INDRA GROUP

THE INDRA GROUP MAGAZINE #3 | GENNAIO | 2026 | ITALY

NOVA

Idee, insights e novità
su tecnologia
e cambiamenti

La mobilità come infrastruttura digitale del futuro

Proteggere le infrastrutture Energy dalle minacce ibride

EUDR: la ridefinizione della supply chain europea

Garantire la trasparenza della catena di approvvigionamento

La cybersecurity negli ambienti industriali in Italia

La sfida delle infrastrutture critiche

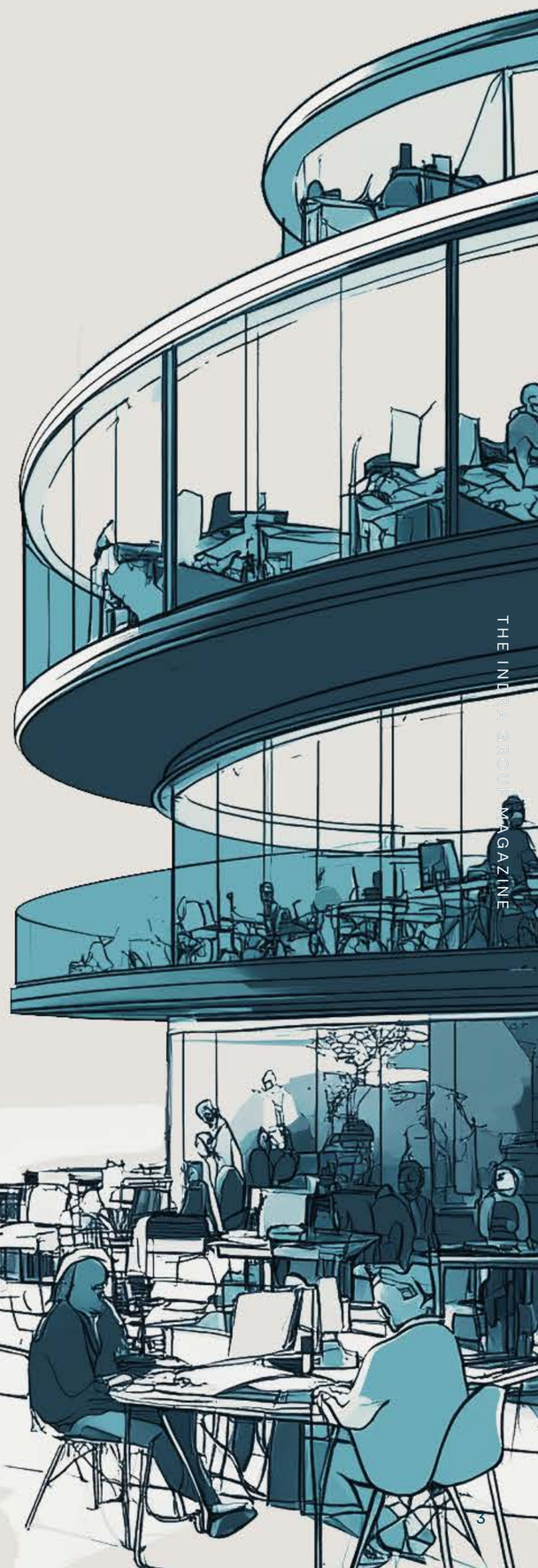
Ci sono giornate in cui il mondo ricorda all'improvviso che Internet non è un servizio "di sfondo", ma un'infrastruttura critica globale. Nell'arco di poche settimane, due blackout di Cloudflare hanno trascinato offline piattaforme social, servizi di pagamento, siti istituzionali, persino gli stessi sistemi che monitorano i disservizi. Poco prima, un guasto in un'unica regione di Amazon Web Services ha propagato i suoi effetti ben oltre la Virginia, bloccando per ore banche, app fiscali, servizi pubblici e applicazioni.

Questi episodi, che ormai si ripetono con inquietante regolarità, ci mostrano due verità scomode. La prima: la nostra vita economica e civile dipende da una manciata di nodi logici tanto quanto da centrali elettriche, ferrovie, oleodotti. La seconda: l'efficienza che abbiamo inseguito nel costruire queste infrastrutture oggi convive con una fragilità sistemica che non possiamo più ignorare.

È lo stesso filo che attraversa i temi di questo numero di NOVA.

Lo vediamo, innanzitutto, nella mobilità, forse la più civica tra le infrastrutture critiche. Un'infrastruttura spesso percepita come "locale", ma diventata globale nel momento in cui città, reti ferroviarie e corridoi logistici sono interconnessi e funzionano come piattaforme di dati. L'articolo che il CEO di Indra Group in Italia, Erminio Polito, dedica alle architetture digitali dei trasporti racconta città e corridoi logistici che funzionano sempre meno come somma di binari, strade, mezzi e sempre più come piattaforme di dati: interoperabilità tra reti, pagamenti integrati, manutenzione predittiva, gemelli digitali capaci di anticipare congestioni e incidenti.
Una mobilità davvero avanzata è quella che diventa "invisibile": quando il cittadino percepisce solo la fluidità del proprio spostamento, non la complessità dei sistemi che lo rendono possibile.
Lo stesso cambio di prospettiva attraversa il mondo industriale, dove IT e OT convergono ormai verso un unico tessuto connesso. In fabbriche, reti idriche, impianti energetici e servizi pubblici, un attacco a un sistema di controllo può fermare linee produttive o interrompere filiere essenziali. La cybersecurity OT, raccontata qui da Giacomo Parravicini e approfondita nel nostro Insight dedicato, non è più una nicchia tecnica: è il nuovo terreno su cui si misura la continuità industriale di un Paese, con tre pilastri – continuità operativa, protezione

Alessandro Anziano
Head of Marketing & Communications
Indra Group Italia



della supply chain, governance – che trasformano la sicurezza in leva competitiva e non solo in costo di conformità.

Lo stesso cambio di sguardo emerge quando spostiamo l'attenzione sull'energia. Nel contributo di Gianluca Sinibaldi, la protezione delle infrastrutture energetiche esce dal perimetro specialistico per diventare condizione abilitante della sicurezza nazionale: minacce ibride, eventi climatici estremi, sabotaggi e collassi di rete impongono piattaforme capaci di integrare domini fisici, IT e OT, di simulare scenari di crisi, di coordinare risposte in pochi minuti. È il passaggio dal rischio alla resilienza, che le direttive europee NIS2 e CER provano a tradurre in regole e standard condivisi.

In parallelo, anche le catene di approvvigionamento si stanno ridisegnando lungo le catene globali del valore. L'EUDR, la normativa europea contro la deforestazione, obbliga migliaia di imprese a dimostrare, con dati verificabili, l'origine sostenibile di materie prime come caffè, cacao, soia, legno o gomma. In questo quadro, come mostrano l'articolo di Marco Artioli e l'e-book su SAP Green Token, la sostenibilità smette di essere un capitolo del bilancio e diventa architettura digitale: catene di custodia tokenizzate, integrazione con gli ERP, automazione delle dichiarazioni di dovuta diligenza, tracciabilità granulare lungo l'intera filiera. Non è più solo "compliance": è accesso al mercato, reputazione, capacità di stare nelle nuove regole del commercio globale.

Se mettiamo in fila queste storie – i blackout di Internet, gli attacchi agli impianti industriali, la protezione delle reti energetiche, la tracciabilità delle filiere, la trasformazione della mobilità – vediamo che parlano tutte della stessa cosa: una nuova generazione di infrastrutture critiche che vive all'incrocio fra piattaforme digitali, dati e regolazione. La vera linea di frattura non passa più fra chi "ha la tecnologia" e chi no, ma fra chi riesce a tradurla in architetture resilienti, trasparenti, governabili e chi continua a costruire dipendenza da pochi nodi centrali, sperando che non si spengano mai.

Questo numero di NOVA prova a spostare il baricentro del discorso: meno attenzione al singolo strumento, più attenzione al sistema; meno enfasi sulla velocità, più sulla capacità di reggere l'imprevisto; meno retorica sull'innovazione, più riflessione su come sicurezza, sostenibilità e dati diventino ingredienti strutturali dei piani industriali.

Buona lettura.

Contenuti

Tech news

Geopolitica dei semiconduttori

Nelle ultime settimane la tensione sull'asse Washington–Pechino è tornata a crescere, proprio nel punto più delicato dell'economia globale: i semiconduttori. Il sostegno di Amazon al GAIN AI Act, dopo Microsoft e Anthropic, rafforza l'idea di un inasprimento dell'export control verso la Cina, imponendo ai produttori come Nvidia di privilegiare la domanda interna. Una strategia che riflette le preoccupazioni del Congresso sul possibile impiego militare delle tecnologie avanzate. Il settore, però, non è compatto. Nvidia avverte che ulteriori limiti rischiano di rallentare l'innovazione e spostare investimenti altrove. Nel frattempo, alcuni dei suoi maggiori investitori, da SoftBank a Druckenmiller fino a Peter Thiel, hanno liquidato quote miliardarie: prese di profitto, certo, ma anche un segnale di cautela sulle valutazioni record e sulle incognite geopolitiche.
A rendere il quadro ancora più complesso è arrivato il lancio dei nuovi modelli di Google, Nano Banana 2 e Gemini 3, sviluppati interamente su TPU proprietarie invece che sulle GPU Nvidia. Una scelta che ha mostrato come si possa competere al vertice senza dipendere dal fornitore dominante dell'hardware AI, riducendo i consumi dei data center e aprendo la strada a un ecosistema più diversificato. L'annuncio ha alimentato interrogativi sulla solidità del vantaggio competitivo di Nvidia, già nel mirino di critiche pubbliche e sospetti di bolla speculativa sollevati da investitori come Michael Burry. Questa fase conferma una tendenza chiara: la competizione sui chip è diventata un terreno di politica industriale, rischio di mercato e potere globale.

Infrastrutture sotto stress

La crescita dell'AI continua a mettere in tensione l'ossatura stessa del web. Di recente, un blackout di Cloudflare ha mandato offline per ore parti significative della rete: dalle dashboard interne a Shopify, X, ChatGPT, Sora e perfino servizi di trasporto pubblico. La causa è stata un file di configurazione cresciuto oltre le aspettative, sufficiente a mandare in crash il sistema che gestisce il traffico. Un episodio che si aggiunge al disservizio di AWS US-EAST-1, con impatti diffusi su Alexa, Snapchat, Fortnite, Canva e altri servizi mainstream. Alle fragilità software si sommano quelle fisiche. A Santa Clara, due nuovi data center non possono accendersi per carenza di energia: la domanda di potenza computazionale supera la capacità delle reti locali, e gli investimenti infrastrutturali necessari non saranno pronti prima del 2028. BloombergNEF stima che il consumo energetico legato all'AI negli Stati Uniti potrebbe raddoppiare entro il 2035. Parallelamente, la concentrazione degli investimenti accelera. Microsoft, Nvidia e BlackRock hanno acquisito Aligned Data Centers per 40 miliardi di dollari, mentre Anthropic ha siglato con Google un accordo che le garantisce un milione di TPU e oltre un gigawatt di capacità computazionale. La corsa all'AI è ormai misurata in megawatt, non solo in parametri.

AI generativa in evoluzione

Sul fronte dell'innovazione, le ultime settimane hanno visto l'arrivo di strumenti che ridefiniscono l'interazione con l'AI.
OpenAI ha presentato Atlas, un browser conversazionale che integra ricerca, sintesi e capacità agentiche: gli utenti possono dialogare con i risultati, ottenere approfondimenti o delegare azioni come prenotazioni e compilazioni di moduli.
Un cambio di paradigma che emerge mentre la quota di mercato di Google nella ricerca scende sotto il 90% per la prima volta in dieci anni. Allo stesso tempo, Anthropic continua la sua espansione fulminea. L'azienda punta a chiudere il 2025 con un fatturato annualizzato di 9 miliardi di dollari, con proiezioni che sfiorano i 26 miliardi nel 2026.
L'80% dei ricavi proviene dal segmento enterprise, mentre il nuovo Claude Haiku 4.5 vuole democratizzare l'accesso a modelli performanti ma più efficienti. La competizione si sposta così sulla integrazione nativa dell'AI nei processi quotidiani, più che sulla sola capacità dei modelli.

Regole e governance

Regolatori e Big Tech stanno cercando un equilibrio tra innovazione e tutela. La Commissione europea ha presentato il Digital Omnibus, un pacchetto che semplifica alcune norme e propone di rinviare al 2027 le parti più stringenti dell'AI Act applicate agli usi ad alto rischio. Sul tavolo c'è anche la possibilità di introdurre deroghe al GDPR per permettere l'utilizzo di dati personali nell'addestramento dei modelli. In Italia, Meta ha fatto ricorso contro la decisione dell'Agcom di equiparare le CDN agli operatori di telecomunicazioni, con il rischio di nuovi oneri e un quadro normativo isolato nel contesto europeo. Si aggiunge il reclamo della FIEG contro Google per le AI Overviews, accusate di penalizzare le testate giornalistiche riducendo il traffico organico.
Negli Stati Uniti, la governance tecnologica si intreccia con le strategie interne delle aziende: Yann LeCun lascia Meta per fondare una nuova startup dedicata ai world models, segnando un passaggio simbolico dal primato della ricerca pura alla centralità del prodotto e della competizione commerciale.

La mobilità come infrastruttura digitale del futuro

A cura di Erminio Polito
CEO Indra Group Italia

C'è un filo rosso che unisce le metropoli congestionate d'Italia e di Europa, i grandi corridoi autostradali americani, le nuove reti metropolitane del Golfo e i porti del Nord Europa: la crescente consapevolezza che la mobilità non dipende più soltanto da binari o asfalto, ma dalla solidità delle architetture digitali che ne regolano il funzionamento. Software, interoperabilità dei dati e integrazione tra reti e servizi sono ormai gli elementi decisivi per garantire sistemi di mobilità capaci di reggere la complessità del presente.

Ci sono, nel percorso che si sta tracciando, in Italia e in Europa, alcuni assi fondamentali. Il primo riguarda la capacità di creare sistemi interoperabili, capaci di abbattere le barriere tra mezzi e territori, semplificando la vita dei cittadini. Il secondo è la sicurezza, che deve essere integrata "by design" in ogni infrastruttura critica: dalle ferrovie agli aeroporti, dalle autostrade alle metropolitane. Il terzo è l'intelligenza dei dati: non più raccolti come archivi statici, ma utilizzati per alimentare modelli predittivi, ottimizzare la manutenzione,

costruire gemelli digitali in grado di anticipare congestioni e inefficienze.

Non è, tuttavia, un processo automatico. Costruire una mobilità senza attriti richiede scelte nette e coraggiose. Servono standard comuni che evitino il proliferare di soluzioni che non comunichino tra loro. Servono partnership pubblico-privato mature, capaci di condividere rischi e benefici su orizzonti di lungo periodo. Servono competenze ibride che sappiano integrare ingegneria dei dati e gestione operativa, design dei servizi e sicurezza informatica. Servono metriche ESG incorporate nei sistemi di monitoraggio, per rendere tangibili i benefici in termini di riduzione di emissioni, tempi di viaggio e incidenti evitati. Infine, serve la capacità di scalare a livello globale senza perdere il radicamento nei contesti locali, adattando ogni soluzione a regole, abitudini e infrastrutture esistenti.

La posta in gioco non è soltanto la modernizzazione dei trasporti, ma la qualità stessa della vita urbana a livello europeo. Una mobilità davvero integrata deve farsi trasparente: il cittadino non deve percepire la complessità tecnica sottostante, ma soltanto la fluidità del proprio spostamento. Pagamenti, accessi, informazioni in tempo reale, cambio di mezzo: tutto dovrebbe accadere in modo naturale, senza barriere visibili. La vera sfida è trasformare questa esperienza in un diritto di cittadinanza, dove muoversi senza attriti, in sicurezza e nel rispetto dell'ambiente diventa una condizione essenziale della vita quotidiana.

In questo scenario il Gruppo Indra si è affermato come uno degli attori più avanzati a livello internazionale, con oltre 2.500 iniziative realizzate in 50 Paesi e in più di 100 città. Dal ticketing integrato in Irlanda, che tiene insieme autobus, tram e ferrovia nazionale, all'avveniristica Brisbane Metro in Australia; dai sistemi di accesso a Riad, capaci di ridurre congestione ed emissioni, ai corridoi intelligenti della East Coast statunitense. Tutti tasselli di una stessa visione: la tecnologia come nuova infrastruttura civica.

Oggi le soluzioni del Gruppo governano la mobilità quotidiana di oltre 78 milioni di persone, contribuiscono a evitare più di 10 milioni di tonnellate di CO_2 l'anno e, grazie a sistemi di sicurezza stradale e ferroviaria, salvano migliaia di vite. È un impatto che spiega perché i mercati più esigenti—dagli Stati Uniti al Regno Unito, dall'Irlanda ai Paesi Baltici fino all'Arabia Saudita—abbiano scelto piattaforme capaci di coniugare efficienza, esperienza utente e sostenibilità, riconoscendone il valore anche negli indici ESG più selettivi, dal Dow Jones Sustainability Index all'annuario S&P.

Dal rischio alla resilienza:

come proteggere le infrastrutture energetiche nell'era delle minacce ibride

Gianluca Sinibaldi
Direttore Energy & Utilities, Minsait in Italia

Nel pieno della trasformazione che sta investendo l'economia globale, la protezione delle infrastrutture critiche energetiche è passata da funzione specialistica a condizione abilitante della sicurezza nazionale e della continuità dei servizi essenziali. La progressiva digitalizzazione dei processi, e la conseguente esposizione a minacce ibride e ad alto impatto, impone un cambio di paradigma: superare la tradizionale separazione tra sicurezza fisica e cybersecurity e adottare un approccio realmente convergente, capace di integrare domini fisici, IT e OT. Gli eventi degli ultimi anni, come attacchi informatici su scala, guerre ibride, sabotaggi a impianti energetici, collassi di rete, calamità naturali e pandemie, hanno dimostrato che servono sistemi interoperabili, rapidi nel decision-making e non più vincolati a schemi di risposta lineari.
Per farvi fronte, l'Unione Europea sta adottando

Questo segmento rappresenterà la quota di mercato più ampia del mercato globale della protezione delle infrastrutture critiche nel periodo 2025–2030, grazie alla crescente necessità di proteggere impianti, personale e asset di diverso genere da minacce fisiche come furti, sabotaggi e terrorismo. Il Medio Oriente e l'Africa, nell'immediato, registrano il tasso di crescita più elevato, visti i numerosi investimenti già avviati, in energia, trasporti, infrastrutture urbane e progetti smart city.

La tecnologia rappresenta certamente il motore, ma ciò che fa davvero la differenza è la capacità di costruire un modello integrato di prevenzione e risposta.

diverse misure: il Fondo Europeo di Difesa per sostenere ricerca e sviluppo di tecnologie innovative, lo Scudo europeo di Cybersecurity con una rete di Centri Operativi coordinati, le direttive NIS 1 e NIS 2 per rafforzare la sicurezza informatica, e la direttiva CER per estendere la resilienza delle infrastrutture critiche a più settori. Inoltre, la European Defence Industrial Strategy mira a potenziare l'industria della difesa, prevedendo nuovi finanziamenti e imponendo agli Stati membri di destinare una quota significativa del loro bilancio al settore.
In questo contesto il mercato della protezione delle infrastrutture critiche sta registrando una crescita esponenziale: secondo il report "Critical Infrastructure Protection Market" pubblicato da MarketsandMarkets, raggiungerà i 197,13 miliardi di dollari entro il 2030.
Le nuove soluzioni devono andare oltre la semplice somma di strumenti: occorre creare un sistema che raccolga e interpreti in tempo reale informazioni provenienti da fonti diverse, che sappia trasformare i dati in decisioni operative immediate e che permetta di coordinare attori diversi con la massima tempestività.

Fondamentale è anche la possibilità di simulare in anticipo scenari di crisi, così da testare strategie e verificare l'efficacia delle azioni prima che un evento si verifichi realmente. Solo piattaforme aperte e modulari, pensate per dialogare con i sistemi già in uso, possono garantire questa agilità, trasformando la tecnologia in un alleato concreto della resilienza energetica.
In pratica, la protezione delle infrastrutture energetiche deve poggiare su una regia unica, capace di integrare sicurezza fisica e digitale. Parliamo di strumenti che spaziano dalla videosorveglianza avanzata ai sistemi di controllo degli accessi, da reti di comunicazione di emergenza a centri di comando che restituiscano una visione complessiva e condivisa della situazione. A questi si affiancano soluzioni più innovative, come l'impiego di droni, l'analisi dei flussi in tempo reale e l'intelligenza artificiale, utili a ridurre i tempi di reazione e a rafforzare la prevenzione. Ciò che conta, tuttavia, è l'architettura di insieme: un sistema aperto, capace di crescere nel tempo e di adattarsi a minacce che cambiano di continuo, senza disperdere gli investimenti già effettuati.

La tutela delle infrastrutture critiche è ormai un asset strategico delle politiche industriali e della sicurezza europee. Normativa (come NIS2 e CER), incentivi e innovazione tecnologica spingono oltre la prevenzione: verso sistemi capaci di anticipare, assorbire e recuperare. In questa traiettoria, il valore risiede nella possibilità di misurare gli esiti concreti — riduzione del rischio operativo e reputazionale, contenimento dei tempi di fermo, conformità by design — e nella capacità di scalare nel tempo: partire dall'integrazione dell'esistente, crescere per moduli, mantenere il controllo dei dati e delle interfacce.

È così che la resilienza si afferma come un vantaggio competitivo, oltre che come presidio essenziale di stabilità per la società.

I pilastri della cybersecurity OT

A cura di Giacomo Parravicini
CEO di Minsait Cyber in Italia

La trasformazione digitale dell'industria degli ultimi anni ha oltrepassato una soglia invisibile. I sistemi di controllo, le reti produttive, le fabbriche, i trasporti e, in generale tutte le infrastrutture critiche, non vivono più in un perimetro isolato: sono diventati nodi di un'infrastruttura connessa, dinamica, in cui la componente IT (Information Technology) e quella OT (Operational Technology) si intrecciano fino a convergere. È un salto che ha moltiplicato l'efficienza, ma anche la superficie d'attacco. La cybersecurity OT è il nuovo terreno su cui si misura la continuità industriale di un Paese. Gli incidenti che colpiscono i sistemi industriali non sono più eccezioni, ma sintomi di una vulnerabilità sistemica. Secondo il rapporto Clusit 2025, i cyber attacchi che hanno colpito esclusivamente la componente operativa sono cresciute in modo significativo, passando dal 17% al 24% in un solo anno. Parliamo di attacchi capaci di bloccare catene produttive, rallentare reti di distribuzione o compromettere infrastrutture critiche, con impatti che si estendono ben oltre l'ambito digitale e mettono alla prova la stessa continuità industriale di interi settori. In questo contesto, una strategia di protezione efficace poggia su tre pilastri essenziali: la continuità operativa, la protezione della supply chain e la governance. Tre dimensioni che si intrecciano e si rafforzano a vicenda, trasformando la sicurezza da funzione difensiva a leva di competitività industriale.

Continuità operativa
Proteggere la tecnologia operativa significa prima di tutto preservare la capacità di funzionare, di garantire servizi essenziali anche sotto pressione. La sicurezza, in questo contesto, non è più un costo di conformità, ma un fattore produttivo: serve a evitare interruzioni, a ridurre i tempi di fermo, a mantenere intatti i flussi di valore. L'attenzione si sposta quindi dal dato, al processo, dall'integrità informatica, alla resilienza industriale. Ma la continuità non si costruisce solo con le tecnologie: nasce dalla capacità di leggere i processi, di individuare le dipendenze critiche, di pianificare interventi che non compromettano la stabilità operativa.

Protezione della supply chain
Questa consapevolezza si estende ben oltre i confini dell'impianto: l'ecosistema industriale contemporaneo è una rete fitta di fornitori, manutentori, partner e operatori remoti, una filiera connessa in cui la vulnerabilità di uno può diventare la vulnerabilità di tutti. È necessario adottare controlli comuni, condividere policy di accesso, formare le persone che operano lungo la catena del valore. La sicurezza, in questo senso, non è una barriera, ma una forma di collaborazione: un contratto di fiducia che attraversa l'intero ecosistema produttivo.

Governance
Questo è l'elemento che tiene insieme tutti gli altri. Senza una regia chiara, la sicurezza resta frammentata: una somma di soluzioni che non fa sistema. Le organizzazioni che raggiungono la maturità in ambito OT sono quelle che trattano la sicurezza come un processo di gestione, con ruoli definiti, metriche, revisioni periodiche e un allineamento costante agli standard internazionali. Tra questi, la norma IEC 62443 è oggi il riferimento più solido: fornisce una cornice per segmentare le reti, definire i livelli di privilegio, gestire l'intero ciclo di vita della sicurezza. Non è un esercizio formale: è il modo per trasformare le buone pratiche in vantaggio competitivo, rendendo la protezione parte della qualità complessiva del sistema industriale.

Alla fine, la sicurezza OT è un linguaggio che obbliga mondi diversi a parlarsi. Ogni ruolo — ingegneri di impianto, esperti IT, manager della produzione e analisti di rischio — ha le proprie responsabilità, ma tutti condividono l'obiettivo della protezione OT. Non si tratta di moltiplicare le regole, ma di creare una cultura in cui la protezione è condizione di sviluppo, la prevenzione è parte del valore e la resilienza è una misura della leadership.

La sostenibilità in evoluzione: come l'EUDR ridefinisce la supply chain europea

A cura di Marco Artioli
Head of SAP Practice, Minsait in Italia

La sostenibilità ha smesso di essere un'opzione per diventare un requisito strategico. La crescente pressione normativa, la consapevolezza dei consumatori e l'urgenza climatica stanno imponendo alle imprese di ripensare radicalmente il modo in cui producono, distribuiscono e tracciano le proprie materie prime. In questo scenario, l'Unione Europea ha compiuto un passo decisivo con l'entrata in vigore dell'EUDR (Regolamento Europeo sulla Deforestazione) prevista per fine anno, che obbligherà le aziende a garantire l'immissione sul mercato di prodotti non associati alla deforestazione e al degrado forestale. Anche il contesto italiano si prepara a recepire nuove misure in materia di sostenibilità. Tra queste, la Plastic Tax, la cui entrata in vigore è prevista per luglio 2026, rappresenta un ulteriore strumento di politica ambientale che conferma la volontà dei legislatori di incentivare l'uso di materiali riciclati e sostenibili.

L'Europa sta ridefinendo il concetto di responsabilità nella catena del valore. Le imprese non saranno più chiamate solo a gestire i fornitori, ma a garantire la tracciabilità end-to-end, raccogliendo informazioni geografiche e legali sull'origine di ogni materia prima, valutando i rischi di non conformità e adottando misure di mitigazione.

Oltre ai rischi operativi, la mancata conformità all'EUDR comporterà anche conseguenze economiche significative. Secondo una stima dalla Commissione europea, i costi annuali di conformità all'EUDR per gli operatori andranno dai 175 milioni di euro ai 2,6 miliardi. Anche le sanzioni previste non sono trascurabili: le autorità potranno imporre multe fino al 4% del fatturato annuo, la confisca

dei prodotti e, nei casi più gravi, l'esclusione dalle gare pubbliche. In questo scenario è facilmente prevedibile un impatto profondo: migliaia di operatori, in settori che spaziano dall'agroalimentare al legno, dalla gomma alla carne bovina, dovranno dimostrare l'origine sostenibile dei propri prodotti attraverso dati verificabili e conformi.

Ma dietro questa sfida normativa si cela una grande opportunità: chi saprà integrare la trasparenza e la tracciabilità nel proprio modello operativo rafforzerà la fiducia del mercato e conquisterà un vantaggio competitivo duraturo. L'obiettivo sarà, quindi, andare oltre la conformità richiesta: l'EUDR impone un modello di trasparenza proattiva, in cui la qualità dei dati diventa garanzia di reputazione, affidabilità e fiducia verso clienti e regolatori. Per molte aziende, questo implica superare barriere tecnologiche e operative, integrando strumenti digitali capaci di automatizzare processi complessi di raccolta, verifica e conservazione delle informazioni.

In un mercato in cui, secondo l'Eurobarometro 2024, l'83% degli europei considera l'impatto ambientale un aspetto importante nelle decisioni d'acquisto, la tracciabilità è ormai un fattore di fiducia e differenziazione.
Il rispetto della EUDR, quindi, non rappresenta solo un obbligo legale, ma un investimento in reputazione e competitività. Le imprese che adotteranno sistemi digitali evoluti potranno offrire ai propri clienti una trasparenza reale, rafforzando la relazione con il mercato e proteggendo il valore del brand.

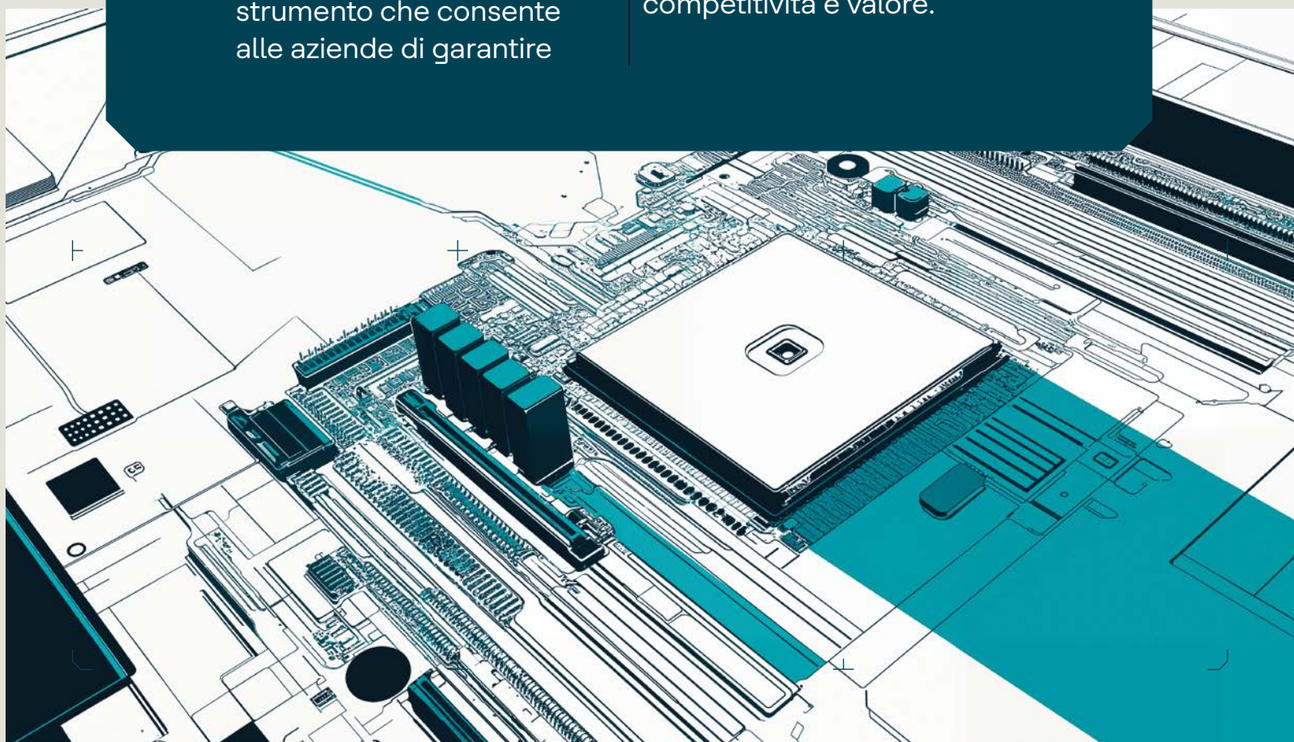
Per rispondere a queste esigenze, l'universo SAP ci offre una piattaforma di tracciabilità digitale che permette di acquisire, verificare e condividere in modo sicuro l'origine e gli attributi di sostenibilità delle materie prime: SAP Green Token. Una soluzione che sfrutta la catena di custodia digitale basandosi su tecnologia blockchain: ogni materia prima riceve un token digitale con informazioni geolocalizzate, certificazioni, impronta di carbonio e dati di produzione. Man mano che il prodotto attraversa gli attori della supply chain i token vengono trasferiti e aggiornati, mantenendo la tracciabilità completa e verificabile.

Il sistema consente, inoltre, di generare automaticamente la documentazione richiesta dalla normativa, assicurando una conformità rapida e senza errori manuali. L'integrazione con sistemi ERP e altre piattaforme europee permette di automatizzare il processo di adozione degli standard richiesti, con possibili risparmi anche sui costi operativi e gestionali. Attraverso report, conversione dei materiali e monitoraggio dei flussi interni, le aziende possono, quindi, migliorare la governance della supply chain e identificare inefficienze o rischi in tempo reale.

Un ulteriore supporto alle aziende, in ottica di sostenibilità, è rappresentato da SAP Responsible Design and Production (RDP), la soluzione pensata per aiutare le imprese a gestire in modo efficiente gli adempimenti legati alla Plastic Tax e alla tracciabilità dei materiali plastici. Già utilizzata in Paesi come la Spagna, dove la normativa è in vigore dal 2023, consente alle aziende di monitorare l'uso della plastica e di adeguarsi alle normative ambientali, contribuendo così a promuovere modelli produttivi più responsabili e circolari.

L'EUDR segna una svolta per il sistema produttivo europeo e italiano: una chiamata all'azione verso modelli industriali più sostenibili, digitali e trasparenti. Le imprese che sapranno rispondere a questa sfida non solo si adegueranno alla legge, ma rafforzeranno la propria leadership nel mercato globale, coniugando sostenibilità, innovazione e fiducia.

In questo percorso, SAP Green Token rappresenta un valido aiuto per garantire compliance e, al tempo stesso, crescita: uno strumento che consente alle aziende di garantire la tracciabilità end-to-end, generare dati verificabili e trasformare la sostenibilità in un autentico motore di competitività e valore.



Contesto: il mercato della Cyber OT

A livello globale, il mercato cybersecurity per OT ha raggiunto i 12,75 miliardi di dollari nel 2023, e si prevede che arriverà a circa 21,6 miliardi di dollari entro il 2028, con un tasso di crescita annuale composto (CAGR) di circa il 9,2%.

In Europa e in Italia, la crescita della cybersecurity industriale e OT si colloca in uncontesto di minacce informatiche sempre più sofisticate, alimentate anche dal progresso dell'Intelligenza Artificiale.
A fronte di 3.541 incidenti gravi registrati a livello globale nel 2024, di cui circa il 10% avvenuti in Italia, emerge la necessità di rafforzare la protezione degli asset critici, in particolare nel mondo Operational Technology (OT), dove l'integrazione tra sistemi digitali e infrastrutture fisiche espone le imprese a rischi sistemici.Il mercato italiano della cybersecurity ha raggiunto nel 2024 i 2,48 miliardi di euro(+15% rispetto al 2023), spinto in parte dall'urgenza di proteggere settori regolamentati come energia, trasporti,manifattura e sanità, in cui la componente OT è centrale.
Tuttavia, l'Italia rimane all'ultimo posto tra i Paesi del G7 per rapporto tra spesa in cybersecurity e PIL, un dato che riflette una

vulnerabilità sistemica, soprattutto in ambito OT, dove l'obsolescenza delle infrastrutture e la dipendenza da terze parti costituiscono fattori di rischio rilevanti.

Secondo l'Osservatorio Cybersecurity & DataProtection del Politecnico di Milano, solo una parte delle grandi organizzazioni italiane ha adottato un approccio realmente proattivo e resiliente: il 51% riconosce di non aver ancora colmato il gap accumulato. Il fattore umano resta il principale vettore di rischio (75%), seguito dall'obsolescenza tecnologica (73%)– due elementi particolarmente critici nei contesti OT, dove sistemi legacy sono spesso integrati con nuove tecnologie senza un'adeguata governance. In questo scenario, la convergenza tra IT e OT rappresenta un fronte strategico, ma ancora poco presidiato.

La NIS2 e il Cyber ResilienceAct spingono le imprese verso standard più elevati di sicurezza anche per gli ambienti OT, ma l'adozione è disomogenea.

La Generative AI, già introdotta dal 9% delle organizzazioni italiane, può diventare un'arma a doppio taglio: da un lato, abilitando la protezione predittiva; dall'altro,amplificando le superfici d'attacco OT attraverso vulnerabilità nei sistemi industriali interconnessi.

Alcuni dati sulla cybersecurity negli ambienti industriali

(Dal Rapporto Ascendant sulla maturità della cybersicurezza 2024, basato su dati da Spagna, Italia, Portogallo e America Latina)

75%

le organizzazioni OT che hanno subito almeno un'intrusione nell'ultimo anno

46%

prevede di sviluppare roadmap specifiche per OT tra il 2023 e il 2025

38%

gestisce le identità e gli accessi OT separatamente rispetto al mondo IT

24%

dispone di programmi disensibilizzazione specifici per OT

23%

considera la gestione del rischio dei terzi lungo l'intero ciclo di vita della supply chain.

Rilevamento e risposta agli incidenti

93%

non include gli ambienti OT neipropri processi di rilevamento e risposta.

53%

prevede di implementare soluzionientro due anni.

23%

possiede strumenti avanzati diprotezione degli asset OT.

15%

effettua penetration test specifici per identificare minacce OT.

Mercato totale cybersicurezza Italia 2024

2,48 miliardi EUR

Mercato OT globale 2023

12,75 miliardi USD

Mercato OT globale 2028 (stima)

21,6 miliardi USD

CAGR mercato OT

9–11 %

Cyberattacchi in Italia, 2024

+56%YoY; 485.000 eventi

Attacchi ransomware annuali in Italia

~4.721

Fonte: Osservatorio Cybersecurity & Data Protection- Politecnico di MilanoFonte: Rapporto Clusit 2025

Cyber OT

6 passaggi per rispondere agli incidenti negli ambienti OT

01

Progettare esercitazioni specifiche per ogni impianto
Gli esercizi "table top" sono uno strumento molto utile per allenarsi nella risposta agli incidenti. Tuttavia, nel caso degli ambienti OT, non è sufficiente un approccio generico o aziendale, come avviene spesso nei contesti IT. Ogni impianto o installazione industriale ha caratteristiche, rischi, sistemi e processi unici, per cui gli esercizi devono essere adattati alla realtà specifica.

02

Integrare IT e OT negli scenari di risposta
Uno degli errori più comuni è separare gliambienti IT e OT quando si pianifica la risposta agli incidenti. Tuttavia, nella pratica, gli attacchi attraversano entrambi i mondi. Per questo motivo è fondamentale che gli esercizi li coinvolgano entrambi, al fine di individuare i punti deboli nell'interazione tra IT e OT, e promuovere la collaborazione tra i team, che tradizionalmente hanno operato separatamente. Il team IT, che storicamente ha affrontato incidenti informatici, possiede una preziosa esperienza nella gestione delle crisi, nell'applicazione dei controlli di sicurezza e nell'uso delle tecnologie di rilevamento. Questa competenza è molto utile per gli ambienti OT, che spesso non hanno affrontato lo stesso livello di minacce. Per questo motivo, unire gli sforzi tra IT e OT è essenziale. L'IT può fornire metodologie, strumenti e pratiche già collaudate, mentre l'OT offre una profonda conoscenza dei processi industriali e delle loro esigenze specifiche. Questa sinergia è fondamentale per una risposta efficace e per costruire una solida cultura della sicurezza in tutta l'organizzazione.

03

Coinvolgere tutte le aree rilevanti e prevedere ostacoli
La risposta ad un incidente in ambiente OT deve coinvolgere anche altre aree dell'azienda, come fornitori esterni, servizi legali, marketing, comunicazione e assistenza clienti. È comune che esistano dipendenze da terze parti, e non prevederle può ritardare o complicare la risposta. È inoltre necessario coordinare i messaggi da diffondere, preparare i portavoce, verificaregli aspetti legali e assicurarsi che tutte le parti coinvolte agiscano in modo coerente.

04

Integrare tecnologie avanzate per rafforzare la risposta
L'intelligenza artificiale (IA), ad esempio, può rilevare comportamenti anomali nelle reti OT prima che si trasformino in attacchi gravi. Può anche contribuire ad automatizzare le risposte iniziali, guadagnare tempo e ridurre l'impatto dell'incidente.

05

Prepararsi a scenari critici e proteggere la disponibilità
Un guasto o un attacco in un ambiente OT può avere conseguenze gravi: dal blocco totale di un impianto fino al danneggiamento di servizi essenziali come l'elettricità o la fornitura d'acqua. È quindi fondamentale considerare scenari catastrofici e preparare strategie per garantire la continuità operativa.

06

Assicurare l'impegno della direzione aziendale
Senza il supporto continuo dei vertici aziendali, un piano di risposta agli incidenti ha poche possibilità di successo. La direzione deve essere coinvolta sin dalla progettazione dell'esercitazione, partecipare attivamente alla sua esecuzione e farsi trovare pronta a prendere decisioni rapide durante una crisi reale.

Come proteggere l’accesso da remoto

È sempre più comune che gli impianti industriali, le centrali elettriche e altre infrastrutture critiche necessitino di accesso remoto per le loro operazioni quotidiane. E quando si tratta di accesso remoto con privilegi elevati, rafforzarne la protezione diventa più cruciale che mai.

Controllare l’accesso in modo sicuro

Esistono strumenti specifici che agiscono come filtri o punti dicontrollo, capaci di verificare chi sta cercando di accedere, qualipermessi possiede, e monitorare ciò che viene fatto durante unasessione. Se rilevano comportamenti anomali, possono bloccareimmediatamente l’accesso. Questi strumenti sono solitamente posizionati in punti strategici dellarete industriale, come il livello 3 o 4 del modello Purdue, all’interno diuna zona speciale chiamata DMZ (zona demilitarizzata), che funge dascudo: controlla tutto ciò che entra ed esce, assicurando che solo gliutenti autorizzati possano accedere ai sistemi più sensibili.

Accesso con controllo delle identità

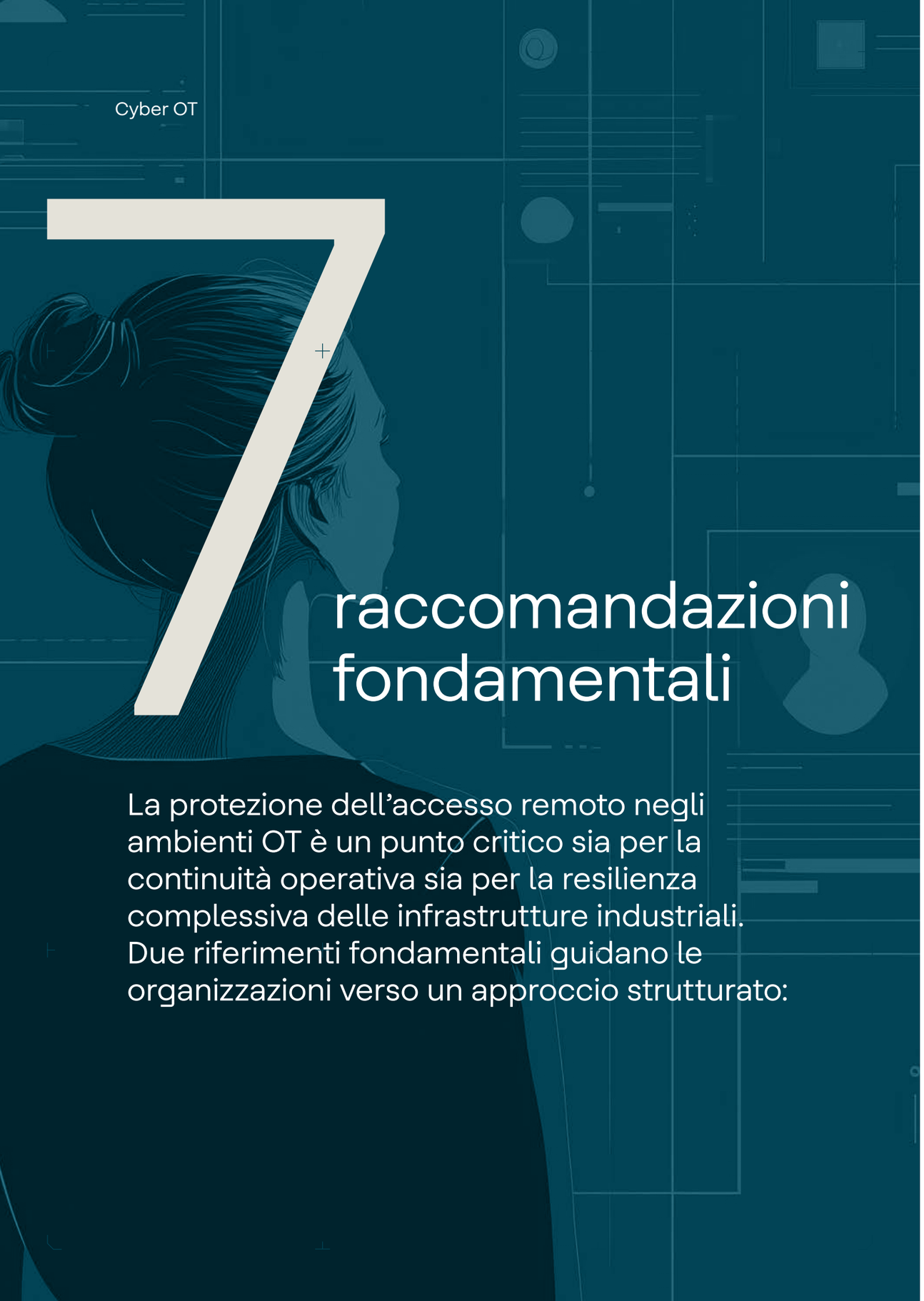
Una buona gestione degli accessi richiede anche il controllodell’identità degli utenti, adattando le pratiche già utilizzate in ambito IT, ma declinate alle specifiche esigenze dell’OT. In altre parole: chi è l’utente, cosa può fare e su quali sistemi può operare.Si raccomanda inoltre di evitare l’uso di strumenti non sicuri come TeamViewer, AnyDesk o VNC. Sebbene siano comodi, queste applicazioni non offrono il livello di sicurezza necessario per ambienti industriali critici.

Organizzazione e separazione

Un centro operativo di cybersicurezza (SOC) può occuparsi della creazione, rimozione o modifica degli utenti, liberando i team OT per concentrarsi sulla produzione. In questo modo, è possibile gestire gli accessi in sicurezza senza ostacolare l’operatività. È anche importante che la gestione degli utenti OT sia indipendente da quella IT. Ad esempio, si raccomanda che i sistemi di autenticazione (come Active Directory) siano separati tra i due ambienti. Così, eventuali problemi di sicurezza in ambito IT non avranno impatti diretti sull’OT.

Sicurezza a più livelli

L’accesso remoto privilegiato deve essere protetto all’interno di una strategia più ampia di sicurezza a strati. Oltre alla DMZ, si possono utilizzare security gateways o altri strumenti per rafforzare le difese, offrendo una protezione più completa. In sintesi, proteggere l’accesso remoto privilegiato non è solo una questione tecnologica, ma implica anche una corretta organizzazione degli accessi, la gestione indipendente delle identità e una collaborazione efficace tra IT e OT. Se implementato correttamente, ciò consente non solo una maggiore sicurezza, ma anche un’operatività più efficiente e continua.



7 raccomandazioni fondamentali

La protezione dell’accesso remoto negli ambienti OT è un punto critico sia per la continuità operativa sia per la resilienza complessiva delle infrastrutture industriali. Due riferimenti fondamentali guidano le organizzazioni verso un approccio strutturato:

IL SANS INSTITUTE, che fornisce raccomandazioni pratiche e immediate per la gestione sicura degli accessi remoti, con un’attenzione particolare ai rischi operativi concreti.

LA NORMA INTERNAZIONALE IEC 62443, lo standard di riferimento per la cybersecurity industriale, che definisce requisiti tecnici e organizzativi basati sul modello zone & conduits, sull’access management e sulla difesa in profondità.

Le best practice del SANS sono sostanzialmente coerenti con la IEC 62443, ma quest’ultima amplia la prospettiva, introducendo principi come il minimo privilegio, la revoca tempestiva degli account, l’uso di meccanismi crittografici perproteggere l’integrità dei dati, e la governance complessiva della sicurezza OT. Integrare entrambi gli approcci significatrasformare delle buone pratiche operative in un vero e proprio **modello di gestione end-to-end, solido e certificabile**

01

CREARE UNA ZONA DI SICUREZZA (DMZ)

Il SANS raccomanda di istituire una zona demilitarizzata (DMZ) tra Internet, la reteIT e la rete industriale interna, così da controllare e filtrare centralmente tutti gliaccessi remoti. La IEC 62443 rafforza questo concetto con il modello delle zone & conduits, che consente di stabilire diversi livelli di sicurezza e canali di comunicazione regolati, definendo in modo preciso i confini e i flussi tra aree operative

02

UTILIZZARE LA MULTIFACTOR AUTHENTICATION (MFA)

Secondo il SANS, l’adozione dellaMFA, basata su password, token e codici di verifica, è fondamentale per ridurre il rischio di accessi non autorizzati. La IEC62443 amplia il perimetro, introducendo requisiti per la gestione completa del ciclo di vita delle identità: dall’assegnazione dei privilegi secondo il principio del minimo necessario, fino alla revoca immediata delle credenziali non più valide.

03

UTILIZZARE I JUMP SERVER

Il SANS suggeriscel'impiego di jump server come punti di controllo intermedi, in grado di filtrare leconnessioni e registrare le sessioni dilavoro. La IEC 62443 inquadra questi meccanismi nel concetto di conduits, canali sicuri tra zone differenti chedevono garantire autenticazione,monitoraggio e protezione continua del traffico.

04

VERIFICARE I FILE TRASFERITI

Per il SANS, ogni file scambiato in sessioni remote va controllato e validato per prevenire malware o data leakage. La IEC 62443 spinge oltre, prescrivendo l'uso di crittografia, checksum e altri strumenti di verifica dell'integrità, così da assicurare non solo la sicurezza del trasferimento ma anche la confidenzialità dei dati.

05

SEPARARE LA GESTIONE DEGLI ACCESSI IT E OT

Il SANS raccomanda di mantenere directory indipendenti (ad esempio Active Directory separati) per distinguere la gestione delle identità nei due domini. La IEC 62443 formalizza questo approccio, richiedendo una segregazione chiara dei privilegi e sistemi di identity management distinti, in grado di prevenire contaminazioni tra ambienti.

06

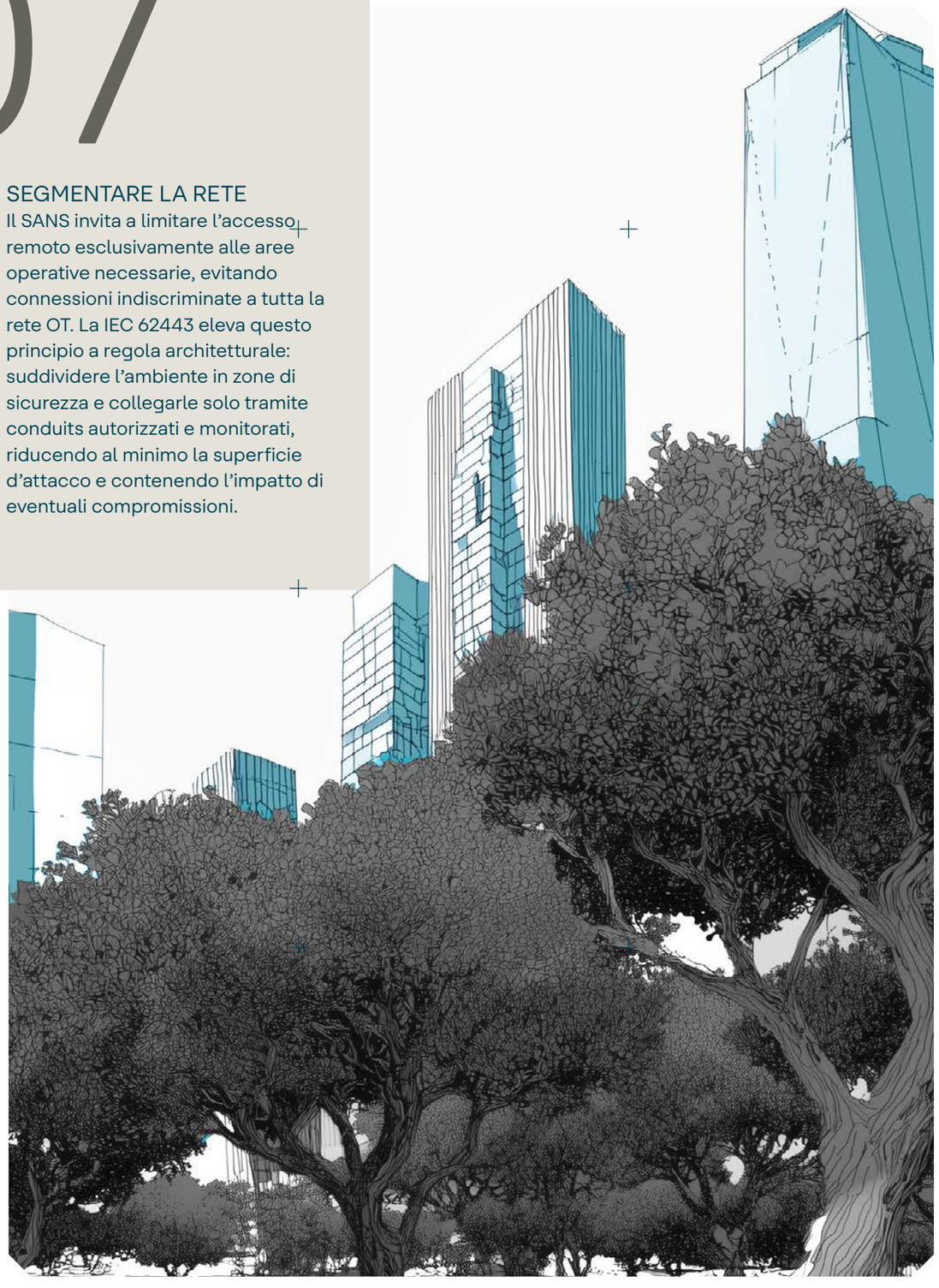
STABILIRE RUOLI CHIARI (RBAC)

Nelle linee guida del SANS, ogni utente deve avere un ruolo ben definito, con permessi specifici e limitati al necessario. La IEC 62443 rende questo principio più strutturato, imponendo l'adozione del modello Role-Based Access Control (RBAC) e una gestione centralizzata dei profili, così da ridurre il rischio di errori e facilitare i controlli periodici.

07

SEGMENTARE LA RETE

Il SANS invita a limitare l'accesso remoto esclusivamente alle aree operative necessarie, evitando connessioni indiscriminate a tutta la rete OT. La IEC 62443 eleva questo principio a regola architetturale: suddividere l'ambiente in zone di sicurezza e collegarle solo tramite conduits autorizzati e monitorati, riducendo al minimo la superficie d'attacco e contenendo l'impatto di eventuali compromissioni.



Un cambio di paradigma nella regolamentazione europea italiana

L'Unione Europea ha **approvato il Regolamento (UE) 2023/1115, noto come EUDR (Regolamento europeo sulla deforestazione)**, che stabilisce requisiti rigorosi per garantire che i prodotti commercializzati nel mercato europeo siano privi di legami con la deforestazione e il degrado forestale.
Al Regolamento si aggiunge la **Plastic Tax italiana**, un'imposta ambientale introdotta con la Legge di Bilancio 2020, ma la cui entrata in vigore è attualmente prevista per il **1° luglio 2026.** L'obiettivo della misura è **ridurre l'uso di plastica monouso e incentivare la produzione di materiali riciclati o biodegradabili**, in linea con le direttive europee sull'economia circolare.

Cosa implica la EUDR?

Il regolamento entrerà in vigore il 30 dicembre 2025 per le grandi imprese e il 30 giugno 2026 per le piccole e medie imprese (PMI).
Tra i prodotti regolamentati figurano alcuni dei più rilevanti per l'economia globale e locale: caffè, cacao, olio di palma, soia, gomma, legno e bestiame bovino, oltre ai loro derivati, come carta e cartone, mobili, cioccolato, bioplastiche, pneumatici o cuoio.

Cosa implica la Plastic Tax?

La tassa si applicherà ai MACSI (Manufatti con singolo impiego), cioè imballaggi e contenitori in plastica destinati a un solo utilizzo, con un'imposta pari a 0,45 euro per chilogrammo di materiale plastico vergine utilizzato. Per le imprese italiane, l'impatto sarà duplice: da un lato un aumento dei costi di produzione per chi continua a utilizzare plastica tradizionale, dall'altro un incentivo all'innovazione verso soluzioni sostenibili, al riciclo e alla tracciabilità del contenuto riciclato.

La due diligence come obbligo

Per poter commercializzare questi beni nell'Unione Europea, gli operatori dovranno dimostrare, tramite una Dichiarazione di Due Diligence (DDS), che la produzione non proviene da terreni deforestati dopo il 31 dicembre 2020 e che rispetta le leggi del Paese d'origine.
Questa dichiarazione dovrà essere registrata elettronicamente su TRACES, il sistema ufficiale della Commissione Europea per la validazione e il controllo dei prodotti agroalimentari, sanitari e ambientali.

Impatto in Italia e sanzioni previste

L'impatto del Regolamento EUDR sarà rilevante anche in Italia, dove migliaia di imprese lungo l'intera filiera agroalimentare, manifatturiera e della bioenergia dovranno adeguarsi ai nuovi obblighi di tracciabilità e due diligence.

Le sanzioni previste in caso di inosservanza non sono trascurabili: le autorità potranno imporre multe fino ad almeno il 4% del fatturato annuo nell'Unione Europea, la confisca dei prodotti non conformi e, nei casi più gravi, l'esclusione dalle gare pubbliche.
Il Governo italiano, tramite il Ministero dell'Ambiente e della Sicurezza Energetica (MASE) e l'Agenzia delle Dogane e dei Monopoli (ADM), sta predisponendo i meccanismi nazionali
di controllo e recepimento del Regolamento, in coordinamento con le autorità forestali e le regioni.

Sono in fase di definizione linee guida operative per la gestione delle dichiarazioni di dovuta diligenza (DDD) e per il monitoraggio delle merci in ingresso e uscita dal mercato unico.

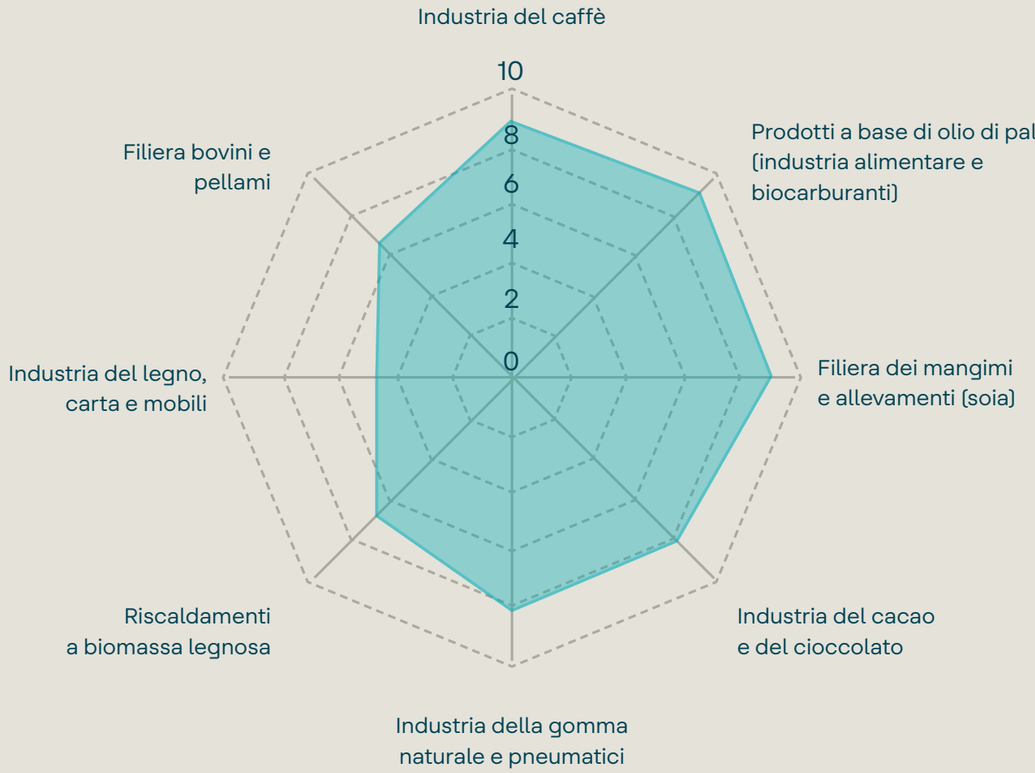
Oltre la conformità: una sfida strutturale

In pratica, la EUDR obbliga le imprese ad andare ben oltre la semplice
gestione dei fornitori. Sarà necessario:
- Raccogliere informazioni geografiche e legali sull'origine di ogni
materia prima,
- Valutare il rischio di non conformità in base al Paese o alla regione
di provenienza,
- Stabilire misure di mitigazione, come audit indipendenti o la
sostituzione dei fornitori in caso di dubbi sulla sostenibilità.

Conseguenze globali con impatto locale

Questo quadro normativo rappresenta una sfida globale con effetti
locali. Non si tratta solo di rispettare un obbligo amministrativo, ma di trasformare la gestione delle catene di approvvigionamento in un
processo trasparente, verificabile e sostenibile, capace di generare
fiducia tra regolatori, consumatori e partner commerciali.

I settori in Italia maggiormente colpiti dall'EUDR



Livello di impatto (1–10)

SAP Green Token: automatizzazione e tracciabilità per l’EUDR

L’EUDR pone le imprese di fronte a una sfida complessa: raccogliere informazioni dettagliate sull’origine delle materie prime, valutare i rischi, dimostrare la tracciabilità e presentare la Dichiarazione di Dovuta Diligenza (DDS) entro i termini stabiliti.

SAP Green Token trasforma queste sfide in processi automatizzati, sicuri e verificabili, consentendo alle organizzazioni di rispettare la normativa in modo fluido ed efficiente.

Generazione automatica delle DDS e connessione con TRACES

SAP Green Token facilita la creazione della DDS per ogni operazione di ingresso, trasformazione o uscita delle merci.

Grazie alla sua integrazione con i sistemi ERP e con le piattaforme della Commissione Europea, lo strumento consente l’invio automatico della documentazione a TRACES, evitando errori manuali e garantendo che le informazioni rispettino pienamente i requisiti formali della normativa.

Geolocalizzazione precisa con GeoJSON

Uno degli aspetti più rigorosi dell’EUDR è la necessità di dimostrare la localizzazione esatta delle parcelle.
SAP Green Token risolve questo punto generando file GeoJSON per ogni piantagione, che assicurano la conformità geografica e permettono un tracciamento chiaro e verificabile lungo tutta la catena di approvvigionamento.

Reporting avanzato per le attività di Audit

La piattaforma include funzionalità di reporting che agevolano i processi di audit e controllo:

- Bilanci di massa per validare le entrate e le uscite dei materiali;
- Report di conversione nei processi di trasformazione;
- Storico dei movimenti dei materiali per ricostruire qualsiasi transazione.

Questi report non solo garantiscono la conformità alla normativa, ma offrono anche alle aziende un maggiore controllo interno e una tracciabilità trasparente, completa e verificabile.

Adatto a scenari multi-stabilimento e multinazionali

SAP Green Token è progettato per contesti aziendali complessi, in cui i materiali attraversano diversi stabilimenti, Paesi o società appartenenti allo stesso gruppo.
La soluzione prevede l’attivazione multi-stabilimento, che consente di gestire i movimenti intercompany e di mantenere una tracciabilità continua in organizzazioni multinazionali.

NOVA
THE INDRA GROUP MAGAZINE

#3 | 2025 | ITALY

Nova è un magazine
prodotto da Indra Group in Italia.

I contenuti editoriali sono a cura
del team Marketing e Comunicazione
di Indra Group in Italia.

I contenuti grafici
sono a cura di Minsait Xtudio in Italia

Per domande o informazioni scrivi a
communityitalia@indracompany.com

Minsait in Italia, Via del Serafico, 200,
00142, Roma
tel: 06 41 21 101