementi utilizzati per gestire e controllare impianti o procedure industriali. Un sistema di controllo industriale include in genere sensori, centri di calcolo, sale di controllo, cavi e impianti. I termini inglesi «Industrial control system, ICS» e «Supervisory control and data acquisition system, SCADA» vengono utilizzati come sinonimi.
Sistemi di intrusion detection	Un sistema di intrusion detection è un sistema che intercetta attacchi indirizzati verso un sistema di computer o una rete. L'IDS può completare un firewall o essere inserito direttamente nel sistema di computer da sorvegliare.
Sistemi di legacy	I sistemi di legacy sono sistemi superati che, per un motivo qualsiasi, non sono ancora sostituibili. Possono costituire un rischio particolare e richiedono pertanto misure di protezione.

Organizzazione del progetto

Committente del progetto
Werner Meier, Ufficio federale per l'approvvigionamento economico del Paese Delegato

Direzione del progetto
Daniel Caduff, Hans-Peter Käser
Ufficio federale per l'approvvigionamento economico del Paese, Sost. responsabile segreteria settore TIC

Direzione strategica
Marcel von Vivis, Approvvigionamento economico del Paese, responsabile settore IKT

Gruppo degli autori

Direzione operativa
- Reto Häni, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, PwC

Gruppo di esperti
- Urs Küderli, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, PwC
- Christian Weigele, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, SAP
- Candid Wüest, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, Symantec
- Marc Holitscher, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, Microsoft
- Markus Pfyffer, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, IBM
- Hansruedi Münger, Approvvigionamento economico del Paese, responsabile sezione Gestori dell'infrastruttura, Atos

Contatti

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

Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Telefono +41 58 462 21 71

Licenza

Citate il documento come segue:

Ufficio federale per l'approvvigionamento economico del Paese UAEP; «Standard minimo per migliorare la resilienza delle TIC», Berna, 2018
Versione maggio 2023, con aggiornamento NIST SP 800-53 Rev. 5 e ISO 27001:2022