



# Utilities: continuità operativa sotto attacco

Il ruolo chiave della resilienza cyber negli ambienti OT delle Utilities

# 01

## Punto di partenza

- Cosa succede in Italia e nel mondo?

# 02

## La sfida

# 03

## La risposta

- Livello di maturità in Italia

# 04

## Riflessioni

- Come passare dalla conformità normativa alla protezione effettiva delle risorse critiche?
- Dove si concentra oggi la vulnerabilità degli ambienti OT nelle Utilities
- Dalla teoria alla pratica



# Punto di partenza

01



Tradizionalmente, le strategie di protezione delle organizzazioni si sono concentrate sulla sicurezza informatica nel perimetro IT, in particolare sul suo ruolo di facilitatore del business digitale nell'era della trasformazione digitale.

Sebbene negli ultimi anni vi sia stata una crescente enfasi sulla sicurezza informatica negli ambienti industriali e operativi (OT), essa rimane ancora, per lo più, una questione irrisolta nelle agende strategiche.

Secondo il Rapporto Clusit 2025, la maggior parte delle organizzazioni italiane adotta un approccio reattivo, intervenendo dopo l'incidente più che in ottica di prevenzione strategica. Il rapporto sottolinea che la mancanza di governance e di responsabilità chiare è uno dei principali fattori di rischio nel settore industriale.

Gli ultimi dati indicano che gli attacchi gravi contro il settore Energy & Utilities sono aumentati del +50% rispetto all'anno precedente. Il comparto, quindi, rappresenta circa il 2,8% degli attacchi gravi globali, con un trend di crescita costante negli ultimi 5 anni, rendendolo un “settore ad alta esposizione futura”.

**Inoltre, le tecnologie IT (Information Technology) e OT (Operational Technology) sono state storicamente isolate l'una dall'altra.**

Secondo l'ultimo Osservatorio Cybersecurity – Politecnico di Milano, oltre il 70% dei budget cyber nel settore Energy italiano è stato destinato all'IT, lasciando l'OT in una posizione residuale.

| IT                                                                                                                        | OT                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Sistemi standard e moderni.                                                                                               | Sistemi legacy.                                                                                                          |
| La riservatezza è la preoccupazione principale e l'attenzione è rivolta alla protezione delle informazioni e dei sistemi. | La disponibilità, la continuità operativa e la produttività sono preoccupazioni fondamentali.                            |
| Connessione diretta a Internet.                                                                                           | Isolati o connessi tramite la rete IT.                                                                                   |
| Il monitoraggio può essere esteso a tutte le reti e a tutti i dispositivi.                                                | Capacità di monitoraggio limitata a causa dell'elettronica di rete e dei protocolli industriali.                         |
| La difesa può essere implementata tramite software e hardware.                                                            | Le valutazioni di sicurezza offensive sono accettabili solo in ambienti controllati e da parte di personale qualificato. |



# 1.1 Cosa succede in **Italia e nel mondo?**

Oggi, la trasformazione digitale ha facilitato l'apertura degli ambienti operativi, collegando le risorse al mondo IT, a Internet o al cloud, esponendo numerose vulnerabilità e aumentando in modo allarmante i **livelli di rischio**.

Un attacco informatico ai sistemi aziendali non comporta solo la perdita di dati, ma mette a repentaglio la stabilità della società e di un intero Paese. Si tratta di blackout regionali, danni fisici ad apparecchiature critiche del valore di milioni di euro, con conseguente compromissione del servizio e, in ultima analisi, un grave impatto sull'economia e sulla sicurezza nazionale del Paese.

Questi sono alcuni dati significativi sul contesto italiano:

|   |                                                                                                                                                                                                                                                                               |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | In <b>Italia</b> , solo nel primo semestre 2025, sono stati censiti 1.549 attacchi cyber, in aumento del 53% rispetto allo stesso periodo dell'anno precedente.                                                                                                               |
| 2 | Il <b>manifatturiero</b> – insieme a <b>sanità</b> e <b>PA</b> – è tra i settori più colpiti, con una crescita degli attacchi nell'ordine del 38% in un solo anno, dovuta in particolare a ransomware e malware.                                                              |
| 3 | La maggior parte degli incidenti analizzati è classificata come <b>grave</b> o <b>critica</b> , con potenziali impatti immediati su continuità operativa e produzione.                                                                                                        |
| 4 | Sul fronte del governo della sicurezza, si registra un <b>miglioramento nella gestione delle vulnerabilità</b> : il tasso di vulnerabilità non patchate rilevate sul territorio italiano è sceso dal 20% al 3% in un anno, pur rimanendo un elemento critico nei contesti OT. |
| 5 | Un <b>attacco ransomware</b> verso una piccola impresa (fatturato fino a 50 milioni €/anno) può generare un danno stimato oltre 55.000 euro, mentre per un'azienda con fatturato 500 milioni €/anno può arrivare a circa 7,9 milioni euro. <sup>2</sup>                       |
| 6 | Permangono <b>criticità</b> legate a competenze, cultura cyber e capacità di rilevamento e risposta, soprattutto nei contesti industriali. <sup>3</sup>                                                                                                                       |

1. Fonte: 2025 Operational Summary, Agenzia per la Cybersicurezza Nazionale.

2. Osservatorio Security Risk curato da AIPSA e The European House – Ambrosetti

3. Rapporto Clusit 2025

| Indicatore                                                            | Valore                                                  | Fonte                                              |
|-----------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------|
| Aumento degli attacchi gravi nel settore Energy & Utilities           | <b>+50%</b> nell'ultimo anno                            | Clusit 2025                                        |
| Quota del settore Energy sugli attacchi gravi globali                 | <b>2,80%</b>                                            | Clusit 2025                                        |
| Aziende con processi OT formalizzati                                  | <b>18%</b>                                              | Fortinet – State of OT Cybersecurity 2025          |
| Scarsa visibilità sugli asset OT e ICS/SCADA                          | <b>42% delle aziende</b>                                | Fortinet 2025                                      |
| Aziende con gestione strutturata degli accessi OT (PAM/Remote Access) | <b>&lt;30%</b>                                          | Fortinet 2025                                      |
| Gap di competenze OT nel settore Energy                               | <b>~60%</b> tra domanda e offerta di specialisti        | ENISA – OT/ICS Cybersecurity Skills Report         |
| Quota del budget cyber destinata all'IT (vs OT)                       | <b>&gt;70%</b> del budget concentrato sull'IT           | Osservatorio Cybersecurity – Politecnico di Milano |
| Gravità media degli incidenti nel settore Energy                      | <b>Superiore alla media degli altri settori critici</b> | Clusit 2025                                        |
| Tempo medio di risposta agli incidenti                                | <b>Tra i più elevati</b> nei settori critici europei    | ENISA Threat Landscape                             |





Sfruttare queste vulnerabilità attraverso minacce sempre più sofisticate e dinamiche aumenta il rischio che alcuni processi industriali che supportano servizi critici vengano compromessi o interrotti, con le conseguenze operative, reputazionali o economiche che tali situazioni comportano.

In questo senso, da un lato, la strategia di sicurezza informatica dell'OT deve affrontare le principali minacce che incidono sulle operazioni e sulle attività delle aziende di questo settore:

- Tempo di inattività nella produzione
- Crittografia delle informazioni e richiesta di riscatto
- Perdita di controllo delle apparecchiature
- Frode
- Attacco a terzi. Responsabilità sussidiaria
- Divulgazione di informazioni strategiche

Si rende necessario un approccio globale alla sicurezza informatica operativo che unisca gli ambienti IT e OT per avere un impatto in termini di business.

Solo un approccio consapevole e completo può aiutare a soddisfare le esigenze di un'industria 4.0 e di un ambiente di produzione cyber-resiliente: comprendere e applicare la sicurezza informatica nella progettazione, implementazione e gestione di qualsiasi progetto.

Per affrontare queste minacce è necessario un approccio che consenta di:

- Garantire la disponibilità dell'operazione;
- Rafforzare la sicurezza in tutti gli elementi e le fasi della catena del valore;
- Garantire la conformità.

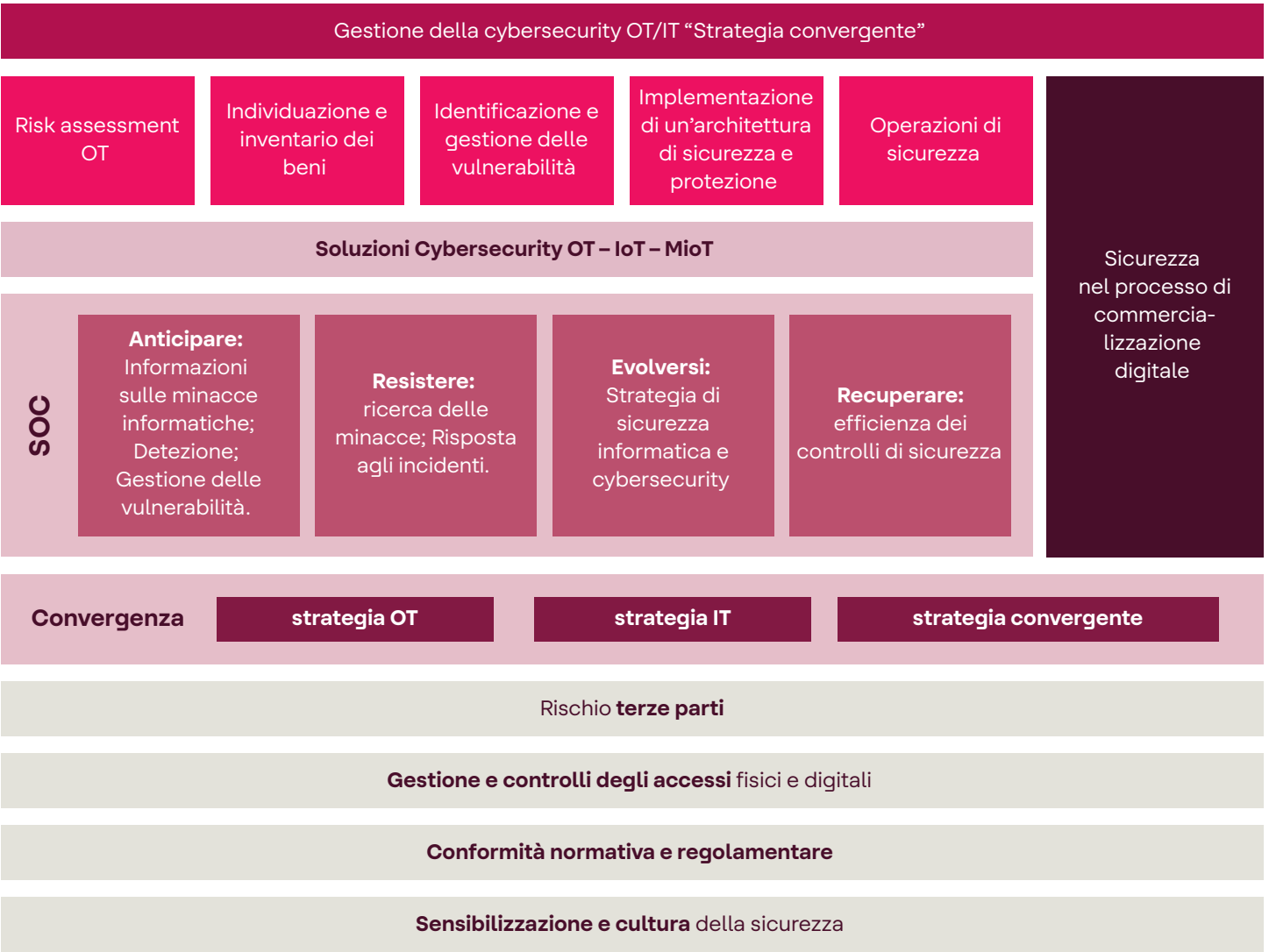






In questi ambienti industriali, le strategie di protezione richiedono un approccio olistico che copra tutte le fasi del ciclo di vita della generazione delle risorse, della distribuzione e dei processi di estrazione.

La risposta a questo scenario deve quindi basarsi su un approccio che metta al centro la protezione della disponibilità delle operazioni e delle informazioni aziendali critiche, rafforzando al contempo la sicurezza lungo l'intera catena di approvvigionamento.







**L'applicazione di queste strategie dipende dal livello di maturità dei modelli di sicurezza informatica.**

**Ogni organizzazione richiede un approccio diverso a seconda della propria situazione.**

Partendo dal presupposto che la produzione non può essere interrotta in nessun momento negli ambienti operativi, una strategia di sicurezza informatica adeguata in questo settore deve basarsi su un'identificazione e un inventario delle risorse, un'analisi dettagliata delle minacce e delle vulnerabilità, proseguire con l'esecuzione di una diagnosi sullo stato dei sistemi critici e dei rischi, e quindi strutturare un piano di iniziative che copra le cinque fasi del ciclo di protezione: identificare, proteggere, rilevare, rispondere e recuperare.

### Cybersecurity OT:

Visibilità, segmentazione delle reti OT, gestione delle minacce, sicurezza sistemi SCADA

#### Tabella di marcia

|                            | Livello 1: Strategia                                                                                                                                                                                                                                                                                                    | Livello 2: Definizione                                                                                                                                                                                                                                                                                                                  | Livello 3: Gestione                                                                                                                                                                                                                                         | Livello 4: Ottimizzazione                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Obiettivi</b>           | <ul style="list-style-type: none"> <li>Assessment IT/OT – Piano strategico;</li> <li>Sequestro dei beni</li> <li>Analisi dei rischi e priorità</li> <li>Quadro normativo e organizzativo/ soluzioni di governance</li> <li>Sensibilizzazione</li> </ul>                                                                 | <ul style="list-style-type: none"> <li>Architettura di sicurezza</li> <li>Controllo degli accessi</li> <li>Gestione backup e continuità</li> <li>Monitoraggio e risposta</li> <li>Bastionatura/ patching</li> </ul>                                                                                                                     | <ul style="list-style-type: none"> <li>Operazioni di sicurezza</li> <li>Gestione di crisi</li> <li>Controllo degli account privilegiati</li> <li>Gestione delle vulnerabilità</li> <li>SOC integrato per IT/OT</li> <li>patching</li> </ul>                 | <ul style="list-style-type: none"> <li>Gestione efficiente dei controlli</li> <li>Informazioni sulle minacce</li> <li>Gestione dell'identità digitale</li> <li>Sicurezza fin dalla progettazione e per default</li> <li>Audit</li> </ul>            |
| <b>Capacità</b>            |  Visibilità e strategia<br> Piano di ripristino<br> Quick wins |  Protezione e isolamento<br> Monitoraggio e risposta<br> Recupero e continuità |  Processo e automatizzazione<br> Misurazione e analisi                                |  Gestione e Conformità<br> Certificazione                                 |
| <b>Elementi distintivi</b> | <ul style="list-style-type: none"> <li>Best practices;</li> <li>campagna di sensibilizzazione;</li> <li>simulazione di crisi.</li> </ul>                                                                                                                                                                                | <ul style="list-style-type: none"> <li>Protezione dei sistemi SCADA;</li> <li>segmentazione delle reti; controllo degli accessi e autenticazione GIS;</li> <li>Sicurezza fisici/ componenti del sistema;</li> <li>3PRM;</li> <li>soluzione di protezione degli endpoint.</li> </ul>                                                     | <ul style="list-style-type: none"> <li>Visibilità delle reti e rilevamento delle minacce OT;</li> <li>gestione degli incidenti OT;</li> <li>priorità aggiornamenti critici/ mitigare lo sfruttamento delle vulnerabilità;</li> <li>supporto DRP.</li> </ul> | <ul style="list-style-type: none"> <li>Penetration test periodici;</li> <li>valutazione della sicurezza per misurare l'efficacia cyber ot;</li> <li>red team/ blue team;</li> <li>barometro;</li> <li>soluzioni di continuità operativa.</li> </ul> |





## 4.1 Come passare dalla conformità normativa alla **protezione effettiva delle risorse critiche**?

Come abbiamo visto, nel settore energetico, parlare di sicurezza informatica OT non è più un esercizio accademico né un requisito cosmetico di audit. È una questione di continuità operativa, sicurezza fisica e fiducia sociale nella fornitura di risorse critiche.

Ma, nonostante l'aumento degli attacchi, le organizzazioni italiane sembrano essere più reattive che proattive. La sicurezza informatica continua ad essere vista sotto una lente prevalentemente normativa: rispettare gli standard o le checklist normative come se fossero il fine ultimo.

La sfida sta nel fatto che essere protetti non equivale ad essere conformi. Un'azienda può vantare politiche impeccabili sulla carta e rimanere comunque esposta a un attacco che blocchi una raffineria, una rete elettrica, cancelli i dischi rigidi dei sistemi SCADA, manipoli un PLC o provochi una fuga non rilevata.

Il divario sta tra ciò che dicono i documenti e ciò che accade realmente sul campo, dove operano PLC, RTU, SCADA, DCS, SIS e la strumentazione critica.



Per passare dalla teoria alla pratica sono necessari tre cambiamenti di **approccio**:

### Prima la visibilità, poi la conformità

Non è possibile proteggere ciò che non si vede. La priorità deve essere quella di ottenere un inventario dinamico e affidabile delle risorse OT, con visibilità delle comunicazioni e delle anomalie in tempo reale. Senza questa base, qualsiasi quadro normativo è un esercizio incompleto.



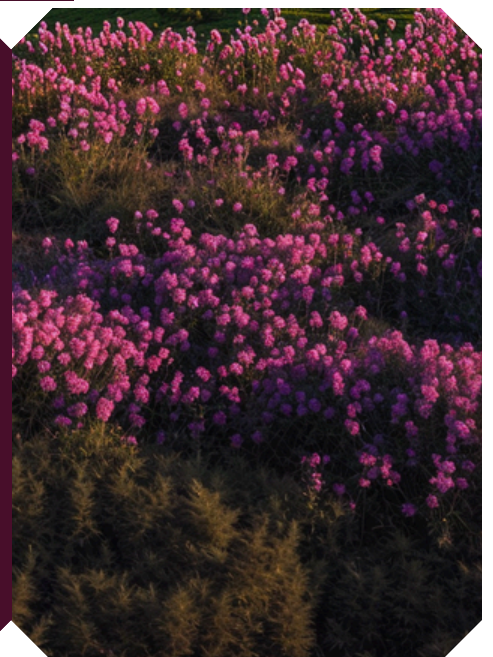
### La cultura come controllo di sicurezza

Nel settore delle utilities la segnalazione di anomalie può risultare meno immediata, anche per ragioni culturali o organizzative. Promuovere un ambiente in cui operatori e fornitori possano comunicare liberamente eventuali criticità rappresenta un passo importante verso una maggiore maturità: la sicurezza informatica è infatti uno strumento di tutela delle persone e delle operazioni, e si fonda sulla collaborazione più che sulla sanzione.

### Dalla checklist al **rischio operativo**

La conformità deve essere un mezzo, non un fine. L'attenzione deve essere spostata sulla risposta a domande chiave:

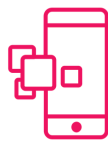
- Cosa succede se un ransomware crittografa la mia HMI durante il funzionamento?
- Quale impatto avrebbe la manipolazione di un PLC sulla sicurezza di valvole o pompe?
- In che modo un attacco alle mie RTU influirebbe sulla capacità di monitorare i pozzi remoti?



Il vero valore sta nel misurare e minimizzare i rischi operativi non solo nello spuntare le caselle di conformità.

Se non si è in grado di rispondere con certezza a queste domande, la strategia di sicurezza informatica OT che si sta adottando si basa su supposizioni, non su dati.

E nel mondo OT, le supposizioni hanno un costo operativo molto elevato.



L'azienda dispone di un elenco aggiornato e dinamico di tutti i suoi dispositivi OT?



Quali comunicazioni avvengono realmente tra i suoi PLC, RTU e HMI?



È in grado di rilevare protocolli non autorizzati o comunicazioni anomale che indicano una configurazione errata o un'intrusione?



Quali vulnerabilità critiche interessano le tecnologie della base installata?



È in grado di identificare se un dipendente collega una USB infetta?



O se un dispositivo tenta di comunicare con un IP esterno non autorizzato?



## 4.2 Dove si concentra oggi la vulnerabilità degli ambienti OT nelle Utilities



La sicurezza informatica negli ambienti di tecnologia operativa (OT) è oggi un elemento determinante per la continuità del settore energetico.

La crescente digitalizzazione dei processi industriali, l'interconnessione con i sistemi IT e la pressione per garantire la continuità in un settore critico espongono le organizzazioni a rischi che vanno ben oltre la perdita di dati: si tratta della sicurezza delle operazioni, della protezione dell'ambiente, dell'integrità dei lavoratori e della resilienza della catena di approvvigionamento energetico.



**Quello che non vedo,  
non posso **proteggerlo****

L'invisibilità che minaccia la continuità del business energetico in Italia.

La sua continuità operativa è minacciata da un pericolo invisibile.



## Mancanza di visibilità:

gran parte delle organizzazioni non dispone di un inventario aggiornato e dinamico delle risorse OT, il che limita la capacità di rilevare anomalie e anticipare gli incidenti.

## Carenza di talenti specializzati:

esiste un deficit di professionisti con esperienza reale nella sicurezza informatica OT. L'83% delle organizzazioni italiane segnala la carenza di professionisti cyber.

## Sensibilizzazione del personale operativo:

sebbene la sicurezza OT abbia un impatto diretto sulle operazioni, prevale ancora la cultura dell'occultamento degli incidenti e la percezione che la sicurezza informatica sia una questione esclusivamente tecnica.

## Convergenza IT/OT:

integrare entrambi i mondi senza compromettere la sicurezza rimane una sfida, soprattutto nei settori con sistemi legacy e ambienti distribuiti geograficamente.

## Conformità normativa disomogenea:

mentre in Nord America e in Europa quadri normativi come NERC CIP o IEC 62443 guidano il settore, in Italia l'allineamento agli standard europei come NIS2 e IEC 62443 fornisce una base solida di riferimento. Tuttavia, la reale sfida non è più normativa, ma culturale e organizzativa: tradurre la conformità in efficaci pratiche di protezione operativa, assicurando che i requisiti regolatori si traducano in resilienza e continuità dei processi industriali.

## Gestione di terzi e della catena di fornitura:

appaltatori, integratori e fornitori di servizi critici rappresentano un anello vulnerabile che spesso non viene gestito con controlli adeguati; non è sufficiente proteggere solo l'organizzazione, ma è necessario garantire l'intero ecosistema.



Tradurre questi elementi in pratica significa passare da un approccio reattivo a un modello operativo strutturato, progressivo e misurabile.

## Condizioni abilitanti per una **sicurezza OT** efficace

Questi elementi rappresentano le condizioni necessarie per rendere efficace e sostenibile nel tempo l'approccio descritto nelle sezioni precedenti.



**Adattare i quadri normativi europei e nazionali alla realtà operativa degli ambienti OT**, trasformando requisiti come NIS2, DORA e IEC/ISA 62443 da obblighi di conformità a strumenti di governo del rischio e della continuità operativa.

**Investire in competenze e cultura della sicurezza lungo tutta l'organizzazione**, superando una visione esclusivamente tecnica e promuovendo consapevolezza e responsabilità condivisa tra IT, OT e personale operativo.

**Favorire la collaborazione tra operatori del settore e istituzioni**, attraverso la condivisione di informazioni, indicatori di compromissione e buone pratiche, per rafforzare la resilienza complessiva del sistema energetico.

**Integrare la gestione del rischio di terze parti nei modelli di sicurezza OT**, considerando fornitori, integratori e partner come parte integrante dell'ecosistema operativo e non come elementi esterni al perimetro di responsabilità.

**Integrare esercitazioni e simulazioni nei processi di gestione della sicurezza**, per testare nel tempo la capacità dell'organizzazione di prevenire, rilevare e rispondere a incidenti cyber, garantendo la continuità operativa anche in scenari di crisi.

La resilienza cyber negli ambienti OT non è il risultato di una singola iniziativa, ma l'esito di un percorso strutturato che integra strategia, persone e processi nel tempo.



## 4.3 Dalla **teoria** alla **pratica**



- Implementare la **visibilità in tempo reale** della rete e delle risorse OT come punto di partenza per qualsiasi strategia di difesa.
- Sviluppare **programmi di formazione** e sensibilizzazione rivolti al personale sul campo e operativo, oltre che al personale IT.
- Adottare **modelli di convergenza IT/OT sicuri**, con architetture a livelli, monitoraggio continuo e un SOC ibrido che comprenda i protocolli industriali.

- Allineare le politiche locali agli **standard internazionali e alle normative europee** riconosciute, come la Direttiva NIS2, il Regolamento DORA, e gli standard tecnici IEC/ISA 62443 ed ISO/IEC 27001, stabilendo roadmap chiare per colmare le lacune di conformità e rafforzare la protezione degli ambienti OT.
- Rafforzare la **gestione dei rischi di terze parti**, effettuare valutazioni di sicurezza obbligatorie (questionari), integrando clausole contrattuali, audit leggeri e inclusione nei piani di risposta agli incidenti informatici che garantiscano la sicurezza lungo tutta la catena di approvvigionamento.
- **Implementare Zero Trust “non fidarti mai, verifica sempre”** non è un'opzione, è una necessità per ogni utente (interno/esterno), dispositivo e connessione.



# Tradurre la strategia in **capacità operative**:



## Visibilità e monitoraggio

- Inventario aggiornato delle risorse OT.
- Integrazione di SIEM specializzati in OT.
- Dashboard di stato in tempo reale, monitoraggio 24 ore su 24, 7 giorni su 7.



## Segmentazione delle reti

- Separazione IT/OT con firewall industriali.
- Applicare zone e condotti (ISA/IEC 62443).



## Gestione delle vulnerabilità e delle patch

- Inventario centralizzato delle vulnerabilità.
- Cicli di patch controllati.
- Test in ambienti di staging.
- Scansioni mensili.
- Gemelli digitali (Digital Twin)



## Identità e accesso

- MFA per accessi remoti.
- Principio del privilegio minimo.
- Audit periodico degli account.



## Risposta agli incidenti

- Piani di risposta testati con simulazioni.
- Coordinamento con CSIRT Italia.
- Registrazione forense post-incidente.

Nel settore delle utilities in Italia, la conformità alla Direttiva NIS2 e agli standard internazionali IEC 62443 rappresenta il “cosa”.

Tradurre questi requisiti utilizzando una strategia che si basa su personale qualificato, processi ben definiti e tecnologie adeguate al contesto industriale, è il **come**.



# Tech for impact

Mettiamo in contatto  
talento, tecnologia e  
business per generare  
una crescita e un impatto  
positivi e sostenibili.

Indra Italia S.p.A.  
Via del Serafico, 200,  
00142 Roma RM  
Tel. 06 4121 10601

[minsait.com](https://minsait.com)

 **MINSAIT**