Standard minimo per garantire la sicurezza delle TIC nello smaltimento dei rifiuti

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

VBSA
ASED
ASIR

Prefazione

Gentili lettori,

Voi tutti lavorate nel settore dei rifiuti, un settore di rilevanza sistemica. Ciò significa che un malfunzionamento dei nostri impianti, soprattutto di quelli di incenerimento dei rifiuti, avrebbe un grave impatto sulla società. Ma in quali situazioni potrebbe verificarsi un malfunzionamento? In cima alla lista dei fattori di rischio vi sono i cyberattacchi. Recentemente, varie aziende, autorità e altre organizzazioni parastatali – tra cui gli IIRU – sono state ripetutamente oggetto di attacchi informatici mirati e altamente professionali. Questi attacchi non solo bloccano o cancellano i dati, ma sono anche in grado di sabotare, manipolare o distruggere i componenti fisici dell'impianto, come la bilancia o le turbine. L'obiettivo dei cybercriminali è solitamente quello di estorcere denaro o di distruggere e disattivare gli impianti.

Un IIRU ha molti punti sensibili che possono risultare vulnerabili agli attacchi informatici. Per esempio la bilancia, la gru, il sistema di controllo distribuito, la turbina o i sensori per la misurazione delle emissioni. A questo si aggiungono gli accessi da remoto da parte dei fornitori per interventi di vario tipo. Il punto più delicato, tuttavia, rimane il fattore umano e l'uso talvolta maldestro delle tecnologie dell'informazione e della comunicazione (TIC). Si potrà garantire una protezione duratura delle informazioni solo se la direzione la incoraggerà e ne darà il buon esempio e se tutti i dipendenti saranno coinvolti e formati.

Dove si colloca oggi il nostro settore? Finora la sicurezza delle informazioni è stata gestita in maniera diversa in ogni struttura. Mentre alcuni IIRU hanno creato dei posti di lavoro specifici in questo campo, in altri impianti l'argomento è stato spesso tralasciato. L'attuale standard minimo per le TIC serve a professionalizzare e standardizzare la difesa contro la criminalità informatica. È stato pensato come un manuale da professionisti per professionisti, si concentra su misure di protezione concretamente attuabili e può dunque risultare utile e non finire semplicemente nel cassetto di un responsabile della sicurezza. Consultando questo manuale e implementando lo «standard minimo per le TIC» raccomandato dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) darete un importante contributo alla resilienza informatica della vostra azienda.

Anche l'ASIR sostiene ogni sforzo nella direzione di una maggiore sicurezza delle informazioni nel settore dei rifiuti. Raccomanda a tutti i suoi membri di implementare lo standard qui presentato, fornisce una piattaforma di scambio e sostiene una comunicazione aperta sugli eventuali incidenti.

Se riusciremo a fermare i criminali informatici, sarà possibile risparmiare denaro e fatica e si potrà garantire un normale riciclaggio dei rifiuti senza ostacoli, nell'interesse dell'ambiente e della nostra società.

Robin Quarter
Ariane Stäubli
Segreteria ASIR

Indice

1 In sintesi

Il presente standard minimo per le TIC riguarda le aziende di rilevanza sistemica nello smaltimento di rifiuti e presenta alcune raccomandazioni su come ridurre i rischi informatici a un livello accettabile, in un'ottica economicamente vantaggiosa e guardando al futuro. Una strategia di sicurezza efficace protegge gli strumenti essenziali di un'organizzazione, necessari per lo svolgimento delle sue attività critiche. Oltre alle misure tecniche, questa strategia dovrebbe includere anche le più importanti procedure da seguire, l'istruzione e la formazione dei dipendenti e la gestione della sicurezza. Un'azienda può trarre profitto da una maggiore sicurezza delle proprie informazioni.

Di seguito mostreremo l'importanza dell'implementazione dello standard minimo per le TIC:

I. In generale le minacce sono in aumento perché la criminalità informatica è un modello di business molto redditizio. Ciò vale anche per i sabotaggi industriali mirati.

II. Con l'avanzare della digitalizzazione aumenta la necessità di scambiare dati all'interno dell'azienda senza interruzioni nei sistemi di comunicazione. Un esempio è la lettura e la valutazione dei sensori durante la depurazione dei gas di combustione. Oggi sono in aumento anche le richieste di scambio di dati tra aziende, per esempio per gli interventi di manutenzione da remoto sui componenti dell'impianto.

III. La crescente dipendenza dai processi guidati dalle TIC può comportare delle vulnerabilità. Nelle operazioni industriali, come per esempio in un impianto di incenerimento dei rifiuti, si fa la distinzione tra sistemi IT e OT. I sistemi IT comprendono l'elaborazione elettronica dei dati, per esempio nei processi amministrativi. I sistemi OT, invece, si riferiscono all'infrastruttura hardware e software per il monitoraggio diretto e/o il comando di impianti e processi industriali. Anche i sistemi OT, come il comando delle turbine, possono essere manipolati o messi fuori uso. Di conseguenza, già oggi è fondamentale mettere in campo e attuare modelli di sicurezza duraturi e resilienti anche per le infrastrutture OT.

IV. Le infrastrutture critiche sono interdipendenti (smaltimento dei rifiuti sanitari, protezione dell'ambiente, ecc.).

Nell'implementazione di una strategia informatica, non bisogna dimenticare che il rafforzamento della sicurezza TIC richiede anche risorse umane aggiuntive, oltre a nuovi sistemi di sicurezza e nuove procedure. Anche il migliore dei sistemi di sicurezza è inefficace se non si tengono in considerazione gli allarmi che questo lancia e se non si esplorano le cause di tali allarmi in maniera sistematica.

Soprattutto negli impianti industriali con procedure essenziali per la sicurezza dell'approvvigionamento, tra cui rientrano anche gli impianti di incenerimento dei rifiuti, è importante continuare a perseguire i seguenti obiettivi di protezione della sicurezza delle informazioni.

- Disponibilità e affidabilità nell'uso dell'IT
- Riservatezza, protezione contro gli accessi non autorizzati
- Integrità, protezione contro la cancellazione e la falsificazione delle informazioni elettroniche

Mentre nella sfera dell'IT (analisi dei dati, gestione, amministrazione, ecc.) la riservatezza, l'integrità e la disponibilità delle informazioni sono ugualmente importanti, nell'OT l'obiettivo primario è invece la disponibilità (cfr. fig. 1).

Nella sezione successiva sarà illustrata la sempre più stretta integrazione tra sistemi IT e OT. Per esempio, una convergenza tra IT e OT consente di effettuare controlli completi sullo stato operativo, indipendentemente dal luogo in cui ci si trova, e permette di analizzare più facilmente i dati provenienti da sistemi complessi. Ciò può migliorare e accelerare lo sviluppo di soluzioni in caso di malfunzionamento, in quanto i fornitori, i dirigenti e i dipendenti avrebbero la possibilità di osservare «i dati in tempo reale» relativi agli impianti e alle strutture.

I seguenti punti mostrano i vantaggi derivanti dall'attuazione di una strategia informatica secondo lo standard minimo per le TIC:

- sistemi IT e OT meno isolati (silos) grazie alle sinergie;
- minori costi di sviluppo, di funzionamento e di assistenza; grazie alla manutenzione predittiva, minori tempi di inattività non pianificati;
- maggiore conformità alle normative, in quanto l'implementazione di una strategia informatica consente di migliorare la trasparenza, la gestione e il controllo dei sistemi IT e OT;
- miglioramento dell'automazione e della visibilità dei sistemi OT decentralizzati (in particolare per i fornitori), grazie alla possibilità di trasmettere e analizzare in tempo reale i dati sulla manutenzione;
- uso più efficiente di energia e risorse, perché i sistemi OT possono essere adattati meglio alle effettive esigenze di produzione. Un esempio è l'uso ottimizzato delle risorse operative basato sulla valutazione dei dati raccolti dai sensori;
- gestione più efficiente degli impianti, in quanto tutti i sistemi IT e OT vengono registrati, gestiti e visualizzati in maniera chiara e secondo una metodologia comune.

Per gli IIRU che in futuro attueranno sistematicamente lo standard minimo per le TIC e che ne sfrutteranno le opportunità risulterà chiaro che la sicurezza TIC non può essere vista meramente come un costo, bensì come un vero e proprio vantaggio commerciale nel più ampio piano di sicurezza dell'approvvigionamento della Svizzera.

Sicurezza IT e OT

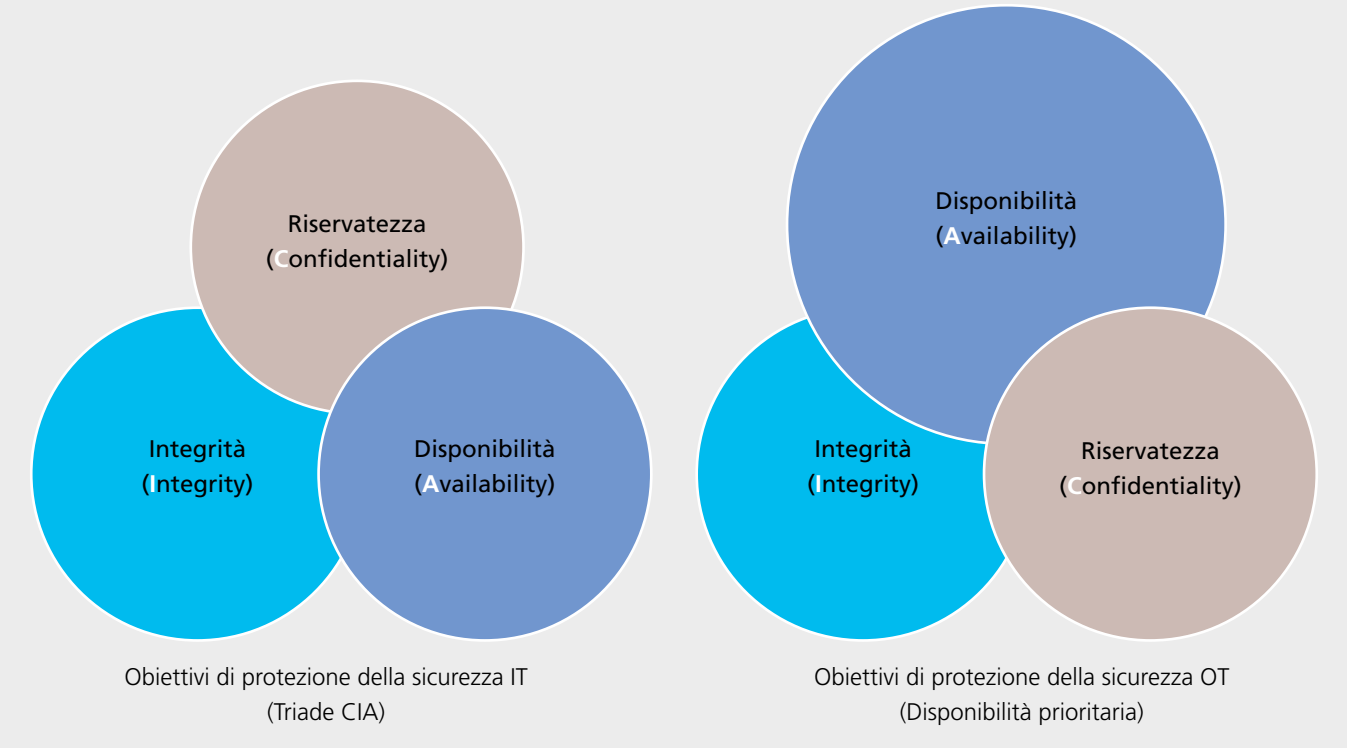


Figura 1: sicurezza IT e OT

2 Contesto iniziale

Ogni anno in Svizzera si producono da 80 a 90 milioni di tonnellate di rifiuti, gran parte dei quali sono materiali di demolizione, di scavo e di sterro non contaminati. Per via dell'elevato tenore di vita, la Svizzera ha uno dei volumi di rifiuti urbani più alti al mondo, con 716 kg di rifiuti per persona. Di questi, poco meno del 53 % viene riciclato. Per ridurre l'elevato consumo di materie prime primarie della Svizzera, la Confederazione intende prendere in considerazione tutti i flussi di materiali e di sostanze lungo la catena del valore, dall'estrazione delle materie prime alla progettazione dei prodotti fino alla gestione dei rifiuti.

Secondo la legge sulla protezione dell'ambiente, i rifiuti possono essere definiti come segue[1]:

Per rifiuti si intendono le cose mobili delle quali il detentore si libera o che devono essere smaltite nell'interesse pubblico.

Lo smaltimento dei rifiuti comprende il loro riciclaggio o deposito definitivo nonché le operazioni preliminari di raccolta, trasporto, deposito provvisorio e trattamento. Per trattamento si intende qualsiasi modificazione fisica, biologica o chimica dei rifiuti.

Per utilizzazione si intende qualsiasi attività relativa a sostanze, organismi o rifiuti, segnatamente la produzione, l'importazione, l'esportazione, la messa in commercio, l'impiego, il deposito, il trasporto o lo smaltimento.

L'insieme delle attività e dei compiti legati alla prevenzione, alla riduzione, al recupero e allo smaltimento dei rifiuti viene definito gestione dei rifiuti. Le attività di gestione dei rifiuti possono essere organizzate in forma pubblica, privata o mista.

La gestione dei rifiuti si occupa di:

- pianificazione strategica della gestione dei rifiuti a livello locale, regionale, cantonale e nazionale;
- possibilità di prevenzione e riduzione dei rifiuti, per esempio attraverso la consulenza sui rifiuti;
- triage dei rifiuti e separazione delle raccolte miste di rifiuti;
- utilizzo e riciclaggio dei rifiuti (p. es. compost, combustibili sostitutivi, rifiuti da costruzione, materiali di scavo, metalli);
- raccolta e trasporto dei rifiuti (punti di raccolta, sistemi di contenitori, veicoli, stazioni di trasferenza);
- trattamento (meccanico, chimico, biologico, termico) dei rifiuti destinati al riciclo a valle (riciclaggio dei rifiuti) oppure alla discarica;
- deposito di rifiuti e residui di trattamento in discarica (selezione del sito, pianificazione, coltivazione della discarica, percolato ecc.)

Trasporto di rifiuti

Il trasporto dei rifiuti comprende i vari servizi di raccolta e il trasporto da e verso gli attori coinvolti nel recupero e nello smaltimento. Il trasporto è in capo alle aziende che raccolgono e trasportano i rifiuti, gestiscono stazioni di trasferenza, effettuano raccolte mobili di rifiuti speciali che provengono dalle economie domestiche per conto di un Comune, consegnando poi i rifiuti senza stoccaggio intermedio a un'azienda di smaltimento o ad aziende di camion aspiratori che gestiscono veicoli senza trattamento integrato delle acque reflue.

Un'interruzione su larga scala dello smaltimento dei rifiuti causerebbe nel medio termine un accumulo di rifiuti nelle città e nei Comuni e, probabilmente, anche uno smaltimento illegale dei rifiuti. La spazzatura depositata nelle strade comporterebbe gravi problemi igienici e possibili rischi per la salute. In breve tempo le aziende e le imprese risentirebbero della situazione: i clienti si allontanerebbero, la produzione non sarebbe più possibile a causa della mancanza di capacità di stoccaggio, le condizioni igieniche non consentirebbero di lavorare normalmente, ecc. Inoltre, nell'ambito del trattamento dei rifiuti pericolosi esiste il pericolo di inquinamento ambientale, di diffusione di malattie o persino di scoppio di epidemie.

[1] *Legge federale sulla protezione dell'ambiente (LPAmb), RS 814.01, art. 7*

La rappresentazione seguente raffigura la struttura del settore e i punti di contatto con altri sottosettori critici:

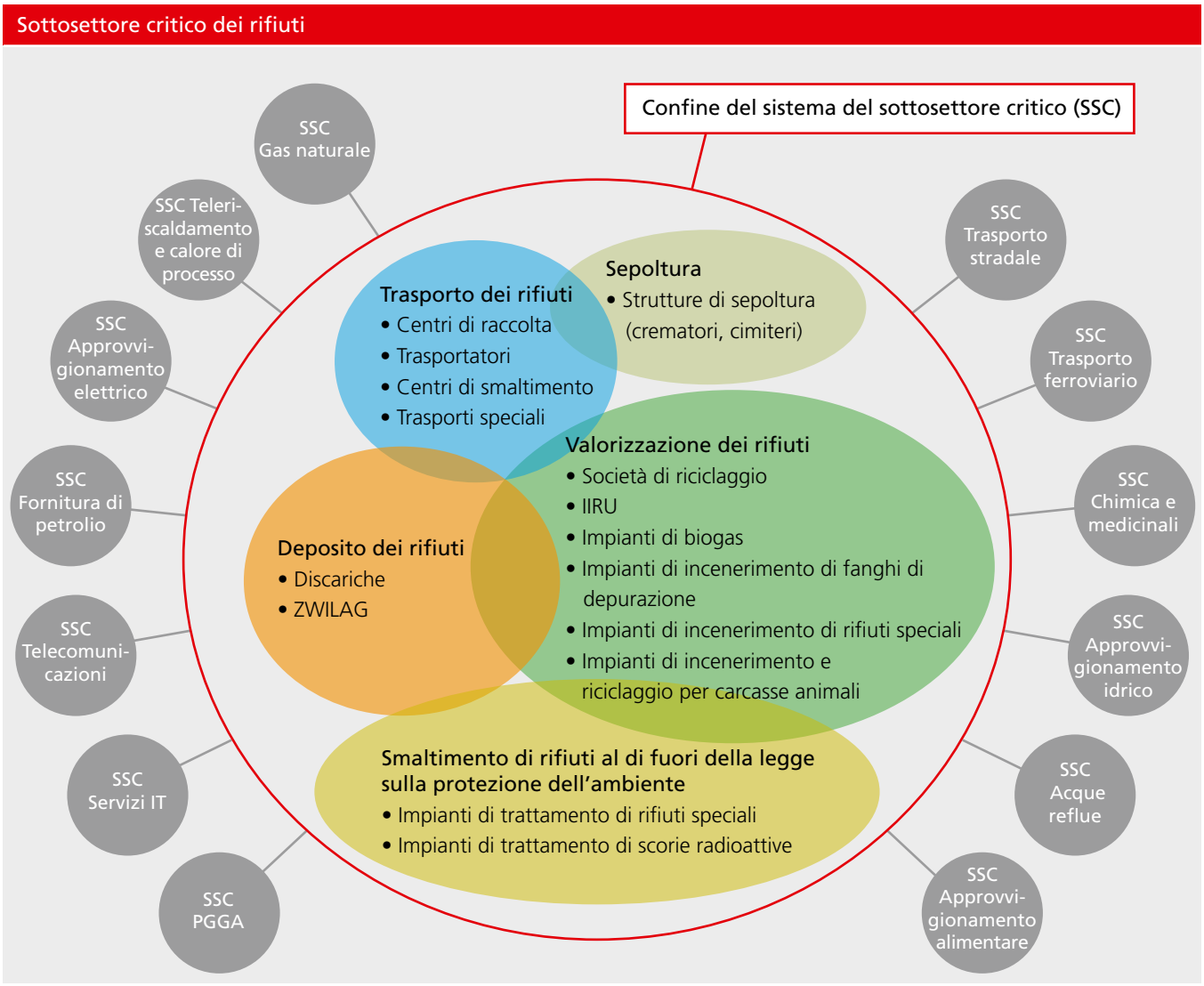


Figura 2: sottosettore critico dei rifiuti

Valorizzazione dei rifiuti

Nell'ambito dello smaltimento dei rifiuti vengono perseguiti diversi obiettivi, come il recupero di materie prime (ove possibile e con misure economicamente proporzionate), il recupero di energia dai rifiuti e la minimizzazione della quantità di rifiuti destinati allo smaltimento di lungo periodo in discarica. Diversi sono i metodi per eseguire la valorizzazione termica, quella materiale o una combinazione di entrambe.

Gli impianti svizzeri di incenerimento dei rifiuti hanno incenerito poco più di 4 milioni di tonnellate di rifiuti nel 2020, attestandosi quindi al 100 % dell'utilizzo delle loro capacità. Il guasto prolungato di un impianto complicherebbe notevolmente la situazione dello smaltimento di rifiuti nel Paese. Inoltre, vengono trattati anche rifiuti di Paesi vicini, azione sensata dal punto di vista ecologico al fine di accorciare i lunghi tragitti di spostamento. La Svizzera esporta inoltre centinaia di migliaia di tonnellate di rifiuti che non possono essere trattati o riciclati sul territorio nazionale (rifiuti speciali, rifiuti plastici raccolti separatamente, ecc.).

Il nostro Paese dispone attualmente di 29 impianti di trattamento dei rifiuti, utilizzati per l'incenerimento ecologico di tutti i rifiuti non valorizzati in altro modo. Il calore generato viene utilizzato per il riscaldamento e per la produzione di elettricità. I metalli e gli altri materiali riciclabili vengono separati dalle scorie e dalle ceneri leggere. La parte rimanente è invece destinata alla discarica.

Oltre agli inceneritori, vi sono altri impianti di tipo termico come quelli di incenerimento dei fanghi di depurazione o le centrali termiche a legna. Per quanto questi impianti siano diversi, hanno come denominatore comune lo smaltimento delle sostanze. I rifiuti trattati, alcuni dei quali hanno un elevato potere calorifico, sono adatti come combustibili sostitutivi per la produzione di energia o per il risparmio di risorse primarie.

Il compostaggio o la fermentazione dei rifiuti biogenici presenta notevoli vantaggi ambientali rispetto all'incenerimento in un impianto, perché le sostanze naturali vengono reintrodotte nel ciclo naturale dopo il processo.

All'incirca la metà dei rifiuti urbani viene raccolta separatamente e può essere in gran parte riciclata. Le principali materie prime riciclate dai rifiuti e reimmesse nel ciclo di produzione includono carta, vetro, scarti vegetali, metallo, legno e tessuti. Anche gran parte dei rifiuti edili minerali, come per esempio il calcestruzzo, vengono riciclati e possono essere riutilizzati come materiali edili.

Un aspetto importante del riciclaggio dei rifiuti è la comunicazione che ne fanno le autorità nell'ambito della gestione dei rifiuti. Senza un'attività costante di sensibilizzazione e informazione, la popolazione perde di vista rapidamente quanto appreso sullo smaltimento corretto ed ecologico dei rifiuti.

Il sottosettore del riciclaggio dei rifiuti ha una ricaduta diretta sull'economia grazie al valore aggiunto generato dall'industria dello smaltimento così come sugli acquirenti dei prodotti riciclabili, delle materie prime e dell'energia rilasciata sotto forma di calore ed elettricità ottenuti dal riciclaggio dei rifiuti.

Deposito dei rifiuti

Questo ambito riguarda il collocamento in discarica e il deposito dei rifiuti.

I rifiuti che non possono più essere riciclati devono essere trattati in modo tale da non provocare danni all'ambiente in seguito al loro collocamento in discarica. A seconda della loro composizione e della concentrazione di inquinanti, i rifiuti vengono destinati a uno dei cinque tipi di discarica (A, B, C, D, E). L'ordinanza sui rifiuti (OPSR) definisce i criteri di assegnazione dei rifiuti da collocare in discarica.

I rifiuti fortemente contaminati, come le ceneri leggere o i residui del lavaggio delle ceneri, vengono in parte esportati all'estero, dove vengono collocati in una discarica sotterranea.

Gran parte dei rifiuti può essere valorizzata come materia prima dal punto di vista termico o materiale. Le procedure di smaltimento in uso in Svizzera sono descritte di seguito.

2.1 Valorizzazione materiale dei rifiuti

Riciclaggio

Il riciclaggio consiste, da un lato, nel riutilizzo diretto di prodotti che non vengono più utilizzati (p. es. abiti usati o parti ancora funzionanti di veicoli fuori uso) e, dall'altro, nel recupero di materiali, cioè l'estrazione di materie prime dai rifiuti (p. es. la produzione di nuovo vetro da rottami, la fusione di rottami di ferro o la produzione di materiali da costruzione da rifiuti edili). Il *downcycling* è invece la trasformazione dei rifiuti in materiali di qualità inferiore rispetto ai materiali originari.

Valorizzazione del materiale di scavo e dei rifiuti edili

Nell'ambito della valorizzazione dei materiali, i materiali di scavo e i rifiuti edili provenienti dalla demolizione di edifici e di opere infrastrutturali rappresentano la quota maggiore in termini di volume. Tali materiali vengono prodotti sia durante la demolizione controllata di interi piani o edifici sia durante il loro ampliamento o la loro conversione. In passato la demolizione di un edificio avveniva in maniera incontrollata mediante palle da demolizione o esplosivi; oggi, invece, si tratta spesso di una decostruzione pianificata con una separazione in loco delle singole frazioni di rifiuti.

Compostaggio e fermentazione

Un'altra componente importante della valorizzazione materiale dei rifiuti è rappresentata dal compostaggio e dalla fermentazione dei rifiuti biogenici o organici. I rifiuti organici sono rifiuti di origine vegetale, animale o microbica che provengono dall'agricoltura, dall'industria alimentare e dai consumi privati.

2.2 Trattamento chimico-fisico o biologico

I trattamenti chimico-fisici o biologici consentono un collocamento sicuro dei rifiuti o ne rimuovono le sostanze nocive. Tramite i processi biologici si convertono le sostanze nocive in prodotti innocui mediante l'impiego di microrganismi o piante. Questo include principalmente le seguenti procedure:

- le sostanze nocive vengono rimosse dai rifiuti acquosi mediante diverse tecniche quali filtrazione, precipitazione e degradazione con microrganismi di modo che le acque possano poi essere immesse nuovamente nella canalizzazione. Le sostanze nocive, invece, vengono incenerite o collocate in discarica, a seconda della loro composizione;
- per riciclare le miscele di sostanze liquide, queste sono separate nei loro singoli componenti mediante processi fisici;
- i rifiuti fangosi spesso devono essere disidratati per poter essere inceneriti o collocati in discarica;
- i rifiuti solidi ad alto contenuto di sostanze nocive non possono essere collocati in discarica senza pretrattamento. Le sostanze nocive presenti negli scavi contaminati possono essere impoverite mediante il lavaggio. Gli inquinanti organici vengono distrutti dal trattamento termico o convertiti in sostanze innocue da microrganismi o piante. I rifiuti con un elevato contenuto di metalli pesanti, come le ceneri leggere degli impianti di trattamento dei rifiuti, vengono lavati con acido prima di essere collocati in discarica così da rimuovere i metalli pesanti dalle ceneri.

Discariche

I residui dell'incenerimento dei rifiuti così come i rifiuti non idonei alla valorizzazione materiale o termica vengono depositati in discariche conformi alla legge, ma vengono pretrattati nel caso in cui non soddisfino i requisiti per il deposito.

2.3 Valorizzazione termica dei rifiuti

In Svizzera si ricorre all'incenerimento per la sterilizzazione e per la riduzione della quantità di rifiuti destinata alle discariche. L'energia rilasciata nel processo viene poi recuperata e riutilizzata. I rifiuti materiali combustibili e non riutilizzabili vengono sottoposti a valorizzazione termica. Questi vengono trattati negli impianti di incenerimento dei rifiuti, in cementifici o in altri impianti industriali. Tutti gli impianti di trattamento dei rifiuti solidi urbani svizzeri utilizzano il calore di combustione per generare elettricità o per alimentare reti di teleriscaldamento e impianti industriali. Inoltre, dalle scorie si recuperano ferro, alluminio, rame e altri metalli.

Nei cementifici e in altri impianti industriali, i rifiuti rappresentano una fonte di energia per la generazione di calore impiegato per la produzione o la lavorazione di prodotti come il cemento.

L'incenerimento dei rifiuti produce inquinanti atmosferici che vengono in gran parte trattenuti da un trattamento dei gas di combustione a più stadi e dalla denitrificazione, cosicché solo piccole quantità di sostante nocive vengano rilasciate nell'ambiente.

Il diagramma seguente mostra la struttura di un impianto di incenerimento dei rifiuti. Nel presente documento viene trattata la parte relativa allo smaltimento dei rifiuti. Per il settore del teleriscaldamento, dell'alimentazione elettrica e delle acque reflue è stato elaborato uno standard minimo per le TIC separato (sebbene gran parte degli impianti comprenda tutti gli aspetti).

Struttura di un IIRU

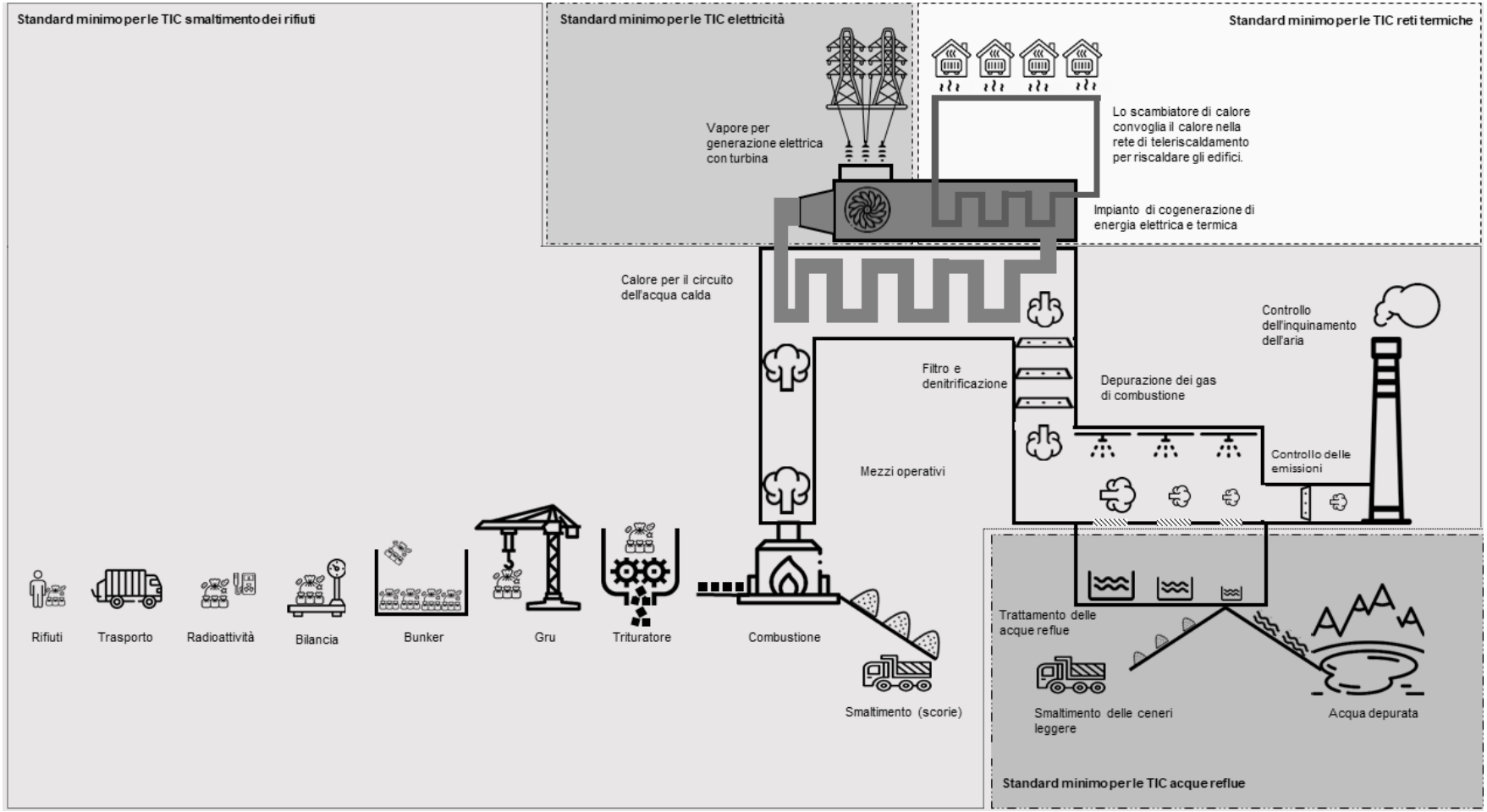


Figura 3: struttura di un IIRU

3 Obiettivi dello standard minimo

Questo documento si rivolge alle aziende di gestione dei rifiuti in Svizzera e presenta una raccomandazione su come ridurre a un livello accettabile i rischi legati alla protezione delle informazioni. Vengono applicati l'«approccio basato sul rischio» e la «strategia *defense in depth*».

Con la valorizzazione termica si persegue anzitutto l'obiettivo di smaltire i rifiuti in modo ecologico e conforme alla legge; nel processo, però, si genera ugualmente energia utilizzabile. Inoltre, dalle scorie si recuperano anche metalli. Ciò che rimane sono residui contaminati derivanti dalla combustione, i quali devono essere depositati in discarica. Il trattamento e il successivo deposito di rifiuti generano flussi di materiale aggiuntivi che, se impediti o interrotti, possono ostacolare l'obiettivo primario della valorizzazione termica. Questa analisi mette in evidenza che un impianto di incenerimento dei rifiuti presenta numerosi vettori di attacco spesso inaspettati, che non vanno sottovalutati.

Perché proteggere le informazioni:

- le minacce sono in aumento perché la criminalità informatica rappresenta un modello di business molto redditizio e in certi casi si trasforma in un sabotaggio industriale mirato;
- con la crescente dipendenza dai sistemi informativi e di controllo si è esposti a diverse vulnerabilità;
- le infrastrutture critiche sono interdipendenti (smaltimento dei rifiuti ospedalieri, protezione dell'ambiente, ecc.);
- chi rende la propria azienda più resiliente potenziando la sicurezza informatica ottiene anche dei vantaggi sul lato commerciale.

L'implementazione della strategia di sicurezza delle informazioni in base a questo standard avviene secondo **l'approccio basato sul rischio.** Ciò significa che i vari processi sono valutati in base ai rispettivi rischi e il loro impatto è quantificato in termini di criticità (cfr. tabella 3: processi critici negli impianti di incenerimento dei rifiuti).

Un altro metodo utilizzato è la strategia *defense in depth*, ossia la difesa in profondità:

La strategia *defense in depth* deriva dal principio militare secondo cui un sistema di difesa complesso a più livelli è più difficile da violare rispetto a uno con un singolo ostacolo. L'obiettivo di questa strategia è quindi quello di applicare molteplici misure di sicurezza a diversi livelli di protezione, costringendo così l'attaccante a superare una moltitudine di complesse barriere di sicurezza.

Perimetro di *defense in depth*

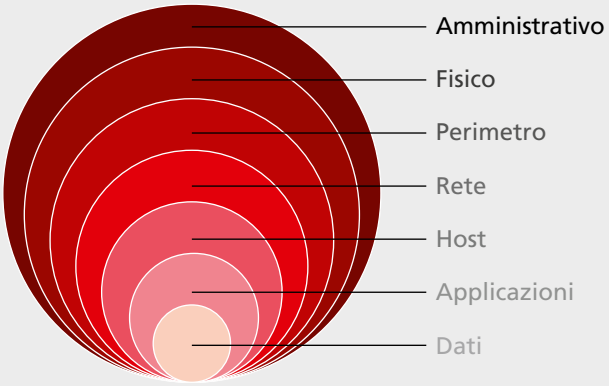


Figura 4: perimetro di defense in depth

4 Processi e attività critici

La seguente figura mostra i possibili obiettivi di attacco a un IIRU:

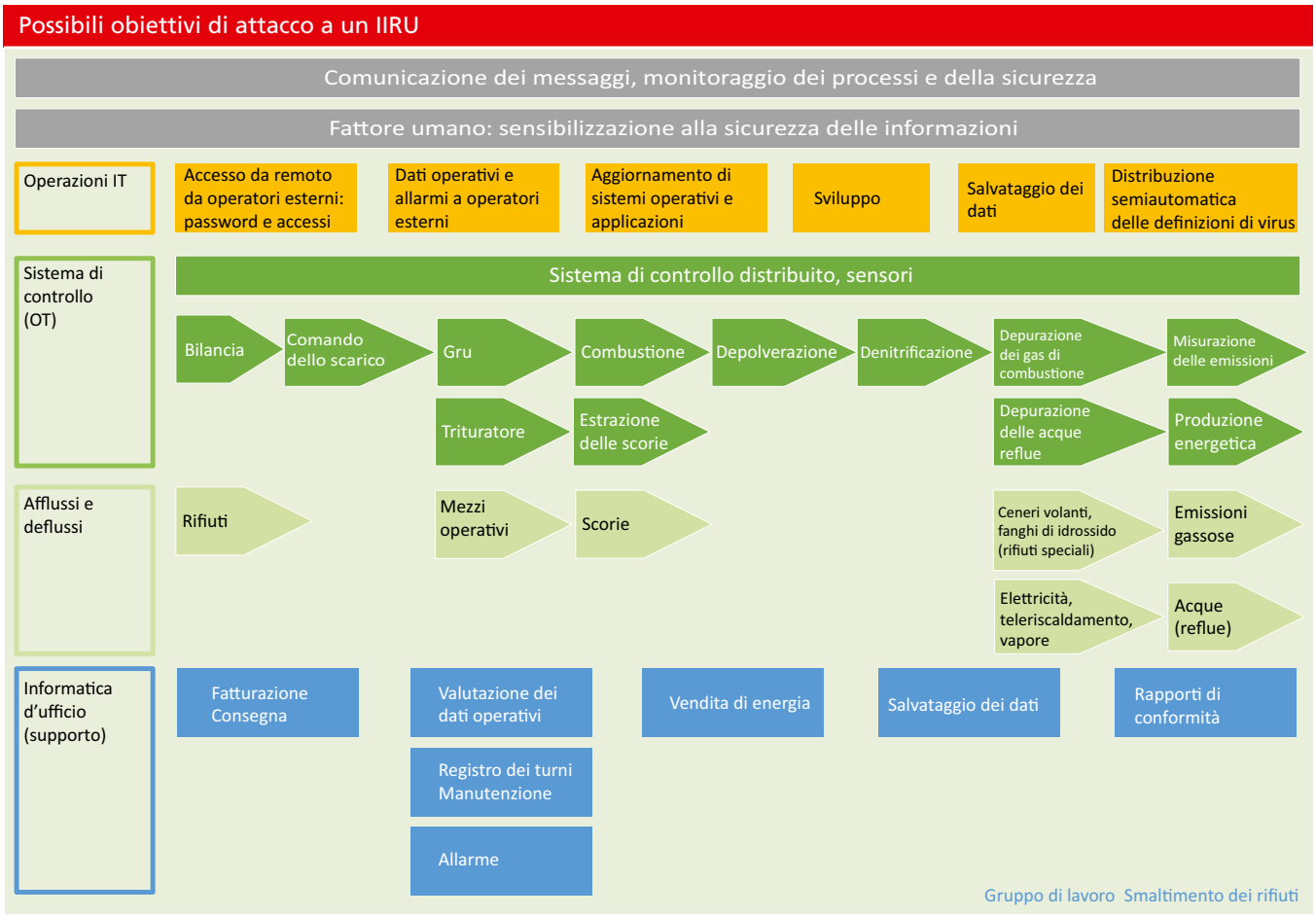


Figura 5: possibili obiettivi di attacco a un IIRU

Per quanto riguarda l'analisi della vulnerabilità, di seguito sono elencate le aree tematiche con le soluzioni proposte.

4.1 Comunicazione

Al giorno d'oggi è necessario disporre di sistemi di comunicazione scritta e orale affidabili e funzionanti, sia che questi vengano utilizzati per il normale svolgimento delle attività, sia che vengano adoperati per garantire che tutto il personale dell'azienda sia reperibile in situazioni d'emergenza.

Da non trascurare è soprattutto la comunicazione di emergenza con gli organismi esterni, in modo che in situazione di crisi possa essere mantenuta la comunicazione con le autorità o le organizzazioni di primo intervento. La designazione dei mezzi e dei canali di comunicazione deve essere fatta in anticipo e non solo in situazioni di crisi. Devono essere definite in anticipo anche le app e gli strumenti *(messenger)* utilizzati per la comunicazione mobile. È importante che vengano utilizzate solo applicazioni in cui sia garantita la sicurezza della trasmissione (p. es. tramite crittografia). È inoltre importante garantire che, quando si utilizzano le app sui dispositivi mobili, i dati non vengano sincronizzati e trasmessi a terzi senza autorizzazione.

Per ovviare a un guasto del sistema, i numeri di telefono importanti e i piani di emergenza devono essere stampati e archiviati in una cartella di emergenza.

Mezzi di comunicazione interni	Mezzi di comunicazione esterni
• telefonia IP • radio e radiocomunicazioni a scopo professionale • telefoni DECT e Wi-Fi, operatori di telefonia senza fili • sistema cercapersone/sistema di evacuazione • operatore sistema GSM, telefoni GSM (dispositivi mobili/ telefoni cellulari)	• linea di emergenza verso la centrale telefonica di quartiere (Swisscom, ecc.) che bypassa la centrale interna • stazione radio Polycom/ricetrasmittente portatile • telefoni GSM (cellulari) • messaggistica sicura • predisporre un sistema di *failover* per le e-mail

Tabella 1: mezzi di comunicazione interni ed esterni

Come spesso accade in ambito tecnico, non esiste un'unica soluzione atta a coprire l'intera gamma di esigenze; piuttosto, è necessario disporre di un insieme di più soluzioni per raggiungere i risultati desiderati.

Per esempio, i sistemi GSM (Natel) sono meno adatti per la comunicazione in edifici schermati come strutture in acciaio o seminterrati perché, senza complessi sistemi di antenne interne, la potenza di ricezione dei dispositivi è notevolmente limitata. Lo stesso vale per le radio tradizionali professionali nelle bande di 4 m, 2 m e 70 cm e per i sistemi di telefonia DECT. Anche queste necessitano di antenne e stazioni a relè per una comunicazione ottimale nei seminterrati e nelle stanze con una forte schermatura elettromagnetica.

Quando si utilizzano i servizi di messaggistica, è necessario assicurarsi che i dati, in particolare quelli di contatto, non vengano copiati dal dispositivo al sistema del fornitore. Il servizio dovrebbe inoltre offrire la crittografia end-to-end dei messaggi vocali e di testo, in modo da rendere sicura la comunicazione fino al livello «confidenziale».

4.2 Fattore umano: formazione e sensibilizzazione del personale

La stragrande maggioranza degli attacchi informatici inizia con un errore di un dipendente. La formazione e la sensibilizzazione dovrebbero ridurre la probabilità di «errore umano». Nel capitolo 6.6 è riportata una descrizione delle tematiche legate alla sensibilizzazione. I dipendenti dovrebbero essere sensibilizzati sui seguenti temi:

Possibilità di attacco	Minaccia
E-mail di spam e phishing	Le e-mail fraudolente rappresentano una minaccia ricorrente per la sicurezza delle informazioni di un'azienda. Per spam o posta indesiderata si intende l'invio in massa e per via elettronica di messaggi non richiesti dal destinatario, spesso molesti o che includono contenuto a carattere pubblicitario. Le e-mail di spam possono «inondare» il server di posta elettronica dell'azienda rallentandolo o addirittura bloccandolo. Una minaccia ben più pericolosa è rappresentata dalle e-mail di phishing. Il phishing consiste nell'invio di messaggi di posta elettronica ingannevoli, volti a indurre il destinatario a cadere in una truffa. Le e-mail di phishing tentano spesso di convincere gli utenti a divulgare informazioni bancarie, credenziali di accesso o altri dati sensibili.
Malware	I «malicious software», abbreviati con «malware», sono programmi che arrecano danni ai sistemi o agli utenti e che solitamente si autoreplicano. I danni possono essere causati, per esempio, da un malintenzionato che spia l'utente (mediante la tastiera o il disco rigido) o ne crittografa i dati oppure ottiene l'accesso dagli amministratori. Le forme più note di malware sono i virus, i trojan, gli spyware o i ransomware.
Ingegneria sociale	Il termine «ingegneria sociale» designa un fenomeno in cui un individuo esercita un'influenza su un altro. Ciò accade, per esempio, quando un hacker tenta di conquistare la fiducia della vittima e di convincerla a divulgare informazioni riservate o a rilasciare dati di carte di credito e password. L'ingegneria sociale si manifesta sia fisicamente che via e-mail, al telefono o sui social.

Tabella 2: possibilità di attacco e minacce

Come già accennato all'inizio del capitolo, le vulnerabilità umane sopra menzionate sono le principali porte d'ingresso per gli attacchi informatici. Per questo motivo, i dipendenti dovrebbero essere formati nell'ambito di un programma di sensibilizzazione svolto regolarmente (2–3 volte l'anno) e incentrato sul tema della sicurezza delle informazioni. L'obiettivo è quello di raggiungere un livello di sensibilizzazione alla sicurezza delle informazioni tale che i collaboratori adottino un comportamento corretto in modo intuitivo sviluppando un livello di «competenza inconscia».

Figura 6: livello auspicato di consapevolezza dei dipendenti

4.3 Sistemi di videosorveglianza

I sistemi di videosorveglianza sono un altro anello indispensabile nella catena della sicurezza fisica. Tuttavia, in mancanza di un'implementazione adeguata e di un uso regolamentato possono comportare alcuni rischi. Uno degli aspetti più importanti è il rispetto della legge sulla protezione dei dati (LPD). Per garantire ciò, è necessario introdurre un metodo operativo che descriva anzitutto cosa viene registrato, dove e quando, quali utenti hanno accesso al materiale registrato, per quanto tempo tale materiale viene conservato e chi può richiederne l'utilizzo e in quali casi. Particolare attenzione va rivolta anche al backup dei dati, in quanto è parimenti necessario garantire che il materiale venga cancellato dopo il periodo di conservazione.

Alcuni esempi di applicazione dei sistemi di videosorveglianza:

- sorveglianza degli accessi al confine perimetrale (ingressi principali e laterali);
- sorveglianza dei processi (bunker, sistema di scarico, bilance, ecc.);
- sorveglianza di locali sensibili (stanze dei server);
- i sistemi di videosorveglianza attuali sono in grado di avviare registrazioni sulla base di eventi scatenanti. Questo meccanismo consente di visualizzare immagini dal vivo dell'evento scatenante direttamente dal centro di controllo, riducendo così al minimo il rischio di interruzione del processo.

4.4 Funzionamento dell'IT

4.4.1 Manutenzione da remoto da parte di fornitori di servizi esterni

I vari sistemi, soprattutto quelli importanti per l'adempimento del mandato di smaltimento o di fornitura, **non** dovrebbero **mai** essere accessibili **in modo permanente** ai fornitori di servizi che accedono da remoto per eseguirne la manutenzione.

Gli accessi dall'esterno dovrebbero essere:

a) bloccati in caso di non utilizzo;
b) effettuati solo in caso di intervento di manutenzione preannunciato, limitato nel tempo ed eseguito tramite connessioni sicure (p es. VPN);
c) consentiti soltanto al numero di utenti strettamente necessari del fornitore di servizi. Tali utenti devono essere identificati per nome e dotati di un proprio account;
d) organizzati mediante un sistema per l'accesso privilegiato alla manutenzione (PAM), gestito a livello centrale con un'autenticazione multifattoriale (MFA) e la funzionalità di log e registrazione (audit trail). Gli accessi dovrebbero essere effettuati seguendo una gestione uniforme. Ogni eventuale deroga che risultasse necessaria deve essere documentata e monitorata.

Le password di accesso al sistema devono essere rinnovate periodicamente dall'amministratore di sistema per garantire che il personale uscente del fornitore di servizi non abbia più accesso al sistema.

4.4.2 Dati di esercizio trasmessi ai fornitori di servizi esterni

I dati di esercizio richiesti dai fornitori di servizi esterni non sono solitamente dati di processo online e possono dunque essere trascritti automaticamente dal sistema di controllo distribuito in una directory esterna alla rete di processo. In questo modo, il fornitore di servizi può disporre dei dati quando ne ha bisogno, senza dover ottenere un'autorizzazione per accedere al sistema di controllo.

La copia diretta delle informazioni durante una sessione di manutenzione da remoto andrebbe vietata. In alternativa, bisognerebbe mettere a disposizione dell'utente un'unità di trasferimento.

Si raccomanda vivamente di specificare nei contratti o negli accordi sul livello di servizio (SLA) con il fornitore (di servizi) esterno quali dati gli saranno trasferiti e per quale scopo, attraverso quali canali, e ancora per quanto tempo questi dati saranno conservati.

4.4.3 Sistemi di allarme

Il termine «sistemi di allarme» include i sistemi antincendio, i sistemi di chiamata (manuale o basata sul workflow) delle organizzazioni di primo intervento in caso di lesioni personali e incidenti gravi, nonché i sistemi di mobilitazione automatica di personale aggiuntivo e unità di supporto. Anche gli allarmi di evacuazione fanno parte di questa categoria.

4.4.4 Aggiornamento dei programmi e dei sistemi operativi

Gli aggiornamenti completamente automatici nelle reti OT sono molto rischiosi e quindi sconsigliati. Gli aggiornamenti nei sistemi industriali devono essere convalidati, rilasciati e (idealmente) anche installati dal produttore. Questi servizi devono essere definiti in uno SLA. Nello SLA è necessario specificare anche il numero di cicli di aggiornamento programmati nell'arco di un anno, il tempo di risposta e la disponibilità di importanti aggiornamenti di sicurezza tra i vari cicli programmati.

Quando le reti OT erano ancora completamente autosufficienti e scollegate da Internet, era sufficiente aggiornare i sistemi 1–2 volte l'anno e colmare le eventuali lacune di sicurezza. Tuttavia, con la crescente interconnessione e la fusione di IT e OT, aumentano anche i requisiti per quanto riguarda gli aggiornamenti regolari dei sistemi. I sistemi per i quali non è o non è più possibile effettuare aggiornamenti regolari del software dovrebbero essere completamente isolati o accessibili solo con limiti molto restrittivi se l'accesso si esegue da zone meno sicure.

La procedura di aggiornamento di un software deve essere descritta e concordata sia in una policy in caso di uso interno sia in uno SLA in caso di uso esterno. La conformità ai servizi SLA, nonché la relativa documentazione, deve essere concordata e rivista almeno una volta l'anno con il fornitore di servizi.

4.4.5 Sviluppo

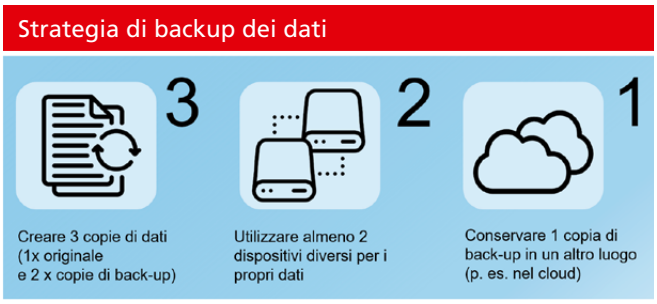
Se si ha intenzione di sviluppare o adattare un proprio software, è pressocché inevitabile creare un sistema di test e integrazione che corrisponda al proprio sistema produttivo. Poiché la gestione di uno, due o addirittura tre paesaggi di sistema è molto costosa in termini di risorse umane e finanziarie, una decisione *make or buy* è particolarmente importante in questo caso: si tratta cioè di capire quali vantaggi, costi e rischi comporti per l'azienda lo sviluppo in proprio di un software o di un'infrastruttura rispetto all'esternalizzazione completa di tale processo a un fornitore di servizi.

4.4.6 Backup e copie di sicurezza

Per ridurre il rischio di una perdita dei dati e le relative conseguenze (p. es. a causa di modifiche non intenzionali dei dati o di guasti all'hardware), è necessario eseguire a intervalli regolari un backup dei dati idealmente di tutti i sistemi IT. La strategia di backup deve prevedere diversi percorsi di backup dei dati. In particolare, si consiglia di mantenere un backup dei dati in locale sui sistemi IT per un accesso rapido e di salvare una copia di sicurezza su un sistema centrale. Per prevenire inoltre il rischio di un attacco ransomware, una copia andrebbe memorizzata su un sistema *air gap* logicamente e fisicamente separato.

La strategia di back-up dei dati 3-2-1

Anche i backup dei dati dei sistemi cloud remoti dovrebbero essere eseguiti con tecnologie appropriate nelle stesse infrastrutture dei sistemi locali, così da garantirne l'accesso in situazioni di crisi. Se ciò non è possibile, è necessario definire con il fornitore di servizi adeguate procedure di gestione della continuità operativa (*Business Continuity Management,* BCM) riguardanti, tra l'altro, la disponibilità, l'accesso, il trasporto e il trasferimento dei dati.



Fonte: computerweekly.de

Figura 7: strategia di backup dei dati

Il backup deve includere le informazioni e i dati seguenti:

- sistemi operativi e firmware;
- configurazioni (p. es. router, switch, applicazioni, regole firewall);
- applicazioni;
- basi di dati;
- dati di produzione;
- altri dati (p. es. dati di protocollo).

4.4.7 Distribuzione delle definizioni di virus

Si raccomanda di evitare una distribuzione automatica e diretta di definizioni di malware in un'infrastruttura OT senza prima eseguire una prova, perché si tratta di una procedura rischiosa. Un file danneggiato o difettoso potrebbe causare il malfunzionamento di uno o più sistemi o addirittura un guasto.

Si consiglia pertanto di controllare accuratamente i pacchetti di definizione del malware su un'installazione di prova prima della distribuzione. L'integrità del file andrebbe inoltre verificata con un *checksum (MD5 hash)*. Se ciò è impossibile a causa della mancanza di infrastrutture, si può optare per una distribuzione sequenziale. Tra le singole fasi di distribuzione è necessario assicurarsi che i sistemi già aggiornati funzionino senza errori e in modo stabile, al fine di ridurre eventuali rischi. Tuttavia, la distribuzione sequenziale non dovrebbe estendersi per settimane, altrimenti c'è il rischio che il malware non venga rilevato nel sistema.

4.5 Processi OT

4.5.1 Bilancia

La bilancia viene utilizzata per pesare tutti i veicoli prima e dopo lo scarico di rifiuti, di fanghi di depurazione, di materiali di consumo (materiali di esercizio) o simili. In questo modo le quantità consegnate vengono registrate e verificate, e sulla base di queste quantità si effettua un conteggio.

Per il buon funzionamento delle linee di incenerimento è essenziale conoscere con precisione tutti i flussi di massa e la loro composizione. Da un lato si determina la quantità di rifiuti o fanghi di depurazione da smaltire o da depositare in un bunker per far funzionare in modo ottimale le linee di incenerimento nel corso dell'intero ciclo; dall'altro, da queste cifre si deduce anche la quantità di beni di consumo (materiali operativi) necessari nel tempo e l'andamento del processo di combustione.

La bilancia è costituita essenzialmente da un sistema di pesatura, da un display, da barriere e/o semafori e da un'interfaccia con uno o più sistemi esterni (dati di esercizio, ufficio, fatturazione) a cui vengono trasmessi i dati. Spesso viene utilizzato un sistema completo con un controllore logico programmabile (PLC).

La pesatura in quanto tale non è un processo particolarmente critico e può essere effettuata anche manualmente in situazioni di emergenza, ma in caso di guasto potrebbe avere conseguenze spesso sottovalutate.

4.5.2 Sistema di scarico, punto di ribaltamento

La consegna dei rifiuti avviene solitamente con camion, treni o, più raramente, con navi. A seconda del tipo di impianto, i rifiuti vengono ribaltati direttamente nel bunker o depositati con un mezzo di scarico. Ciò avviene in diversi modi. In alcuni casi, i rifiuti vengono rovesciati su un tavolo di scarico e solo successivamente vengono depositati nel bunker tramite un dispositivo di ribaltamento. Di norma, un sistema di questo tipo è controllato da un PLC. Il PLC può essere gestito autonomamente con un pannello di controllo, ma anche con un'interfaccia hardware al sistema di controllo o essere integrato direttamente nel sistema stesso. Un IIRU possiede solitamente diverse linee di scarico. A seconda del tipo di impianto, il sistema di controllo deve essere

progettato in modo tale che un guasto non impedisca completamente di conferire o scaricare i rifiuti, in quanto ciò può comportare problemi di alimentazione o un intasamento dei rifiuti durante il conferimento. Il rischio di un guasto completo può essere evitato o ridotto al minimo grazie a sistemi di controllo indipendenti o ridondanti.

4.5.3 Gru (e scarico)

Con l'aiuto di una gru, i rifiuti depositati nel bunker vengono mescolati, ammassati e, infine, immessi nel pozzo di caricamento del forno. La gru viene solitamente azionata da un operatore a partire dalla sala di controllo, dalla quale viene monitorato anche l'intero processo di combustione.

Il grado di automazione di queste gru è talmente elevato che il caricamento del forno è spesso completamente automatizzato. Questi sistemi hanno dunque spesso un'interfaccia al sistema di controllo con cui si determina la quantità di rifiuti necessaria. Le gru sono dotate di un proprio sistema di pesatura che permette di misurare e registrare la quantità richiesta o quella consegnata.

Anche il controllo delle gru avviene solitamente mediante un PLC e, a seconda del grado di automazione, sono disponibili diverse interfacce verso sistemi esterni. Le gru vengono solitamente azionate tramite joystick e con l'ausilio di telecamere ed eventualmente di un display. A causa dell'elevata disponibilità richiesta, le gru vengono spesso utilizzate in modo ridondante. Ciò significa che viene resa disponibile una seconda gru in caso di guasto.

4.5.4 Trituratore

Il trituratore viene utilizzato per ridurre in pezzi materiali ingombranti o simili. Di solito il materiale da triturare non viene consegnato insieme ai rifiuti domestici.

A seconda dell'impianto, tale materiale viene stoccato separatamente oppure viene triturato subito dopo la consegna e mescolato successivamente con i rifiuti domestici.

Spesso, tuttavia, i rifiuti ingombranti vengono semplicemente stoccati in un bunker, e l'operatore della gru decide al momento della consegna se sia necessario triturarli prima di mescolarli con il resto dei rifiuti. In questo caso si ricorre a processi e applicazioni di diverso tipo, ragion per cui il rischio di guasto nel caso dei trituratori deve essere valutato caso per caso. Se i rifiuti ingombranti non possono essere triturati a causa di un guasto al trituratore e non c'è altra possibilità di triturarli o stoccarli separatamente, ci si può trovare ben presto in una situazione di impasse. Per esempio, le proprietà di combustione dei rifiuti possono cambiare molto rapidamente e di conseguenza risulta più difficile regolare il forno.

Anche il comando del trituratore avviene spesso con un PLC. A seconda del sistema possono essere presenti più trituratori (indipendenti) che vengono alimentati singolarmente. I rifiuti ingombranti vengono spesso immessi nel trituratore mediante una gru. Il comando del trituratore presenta di solito meno interfacce a sistemi esterni, in quanto di solito è l'operatore della gru a decidere quali materiali debbano essere triturati prima di essere mescolati nel bunker. Un trituratore è normalmente dotato di un sistema di rilevamento precoce degli incendi, perché la triturazione può produrre scintille causando un incendio dei rifiuti.

4.5.5 Combustione

Il processo chiave nello smaltimento dei rifiuti è quello dell'incenerimento. Con l'aggiunta di aria come agente ossidante, si innesca una reazione redox in cui si genera energia sotto forma di calore e luce. Un regolatore del rendimento del fuoco controlla con precisione l'apporto di combustibile e il sistema di aria comburente, con o senza ricircolo dei gas di combustione, al fine di ottenere il rendimento termico richiesto con il minor eccesso d'aria possibile e in conformità ai limiti sulle emissioni. A seconda della versione, la compromissione del regolatore può causare il danneggiamento totale della caldaia. Il regolatore deve essere posizionato nel livello 1 – cfr. par. 7.1 Segmentazione della rete.

4.5.6 Estrazione delle scorie

L'estrazione delle scorie avviene subito dopo il processo di combustione. Le ceneri e i residui incombustibili devono essere raffreddati e trasportati in un impianto di stoccaggio provvisorio (bunker per scorie) fino al successivo trasporto in discarica. Se il trasporto al bunker per scorie non dovesse più risultare possibile, è necessario interrompere il processo di combustione.

4.5.7 Depolverazione

I leggeri residui di ceneri prodotti nella camera di combustione e trasportati insieme all'aria comburente attraverso la caldaia sono definiti ceneri leggere. Queste vanno rimosse elettrostaticamente o meccanicamente in modo che i sistemi posti a valle del percorso dei gas di combustione (catalizzatore, scrubber, ecc.) possano continuare a funzionare normalmente. In caso di guasto del sistema di depolverazione, il processo di combustione viene solitamente interrotto e l'impianto si ferma.

4.5.8 Denitrificazione

Se si esegue la denitrificazione con procedure che hanno luogo dopo l'incenerimento vero e proprio, si parla di misure secondarie. Queste permettono di ridurre in larga misura gli ossidi di azoto contenuti nei gas di combustione, che sono nocivi sia per l'uomo sia per l'ambiente. Un eventuale guasto dell'impianto di denitrificazione può comportare la revoca temporanea dell'autorizzazione d'esercizio.

4.5.9 Depurazione dei gas di combustione

La depurazione dei gas di combustione è di solito l'ultima procedura che si esegue prima che tali gas vengano rilasciati nell'atmosfera. Per soddisfare i requisiti ambientali, nel corso della procedura gli inquinanti ancora presenti vengono rimossi. Un eventuale guasto del sistema di depurazione può comportare la revoca temporanea dell'autorizzazione d'esercizio.

4.5.10 Misurazione delle emissioni

Dopo la depurazione dei gas di combustione e prima che questi vengano rilasciati nell'atmosfera, è necessario verificare la presenza di sostanze inquinanti al loro interno. Ciò permette di controllare in ultima istanza il corretto funzionamento dei processi a monte. Eventuali anomalie influiscono direttamente sul regolatore. In questo caso si interviene automaticamente o manualmente sul sistema di controllo. La mancata misurazione dei valori di emissione o la loro manipolazione può comportare la revoca temporanea dell'autorizzazione d'esercizio.

4.5.11 Depurazione delle acque reflue

A seconda della progettazione dell'intero impianto, i processi a monte possono generare grandi quantità di acque reflue contaminate, che devono essere trattate adeguatamente prima di essere scaricate nelle acque pubbliche. La pulizia può essere effettuata internamente o da terzi. Un eventuale guasto del sistema di trattamento delle acque reflue può comportare la revoca temporanea dell'autorizzazione d'esercizio.

4.5.12 Produzione di energia

Uno dei sottoprodotti della combustione è l'energia sotto forma di calore e luce. Il calore genera in circuiti separati vapore o elettricità oppure può essere impiegato per il teleriscaldamento. Per evitare un arresto della combustione è però fondamentale garantire il rilascio dell'energia.

4.6 Informatica d'ufficio

A causa dei diversi requisiti di sicurezza, l'OT e l'IT d'ufficio devono essere rigorosamente separate. La separazione avviene tramite la segmentazione della rete. La prassi migliore è quella di collocare l'IT d'ufficio nei livelli superiori (livello 5/6) del modello di rete a zone e di separarlo dall'OT con una zona demilitarizzata (DMZ) (cfr. par. 7.1). È necessario evitare l'accesso diretto dalle zone IT ai sistemi OT senza interruzione del protocollo. Tali accessi devono essere effettuati idealmente tramite un sistema di PAM o almeno tramite *jump host* nella ICS – DMZ. I vantaggi di un accesso tramite un sistema PAM includono la registrazione completa degli accessi e la gestione sicura di credenziali altamente privilegiate.

5 Dipendenza, criticità e maturità

La tabella seguente riflette il livello di dipendenza dalle TIC per ciascuno dei processi critici sopra elencati. In questa sezione ci si chiede principalmente se il processo possa essere svolto senza le TIC (dipendenza dalle TIC). Il grado di dipendenza dalle TIC è espresso nelle categorie «basso», «medio» e «alto». Un basso livello di dipendenza dalle TIC è attribuito ai processi che possono essere svolti in gran parte anche senza l'ausilio di strumenti TIC. Se un processo può essere eseguito solo con l'ausilio di risorse supplementari (tempo, collaboratori, ecc.), a tale processo viene attribuito un livello medio di dipendenza dalle TIC. Se un processo non può invece essere eseguito in caso di guasto agli strumenti TIC, presenta un alto livello di dipendenza dalle TIC.

I criteri di classificazione si riferiscono esclusivamente al livello di dipendenza dei singoli processi dall'OT/IT e tengono conto delle possibili alternative.

- Autonomo = nessuna dipendenza da sistemi OT/IT monitorabili
- Basso = un guasto può essere gestito anche manualmente senza OT/IT
- Medio = un guasto influisce direttamente sul processo, che risulta dunque eseguibile solo in misura limitata; sono talvolta presenti delle alternative
- Alto = un guasto rende impossibile eseguire il processo; non è disponibile alcuna alternativa

Questa proposta è adattabile individualmente in base alle analisi d'impatto aziendale (BIA, cfr. descrizione in allegato al presente documento) e alle analisi delle interfacce svolte concretamente dalle aziende. Tuttavia, il livello di maturità non dovrebbe scendere al di sotto del livello 2 (requisito minimo per la sicurezza delle informazioni, cfr. figura seguente).

Le criticità dei sottoprocessi riportate nella tabella 3, indipendentemente dalle dimensioni dell'impianto, hanno lo scopo di fornire informazioni sulla fattibilità del processo chiave di smaltimento dei rifiuti. In caso di guasto alla gru dei rifiuti, per esempio, l'incenerimento e quindi anche lo smaltimento non sono più eseguibili nella maggior parte dei casi, e ciò comporta un arresto totale dell'intero processo. In caso di guasto al sistema di depurazione dei gas di combustione, le conseguenze per l'ambiente sarebbero drammatiche. A seconda dell'impianto, ciò può ostacolare lo smaltimento. Se è presente un bypass, invece, l'impianto può rimanere funzionante. In questa tabella NON sono considerati i processi a valle dello smaltimento, come l'approvvigionamento termico o elettrico di terzi, indipendentemente dal fatto che appartengano all'infrastruttura critica!

4 = guasto totale del processo chiave di smaltimento dei rifiuti
3 = impatto lieve sullo smaltimento, impatto maggiore sui sistemi circostanti
2 = nessun impatto diretto sullo smaltimento, sistemi periferici provvisoriamente sostituibili con altri mezzi
1 = nessun impatto diretto sullo smaltimento, ma altre conseguenze a lungo termine

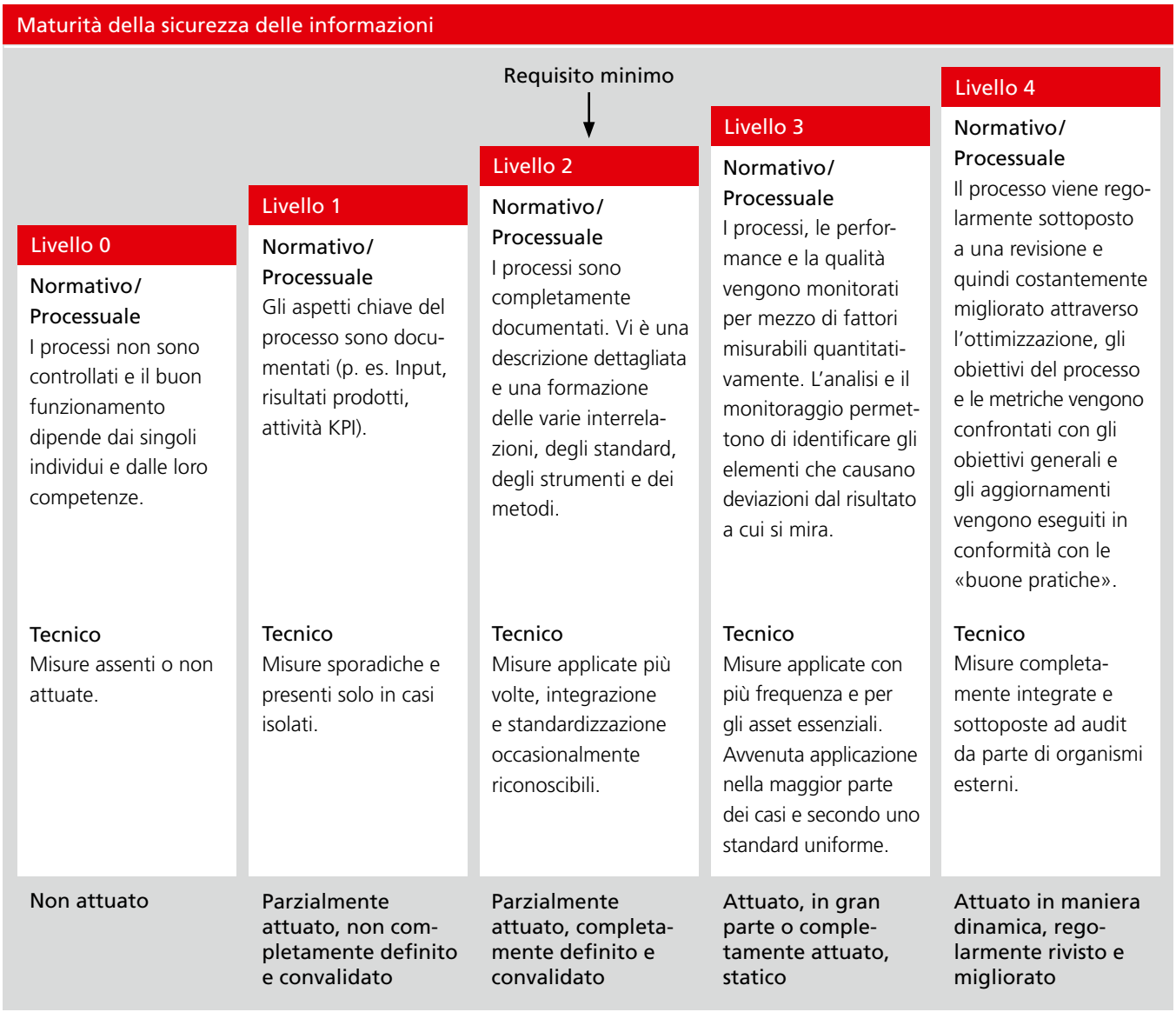


Figura 8: maturità della sicurezza delle informazioni

La maturità raccomandata per gli impianti di incenerimento dei rifiuti si basa sulla tabella 3 qui di seguito:

n/a = processo non disponibile
0 = non attuato
1 = parzialmente attuato, non completamente definito e convalidato
2 = parzialmente attuato, completamente definito e convalidato
3 = attuato, in gran parte o completamente attuato, statico (nessun miglioramento continuo dei processi)
4 = attuato in maniera dinamica, regolarmente rivisto e migliorato

Osservazioni su n/a:
In linea di massima si dovrebbe dare una valutazione da 0 a 4. Si può ricorrere a n/a solo se il processo in questione non esiste nell'azienda.

5.1 Livello minimo di maturità consigliato

Nella tabella seguente sono riportati i livelli minimi di maturità consigliati per ogni singolo processo critico di incenerimento dei rifiuti.

La raccomandazione si basa sulla valutazione del rischio relativo all'adempimento del compito principale in caso di interruzione del processo e sulla dipendenza del processo dal supporto informatico.

Processi critici negli IIRU			
	Grado di dipendenza dalle TIC	Rischi per il corretto svolgimento del mandato	Maturità consigliata per la sicurezza delle informazioni
Comunicazione dei messaggi	Medio	Medio	2–3
Fattore umano	Alto	Alto	2–3
Accesso da remoto per operatori esterni	Alto	Medio	4
Valutazione dei dati operativi	Alto	Basso	2–3
Aggiornamento di sistemi operativi e applicazioni	Medio	Basso	2–3
Sviluppo	Alto	Basso	2–3
Backup dei dati OT	Alto	Basso	3–4
Distribuzione semiautomatica delle definizioni di virus	Medio	Basso	2–3
Bilancia	Medio	Medio	2–3
Comando dello scarico	Medio	Basso	2–3
Gru	Alto	Alto	4
Combustione e caldaia	Alto	Alto	4
Depolverazione	Autonomo	Medio-alto	3
Denitrificazione	Medio	Medio	3
Depurazione dei gas di combustione	Alto	Medio-alto	4
Misurazione delle emissioni	Alto	Medio	3–4
Trituratore	Medio	Basso	2
Estrazione delle scorie	Alto	Alto	3–4
Trattamento delle acque reflue	Alto	Medio	3–4
Mezzi operativi	Medio	Medio-alto	3
Misurazione della radioattività	Basso	Basso	2–3
Scorie (rimozione)	Basso	Basso	2–3
Turbina	Medio	Basso	3
Ceneri leggere	Medio	Medio-alto	2–3
Teleriscaldamento, elettricità, vapore	Medio	Alto	3–4
Aria compressa	Basso	Alto	3–4
Produzione di acqua grezza	Medio	Alto	3–4
Trattamento delle acque	Alto	Alto	4
Accesso e autorizzazione	Medio	Basso	3–4
Videosorveglianza	Basso	Basso	2–3
Componenti di rete OT-IT	Basso	Basso	2–3
Fatturazione, consegna	Alto	Basso	2–3
Valutazione dei dati operativi	Alto	Basso	2–3
Vendita di energia	Medio	Basso	2–3
Backup dei dati IT	Alto	Basso	3–4
Conformità e reporting	Alto	Basso	2–3
Registro dei turni	Basso	Basso	2–3
Emergenze (primo intervento, autorità, personale)	Medio	Basso	2

Tabella 3: processi critici negli IIRU

La figura 9 illustra la forte dipendenza dei processi principali (infrastrutture, smaltimento e gestione aziendale) dai sistemi o sottoprocessi definiti critici. In questo modo vogliamo dimostrare che la mancata esecuzione di un sottoprocesso solitamente non si ripercuote solo su un processo principale, bensì su più processi allo stesso tempo.

L'impatto dei sottoprocessi sui processi principali è illustrato nella tabella a pagina 23.

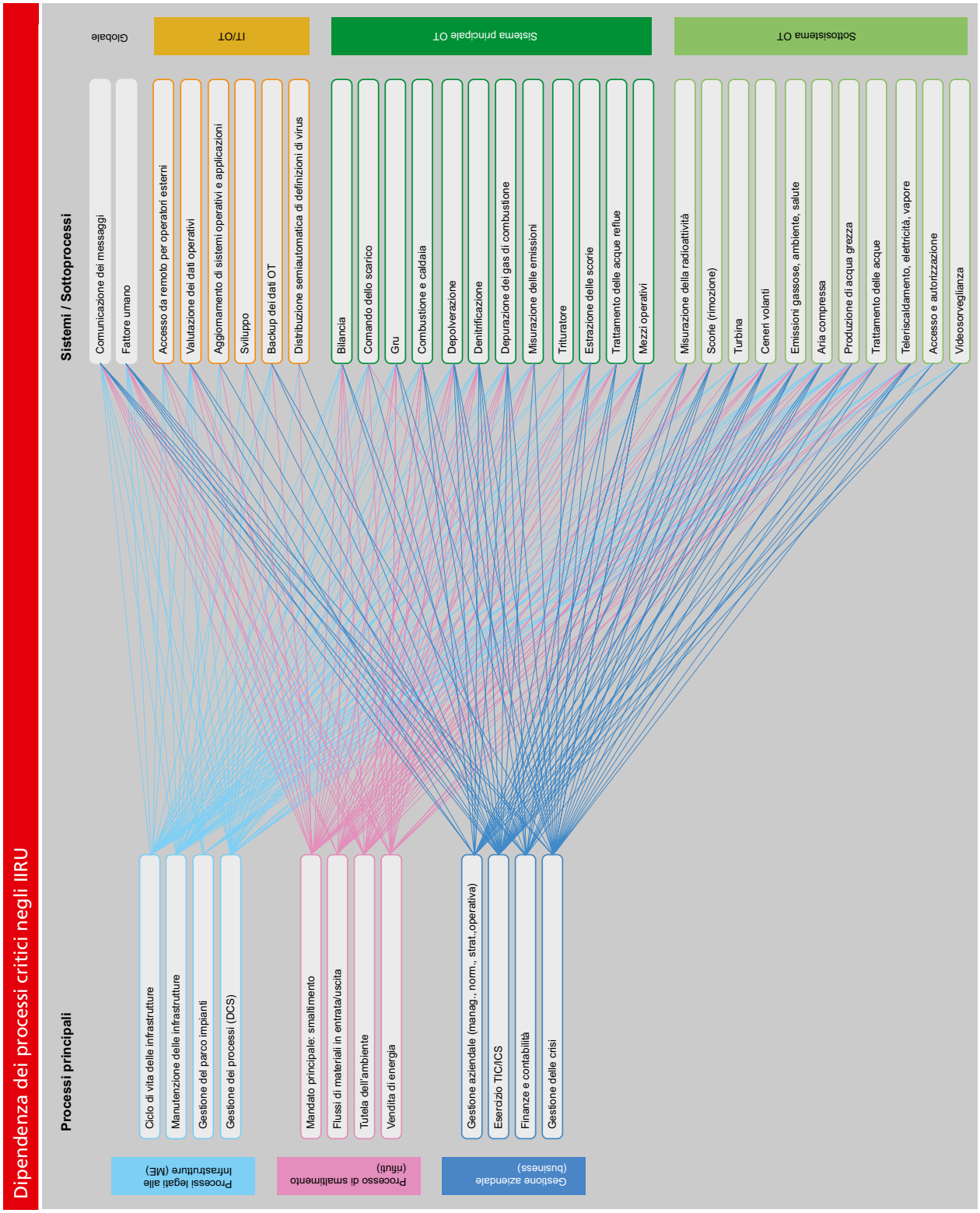


Figura 9: dipendenza dei processi critici negli IIRU

Dipendenza dai sistemi IT/OT dei processi critici negli IIRU															
Categoria	Sistemi/Sottoprocessi	Processi principali													
		Processi legati alle infrastrutture (ME)				Processo di smaltimento (rifiuti)				Gestione aziendale (business)					
		Ciclo di vita delle infrastrutture	Manutenzione delle infrastrutture	Gestione del parco impianti	Gestione dei processi (DCS)	Mandato principale: smaltimento	Flussi di materiali in entrata/uscita	Tutela dell'ambiente	Vendita di energia	Gestione aziendale (manag., norm., strat., operativa)	Esercizio TIC/ICS	Finanze e contabilità	Gestione delle crisi		
Globale	Comunicazione dei messaggi	x	x	x	x	x	x	x	x	x	x	x	x		
	Fattore umano	x	x	x	x	x	x	x	x	x	x	x	x		
Operazioni IT	Accesso da remoto per operatori esterni	x	x		x	x		x			x				
	Valutazione dei dati operativi	x	x	x	x	x	x	x	x	x		x			
	Aggiornamento di sistemi operativi e applicazioni		x		x	x					x				
	Sviluppo		x		x	x					x				
	Backup dei dati OT	x	x		x	x					x		x		
	Distribuzione semiautomatica di definizioni di virus				x	x					x				
Sistema principale OT	Bilancia/controllo in entrata	x	x		x	x	x	x			x	x			
	Comando dello scarico	x	x		x	x	x		x		x				
	Gru	x	x		x	x	x		x		x		x		
	Combustione e caldaia	x	x		x	x		x	x	x	x		x		
	Depolverazione	x	x		x	x	x	x	x	x	x	x	x		
	Denitrificazione	x	x		x	x	x	x	x	x	x	x	x		
	Depurazione dai gas di combustione	x	x		x	x	x	x	x	x	x	x	x		
	Misurazione delle emissioni	x	x		x	x	x	x			x		x		
	Trituratore	x	x				x						x		
	Estrazione delle scorie	x	x		x	x	x	x		x	x	x	x		
	Trattamento delle acque reflue	x	x		x	x	x	x		x	x	x	x		
	Mezzi operativi	x	x		x	x	x	x		x	x	x	x		
Sottosistema OT	Misurazione della radioattività	x	x		x		x	x		x	x		x		
	Scorie (rimozione)					x	x	x		x	x	x	x		
	Turbina	x	x		x			x		x	x	x	x		
	Ceneri volanti	x	x		x	x	x	x		x	x	x	x		
	Emissioni gassose, ambiente e salute	x	x	x	x	x	x	x		x	x	x	x		
	Teleriscaldamento, elettricità, vapore			x	x	x	x		x	x	x	x	x		
	Aria compressa	x	x	x	x	x			x		x		x		
	Produzione di acqua grezza	x	x	x	x	x	x	x	x	x	x		x		
	Trattamento delle acque	x	x	x	x	x			x		x		x		
	Accesso e autorizzazione	x	x							x	x		x		
	Videosorveglianza	x	x							x	x				

Tabella 4: dipendenza dai sistemi IT/OT dei processi critici negli IIRU

La tabella seguente descrive le possibilità di attacco ai processi e i loro effetti:

Processo	Possibilità di attacco	Effetto
Bilancia	Blocco	Arresto per impossibilità di inserimento rifiuti. In caso di emergenza è possibile effettuare manualmente un rilevamento della tipologia, del cliente, del peso?
Comando dello scarico	Blocco	Arresto per impossibilità di inserimento rifiuti.
Trituratore	Blocco	Riduzione dell'efficienza, una parte dei rifiuti (merce ingombrante) non può più essere riciclata.
Gru	Blocco o manipolazione	Arresto per impossibilità di caricamento della linea del forno.
Combustione e caldaia	Manipolazione del regolatore del rendimento del fuoco, alimentazione dell'acqua di caldaia	Arresto per impossibilità di combustione o per cattiva combustione; conseguente impossibilità di smaltimento in discarica. Rischio di danno completo alla caldaia a causa del surriscaldamento della muratura, della tubatura della caldaia e della griglia.
Estrazione delle scorie	Malfunzionamento nell'estrazione e nel trattamento	Arresto in caso di impossibilità di estrazione delle scorie o di materiale incombusto.
Depolverazione	Blocco	Emissione di polveri o ceneri leggere, con conseguente guasto totale del catalizzatore a valle.
Denitrificazione	Blocco dell'iniezione di ammoniaca o della regolazione della temperatura del catalizzatore (bruciatore/vapore)	Mancato rispetto dell'ordinanza contro l'inquinamento atmosferico (OIAt), con conseguente spegnimento dell'impianto. Guasto totale dell'impianto quando il catalizzatore diventa inutilizzabile a causa della manipolazione di processi a monte. Bypass del catalizzatore consentito solo per un breve periodo di tempo.
Depurazione dei gas di combustione	Manipolazione o blocco dello scrubber dei gas di combustione	Distruzione dello scrubber per surriscaldamento e conseguente spegnimento della linea di combustione.
Alimentazione (aria compressa, acqua di raffreddamento, prodotti chimici)	Manipolazione o blocco di vari sottosistemi rilevanti per il processo	Le valvole di controllo entrano in posizione di sicurezza senza aria compressa, ecc. Arresto delle linee di combustione.

Tabella 5: processi, possibilità di attacco ed effetti

La tabella seguente descrive le possibilità di attacco ai prodotti/output e i loro effetti:

Prodotti e output	Possibilità di attacco	Effetto
Ceneri, scorie, residui di filtraggio	Perturbazione del processo di smaltimento	Stoccaggio indesiderato sul sito, impossibilità di onorare i contratti di fornitura con le discariche (p. es. discarica o sito di stoccaggio sotterraneo per le ceneri leggere).
Acque reflue	Perturbazione del processo	Inquinamento delle acque, interruzione di tutti i processi a monte e conseguente spegnimento dell'intero impianto. Perdita dell'autorizzazione d'esercizio.
Elettricità e calore	• Manipolazione del processo di estrazione del calore • Manipolazione della turbina	• Destabilizzazione della rete di teleriscaldamento • Minaccia a infrastrutture critiche come ospedali o edifici governativi. • Distruzione meccanica per eccesso di velocità, con conseguente guasto operativo.
Emissioni gassose	Misurazione assente o errata	Minaccia di perdita dell'autorizzazione d'esercizio, danni alla reputazione. Responsabilità in caso di emissioni indesiderate e dannose per la salute.

Tabella 6: prodotti e output, possibilità di attacco ed effetti

Nella maggior parte dei processi, il pericolo maggiore è rappresentato da un blocco o da una manipolazione. Tutti gli incidenti comportano un guasto operativo e costi elevati/molto elevati.

6 Protezione delle informazioni

6.1 Protezione delle informazioni

La protezione delle informazioni mira a proteggere adeguatamente le informazioni e l'infrastruttura TIC in base agli obiettivi prefissati quali la confidenzialità, l'integrità e la disponibilità. Si tratta di impedire l'accesso non autorizzato ai sistemi o la manipolazione di dati e di ridurre il più possibile i rischi e i conseguenti danni economici.

È irrilevante che i dati si riferiscano a persone o meno. Le informazioni possono essere conservate in forma cartacea o elettronica.

Nella vita quotidiana le espressioni «protezione delle informazioni», «protezione dei dati» e «sicurezza informatica» vengono spesso confuse o utilizzate nel contesto sbagliato.

Come si evince dalla figura seguente, la protezione dei dati e la sicurezza informatica fanno parte della protezione delle informazioni, che a sua volta è un elemento essenziale della gestione dei rischi dell'impresa e della gestione della continuità operativa.

6.2 Strategia di protezione delle informazioni

Una strategia di protezione delle informazioni efficace protegge i mezzi di cui dispone un'organizzazione per eseguire i processi interni (critici). Non esiste una definizione generale valida dei requisiti o delle soluzioni.

Per individuare e trattare i rischi per la sicurezza nell'ambito dei sistemi critici di informazione e di comunicazione è necessaria una strategia di protezione delle informazioni a più livelli con un approccio *defense in depth*[2].

Oltre alle **misure tecniche** questa strategia dovrebbe comprendere anche **i relativi processi, la formazione e l'istruzione** dei collaboratori nonché la necessaria **governance della sicurezza** per attuare e gestire correttamente la sicurezza delle informazioni.

[2] *Cfr. capitolo 3 Obiettivi dello standard minimo*

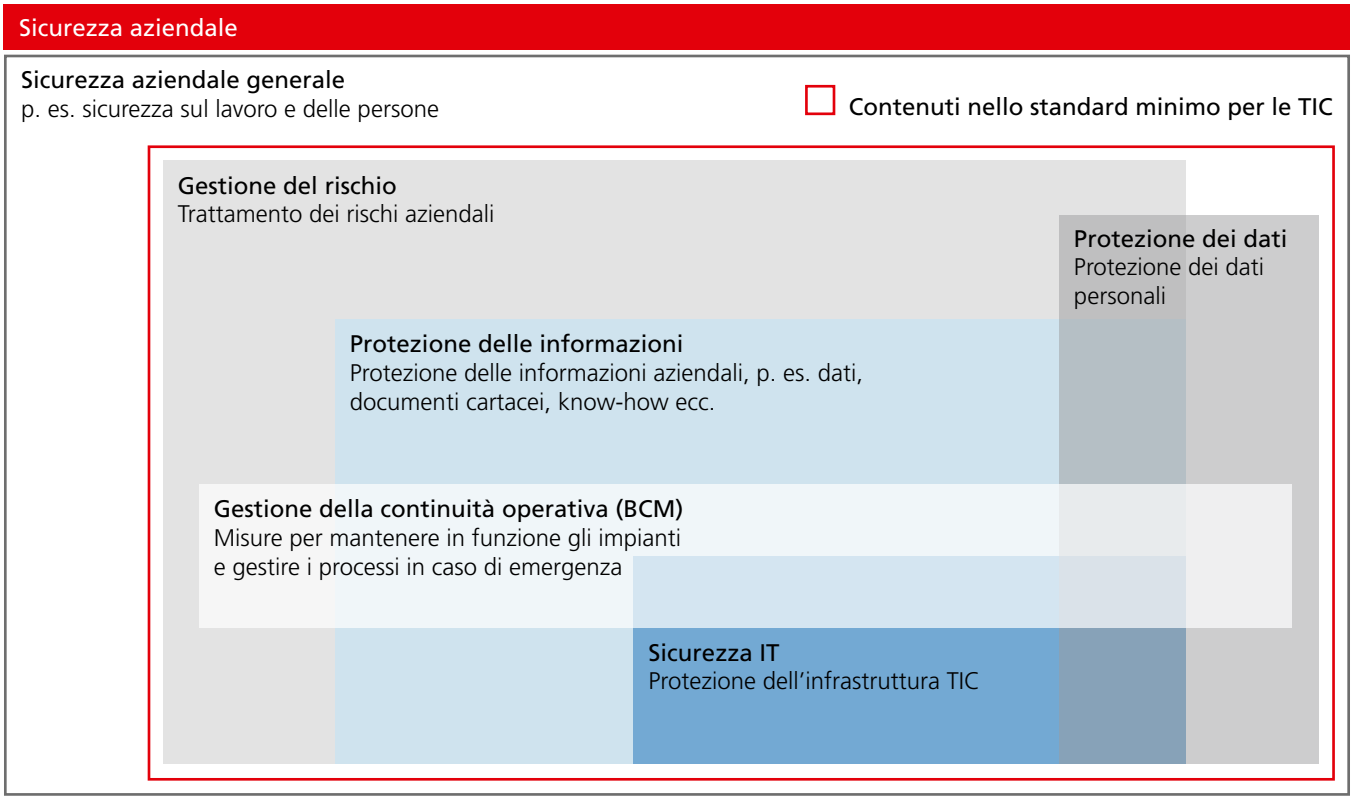


Figura 10: sicurezza aziendale

Figura 11: aspetti della sicurezza delle informazioni

Le strategie *defense in depth* sono individuali e devono considerare le esigenze, le possibilità e i rischi ai quali è esposta l'organizzazione. L'approccio basato sul rischio tiene conto della dipendenza dai processi o dalle risorse esterni oltre che da quelli interni.

La strategia parte dal presupposto che non è possibile garantire una protezione totale contro qualsiasi tipo di cyberrischi. L'organizzazione è consapevole della propria vulnerabilità e sviluppa strategie e misure per identificare il grado di esposizione ai rischi legati alla protezione delle informazioni *(identify)*, proteggersi al meglio *(protect)*, individuare le lacune nella cybersicurezza *(detect)* e reagire di conseguenza *(respond)* per ripristinare quanto prima una situazione normale *(recover)*.

N.B.: la sicurezza delle informazioni non è da intendersi come un progetto una tantum, ma come un processo continuo di garanzia della qualità basato sul ciclo PDCA (*Plan-Do-Check-Act,* pianificare-fare-verificare-agire).

6.3 Possibili misure per una maggiore protezione delle informazioni

Dati	Misura
E-mail	Non inviare informazioni classificate o password per e-mail.
Classificazione di dati	Classificare i dati in maniera corretta.
Diritti di accesso ai dati	Gestire le autorizzazioni in maniera corretta.
Luogo di salvataggio dei dati	Salvare i dati classificati soltanto su supporti sicuri.
Scambio di dati con fornitori	Utilizzare una piattaforma di scambio dati sicura, scambiare soltanto dati rilevanti.
Backup	Effettuare controlli regolari dei dati salvati, conservare i supporti dati esternamente o offline.
Dati nel cloud	Assicurare la disponibilità anche offline dei dati importanti qualora non fosse possibile collegarsi al cloud.
Piani di emergenza	Rendere disponibili i piani in formato cartaceo.
Dati nei social media	Pubblicare solo lo stretto necessario per evitare che si possa risalire alla fonte.
Password	Assicurare la complessità (direttiva in materia di password). La pratica migliore è l'autenticazione multifattoriale (MFA). Cfr. Centro nazionale per la cibersicurezza (NCSC): Proteggete i vostri account

Tabella 7: misure di attuazione della sicurezza delle informazioni (elenco non esaustivo)

6.4 Protezione dei dati

La protezione dei dati comprende la protezione dei «dati personali»[3] e dei «dati personali degni di particolare protezione»[4] nonché la protezione del diritto all'autodeterminazione di ogni individuo per quanto riguarda le informazioni che lo riguardano. Prevede misure organizzative e tecniche contro il trattamento e l'utilizzo abusivi dei dati personali.

In Svizzera, la protezione dei dati si basa sulla legge federale sulla protezione dei dati (LPD) e sulla relativa ordinanza (OLPD). Se però vengono trattati dati di cittadini europei (clienti, collaboratori) potrebbe essere necessario tener conto anche delle prescrizioni del Regolamento generale dell'UE sulla protezione dei dati (RGPD).

La digitalizzazione ha permesso di conservare, trattare, raccogliere, trasmettere e analizzare in maniera via via più semplice una quantità crescente di dati e pertanto la loro protezione ha assunto un'importanza sempre maggiore. Le innovazioni digitali come Internet, l'e-mail, il telefono cellulare, la videosorveglianza e i metodi di pagamento elettronico ampliano sempre più le possibilità di raccolta di dati personali.

Al salvataggio e al trattamento dei dati personali si applicano, tra l'altro, i seguenti principi:

- i dati personali possono essere trattati soltanto in modo lecito;
- il trattamento dei dati deve essere conforme al principio della buona fede e della proporzionalità.

I dati personali possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, legato alle circostanze o previsto dalla legge.

6.5 Sicurezza IT

In quanto sottoambito della protezione delle informazioni, la sicurezza informatica serve a proteggere le informazioni salvate elettronicamente (dati), ad assicurarne il trattamento e a raggiungere gli obiettivi di confidenzialità, disponibilità e integrità. Deve inoltre garantire il funzionamento senza interruzioni e l'affidabilità dei sistemi TIC.

Vanno presi in considerazione anche i sistemi che spesso non sono considerati propriamente sistemi TIC, p. es. impianti telefonici, ICS o l'Internet delle cose (IoT).

Con l'utilizzo di sistemi cloud, il campo d'azione della sicurezza IT tradizionale va oltre il perimetro dell'azienda e si estende al cyberspazio.

I fornitori sono sempre più interessati a raccogliere e ad analizzare dati, da un lato, per migliorare i loro prodotti e, dall'altro, per tracciarne l'impiego. La comunicazione di questi dati richiede un esame preliminare minuzioso, un accertamento preciso e una regolamentazione per contratto. Andrebbe anche definito attraverso quali connessioni sicure e con quali intervalli (in tempo reale, quotidianamente, settimanalmente) i dati vengono trasmessi ai fornitori.

[3] Definizione secondo l'art. 3 lett. a LPD
[4] Definizione secondo l'art. 3 lett. c LPD

6.6 Consapevolezza dei collaboratori *(awareness)*

L'esperienza degli ultimi anni ha mostrato che la tecnologia in materia di sicurezza non è sufficiente per contrastare gli attacchi sempre più sofisticati e le minacce crescenti provenienti dal cyberspazio.

Per questo motivo, tutti i collaboratori dovrebbero seguire regolarmente una formazione sulla sicurezza informatica, in modo da acquisire una maggiore consapevolezza in materia.

Tramite una formazione dei collaboratori che tenga conto del loro livello di competenze si riduce notevolmente il rischio di comportamenti sbagliati involontari.

Obiettivi della formazione:

- motivare i collaboratori ad adottare un comportamento consapevole in materia di sicurezza;
- insegnare come gestire i rischi e gli incidenti;
- promuovere e rafforzare l'accettazione della tematica della sicurezza delle informazioni;
- fornire ai collaboratori i mezzi per capire e sostenere attivamente le misure riguardanti la sicurezza.

Lo scopo di un programma di sensibilizzazione è di conferire ai collaboratori una competenza inconscia in materia di sicurezza delle informazioni, ossia fare in modo che adottino spontaneamente il comportamento corretto in situazioni difficili e delicate. Per raggiungere questo obiettivo è necessario attuare in maniera continua un programma di sensibilizzazione.

6.7 Governance

La governance indica l'insieme di principi e regole che permettono ai quadri superiori di gestire e monitorare strutture e comportamenti.

La governance è fondamentale per l'attuazione efficace e duratura della strategia di sicurezza delle informazioni: crea le condizioni necessarie per individuare, valutare e trattare le minacce che incombono sulla sicurezza delle informazioni nell'impresa. La governance rappresenta una metastruttura volta a sostenere l'impresa nella realizzazione dei suoi obiettivi in materia di sicurezza delle informazioni sul piano strategico, funzionale e operativo. Prima di rendere operative le proprie misure di sicurezza, l'impresa deve 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 sicurezza TIC definiscono le regole, le procedure, le metriche e le strutture organizzative necessarie per renderne efficaci il controllo e la pianificazione.

7 Temi chiave

7.1 Segmentazione della rete

7.1.1 Separazione fisica

Il metodo più affidabile per controllare e delimitare il traffico tra più reti consiste nel separare fisicamente i segmenti della rete. La separazione fisica richiede l'impiego di numerosi dispositivi, come switch, router e gateway di sicurezza ed è pertanto molto costosa. Si consiglia pertanto di effettuarla principalmente nei punti più sensibili della rete, per esempio:

- connessioni tra varie sedi;
- connessioni tra zone sensibili della rete, per esempio il sistema di controllo o i sistemi informatici degli uffici di una sede;
- connessioni tra la rete dell'impresa e le reti esterne, per esempio Internet.

7.1.2 Rete di area locale virtuale (VLAN)

Se una volta eseguita l'analisi dei rischi la separazione fisica dei segmenti di rete non risultasse strettamente necessaria, si può optare per una segmentazione logica tramite VLAN. Ne risulta un rischio residuale maggiore rispetto alla separazione fisica, dovuto per esempio a errori di configurazione o a scenari di attacco quali il salto di VLAN.

7.2 Segmentazione della rete secondo il modello «Purdue»[5]

Il modello di riferimento Purdue è stato sviluppato negli Stati Uniti nei primi anni 1990 da Theodore J. Williams all'Università Purdue, in Indiana. Concepito originariamente per reti non industriali, è in seguito stato adattato per l'impiego su reti di automazione.

Il modello Purdue suddivide una rete industriale in maniera astratta in diversi livelli e può così servire da punto di partenza per misure elaborate secondo il principio *defense in depth*.

Nel modello Purdue si ritrova anche il principio di suddividere una rete di questo tipo in zone e in passaggi tra zone, tenendo presente che va fatta una distinzione tra «zona» e «livello». Un livello rappresenta una classificazione gerarchica all'interno della rete dell'impresa, mentre una zona indica la segmentazione specifica in base ai requisiti di sicurezza. Una zona può in certi casi estendersi su vari livelli.

7.2.1 Segmentazione orizzontale della rete

Questo modello protegge i processi di automazione critici e sensibili contro gli accessi non autorizzati da segmenti di rete non affidabili. Il modello a zone prevede sette zone che assumono determinate funzioni e comprendono una serie di sistemi suddivisi in base alla loro necessità di protezione. I terminali critici sono disposti esclusivamente nelle zone 1 e 2 e separati da altre zone mediante adeguati gateway di sicurezza.

7.2.2 Segmentazione verticale della rete

La segmentazione verticale suddivide per esempio la rete per sedi o sistemi. In questo modo è possibile gestire sullo stesso livello orizzontale di rete varie sedi che presentano esigenze di protezione diverse. I canali di comunicazione e le interfacce necessarie sono realizzati mediante gateway di sicurezza. La comunicazione tra le zone avviene tramite canali di comunicazione sicuri, documentati e definiti in maniera chiara.

In caso di evento di sicurezza i danni possono essere circoscritti alla rispettiva zona e ai sistemi che vi si trovano. I sistemi vengono classificati in base a criteri predefiniti, assegnati alle diverse zone orizzontali e raggruppati all'interno di queste ultime.

I criteri di raggruppamento possono essere la criticità, i rischi, le tecnologie, gli ambiti di responsabilità organizzativi e le condizioni fisiche.

[5] *Fonte: www.sichere-industrie.de (disponibile solo in tedesco). Descrizione delle zone e del modello.*

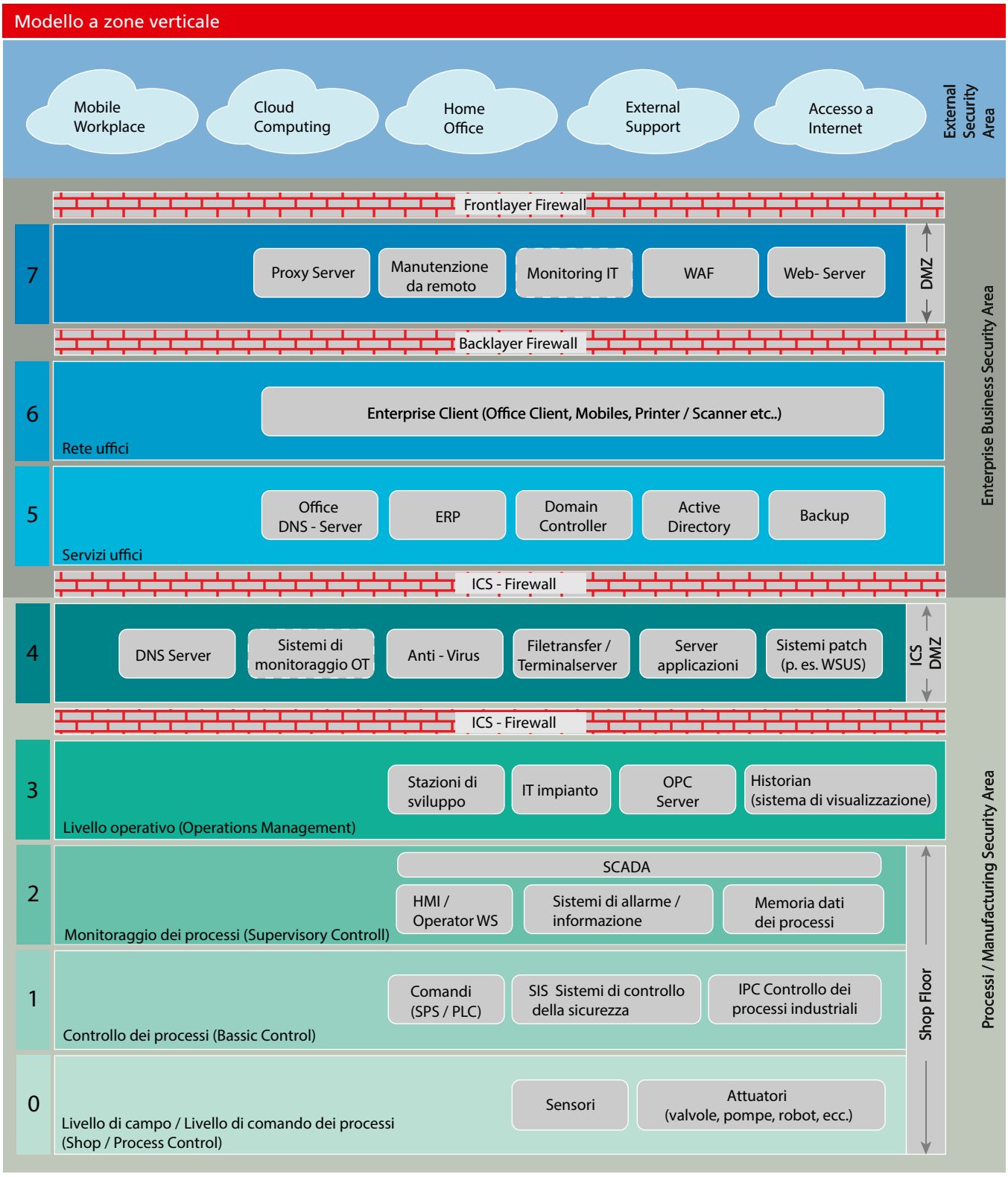


Figura 12: modello a zone verticale

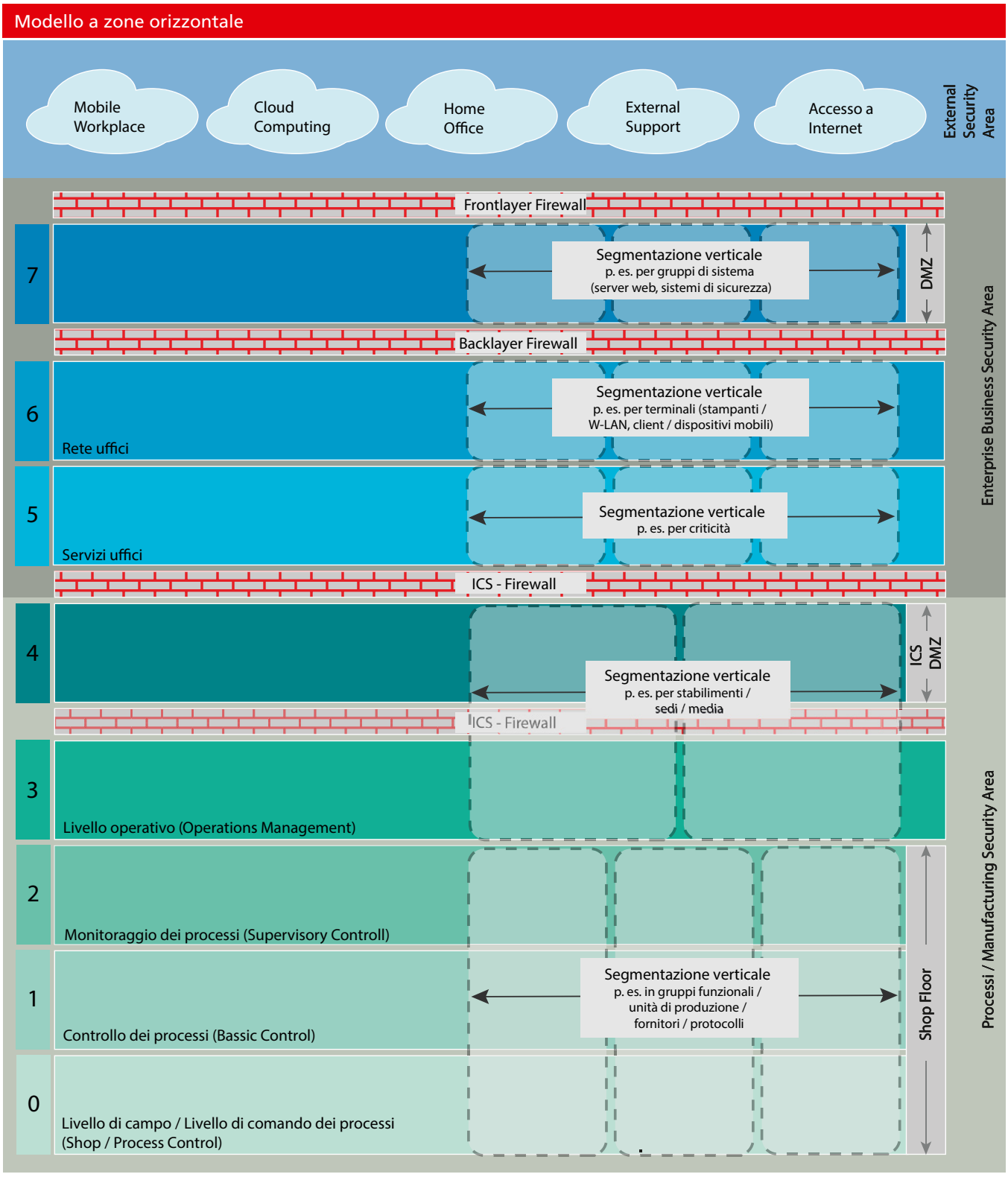


Figura 13: modello a zone orizzontale

Livello di campo/Livello di controllo dei processi (livello 0)

Al livello più basso si svolge il processo fisico vero e proprio delle attività. I comandi dei sistemi che si trovano al livello 1 vengono attuati in tempo reale. Questo livello viene definito anche «livello di dispositivo» *(device)* o «livello di campo».
Sistemi tipici: motori, valvole, pompe, comandi a distanza ingresso/uscita *(Remote I/O)*

Controllo dei processi (livello 1)

Qui si trovano i sistemi che influiscono direttamente sull'esecuzione e sul comando dei processi fisici. Tra i loro compiti rientrano la sorveglianza dei sensori e il mantenimento del funzionamento corretto dell'impianto. Questi sistemi lavorano in tempo reale e un guasto a questo livello condiziona direttamente il processo di automazione.
Sistemi tipici: controllori logici programmabili (PLC), sistemi di controllo, di supervisione e acquisizione dati (SCADA), sistemi di controllo distribuito (DCS), unità terminali remote (RTU)

Monitoraggio del processo (livello 2)

I sistemi del livello 2 riguardano la sorveglianza e il controllo di processi specifici. L'elaborazione dei dati non avviene ancora in tempo reale e pertanto un guasto dei sistemi locali non ha alcun impatto diretto sulla disponibilità della soluzione di automazione.
Sistemi tipici: interfacce uomo-macchina (HMI), sistemi di allarme e di notifica, memorie dei dati di processo

Livello operativo (livello 3)

Al livello 3 si trovano i sistemi che servono principalmente all'esercizio. Questo livello riguarda, da un lato, la messa a disposizione dei sistemi, dei servizi e delle applicazioni necessari alla rete industriale e, dall'altra, la pianificazione delle varie fasi di automazione.
Sistemi tipici: IT impianto, ovvero sistema dei nomi di dominio (DNS), protocollo di configurazione IP dinamica (DHCP), *Active Directory,* ecc., le stazioni di sviluppo, i sistemi di gestione e di controllo della funzione produttiva (MES)

ICS DMZ (livello 4)

La DMZ è una sottorete nella quale si trovano connessioni provenienti da segmenti con una necessità di protezione maggiore. Una DMZ viene classicamente interposta tra la rete degli uffici e Internet; vi si trovano sistemi quali i server web che devono essere accessibili da Internet. Nel presente contesto, la zona demilitarizzata viene impiegata tra la zona uffici e la zona impianti per depositarvi per esempio le risorse condivise.
Sistemi tipici: sistemi antivirus, sistemi di manutenzione a distanza, server di scambio di file, sistemi patch

Servizi uffici/Rete uffici (livelli 5 e 6)

Qui si trovano i sistemi che sostengono le attività dell'impresa, tra cui quelli utilizzati dagli uffici contabilità, vendite e del personale. Tra i livelli 4 e 3 si trova l'interfaccia con la rete dell'impianto, per la quale la rete dell'impresa risulta estremamente poco sicura.
Sistemi tipici: sistemi di pianificazione delle risorse d'impresa (ERP), accesso a Internet, accessi per la manutenzione da remoto, postazioni di lavoro degli uffici

DMZ (livello 7)

Questo livello di rete rappresenta una specie di «zona cuscinetto» che assicura l'integrazione tra la rete IT dell'impresa e Internet o altre reti esterne.

Traffico di dati tra le zone

In linea di massima le zone sono isolate le une dalle altre e non possono comunicare. In caso di esigenza di comunicazione è necessario definire, documentare e aprire tramite gateway di sicurezza la sorgente, la destinazione e la porta IP. Queste eccezioni vanno verificate periodicamente.

Reti wireless

Le reti wireless consentono di accedere facilmente e senza cavi alla rete dell'impresa. Per questo motivo, alla protezione di queste reti va dedicata particolare attenzione.

Molti sistemi offrono inoltre la possibilità di connettersi tramite Bluetooth, raggi infrarossi o comunicazione di prossimità (NFC). In genere queste connessioni sono scarsamente protette e possono essere utilizzate come vettori di attacco.

Si raccomanda pertanto di non utilizzarle. Nei sistemi nei quali non è possibile disattivarle è necessario adottare misure di protezione speciali.

Misure possibili:
A seconda della posizione del trasmettitore, le radiazioni Bluetooth possono superare l'involucro dell'edificio ed essere captate nello spazio pubblico entro un raggio di 100 m; eventuali misure edilizie possono impedirlo. Il Bluetooth utilizza la banda di 2,4 GHz e quindi ha una lunghezza d'onda di circa 12 cm. Una griglia metallica con messa a terra e una maglia inferiore a 12 cm posta tra il trasmettitore e l'involucro dell'edificio è in grado di schermare in maniera efficace le radiazioni.

7.2.3 Telefoni cellulari e tablet[6]

Oggi gli smartphone e i tablet sono sempre più usati in ambito professionale e costituiscono in molti casi il principale strumento di lavoro. Gli innumerevoli apparecchi attualmente disponibili funzionano con vari sistemi operativi. Gli smartphone e tablet dotati di sistema operativo iOS o Android, moderni e semplici da utilizzare, sono destinati più al grande pubblico che a un uso professionale, che invece richiede un livello di protezione elevato.

Sono quindi molto diversi dai terminali mobili concepiti specificamente per le imprese. Ciononostante, i dispositivi iOS e Android sono sempre più usati dai professionisti, al punto di soppiantare soluzioni consolidate come i laptop.

Il tipo di impiego e la gestione dei terminali mobili vanno valutati in base alle esigenze di protezione: per una protezione ridotta o normale, è sufficiente utilizzare programmi nativi, per una protezione maggiore o elevata va utilizzata una soluzione per la gestione dei dispositivi mobili (MDM), associata eventualmente a un programma di registrazione dei dispositivi (DEP). Se è necessaria una protezione elevata, si consiglia l'impiego di un container sicuro *(secure container)*, che rappresenta l'unico modo per evitare il più possibile l'interazione tra un uso professionale e un uso privato del terminale mobile e per conservare in maniera sicura i dati dell'impresa.

Prima di integrare i terminali mobili nella struttura di un'impresa, è opportuno definire regole chiare per l'integrazione. Queste direttive di sicurezza definiscono tra l'altro le condizioni generali per la scelta dei dispositivi, la selezione dei dati che possono essere elaborati sui dispositivi, le restrizioni per gli utenti e la limitazione delle possibilità offerte dagli apparecchi (hardware e software).

Un rischio residuo permane anche quando sui terminali mobili si applicano impostazioni sicure, che limitano ampiamente le libertà d'uso degli utenti e le possibilità offerte dalle applicazioni. Questo rischio è dovuto in primo luogo al fatto che i dispositivi vengono utilizzati al di fuori di un ambiente protetto, spesso in una situazione in cui non si utilizzerebbe per esempio un laptop. C'è sempre il rischio che i dispositivi (e quindi i dati che contengono) possano andare perduti. In questo caso si può solo fare affidamento sul fatto che i meccanismi impiegati per proteggere i dati siano ancora efficaci e che le misure prese a posteriori funzionino (p. es. la pulizia remota, *remote wipe*).

La presenza di rischi residui difficili da contrastare non può essere esclusa nemmeno in caso di impiego di un container sicuro, per esempio se il microfono del dispositivo viene usato illegalmente per effettuare intercettazioni.

Ulteriori informazioni sulle misure di protezione dei dispositivi mobili si trovano nel documento «Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit» del BSI.

7.3 Servizi cloud

Il termine «cloud» è la forma abbreviata di «cloud computing». Un cloud è composto da vari server distanti gli uni dagli altri, ai quali è possibile accedere in qualsiasi momento da ovunque tramite una connessione Internet sicura e protetta.

Cloud privato

Quando un'impresa usa i propri server per il cloud computing, si parla di cloud privato. In questo caso gli utenti accedono ai server dell'impresa. I dati e i servizi che vi sono conservati non sono accessibili al pubblico. I dati critici dal punto di vista della sicurezza rimangono quindi all'interno dell'impresa. L'uso di un cloud privato implica tuttavia molto lavoro per l'amministrazione di sistema, richiede molto tempo ed è costoso.

Cloud pubblico

Un cloud pubblico offre i suoi servizi a vari utenti contemporaneamente via Internet (infrastruttura condivisa). Il fornitore assicura la sorveglianza, la manutenzione e l'adeguamento continuo del sistema alle esigenze dell'utente. L'impresa non deve quindi sostenere i costi per la creazione, il mantenimento e l'aggiornamento di un'architettura di server interna.

[6] Fonte: Pubblicazione dell'Ufficio federale tedesco per la sicurezza delle tecnologie dell'informazione (BSI) relativa alla cybersicurezza, iOS, disponibile solo in tedesco (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_074.pdf?__blob=publicationFile&v=1)

Cloud ibrido

La combinazione delle due soluzioni è definita «cloud ibrido». In questo caso i dati sensibili sono conservati presso l'impresa, mentre altri dati di lavoro sono accessibili in maniera sicura tramite un'infrastruttura condivisa.

Esempi di applicazione dei servizi cloud:

- analisi dei dati di esercizio (processi OT);
- applicazioni di comunicazione e di workflow;
- protezione degli endpoint;
- gateway e servizi e-mail;
- sistemi di telefonia;
- informatica d'ufficio;
- sistemi di allarme (SMS, e-mail, workflow).

Modelli di servizi cloud

I modelli di servizi disponibili in cloud sono:
- infrastruttura come servizio (IaaS);
- piattaforma come servizio (PaaS);
- software come servizio (SaaS);
- desktop come servizio (DaaS).

Architettura di sicurezza del cloud

Ogni modello di servizi cloud ha una propria architettura di sicurezza, gestita dal fornitore e dal cliente. Le architetture di sicurezza sono diverse a seconda che si tratti di un cloud pubblico, privato o ibrido.

In base alla criticità delle informazioni trattate, anche un'applicazione cloud (cloud privato) deve essere inserita nella corrispondente categoria di protezione ed essere protetta con misure adeguate.

Responsabilità in materia di sicurezza nel cloud

Queste responsabilità dipendono dal modello di servizio e di fornitura; fondamentalmente, fino a un certo punto, è condivisa.

Nel caso di una soluzione IaaS di servizi cloud di tipo pubblico, il fornitore gestisce per esempio le interfacce di rete fisiche, gli ipervisori e l'archivio dati, mentre il cliente si occupa dei sistemi operativi, delle applicazioni e dei dati.

In questa architettura il provider del cloud sorveglia la sicurezza «esterna» del cloud, ovvero l'hardware e il software essenziali, per esempio banche dati e capacità di calcolo di un centro di calcolo. Il cliente si concentra invece sulla sicurezza «interna», per esempio come concedere o rifiutare le richieste di accesso, come configurare i firewall dell'impresa e come gestire altre attività al momento dell'utilizzo di un servizio cloud.

Nel caso dei modelli PaaS, SaaS e DaaS impiegati in un cloud pubblico, il fornitore di servizi ha una maggiore responsabilità in materia di sicurezza rispetto al modello IaaS. Il cliente che opta per esempio per il modello SaaS non deve occuparsi della gestione dei server, delle banche dati e dei rispettivi meccanismi di sicurezza (come la crittografia end-to-end). Un simile accordo non significa però che il SaaS sia privo di rischi: il cliente deve effettuare un esame approfondito del provider del cloud e verificare che l'accesso alle applicazioni sia sufficientemente sicuro.

I cloud privati e i cloud ibridi che un'organizzazione utilizza per gestire le risorse per uso proprio richiedono in genere maggiori responsabilità da parte del cliente per quanto riguarda la conservazione sicura dei dati. La gestione di dati nei cloud privati o ibridi presenta alcuni vantaggi, perché questi dati dipendono meno da un'infrastruttura condivisa rispetto ai dati conservati in un cloud pubblico. L'onere diretto in materia di sicurezza per il cliente può tuttavia essere maggiore.

Accordo sul livello di servizio (SLA)

Un cloud SLA è un accordo concluso tra un fornitore di servizi cloud e un cliente con lo scopo di assicurare il livello minimo accettabile del servizio. L'accordo garantisce un certo grado di affidabilità, disponibilità e reattività dei sistemi e delle applicazioni, stabilisce le responsabilità in caso di interruzione del servizio e descrive le sanzioni previste se il livello di servizio non viene raggiunto.

La funzione di uno SLA è in fondo la stessa di un contratto: si tratta di un documento che disciplina i rapporti tra il cliente e il fornitore. Queste regole concordate formano la base della collaborazione.

Il livello di servizio definito nello SLA deve essere specifico e misurabile per consentire un'analisi comparativa e, se l'accordo lo prevede, versare premi o applicare penali.

8 Conclusioni

La sicurezza delle informazioni non è fine a sé stessa. Le misure di protezione contro i cyberattacchi sono intese ad assicurare l'esercizio e l'affidabilità dell'intero impianto. Gli impianti di trattamento dei rifiuti hanno una rilevanza sistemica per quanto riguarda il loro compito primario di smaltimento dei rifiuti e quello secondario di approvvigionamento energetico per l'industria e le economie domestiche. La cybersicurezza e la cyberresilienza sono dunque parte integrante della gestione globale dei rischi e rappresentano un tema chiave per i decisori.

La sicurezza delle informazioni non è tuttavia solo compito dei dirigenti d'impresa: è fondamentale sensibilizzare tutti i collaboratori in merito a scenari di attacco sempre più ingegnosi.

Il presente standard per le TIC ha un duplice obiettivo: aiutare gli utenti a valutare lo stato del loro ambiente informatico e permettere loro di stabilire il grado di maturità della sicurezza delle informazioni, ponendosi per esempio le seguenti domande:

- sono state elaborate delle direttive e sono stati definiti dei processi?
- le misure vengono attuate in parte o interamente?
- tali misure sono sottoposte a valutazioni periodiche?
- è stato implementato un processo continuo di miglioramento?

Se i cyberattacchi vanno a buon fine possono perturbare massicciamente le attività e comportare perfino l'arresto dell'impianto, con conseguenze economiche e danni per l'immagine dell'impresa. Quando sono diretti contro le PMI del settore privato possono spesso metterne a rischio la sopravvivenza. Le buone pratiche formulate nel presente standard per le TIC e un processo di miglioramento continuo hanno lo scopo di rafforzare l'affidabilità dell'esercizio.

Oltre al presente manuale, l'AEP propone alle imprese che operano nel settore del trattamento dei rifiuti uno strumento di valutazione in formato Excel che riprende le raccomandazioni dello Standard minimo per le TIC[7]. Questo strumento è utile per valutare il grado di maturità di un'impresa o di un'organizzazione.

I contenuti del presente manuale non sono vincolanti, ma sono intesi a stimolare gli attori del settore del trattamento dei rifiuti a riflettere sul tema della cybersicurezza. La sicurezza delle informazioni non è uno stato, ma un processo. Il manuale mira a sostenere questo processo e a facilitarne l'attuazione.

[7] *Link allo strumento Excel «Standard minimo per le TIC»*

9 Basi, documenti e norme

Il presente manuale tiene conto di concetti, raccomandazioni e misure che si basano su diversi standard e altri documenti normativi (v. tabella qui di seguito).

Titolo	Anno	Editore/Breve descrizione
Misure di protezione dei sistemi di controllo industriali (ICS)	2018	Editore: **Centro nazionale per la cibersicurezza NCSC** Questa guida, che si basa sui documenti dell'Industrial Control Systems Cyber Emergency Response Team del Department of Homeland Security (ICS-CERT) e del National Institute of Standards and Technology (NIST) statunitensi descrive in modo sintetico e pragmatico, in sole 8 pagine, le 11 principali misure che deve attuare chi utilizza i sistemi SCADA.
Analisi dei rischi e delle vulnerabilità di un sottosettore	2015/ 2017	Editore: **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 cyberrischi (SNPC) e sulla Strategia nazionale per la protezione delle infrastrutture critiche (PIC). Scopo perseguito è l'analisi delle vulnerabilità in caso di guasti alle TIC.
Guida per la protezione delle infrastrutture critiche (Guida PIC)	2018	Editore: **Ufficio federale della protezione della popolazione (UFPP)** La guida è uno strumento inteso a verificare ed eventualmente migliorare la resilienza delle infrastrutture critiche; in particolare, è stata ideata per l'applicazione in sottosettori critici da parte di gestori, associazioni di categoria e autorità specializzate. Il documento descrive una delle possibili modalità di gestione dei rischi suddividendola nelle fasi di analisi (identificazione delle risorse, vulnerabilità e rischi), valutazione, misure e attuazione (verifica e miglioramento). La procedura può, anzi dovrebbe, essere integrata nella gestione dei processi oppure attuata su tale base.
Strategia nazionale per la protezione delle infrastrutture critiche (PIC)	2018	Editore: **Ufficio federale della protezione della popolazione (UFPP)** La strategia delinea il campo d'applicazione, definisce le infrastrutture critiche e fissa principi generali per la protezione delle infrastrutture critiche. La strategia nazionale si rivolge a tutti gli uffici attivi in materia di protezione delle infrastrutture critiche e, in particolare, alle autorità competenti, agli attori politici e ai gestori di infrastrutture critiche.
Strategia nazionale per la protezione della Svizzera contro i cyberrischi (SNPC)	2018	Editore: **Organo direzione informatica della Confederazione (ODIC)** Proteggere le infrastrutture d'informazione e comunicazione dai cyberrischi è un compito d'interesse nazionale. Il Consiglio federale ha quindi commissionato l'elaborazione di una strategia per difendere il nostro Paese dalle cyberminacce. La strategia è un ausilio per riconoscere questi rischi, imparare ad affrontarli, individuare le lacune e colmarle nel modo più efficiente ed efficace possibile. Il documento presenta inoltre le strutture già esistenti, definisce gli obiettivi con le relative misure (p es. analisi dei rischi e delle vulnerabilità di un sottosettore).

Tabella 8: basi e documenti

Titolo	Anno	Editore/Breve descrizione
Legge federale sull'approvvigionamento economico del Paese (legge sull'approvvigionamento del Paese, LAP)	Stato 2016	Editore: **Assemblea federale della Confederazione Svizzera** La LAP disciplina misure volte a garantire l'approvvigionamento del Paese con 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 crediti 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 delle misure è costituita dal presente manuale.

Tabella 8: basi e documenti

La seguente tabella presenta una serie di norme internazionali prese in considerazione per il presente manuale.

Titolo	Editore/Breve descrizione
ISO 27001 Information technology – Security techniques – Information security management systems – Requirements	Editore: **Organizzazione internazionale per la normazione (ISO)** Espone in dettaglio i requisiti di un sistema di gestione per la sicurezza delle informazioni (ISMS). La serie ISO 27000 comprende diversi standard di sicurezza informatica, fra cui sono da menzionare in particolare:
ISO 27002 Information technology – Security techniques – Code of practice for information security controls	• 27000 Panoramica e terminologia • 27001 Requisiti: basi e controllo degli obiettivi in allegato • 27002 Linee guida per le misure di sicurezza delle informazioni • 27003 Sistemi di gestione della sicurezza delle informazioni – Guida per l'attuazione • 27005 Gestione dei rischi • 27019 Misure di gestione della sicurezza delle informazioni per l'approvvigionamento energetico La serie di norme di sicurezza ISO 27000 è ampiamente diffusa e dovrebbe diventare determinante nei prossimi anni. Già oggi, osservare le norme ISO è considerato un buon approccio. Contrariamente ad altri standard o framework gli standard ISO sono meno dettagliati e quindi più flessibili, e possono essere costantemente migliorati ed ampliati su un lungo periodo. L'ISMS e il contenuto delle misure devono essere adattati e attuati tenendo conto delle specificità del settore.
ISO 22301 Security and resilience – Business continuity management systems – Requirements	Editore: **Organizzazione internazionale per la normazione (ISO)** Descrive in maniera dettagliata i requisiti ai quali deve rispondere un sistema di gestione della continuità operativa (BCMS).
ISO 31000 Risk management	Editore: **Organizzazione internazionale per la normazione (ISO)** Questa norma definisce le modalità di gestione dei rischi all'interno di un'organizzazione, che possono essere adattate all'ambiente specifico di ogni impresa. La norma presenta un approccio molto generale, non legato specificamente a un'industria o a un settore, e applicabile a qualsiasi tipo di rischio. Può essere utilizzata per tutta la durata di vita di un'impresa ed è implementabile a tutti i livelli aziendali nonché nel processo decisionale.
ISO 27005 Information security risk management	Editore: **Organizzazione internazionale per la normazione (ISO)/ Commissione elettrotecnica internazionale (IEC)** Questo standard contiene le linee direttrici per una gestione dei rischi sistematica e orientata ai processi che può supportare anche l'osservanza dei requisiti di gestione dei rischi previsti da ISO/IEC 27001.

Tabella 9: standard nazionali e internazionali sulla sicurezza TIC

Titolo	Editore/Breve descrizione
ISO 27019 Information security controls for the energy utility industry	Editore: **Organizzazione internazionale per la normazione (ISO)** La norma riguarda i sistemi e le reti per il controllo, la regolazione e il monitoraggio dei processi che servono per la produzione, il trasporto, lo stoccaggio e la distribuzione di energia elettrica, gas, petrolio e calore. Vi rientrano i sistemi di controllo, di automazione, di protezione, di sicurezza e di misurazione, comprese le tecnologie di comunicazione. La norma li riunisce nella definizione di processo di controllo. Rispetto alla norma ISO/IEC 27002, l'accento è posto sulle infrastrutture critiche necessarie per l'esercizio sicuro e affidabile e di cui tenere di conseguenza conto nei processi di gestione (disponibilità e integrità dei dati).
IEC 62264 e segg. Enterprise Control System Integration	Editore: **Commissione elettrotecnica internazionale (IEC)** Serie composta da 4 standard per integrare i sistemi informatici d'impresa e i sistemi di controllo/gestione.
IEC 62443 e segg. Industrial communication networks – Network and system security	Editore: **Commissione elettrotecnica internazionale (IEC)** Serie di 13 norme di sicurezza e specifiche tecniche in materia di sistemi di automazione e controllo industriali (IACS). Le norme IEC 61508 e segg. (principi fondamentali per la sicurezza dei PLC) vengono ampliate con il tema della sicurezza delle informazioni e trattano in maniera completa il tema dell'IACS. Vengono esaminati quattro aspetti o livelli di sicurezza delle informazioni: • aspetti generali (concetti, terminologia, metriche ecc.): IEC 62443-1-x • gestione della sicurezza informatica: IEC 62443-2-x • il livello «sistema»: IEC 62443-3-x • il livello «componenti»: IEC 62443-4-x Va in particolare menzionato il trattamento delle architetture di rete e a zone, molto più dettagliato rispetto ad altre norme. Questa serie di norme sta diventando fondamentale nel contesto delle norme del CENELEC (EN 50126 e altre) in materia di affidabilità, disponibilità, manutenibilità e sicurezza (RAMS).
BDEW Whitepaper Anforderungen an sichere Steuerungs-und Telekommunikationssysteme	Editore: **BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Österreichs E-Wirtschaft** Il libro bianco della BDEW contiene le misure di sicurezza fondamentali riguardanti i sistemi di controllo e di telecomunicazione dell'industria dell'energia. L'obiettivo strategico di questo documento consiste nell'influenzare positivamente lo sviluppo di prodotti per i sistemi summenzionati sotto il profilo della sicurezza informatica e di rafforzare la consapevolezza del settore per quanto riguarda l'importanza della protezione di questi sistemi. Nella regione DACH (Germania, Austria, Svizzera) il libro bianco della BDEW è diventato un documento di riferimento per l'approvvigionamento nel settore della corrente di trazione. Il documento è completato da indicazioni sull'esecuzione.

Tabella 9: standard nazionali e internazionali sulla sicurezza TIC

Titolo	Editore/Breve descrizione
Guide to Industrial Control Systems (ICS) Security SP 800-82	Editore: **National Institute of Standards and Technology (NIST)** La guida introduce ai sistemi SCADA, alla topologia e all'architettura, identifica le minacce e le vulnerabilità e fornisce raccomandazioni per diminuire e contrastare i rischi. Presenta inoltre i controlli SCADA specifici basati sul NIST 800-53 Framework.
Framework for Improving Critical Infrastructure Cybersecurity	Editore: **National Institute of Standards and Technology (NIST)** Questo quadro di riferimento nasce dalla richiesta formulata nel 2013 nel decreto presidenziale USA «Improving Critical Infrastructure Cyber Security». Il documento comprende diverse linee guida per rilevare lo status quo di un'azienda e istituire una roadmap per migliorare le pratiche in materia di cybersicurezza e i rimandi ad altri quadri di riferimento e standard come ISO 27001, ISA 62443, NIST 800-53 e Cobit.
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	Editore: **Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Si tratta di un'introduzione molto esaustiva alla strategia di *defense in depth* per i sistemi di controllo industriali.
IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit	Editore: **Bundesamt für Sicherheit in der Informationstechnik (BSI) – Germania** Questo compendio sulla protezione informatica di base *(IT-Grundschutz)* rappresenta, insieme alle norme BSI, la pubblicazione di riferimento per esaminare la tematica della sicurezza delle informazioni. Il documento descrive i diversi elementi della protezione informatica di base. Le potenziali minacce sono presentate nella prima parte, seguite dai requisiti fondamentali in materia di sicurezza. Gli elementi della protezione informatica di base sono ripartiti in dieci sottocategorie e riguardano tematiche quali: applicazioni (APP), informatica industriale (IND) e gestione della sicurezza (ISMS). Vengono esaminati vari livelli di protezione.
Norme BSI	Editore: **Bundesamt für Sicherheit in der Informationstechnik (BSI) – Germania** Le norme BSI sono un elemento chiave della metodologia relativa alla protezione informatica di base. Contengono raccomandazioni sui metodi, sui processi e sulle procedure nonché misure riguardanti vari aspetti della sicurezza delle informazioni. Esempi di norme BSI: 200-1 (ISMS); 200-2 (procedura da seguire per la protezione informatica di base), 200-3 (analisi dei rischi basata sulla protezione informatica di base) e 100-4 (analisi dettagliata della gestione delle situazioni di emergenza sotto forma di guida pratica).
Certificazione BSI secondo ISO 27001 sulla base di IT-Grundschutz	La sicurezza può essere impostata e controllata secondo quanto stabilito dal BSI, ma anche in base agli standard del gruppo ISO 27000. I due approcci sono compatibili e permettono di istituire un ISMS per individuare e ridurre a un livello accettabile i rischi nell'ambito della sicurezza delle informazioni.

Tabella 9: standard nazionali e internazionali sulla sicurezza TIC

Titolo	Editore/Breve descrizione
Zuordnungstabelle ISO zum modernisierten IT-Grundschutz	La norma BSI 200-2 relativa alla protezione informatica di base interpreta i requisiti e le misure previsti dalle norme ISO 27001 e 27002. La tabella delle corrispondenze aiuta gli utenti nella trasposizione del contenuto di queste due norme ISO.
Industrielle Steuerungs- und Automatisierungssysteme (ICS) – Allgemeine Empfehlungen	Editore: **Bundesamt für Sicherheit in der Informationstechnik (BSI) – Germania** Il compendio è un documento di riferimento inteso a facilitare l'accesso ai sistemi di sicurezza IT SCADA. Illustra i principi generali dell'automazione e le specificità e indica le norme pertinenti in questo ambito. Contiene inoltre un insieme di misure e una procedura per l'attuazione. Sul sito del BSI vengono messi a disposizione dell'utente ulteriori strumenti.
Tabella di corrispondenza – Mapping of Dependencies to International Standards	Editore: **European Union Agency for Network and Information Security (ENISA)** Questo rapporto analizza le dipendenze e le interazioni tra operatori di servizi essenziali (OES) e fornitori di servizi digitali (DSP) e propone una serie di indicatori per la loro valutazione. Gli indicatori sono associati a norme e a condizioni quadro generali internazionali (ISO IEC 27002, COBIT5, misure di sicurezza del gruppo di cooperazione NIS e NIST Cybersecurity Framework).
Communication network dependencies for ICS/SCADA Systems	Editore: **European Union Agency for Network and Information Security (ENISA)** Il rapporto si focalizza sulle reti di comunicazione, sull'intercomunicazione fra i sistemi ICS/SCADA e sull'identificazione di vulnerabilità, rischi, minacce e conseguenze in materia di sicurezza dovute ai sistemi cyberfisici; presenta anche una serie di raccomandazioni per minimizzare i rischi. Lo studio ha permesso in particolare di redigere una lista di buone pratiche e direttive per ridurre quanto più possibile lo spazio vulnerabile dei sistemi ICS/SCADA. Con il documento si intende offrire una panoramica della dipendenza dalle reti di comunicazione dei sistemi ICS/SCADA e permettere di identificare le minacce e gli scenari di attacco più realistici a questi sistemi.
ENISA Threat Landscape/Taxonomy	Editore: **European Union Agency for Network and Information Security (ENISA)** Il rapporto dell'ENISA fornisce una panoramica delle minacce e delle tendenze attuali o emergenti. Si basa su dati pubblici e offre una visione indipendente delle minacce identificate, dei loro autori e delle possibili tendenze. La tassonomia classifica le minacce in maniera sistematica.

Tabella 9: standard nazionali e internazionali sulla sicurezza TIC

10 Basi legali in materia di trattamento dei rifiuti

Le seguenti normative nazionali e internazionali si applicano in materia di trattamento dei rifiuti:

Basi legali nazionali

Responsabilità di un organo secondo il Codice delle obbligazioni, art. 754
RS *220* – Legge federale del 30 marzo 1911 di complemento del Codice civile svizzero (Libro quinto: Diritto delle obbligazioni)

Legge federale del 7 ottobre 1983 sulla protezione dell'ambiente (legge sulla protezione dell'ambiente, LPAmb; RS *814.01*)
RS *814.01* – Legge federale del 7 ottobre 1983 sulla protezione dell'ambiente (legge sulla protezione dell'ambiente, LPAmb)

Ordinanza del 4 dicembre 2015 sulla prevenzione e lo smaltimento dei rifiuti (ordinanza sui rifiuti, OPSR; RS *814.600*)
RS *814.600* – Ordinanza del 4 dicembre 2015 sulla prevenzione e lo smaltimento dei rifiuti (ordinanza sui rifiuti, OPSR)

Ordinanza del 22 giugno 2005 sul traffico di rifiuti (OTRif; RS *814.610*)
RS *814.610* – Ordinanza del 22 giugno 2005 sul traffico di rifiuti (OTRif)

Ordinanza del DATEC del 18 ottobre 2005 sulle liste per il traffico di rifiuti (RS *814.610.1*)
RS *814.610.1* – Ordinanza del DATEC del 18 ottobre 2005 sulle liste per il traffico di rifiuti

Ordinanza del 20 ottobre 2021 concernente la restituzione, la ripresa e lo smaltimento degli apparecchi elettrici ed elettronici (ORSAE; RS *814.620*)
RS *814.620* – Ordinanza del 20 ottobre 2021 concernente la restituzione, la ripresa e lo smaltimento degli apparecchi elettrici ed elettronici (ORSAE)

Ordinanza del 5 luglio 2000 sugli imballaggi per bevande (OIB; RS *814.621*)
RS *814.621* – Ordinanza del 5 luglio 2000 sugli imballaggi per bevande (OIB)

Ordinanza del 7 settembre 2001 relativa all'ammontare della tassa di smaltimento anticipata sugli imballaggi per bevande in vetro (RS *814.621.4*)
RS *814.621.4* – Ordinanza del 7 settembre 2001 relativa all'ammontare della tassa di smaltimento anticipata sugli imballaggi per bevande in vetro

Ordinanza del DATEC del 28 novembre 2011 sull'ammontare della tassa di smaltimento anticipata per pile (RS *814.670.1*)
RS *814.670.1* – Ordinanza del DATEC del 28 novembre 2011 sull'ammontare della tassa di smaltimento anticipata per pile

Ordinanza del 26 agosto 1998 sul risanamento dei siti inquinati (ordinanza sui siti contaminati, OSiti; RS *814.680*)
RS *814.680* – Ordinanza del 26 agosto 1998 sul risanamento dei siti inquinati (ordinanza sui siti contaminati, OSiti)

Ordinanza del 26 settembre 2008 sulla tassa per il risanamento dei siti contaminati (OTaRSi; RS *814.681*)
RS *814.681* – Ordinanza del 26 settembre 2008 sulla tassa per il risanamento dei siti contaminati (OTaRSi)

Legge federale del 21 marzo 2003 sull'energia nucleare (LENu; RS *732.1*)
RS *732.1* – Legge federale del 21 marzo 2003 sull'energia nucleare (LENu)

Ordinanza del 10 dicembre 2004 sull'energia nucleare (OENu; RS *732.11*)
RS *732.11* – Ordinanza del 10 dicembre 2004 sull'energia nucleare (OENu)

Ordinanza del 25 maggio 2011 concernente i sottoprodotti di origine animale (OSOAn; RS *916.441.22*)
RS *916.441.22* – Ordinanza del 25 maggio 2011 concernente i sottoprodotti di origine animale (OSOAn)

Ordinanza del 16 dicembre 1985 contro l'inquinamento atmosferico (OIAt: RS *814.318.142.1*)
RS *814.318.142.1* – Ordinanza del 16 dicembre 1985 contro l'inquinamento atmosferico (OIAt)

Ordinanza del 28 ottobre 1998 sulla protezione delle acque (OPAc; RS *814.201*)
RS *814.201* – Ordinanza del 28 ottobre 1998 sulla protezione delle acque (OPAc)

Legge federale del 19 giugno 1992 sulla protezione dei dati (LPD; RS *235.1*)
RS *235.1* – Legge federale del 19 giugno 1992 sulla protezione dei dati (LPD)

Ordinanza del 22 giugno 1994 sulla radioprotezione (ORaP; RS *814.501*)
RS *814.501* – Ordinanza del 22 giugno 1994 sulla radioprotezione (ORaP)

Ordinanza del 26 aprile 2017 sulla radioprotezione (ORaP; RS *814.501*)
RS *814.501* – Ordinanza del 26 aprile 2017 sulla radioprotezione (ORaP)

Standard nazionali e raccomandazioni

Ufficio federale della sanità pubblica, smaltimenti di sostanze radioattive, pagina generale

Smaltimento di sostanze radioattive, guida UFSP, PDF
https://www.bag.admin.ch/dam/bag/it/dokumente/str/str-wegleitungen/abfaelle/artikel-114.pdf.download.pdf/220617_V1-1_Radioprotezione_Guida_art-114.pdf

IEEE802.11i Network Standards

Comportamento sicuro nello spazio digitale
R come «Ridurre i rischi» - S-U-P-E-R.ch

Standard minimo per le TIC, parte principale e strumento Excel

Standard minimo per le TIC Elettricità

Standard minimo per le TIC Acque di scarico

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für Fernwärme- und Fernkälteversorgung

Password sicure
Proteggete i vostri account

Norme internazionali

Halbzeitbilanz auf hoher Ebene des Europäischen Prozesses Umwelt und Gesundheit

WHO World Health Assembly 2015 resolution
https://www.euro.who.int/en/health-topics/environment-and-health/air-quality/news/news/2015/05/air-quality-and-health-resolution-adopted-at-the-sixty-eighth-world-health-assembly

ISA-62443-1-1, Security for industrial automation and control systems

NIST, Cybersecurity Framework

Glossario

Termine	Descrizione
Awareness	Consapevolezza, percezione
Competenza inconscia	Quando una persona dispone di un'esperienza tale che le sue competenze sono quasi come una seconda natura che può richiamare in qualsiasi momento e ripetutamente, senza grandi sforzi. Non essendo consapevole delle proprie competenze, questa persona avrà difficoltà a trasmetterle facilmente. Le persone dotate di competenze inconsce agiscono in maniera intuitiva ma hanno difficoltà ad analizzare le proprie azioni.
ESXi	VMware ESXi (in precedenza ESX) è un ipervisore *bare metal* installato su un server e che lo suddivide in varie macchine virtuali.
POLYCOM	Rete di radiocomunicazione svizzera basata su Tetrapol.
Resilienza	Resistenza psichica, capacità di far fronte a situazioni difficili della vita senza subire danni permanenti.
Shop Floor	Officina e produzione
Telefonia SIP	Comunicazione vocale tramite protocollo Internet.

Altre definizioni si possono trovare nel glossario del NCSC:
https://www.ncsc.admin.ch/ncsc/de/home/glossar.html

Elenco delle abbreviazioni

Abbreviazione	Descrizione
ASIR	Associazione svizzera dei dirigenti e gestori degli impianti di trattamento dei rifiuti
BCM	Business Continuity Management
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germania)
CNA	Corporate Network Access
DaaS	Desktop as a Service
DCS	Distributed Control System
DCS o ICS	Industrial Control Systems, impianti di controllo industriale, per es. PLC
DECT	Digital Enhanced Cordless Telecommunications
DEP	Device Enrollment Program
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DSP	Digital Service Providers
EMS	Energy Management System
ERP	Enterprise-Resource-Planning
GSM	Global System for Mobile Communications
HMI	Human-Machine Interface
IaaS	Infrastructure as a Service
IACS	Industrial Automation and Control Systems
ICS	Informations Controll System
IEC	International Electrotechnical Commission (norme e standard)
IIRU	Impianto di incenerimento dei rifiuti urbani
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology, classica infrastruttura di una rete per uffici
KPI	Key Performance Indicator
LPD	Legge federale sulla protezione dei dati
MDM	Mobile Device Management
ME	Manutenzione, esercizio
MES	Manufacturing Execution System
MFA	Multifactor Authentication

Abbreviazione	Descrizione
NCSC	Centro nazionale per la cibersicurezza
NFC	Near-Field Connection
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
OIAt	Ordinanza contro l'inquinamento atmosferico
OPAc	Ordinanza sulla protezione delle acque
OPSR	Ordinanza sulla prevenzione e lo smaltimento dei rifiuti (ordinanza sui rifiuti)
ORaP	Ordinanza sulla radioprotezione
OS	Operating System
OT	Operation Technology, infrastruttura di rete, sistema operativo
PaaS	Platform as a Service
PDCA	Ciclo Plan-Do-Check-Act, ciclo di Deming
PGGA	Parlamento, Governo, Giustizia, Amministrazione
PIC	Protezione delle infrastrutture critiche
PLC	Programmable Logic Controller
RAMS	Reliability, Availability, Maintainability
RTU	Remote Terminal Unit
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition, sistema di controllo distribuito
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
TIC	Tecnologie dell'informazione e della comunicazione
UE	Unione europea
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFPP	Ufficio federale della protezione della popolazione
UFSP	Ufficio federale della sanità pubblica
VLAN	Virtual Local Area Network
WAF	Web Application Firewall
WLAN	Wireless Local Area Network
WSUS	Windows Server Update Services, servizi di aggiornamenti per sistemi operativi Windows

Indice delle figure

Indice delle tabelle

11 Appendice

11.1 Analisi del business impact (BIA)

La BIA adattata al tema dello smaltimento dei rifiuti esamina i processi critici individuati come vettori di attacco nella «tabella 3: processi critici negli impianti di incenerimento dei rifiuti» dello standard minimo. In questo modo le conoscenze acquisite possono essere facilmente trasferite nella BIA, allegata qui come esempio. Poiché i criteri di valutazione finanziari dipendono dall'impianto, le somme che figurano nelle matrici di rischio sono da considerarsi degli esempi.

Il risultato della BIA è il prodotto della disponibilità al rischio residua nonostante le misure attuate.

Matrici di rischio (ordini di grandezza)

Processo di smaltimento (rifiuti) riferito all'intero impianto							
E	Situazioni che causano interruzioni prolungate dell'esercizio (>1 giorno)	E1	E2	E3	E4	E5	E6
D	Situazioni che causano interruzioni prolungate dell'esercizio (< 1 giorno)	D1	D2	D3	D4	D5	D6
C	Situazioni che causano interruzioni brevi dell'esercizio (< 12 h)	C1	C2	C3	C4	C5	C6
B	Situazioni che causano una limitazione contenuta dell'esercizio	B1	B2	B3	B4	B5	B6
A	Situazioni con effetti trascurabili	A1	A2	A3	A4	A5	A6

	Processi legati alle infrastrutture (ME)						
E	>60 mio. CHF	E1	E2	E3	E4	E5	E6
D	30-60 mio. CHF	D1	D2	D3	D4	D5	D6
C	10-30 mio. CHF	C1	C2	C3	C4	C5	C6
B	1-10 mio. CHF	B1	B2	B3	B4	B5	B6
A	<1 mio. CHF	A1	A2	A3	A4	A5	A6

	Processi di gestione aziendale						
E	>60 mio. CHF	E1	E2	E3	E4	E5	E6
D	30-60 mio. CHF	D1	D2	D3	D4	D5	D6
C	10-30 mio. CHF	C1	C2	C3	C4	C5	C6
B	1-10 mio. CHF	B1	B2	B3	B4	B5	B6
A	<1 mio. CHF	A1	A2	A3	A4	A5	A6

	Molto bassa	Bassa	Ridotta	Maggiore	Alta	Molto alta
In 10 anni	< 5%	5-25%	15-30%	50-75%	>75-90%	>95-100%
	1	2	3	4	5	6
	Probabilità di insorgenza del rischio					

Figura 14: matrici di rischio (ordini di grandezza)

Dettagli dell'analisi

	Rischi						Mitigazione				Misure correttive
N..	Categoria del rischio	Dettagli sulla categoria del rischio	Descrizione dettagliata	Processo di smaltimento	Processi legati alle infrastrutture (ME)	Gestione aziendale (business)	Mitigazione del rischio	Processo di smaltimento Processi legati alle infrastrutture(ME)		Gestione aziendale (business)	Misura
1a	Globale	Comunicazione dei messaggi	Interruzione della comunicazione, nessun dato di processo per il calcolo e la manutenzione, PLC non coinvolti								
1b	Globale	Comunicazione dei messaggi	Interruzione della comunicazione: messaggi vocali, Internet, telefono e radio								
2a	Globale	Fattore umano	Comandi errati, stress, disattenzione, mancanza di stimoli								
2b	Globale	Fattore umano	Insoddisfazione, sabotaggio								
2c	Globale	Fattore umano	Vittima involontaria (phishing, ingegneria sociale)								
3a	Manutenzione da remoto IT/ OT	Accesso da remoto per operatori esterni	Modifiche incontrollate nei programmi e nella gestione dei processi								
3b	Manutenzione da remoto IT/ OT	Accesso da remoto per operatori esterni	Interruzioni nell'accesso alla manutenzione da remoto								
4a	Manutenzione da remoto IT/ OT	Dati operativi	Flusso incontrollato, modifiche, eliminazioni								
4b	Manutenzione da remoto IT/ OT	Dati operativi	Dati operativi non più accessibili								
5	Manutenzione da remoto IT/ OT	Aggiornamenti automatici	Aggiornamenti errati, fonte degli aggiornamenti non verificata								
6	Manutenzione da remoto IT/ OT	Sviluppo	A causa dell'assenza di un sistema di manutenzione, sviluppo e aggiustamenti al sistema produttivo (a cuore aperto)								
7a	Manutenzione da remoto IT/ OT	Salvataggio del backup dei dati OT	Backup assente, errato o non plausibile								

Figura 15: Dettagli dell'analisi secondo la tabella 3: processi critici negli impianti di incenerimento dei rifiuti

Il documento della BIA può essere scaricato mediante questo link:

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abfallentsorgung.html

Autori ed esperti della prima edizione

Cognome, nome	Azienda o ente	Funzione
Hans-Peter Käser	UFAE	Capoprogetto
Sven Peter	UFAE	Esperto/assicurazione qualità
Sandra Rüfenacht	UFPP	Esperto/assicurazione qualità
Ariane Stäubli	ASIR	Capoprogetto ASIR/esperta/ assicurazione qualità
Patric Imhof	Eniwa	Esperto/assicurazione qualità
Thomas Bücherer	EWB	Esperto/assicurazione qualità
Andreas Tschanz	EWB	Esperto/assicurazione qualità
Christoph Beleda	IWB	Esperto/assicurazione qualità
Bruno Hottinger	KVATG	Esperto/assicurazione qualità
Marco Weber	KVATG	Esperto/assicurazione qualità
Martin Muheim	Renergia	Esperto/assicurazione qualità
Jonas Tschudi	SAIDEF	Esperto/assicurazione qualità

Dati editoriali e indirizzi di contatto

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

Associazione consultata
Associazione svizzera dei dirigenti e gestori degli impianti di trattamento dei rifiuti ASIR