

Vedi niente ?

Bene !

Neanche il ladro

InFOG

Security Fogging System



InFOG è il **nebbiogeno integrato Inim** che, azzerando la visibilità in pochi secondi, rende impossibile agire. Il **90%** dei furti viene sventato prima di iniziare. La sua nebbia è atossica e certificata food-grade: sicura anche in ambienti con presenza di alimenti. **Doppia connessione cablata e via radio**, antisabotaggio immediato, prova di sparo e serbatoio sempre sotto controllo tramite app.

Passa a un livello superiore di protezione con un sistema che cambia le regole della sicurezza.

Scopri di più su www.inim.it

VIGILANZA



La **tecnologia** che guarda al **futuro** della **sicurezza**

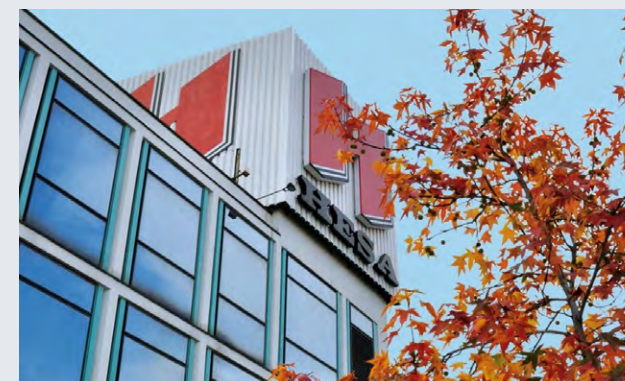
Urmet ATE sviluppa soluzioni per la vigilanza professionale, integrando tecnologia, sistemi e competenze per supportare in modo concreto l'attività degli operatori. Piattaforme progettate per semplificare la gestione, coordinare le operazioni e migliorare il controllo in tempo reale, ottimizzando i processi e riducendo la complessità. Dall'evoluzione delle centrali operative, come **Ate Argo Next**, all'introduzione di strumenti avanzati come l'operatore virtuale **NEXTY**, ogni soluzione è pensata per rendere la vigilanza più efficiente e affidabile. Da oltre 20 anni, Urmet ATE è un punto di riferimento per una protezione che guarda al futuro.

L'editoriale del direttore



Cambia il mondo della sicurezza: HESA passa di mano

Avremmo voluto dedicare, come al solito, l'editoriale di mezza estate alle ultime tendenze che potranno influire sul mercato della sicurezza privata ma è arrivata una breaking news che ruba la scena alle altre: [la vendita di HESA](#) da parte della famiglia Hruby al gruppo danese EET. Una notizia che segna la conclusione di un ciclo fondamentale per la storia della sicurezza moderna, segnato dall'arrivo delle tecnologie elettroniche per proteggere banche, fabbriche e case private dalle intrusioni non autorizzate.



Enzo Hruby, il fondatore, aveva intuito alla fine degli anni '60 che certi dispositivi prodotti negli USA e in Gran Bretagna con tecnologie sviluppate in ambito militare (microonde, ultrasuoni, rfid), avrebbero avuto successo anche in Italia e con la sua ditta "Hruby Enzo Sistemi Automatici (HESA)" divenne importatore e distributore in esclusiva di importanti produttori internazionali. HESA è stata per molti anni l'hub di riferimento delle tecnologie per la sicurezza fisica, selezionando da una parte prodotti e produttori da proporre al mercato; dall'altra, raccogliendo, formando e promuovendo generazioni di installatori professionali.

L'arrivo di internet, il progressivo orientamento dei produttori ad accorciare la catena distributiva assieme alla crescita dimensionale degli installatori, hanno modificato poco per volta il ruolo del distributore specializzato e così Carlo e Andrea, i figli di Enzo che nel frattempo gli erano subentrati alla guida della HESA, hanno deciso che era arrivato il momento di venderla a uno dei maggiori distributori europei, in grado di valorizzare lo storico marchio e di garantirne lo sviluppo in un mercato sempre più competitivo.

A parte la storia imprenditoriale di successo, si deve riconoscere alla famiglia Hruby il grande merito di aver costituito uno straordinario modello di partenariato privato/pubblico per la tutela del patrimonio artistico, la Fondazione Enzo Hruby, senza uguali nemmeno a livello internazionale. Voluta e animata da Carlo, ha sostenuto direttamente interventi per la messa in sicurezza di siti e di singole opere in tutta Italia, realizzato pubblicazioni, commissionato ricerche e, in ultimo, avviato collaborazioni con Università per formare security manager specializzati nei beni culturali.

La Fondazione è una dimostrazione tangibile di quanto possa essere efficace l'iniziativa privata per supportare la pubblica amministrazione nell'esercizio di funzioni istituzionali che riguardano il bene pubblico come, in questo caso, la tutela del patrimonio artistico, un esempio da manuale di "sussidiarietà orizzontale" prevista dall'art. 118 della Costituzione.

Per tutto questo, per l'impegno costante nella divulgazione della "cultura della sicurezza" con importanti contributi pubblicati negli anni anche sulle nostre testate, per aver condiviso i valori della professionalità, della competenza e dell'etica per chiunque lavori nella sicurezza, diciamo grazie a Enzo, Carlo e Andrea Hruby, è stato davvero un piacere lavorare insieme!

GLI EVENTI DI SECURINDEX

calendario autunno 2026



**IA AL LAVORO PER LA COMPLIANCE
DELLE ORGANIZZAZIONI**
martedì 6 ottobre

Si terrà il 6 ottobre a Palazzo Cusani, sede del Circolo Ufficiali di Milano, la seconda edizione del workshop "IA al lavoro", dedicata alle applicazioni per il monitoraggio della compliance delle organizzazioni alle normative di pertinenza.



**SFR 2026 - KEEP CALM AND CARRY
CASH, IL CAMBIO DI PARADIGMA**
martedì 20 ottobre

Come sta reagendo il sistema della distribuzione al dettaglio ai nuovi scenari prodotti dall'introduzione del modello "Bank in shop"? Quali sono gli effetti in termini di sicurezza degli store della GDO e dei negozi di prossimità? A questi e altri punti caldi è dedicata la XII edizione dell'evento rivolto ai security manager del retail.

GLI EVENTI DI SECURINDEX

calendario autunno 2026



SANITÀ E SICUREZZA PRIVATA 2026
giovedì 12 novembre

Concepita per promuovere l'incontro tra il sistema sanitario e la filiera della sicurezza privata, la seconda edizione di SSP entra più direttamente nel merito dell'applicazione in ambito sanitario di soluzioni e tecnologie sviluppate in ambito security. Il convegno è abbinato all'evento annuale di Reliver OdV, quest'anno con un concerto musicale.



**APR 2026 - IL SISTEMA PORTUALE E
AEROPORTUALE DELLA PUGLIA**
mercoledì 18 novembre

I sistemi di trasporto marittimo e ferroviario devono affrontare due sfide formidabili: la competizione a livello globale e la sicurezza delle persone, delle merci, dei mezzi e delle infrastrutture. Oggi è possibile migliorare l'efficienza operativa e aumentare la sicurezza? Sono pronti i gestori all'impiego delle nuove tecnologie?

Sommario

- 05 Compliance, perché interessa alle Procure della Repubblica
- 06 Dalla bussola all'uscita di emergenza: le porte di sicurezza certificate di CoMETA
- 08 Studio di settore GENETEC su sicurezza fisica e cloud: le aziende scelgono l'ibrido per non rischiare il blackout operativo
- 12 Dalla supervisione alla governance: Cubesuite per la sicurezza integrata degli edifici
- 14 Urmet Ate: tecnologia e visione al servizio della vigilanza professionale
- 16 Camere corazzate: principi di classificazione, prove e interpretazioni della UNI EN 1143-1
- 18 Vigilanza come ti vorrei. La parola al sindacato – Silvia Avanzini (EBIVER)
- 20 Guerra al caporalato, arriva la blockchain per certificare le retribuzioni

Compliance, perché interessa alle Procure della Repubblica

intervista a Ciro Santoriello, Procuratore aggiunto della Procura di Cuneo

Negli ultimi anni diverse Procure della Repubblica sono dovute intervenire più volte per contrastare fenomeni di sfruttamento e di caporalato nelle filiere dei subappalti, in particolare nei servizi, imponendo l'allineamento delle retribuzioni dei lavoratori dei subappaltatori ai criteri minimi indicati dalla Costituzione. Ritiene che queste forme di patologia del mercato del lavoro siano ancora diffuse nel sistema italiano?

Sicuramente, nonostante il meritorio intervento di magistratura e forze dell'ordine, il problema dello sfruttamento dei lavoratori è ancora assai diffuso.

Occorre tuttavia prendere atto di una significativa modifica rispetto al passato. Intendo riferirmi alla circostanza che, probabilmente, oggi il fenomeno in discorso è confinato ad un settore imprenditoriale maggiormente limitato e rappresentato da aziende marginali, che fanno dell'abbattimento dei costi l'unica chiave di accesso al mercato. In sostanza, penso di poter sostenere che le aziende maggiormente strutturate e significative - per fatturato, rilevanza massmediatica, ecc., - sono decisamente più attente a questi aspetti.

Ad ogni intervento, ai Procuratori è stata mossa l'accusa di invadere la sfera della contrattazione collettiva arrogandosi il ruolo demandato alle parti sociali. Qual è la Sua opinione in merito?

Mi pare una polemica priva di senso. Intanto, l'intervento non è certo diretto a modificare i contenuti della contrattazione collettiva, ma proprio a farli rispettare. Sono sanzionate proprio quelle imprese che, direttamente o all'interno della loro filiera, non si preoccupano (quando non agiscono intenzionalmente in tal senso) di rispettare gli standard minimi che le imprese stesse hanno fissato.

In secondo luogo, è appena ovvio che la magistratura, specie quella penale, è inevitabilmente destinata a rivestire (anche) un ruolo interventista, quando non di supplenza, laddove i diritti subiscano (sul luogo di lavoro, ma anche in famiglia o nella scuola, ecc.) inaccettabili forme di compromissione e violazione.

Quali misure devono adottare i responsabili delle organizzazioni per poter dimostrare la propria estraneità agli illeciti eventualmente commessi dai propri fornitori?



Ecco, questo semmai è il vero profilo su cui riflettere ed in ordine al quale anche la magistratura deve soffermarsi.

Ovviamente, occorre evitare di pensare all'impresa come una sorta di guardiano, di garante di quanto accade (non al proprio interno, il che sarebbe ovvio) ma presso terzi soggetti di cui l'impresa si serve per le proprie forniture o per lo svolgimento della propria attività. Bisogna dunque trovare un giusto equilibrio fra forme di compliance attente anche a quanto accade presso i propri fornitori e il rischio di ingessare l'attività imprenditoriale trasformando le grandi aziende in sorveglianti, sostituti delle forme di controllo pubblico.

Occorre tuttavia fare una precisazione. Le vicende in cui la magistratura è intervenuta si caratterizzavano per la gravità delle violazioni riscontrate e le enormità delle inosservanze riscontrate nella azienda capofiliera. In sostanza, la domanda solleva un problema fondato e su cui riflettere, ma ancora non attuale

Ritiene possano aiutare il sistema proposte formative rivolte ai manager?

Si senz'altro. Specie con riferimento alle seconde linee

Oltre agli illeciti riguardanti la gestione delle risorse umane, quali sono le forme d'infrazione o di reato che avvengono più frequentemente tra quelli che possono pregiudicare la compliance delle aziende?

Le violazioni tributarie. Senz'altro.

Dalla bussola all'uscita di emergenza: le porte di sicurezza certificate di CoMETA

comunicato aziendale

Per lungo tempo la porta è stata considerata semplicemente il punto di ingresso di un edificio. Oggi è molto di più: rappresenta il primo livello di protezione, il luogo in cui controllo degli accessi, sicurezza fisica, continuità operativa ed esperienza dell'utente si incontrano. E, a differenza di quanto si potrebbe pensare, non è affatto un elemento passivo. È un cambiamento che interessa banche, data center, sedi istituzionali, infrastrutture critiche, aeroporti, industrie e tutti quei contesti nei quali la protezione degli ambienti non può più limitarsi alla videosorveglianza o ai sistemi elettronici di identificazione. Perché se il varco fisico non è adeguatamente protetto, anche il più sofisticato sistema di controllo perde parte della propria efficacia: un accesso debole vanifica qualsiasi strategia costruita a monte.

In questo scenario **CoMETA**, azienda del **Gruppo FAAC Technologies** specializzata nelle soluzioni per la sicurezza degli accessi, propone una gamma completa di sistemi certificati secondo la norma UNI EN 1627, con prodotti che raggiungono i livelli di resistenza **RC3** e **RC4**, progettati per rispondere alle esigenze di differenti applicazioni mantenendo un comune denominatore: elevata resistenza all'effrazione, affidabilità e integrazione architettonica.

Bussole di sicurezza: il primo livello di controllo degli accessi

Le **bussole di sicurezza CT484** e **CT496**, entrambe disponibili in configurazione RC4, rappresentano il primo presidio di un edificio ad alta sicurezza. Pur condividendo la stessa filosofia progettuale, interpretano il controllo degli accessi in modo differente.



La **CT484**, caratterizzata dalla base quadrata, nasce per ambienti come istituti bancari, ministeri, industrie e aeroporti. La struttura può essere realizzata sia monoblocco sia smontabile, per facilitare trasporto e installazione anche in situazioni logistiche complesse. Il sistema a porte interbloccate, associato ai dispositivi di unicità di passaggio, pesatura, anti-ostaggio e controllo degli oggetti trasportati, permette di gestire il transito mantenendo elevati standard di sicurezza. Nella versione certificata RC4, disponibile su richiesta, la bussola offre una significativa protezione contro i tentativi di effrazione senza rinunciare alla possibilità di integrare sistemi biometrici, lettori badge e altre tecnologie di controllo accessi.

La **CT496** adotta invece una geometria circolare che privilegia trasparenza, eleganza e fluidità del passaggio. La struttura ampiamente vetrata, disponibile anche smontata per il montaggio direttamente in cantiere, è pensata per edifici direzionali, sedi corporate e contesti rappresentativi dove la sicurezza deve convivere con l'estetica senza fare rumore. Anche in questo caso la versione RC4, disponibile su richiesta, abbina resistenza antieffrazione, gestione intelligente del transito, batterie di backup, diagnostica elettronica e predisposizione per sistemi di identificazione avanzati, mantenendo un'elevata capacità di passaggio.

Porte girevoli e portali di sicurezza: protezione e gestione dei flussi

Quando il controllo degli accessi richiede di gestire flussi elevati senza compromettere la protezione, entrano in gioco le **porte girevoli di sicurezza**.



La **Revolving Door Co146.230** interpreta la tradizionale porta girevole in una chiave completamente diversa: non si limita a regolamentare gli ingressi, ma diventa un vero elemento di sicurezza fisica capace di integrare controllo accessi, resistenza antieffrazione e gestione continua dei flussi di persone. Nelle varianti certificate RC4, la Co146.230 diventa una soluzione particolarmente indicata per sedi direzionali, istituzioni finanziarie e infrastrutture nelle quali comfort d'ingresso e protezione devono procedere di pari passo, senza che l'una comprometta l'altra.

Diverso, ma complementare, è il ruolo del **portale rototraslante Co158**, certificato RC3. La particolare movimentazione delle ante, impernata su uno spostamento del cardine di rotazione, consente di realizzare ingressi di grandi dimensioni mantenendo una struttura autoportante

moderna e leggera dal punto di vista architettonico, capace anche di reggersi in facciate interamente vetrate. Pensato per edifici rappresentativi e ambienti corporate, il Co158 dimostra come anche un accesso di ampie dimensioni possa raggiungere elevati livelli di protezione senza trasformarsi in una barriera visivamente invasiva. La certificazione RC3 garantisce una resistenza significativa ai tentativi di effrazione, in una soluzione che privilegia anche l'inserimento armonioso nell'architettura dell'edificio — ed è, non da ultimo, conforme come via di fuga.

Porte blindate e uscite di emergenza: sicurezza certificata per le aree più sensibili

La sicurezza di un edificio, tuttavia, non termina all'ingresso.



La **porta blindata Co155**, certificata RC4, rappresenta uno degli elementi più robusti della gamma CoMETA. Realizzata in ferro e acciaio, è dotata di serratura meccanica a 11 punti di chiusura, espandibili a dodici con l'aggiunta di un'elettroserratura, e nasce per proteggere locali sensibili, caveau, aree riservate e ambienti nei quali la resistenza all'effrazione costituisce un requisito imprescindibile. L'elevato livello di protezione si accompagna a una progettazione che facilita l'integrazione con i sistemi di sicurezza dell'edificio.



Anche le vie di fuga possono diventare parte integrante della strategia di sicurezza, e non un punto debole da tollerare per obbligo normativo. L'**uscita di emergenza Co156**, anch'essa certificata RC4, dimostra come non sia più necessario scegliere tra protezione e conformità: la porta è progettata per garantire la funzione di esodo prevista dalle normative, offrendo allo stesso tempo un'elevata resistenza ai tentativi di intrusione. Nelle versioni dedicate integra inoltre caratteristiche antiproiettile e vetri certificati, risultando particolarmente adatta per edifici pubblici, infrastrutture critiche e siti ad alta sensibilità.

L'approccio CoMETA non si limita a proporre singole porte di sicurezza, ma un ecosistema integrato di soluzioni certificate. Bussole, porte girevoli, portali, porte blindate e uscite di emergenza non sono elementi indipendenti, ma tasselli di un percorso di accesso progettato per garantire una protezione coerente lungo tutto il ciclo di ingresso, permanenza ed evacuazione.

FAAC

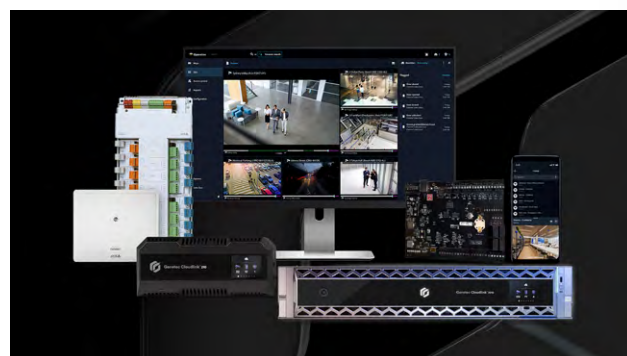
Contatti:
FAAC
www.faac.it

Studio di settore GENETEC su sicurezza fisica e cloud: le aziende scelgono l'ibrido per non rischiare il blackout operativo

di Giovanni Taccori, SaaS Commercial Lead di Genetec

Nel percorso della trasformazione digitale, la **transizione verso il cloud** viene spesso descritta come lineare e priva di ostacoli, un'evoluzione inevitabile. Tuttavia, quando si tratta della sicurezza fisica – dove la protezione si misura in telecamere, varchi di accesso e continuità dei processi operativi degli impianti di produzione – il panorama reale delle aziende italiane si rivela decisamente più sfaccettato e prudente. A fotografare questa complessa transizione è lo [studio di settore condotto da Genetec](#) che mette in evidenza un cambio di approccio fondamentale: l'adozione del cloud non è una semplice questione di preferenza tecnologica, ma una rigorosa scelta strategica di gestione del rischio.

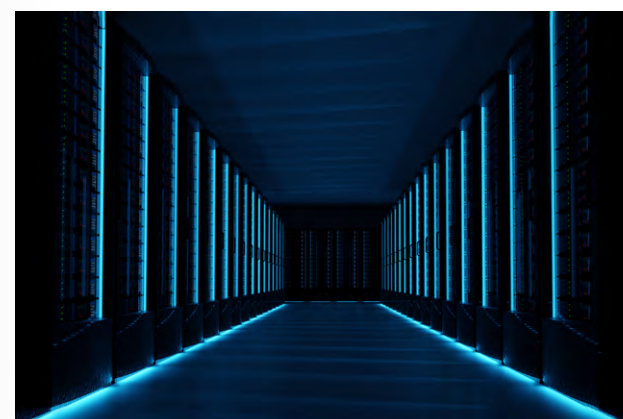
Per il tessuto delle imprese italiane, storicamente caratterizzato da una rete di piccole e medie aziende, da realtà industriali radicate sul territorio e anche multinazionali, i modelli di digitalizzazione pensati oltreoceano possono mostrare dei limiti. Un'azienda quando deve proteggere i propri asset, non cerca una rivoluzione, ma un'evoluzione sostenibile. Le dimensioni e la distribuzione geografica cambiano radicalmente le priorità: gestire più sedi, magazzini o filiali significa dover fare i conti con cicli di vita tecnologici lunghi, normative locali stringenti e la necessità assoluta di non interrompere mai le attività commerciali o produttive. I dati emersi dall'inchiesta Genetec scardinano il concetto della migrazione totale e immediata verso il cloud. Infatti, il 63,9% delle organizzazioni analizzate dallo studio dichiara di mantenere tuttora un sistema di controllo accessi esclusivamente on-premise, ovvero su server fisici in locale. Questo dato non deve essere interpretato come un segnale di arretratezza culturale o di diffidenza verso l'innovazione, bensì come il risultato di una precisa strategia di preservazione degli investimenti esistenti e di controllo diretto. A conferma di ciò,



solo il 18,7% delle realtà intervistate esprime l'intenzione di sostituire integralmente la propria infrastruttura locale con una soluzione completamente cloud.

Di fatto, la vera tendenza che sta ridisegnando la sicurezza delle aziende più strutturate è la via dell'ibrido: ben il **42,5% prevede per i prossimi cinque anni un modello misto, capace di far dialogare l'affidabilità dell'hardware on-prem con la flessibilità e la centralizzazione offerte dal cloud**. Come evidenziato direttamente dalle testimonianze raccolte sul campo da Genetec, «la decisione di adottare il cloud per le applicazioni di sicurezza fisica nasce dalla necessità di scalabilità e flessibilità, per poter ampliare le risorse senza investimenti significativi in infrastrutture on-premise». Per le aziende italiane, il cloud non serve a cancellare il passato, ma a crescere in modo sostenibile, aggiungendo per esempio telecamere o controlli biometrici dove e quando serve.

Questa transizione è accelerata da un fenomeno ormai irreversibile: **la convergenza tra la sicurezza fisica e i dipartimenti IT**. I tempi in cui la gestione dei sistemi di sorveglianza e quella della infrastruttura informatica viaggiavano su binari paralleli e in modalità silos sono tramontati. Oggi, il **42,4% delle decisioni d'acquisto**



legate alla sicurezza fisica vede il coinvolgimento diretto dei professionisti IT. Questa sinergia strategica è dettata da un panorama delle minacce sempre più aggressivo e interconnesso. Nell'ultimo anno, il 41,7% delle aziende ha registrato un netto incremento degli incidenti sia fisici che informatici, con una pressione fortissima sul fronte del social engineering: gli attacchi di phishing e smishing hanno infatti segnato una crescita del 58,7%.

Per un'azienda strutturata, dunque, la scelta di una piattaforma di sicurezza diventa anche una priorità di cybersecurity. Mentre le realtà molto piccole tendono a subire maggiormente l'hacking diretto dei dispositivi hardware per accedere alla rete, le realtà più organizzate devono proteggere filiere complesse e blindare i propri sistemi da accessi non autorizzati. In questo scenario, le garanzie fornite dai fornitori tecnologici giocano un ruolo decisivo: l'adozione di soluzioni conformi a rigorosi standard internazionali di protezione dei dati, come il **RGPD (GDPR)** europeo, e certificate secondo gli standard **ISO 27001:2022** (per la gestione dei rischi cyber) e **ISO 27017** (specifico per la sicurezza del cloud), non è più un optional. Sottoporre le piattaforme ad audit indipendenti come il **SOC2 Type 2** assicura alle imprese la necessaria coerenza ed efficacia nei controlli di sicurezza, rafforzando quella fiducia a lungo termine che i dipartimenti IT oggi esigono.



Da notare che per le aziende più strutturate, la spinta verso l'ibrido è favorita da due fattori decisionali speculari: la scalabilità (pari al 39,3%) e la ridondanza (38,1%) che rappresenta la vera soluzione per garantire che, anche in caso di blackout della rete esterna o di un attacco cyber, le telecamere continuino a registrare e i varchi aziendali rimangano presidiati in totale autonomia.

Una conferma della maturità di approccio arriva anche dall'uso trasversale dei dati all'interno della propria organizzazione: il 37,4% delle aziende intervistate utilizza oggi le informazioni provenienti dai sistemi di sicurezza al di fuori del perimetro della vigilanza, condividendole con altri reparti per ottimizzare l'efficienza dei processi produttivi, della logistica o della gestione degli spazi. Inoltre, il 26,5% adotta già piattaforme unificate che integrano nativamente videosorveglianza e controllo accessi, mentre il 19,5% condivide i metadati delle analisi video con gli altri sistemi di gestione aziendale.

Giovanni Taccori, SaaS Commercial Lead di Genetec, commenta: *“La sicurezza fisica sta insomma vivendo una profonda evoluzione, trasformandosi da centro di costo a fonte di ‘business intelligence’ e resilienza per l'intera organizzazione. La posizione che emerge dai dati del rapporto Genetec è chiara: la modernizzazione non richiede salti nel buio né l'abbandono acritico delle proprie infrastrutture”*.

Genetec

Contatto:
Genetec
www.genetec.com/it

Dalla supervisione alla governance: Cubesuite per la sicurezza integrata degli edifici

comunicato aziendale

La sicurezza fisica sta vivendo una trasformazione profonda. Per anni il mercato ha ragionato per sottosistemi: antintrusione, videosorveglianza, controllo accessi, rivelazione incendio, interfonie e automazioni. Ogni impianto aveva la propria logica, il proprio software e spesso una gestione separata. Questo modello ha funzionato quando gli edifici erano meno connessi, i rischi più prevedibili e il presidio operativo affidato soprattutto alla presenza fisica.

Oggi lo scenario è cambiato. Le aziende gestiscono sedi distribuite, stabilimenti, magazzini logistici, immobili direzionali, punti vendita e aree ad accesso controllato. La security deve dialogare con safety, IT, manutenzione, compliance e facility management. Allo stesso tempo cresce il numero di eventi generati dai sistemi: allarmi, anomalie, stati porta, flussi video, transiti, guasti, esclusioni, interventi manutentivi e report. Il problema non è più raccogliere dati, ma trasformarli in decisioni operative coerenti.

È in questo contesto che nasce il valore di Cubesuite, sviluppata da Life3 per integrare e governare i sistemi di sicurezza fisica, fire safety e automazione degli edifici. Cubesuite non si propone come un ulteriore software isolato, ma come un ambiente modulare capace di mettere in relazione impianti, informazioni, operatori, procedure e obblighi di gestione. L'obiettivo è rendere la sicurezza più leggibile, controllabile, documentabile e misurabile.

L'estensione della piattaforma è Cube Protection Central, modulo dedicato alla supervisione e centralizzazione degli eventi di security. In una control room o in un centro di monitoraggio remoto, la differenza non la fa soltanto la quantità di sistemi collegati, ma la capacità di presentare all'operatore l'informazione corretta nel momento corretto.

Un allarme intrusione, ad esempio, non dovrebbe rimanere un semplice codice proveniente da una centrale: dovrebbe essere collegato alla planimetria, alle telecamere dell'area, allo stato dei varchi, alle procedure previste, alla lista dei referenti e alla tracciabilità delle azioni eseguite.

Cube Protection Central raccoglie gli eventi dai sistemi connessi, li normalizza, li rappresenta su mappe grafiche e dashboard operative e permette di gestirli secondo flussi definiti. L'operatore non deve saltare da un'applicazione all'altra per capire cosa sta accadendo, ma può seguire una sequenza guidata: identificazione dell'evento, verifica visiva, consultazione delle informazioni correlate, presa in carico, escalation, chiusura e rendicontazione.

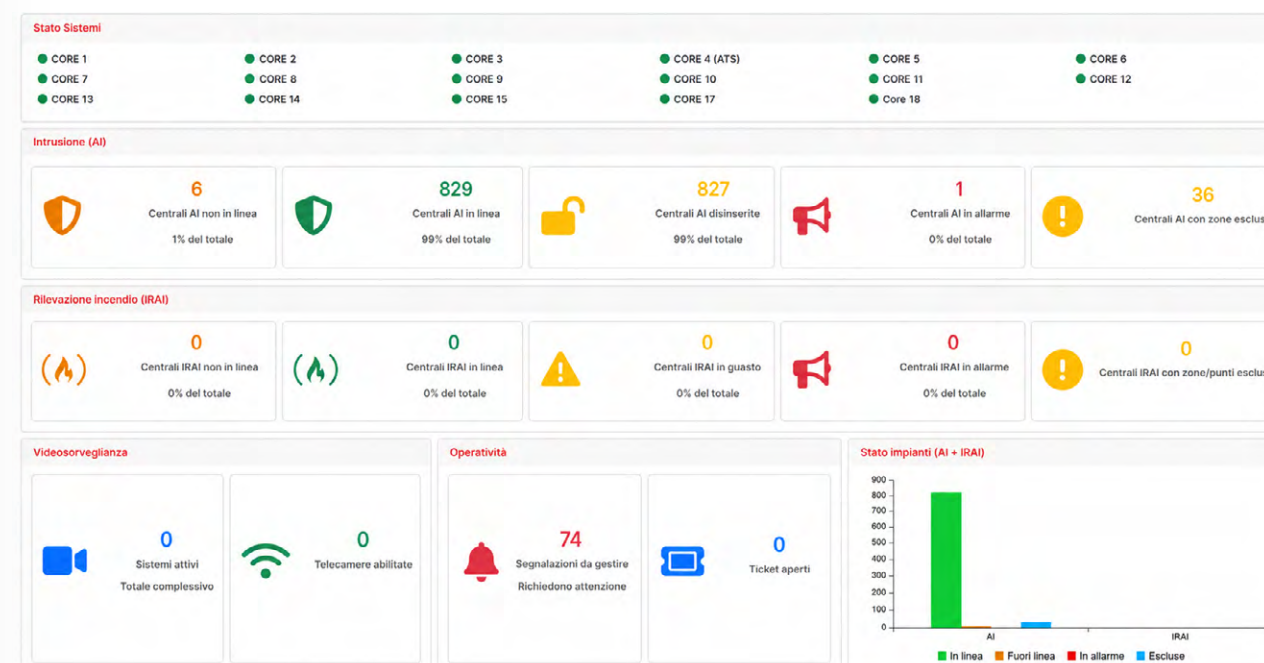
Questo approccio è decisivo negli ambienti complessi, dove il rischio non nasce da un singolo impianto ma dall'interazione tra più condizioni. Un varco forzato in orario di apertura ha un significato; lo stesso evento in orario notturno, in un'area ad alto valore o con telecamera oscurata, ne assume un altro. La piattaforma consente di contestualizzare l'evento e ridurre il margine di interpretazione soggettiva.

La stessa logica viene estesa alla rivelazione incendio attraverso Cube Fire, il modulo di Cubesuite dedicato all'integrazione delle centrali IRAI e alla gestione operativa degli impianti di rivelazione automatica e manuale incendio. Le centrali possono essere monitorate in termini di stato, allarmi, guasti, esclusioni, anomalie e disponibilità del sistema, offrendo una visione centralizzata anche su siti distribuiti.

L'integrazione degli impianti IRAI assume particolare valore quando viene collegata alla gestione delle manutenzioni.

Cube Fire: dal monitoraggio alla prevenzione

Dove disponibile, Cube Fire può monitorare i valori analogici dei rivelatori e generare avvisi al superamento di soglie di attenzione. Il dato tecnico diventa così un indicatore predittivo per orientare manutenzioni, ridurre falsi allarmi e prevenire indisponibilità del sistema.



Dashboard operativa Cubesuite: supervisione integrata di impianti antintrusione, IRAI, videosorveglianza e attività operative

Cubesuite consente di strutturare le attività manutentive secondo le logiche previste dalla UNI 11224, supportando la pianificazione dei controlli, la registrazione degli esiti, la gestione delle anomalie, la tracciabilità degli interventi e la produzione della documentazione utile al presidio tecnico e normativo. In questo modo la piattaforma non si limita a segnalare lo stato dell'impianto, ma accompagna l'intero ciclo di gestione: supervisione, manutenzione, verifica, chiusura delle non conformità e rendicontazione.

Per le organizzazioni multi-sito, questo passaggio è particolarmente importante. Una catena retail, un gruppo industriale, una rete logistica o un patrimonio immobiliare distribuito devono poter sapere quali impianti sono in servizio, quali presentano guasti, quali hanno zone escluse, quali manutenzioni sono state eseguite e quali attività richiedono attenzione. La dashboard operativa di Cubesuite consente di aggregare queste informazioni e trasformarle in indicatori immediatamente leggibili.

La modularità della piattaforma estende la supervisione oltre la gestione degli allarmi. Cubesuite può integrare controllo accessi, videosorveglianza, antintrusione, rivelazione incendio, sensoristica, automazioni e gestione tecnica. L'edificio diventa un ecosistema connesso, nel quale ogni informazione contribuisce alla valutazione del rischio, alla continuità operativa e alla conformità dei processi.

Un aspetto centrale è la tracciabilità. In molti contesti corporate, logistici, industriali e terziari non basta sapere che un evento è stato gestito: occorre dimostrare come, quando, da chi e con quali esiti. La registrazione delle attività consente di produrre report, analizzare ricorrenze, individuare criticità impiantistiche o organizzative e supportare audit interni. La sicurezza diventa così un processo misurabile, non solo una funzione reattiva.

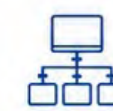
Questo vale ancora di più per gli impianti antincendio, dove la manutenzione non è solo un'esigenza tecnica,

Un'unica suite. Più controllo, meno complessità.

La piattaforma modulare Life3 per governare edifici, impianti, sicurezza, accessi ed energia.



Modulare
Attiva solo
i moduli necessari.



Centralizzata
Un unico ambiente
per dati, eventi e attività.



Tracciabile
Ogni attività è
verificabile nel tempo.



Integrabile
Sistemi e processi
dialogano tra loro.

I MODULI



Scopri la configurazione più adatta al tuo progetto
Richiedi una demo su life3.it/cubesuite/



Cubesuite e IoT: integrazione aperta tramite MQTT

Attraverso il protocollo MQTT, Cubesuite può dialogare con dispositivi, sensori, gateway e piattaforme esterne. La piattaforma diventa un nodo software dell'ecosistema IoT, connettendo security, safety, building automation e dati di campo in una logica scalabile.

ma un elemento essenziale della gestione del rischio. La possibilità di associare eventi, guasti, esclusioni, ticket, verifiche e manutenzioni consente di avere una visione integrata tra stato dell'impianto e azioni correttive. Il dato non rimane confinato alla centrale o al rapporto cartaceo, ma diventa parte di un sistema informativo condiviso.

La convergenza tra sicurezza fisica, safety e cybersecurity impone inoltre attenzione alla governance delle integrazioni: gestione degli accessi, ruoli, credenziali, continuità del servizio, logging e controllo delle interfacce. Una piattaforma moderna deve quindi integrare in modo controllato e documentabile.

Cubesuite, Cube Protection Central e Cube Fire si collocano in questa prospettiva: non come semplice supervisione grafica, ma come infrastruttura software per la governance integrata della sicurezza fisica e della fire safety. Per Life3, software & automation significa portare nella gestione degli edifici un livello superiore di controllo, integrazione e consapevolezza operativa. Perché proteggere un edificio non vuol dire solo rilevare un evento, ma comprenderlo, gestirlo, documentarlo, mantenerlo correttamente e imparare da ciò che accade.



Perché Cubesuite

- ✓ Supervisione centralizzata multi-sito
- ✓ Integrazione antintrusione, IRAI e videosorveglianza
- ✓ Cube Fire per centrali IRAI e manutenzioni
- ✓ Controllo accessi di persone e veicoli



Cube Fire e UNI 11224

Cube Fire integra le centrali IRAI e supporta la gestione manutentiva in conformità alla UNI 11224. Permette la pianificazione dei controlli, la registrazione degli esiti, la gestione delle anomalie, la tracciabilità degli interventi e la generazione dei report per una compliance completa e documentabile.



Urmet Ate: tecnologia e visione al servizio della vigilanza professionale

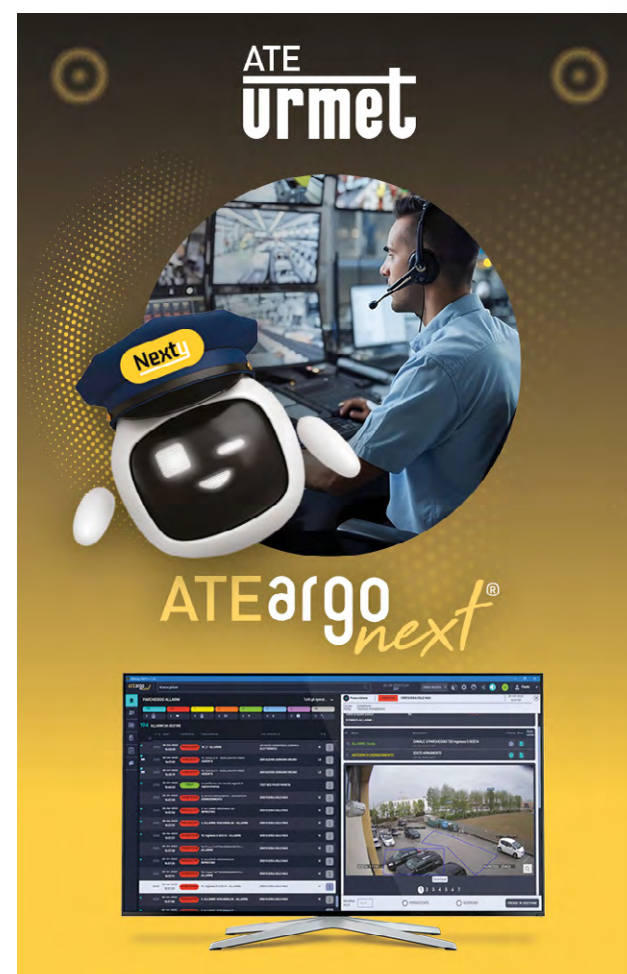
comunicato aziendale

Da oltre trent'anni sul mercato della sicurezza, Urmet ATE si è creata un ruolo di riferimento per gli istituti di vigilanza e per il telesoccorso italiano. Fondata nel 1991 ed entrata a far parte del Gruppo Urmet nel 2003, l'azienda vicentina continua a rinnovarsi e ad offrire ai clienti e al mercato soluzioni innovative e tecnologicamente avanzate per rispondere alle esigenze del settore, come l'ecosistema **ATEARGO NEXT**, che è il cuore pulsante nella gestione eventi, o la novità presentata all'ultima edizione di Fiera Sicurezza 2025, Nexty, il primo assistente virtuale pensato per le centrali operative. Urmet Ate è una realtà caratterizzata da innovazione, attenzione al servizio, un forte impegno verso la qualità e un'aderenza alla realtà, fondamentale per interpretare la complessità del mercato. Questi principi guidano tutti i giorni ogni azione e decisione, permettendo di offrire soluzioni che non solo soddisfano le aspettative dei clienti, ma spesso le anticipano.

Urmet Ate sviluppa i propri prodotti internamente e questa offerta "made in Italy" è garanzia di attenzione verso le reali esigenze di mercato. Ma non è solo questo. Dal 2025 l'azienda ha acquisito la certificazione ISO/IEC 27001, che non è "bollino" da apporre, ma un vero cambiamento culturale e strutturale interno volto a gestire, proteggere e valorizzare le informazioni. La certificazione è legata ad una nuova consapevolezza sulla cybersecurity, che genera anche maggiore fiducia e diventa una leva competitiva e distintiva importante, permettendo all'azienda di integrarsi con clienti che applicano controlli di sicurezza avanzati. Urmet Ate è anche telesoccorso: l'offerta aziendale, ad oggi sviluppata in ambito BtoB, è perfettamente in linea con lo spirito innovativo e la mission in sicurezza e protezione, con un'attenzione all'evoluzione della nostra società.

ATEARGO Next: la differenza di un system integrator efficiente

Al centro dell'offerta per gli Istituti di Vigilanza c'è l'Ecosistema ATEARGO NEXT, il gestionale eventi certificato EN50518 per le centrali operative. È una piattaforma aperta



e componibile, flessibile e integrata, capace di gestire centinaia di protocolli diversi - video, antintrusione, antincendio - attraverso un'unica interfaccia, dialogando anche con dispositivi di altri produttori o con automatismi correlati ad altri software (come, ad esempio, il gestionale pattuglie).

L'ecosistema si sviluppa su più livelli. I servizi di centrale, con Contact EVO per la telefonia integrata e l'app Vigilante; le soluzioni di campo, come Unify video e alarm Next, o Fire Next, che permettono di ottimizzare il lavoro e semplificare i processi. Completano l'ecosistema One Click, la nuova

funzionalità dei moduli multiprotocollo che permette in un solo gesto di ricevere il segnale di allarme, visualizzare l'evento e prendere una decisione, e un servizio di assistenza attivo tutti i giorni, ventiquattro ore su ventiquattro, sia da remoto sia on site. I numeri restituiscono la dimensione del progetto: oltre 110 centrali operative lo utilizzano oggi, per una media di 50.000 eventi gestiti al giorno per centrale, su un parco di oltre 350.000 periferiche installate sul campo. Accanto al gestionale, Urmet ATE porta avanti una gamma di prodotti hardware pensati per lavorare in modo nativo con ATEARGO NEXT, così da garantire agli Istituti di Vigilanza tutte le funzionalità operative disponibili.

Per l'antincendio, **Fire 4G PRO** è la soluzione certificata EN54-21 sviluppata interamente da Urmet ATE per il monitoraggio degli impianti: una risposta proprietaria pensata per coprire le esigenze normative e operative del comparto.

Sul fronte delle periferiche di teleallarme, **Webu 4g Next** resta tra i prodotti più conosciuti dell'azienda. L'ultima versione estende la connettività al 4G con fallback automatico su 3G e 2G - una scelta che garantisce continuità anche quando le infrastrutture di rete cambiano - ed è disponibile anche con opzione WiFi.

Nexty, l'assistente per le centrali operative

La novità più rilevante degli ultimi mesi si chiama **Nexty**: l'assistente virtuale basato su intelligenza artificiale, accolto con grande interesse dal settore, per cui è possibile prenotare una demo per provare tutte le funzionalità.

Nexty è pensato per affiancare gli operatori delle centrali operative, non per sostituirli. Si integra con i sistemi già in uso dal cliente e si adatta ai suoi flussi di lavoro,

occupandosi in autonomia delle richieste più semplici e ricorrenti - segnalazioni standard, informazioni operative, richieste di routine. In questo modo libera tempo per le attività che richiedono davvero competenza ed esperienza. L'obiettivo non è quello di eliminare il lavoro delle persone, ma alleggerirle dai compiti ripetitivi, lasciando agli operatori la gestione delle situazioni più delicate.

Durante la gestione degli eventi in tempo reale, Nexty aiuta a filtrare le informazioni, organizzare i flussi di lavoro e suggerire le azioni più adatte, con ricadute dirette su tempi di risposta, precisione e carico di lavoro degli operatori. La sua configurazione viene personalizzata caso per caso, monitorata nel tempo e aggiornata, per un utilizzo sicuro e affidabile.

Per Urmet ATE, Nexty rappresenta prima di tutto una scelta di equilibrio: l'intelligenza artificiale si occupa di continuità, velocità e volumi di lavoro, mentre agli operatori restano l'empatia, il giudizio e l'esperienza necessari nei momenti più delicati del rapporto con il cliente finale.

Un equilibrio che, secondo l'azienda, è destinato a diventare centrale anche per gli altri operatori del settore, a mano a mano che i volumi di eventi gestiti dalle centrali operative continueranno a crescere. Un percorso che, in fondo, racconta bene l'intera storia dell'azienda vicentina: fatta di tecnologia sviluppata guardando sempre al lavoro quotidiano di chi la usa.

Urmet Ate sarà presente alla fiera MIBA Levante a Bari a novembre a testimoniare la costante ricerca e presenza diretta dell'azienda, per cui tecnologia, innovazione, attenzione umana e personalizzazione del servizio sono drive irrinunciabili del lavoro.

ATE
urmet

Contatto:
Urmet ATE
www.urmet-ate.it
info@urmet-ate.it
Tel. 0444 268211

Camere corazzate: principi di classificazione, prove e interpretazioni della UNI EN 1143-1

di Marco Albanese, Association Manager ANIMA SICUREZZA - federata ANIMA Confindustria

Le camere corazzate rappresentano una delle più elevate espressioni della protezione fisica passiva applicata alla tutela di valori, beni sensibili e informazioni riservate. Utilizzate in ambito bancario, industriale, commerciale e istituzionale, queste strutture sono progettate per garantire livelli di sicurezza estremamente elevati contro i tentativi di effrazione, assicurando la protezione del contenuto anche in presenza di attacchi particolarmente aggressivi e prolungati.

La loro natura architettonica è particolarmente complessa e diversificata. Esse possono essere realizzate mediante getto in opera di calcestruzzo speciale, attraverso l'assemblaggio di pannelli prefabbricati oppure mediante una combinazione di entrambe le tecnologie costruttive. Ogni soluzione presenta specifiche caratteristiche tecniche, vantaggi applicativi e differenti modalità di installazione, rendendo il settore delle camere corazzate estremamente articolato dal punto di vista progettuale e realizzativo.

Proprio in ragione di questa eterogeneità costruttiva, è fondamentale garantire che la realizzazione avvenga nel pieno rispetto dei requisiti previsti dalla normativa tecnica di riferimento. La sola analisi progettuale, infatti, non è sufficiente a dimostrare l'effettiva capacità di una struttura di opporsi a un attacco reale. Materiali, tecnologie costruttive, sistemi di giunzione e dettagli esecutivi possono influenzare in maniera significativa il comportamento della struttura sotto attacco, rendendo indispensabile una verifica sperimentale delle prestazioni.

Considerata la complessità progettuale di tali opere e la rilevanza delle funzioni di sicurezza che esse sono chiamate a svolgere, risulta pertanto necessario verificare l'efficacia della protezione finale mediante prove oggettive aventi l'obiettivo di valutare la resistenza agli attacchi fisici. Questi test devono essere eseguiti esclusivamente da laboratori accreditati su campioni reali rappresentativi della struttura da certificare. Le verifiche sperimentali costituiscono infatti il presupposto essenziale per il rilascio di certificazioni affidabili, poiché consentono di valutare direttamente le prestazioni del manufatto e di determinarne il



livello di resistenza effettivo, superando i limiti delle valutazioni basate esclusivamente su modelli teorici o considerazioni progettuali.

In un settore caratterizzato da requisiti di sicurezza sempre più elevati e da minacce in continua evoluzione, la definizione di criteri oggettivi e condivisi per la valutazione delle prestazioni ha quindi un'importanza fondamentale. La capacità di una struttura di resistere a un tentativo di effrazione non può essere affidata a valutazioni soggettive o a semplici dichiarazioni del costruttore, ma deve essere dimostrata attraverso procedure di prova rigorose, ripetibili e riconosciute a livello internazionale. In questo contesto, il riferimento normativo principale è rappresentato dalla norma UNI EN 1143-1:2019, che specifica le prove di resistenza all'effrazione e la classificazione di casseforti, sportelli automatici bancari (ATM), porte per camere corazzate e camere corazzate. In particolare, la norma definisce metodologie di prova particolarmente severe, basate su attacchi reali effettuati da laboratori indipendenti mediante l'impiego di utensili e tecniche codificate. Sulla base dei risultati ottenuti viene attribuita una specifica classe di resistenza, che costituisce un parametro oggettivo e riconosciuto a livello internazionale per valutare il grado di protezione offerto dal prodotto.

Di fatto, la classificazione secondo la UNI EN 1143-1 rappresenta oggi uno strumento indispensabile per progettisti, produttori, committenti, utilizzatori finali e compagnie assicurative. Essa consente infatti di confrontare in modo trasparente soluzioni differenti e di individuare il livello di sicurezza più adeguato rispetto al rischio da fronteggiare. L'importanza della norma non si limita tuttavia al solo ambito certificativo, in quanto essa costituisce un vero e proprio riferimento culturale per l'intero settore della sicurezza fisica, promuovendo un approccio fondato sulla misurazione delle prestazioni e sulla verifica concreta dell'efficacia dei sistemi di protezione.

Proprio al fine di favorire una corretta interpretazione dei principi normativi e contrastare letture improprie dei criteri di classificazione, ANIMA SICUREZZA ha recentemente pubblicato un Position Paper dedicato alle camere corazzate. Il documento, disponibile sul sito dell'Associazione (www.animasicurezza.it), richiama alcuni principi fondamentali della UNI EN 1143-1:2019, ribadendo come la classificazione di un mezzo di custodia debba sempre rappresentare un dato oggettivo e verificabile, riferito alla resistenza effettiva dell'intero sistema e non alla semplice sommatoria teorica delle prestazioni attribuite ai singoli componenti.

Secondo l'Associazione dalla puntuale lettura della norma si evince chiaramente che la classificazione complessiva di una camera corazzata composta da più elementi costruttivi non può in alcun caso essere ottenuta attraverso deduzioni teoriche o calcoli ingegneristici che combinino i valori di resistenza delle diverse parti. Un simile approccio risulterebbe infatti in contrasto con i principi stessi della norma, che impone la valutazione sperimentale dell'esatto assieme costruttivo e richiede che il giudizio finale sia basato esclusivamente su prove oggettive. Il Position Paper evidenzia inoltre come, nella valutazione di un sistema composto da pareti e porta corazzata, il livello di classificazione finale debba necessariamente essere determinato dall'elemento caratterizzato dalla minore resistenza certificata. In altre parole, il sistema non può mai conseguire una classe superiore a quella del proprio componente più debole. Ne deriva, per esempio, che l'abbinamento di una porta certificata in Grado VII con pareti certificate in Grado V, non consente in alcun modo di attribuire alla camera corazzata una classificazione superiore al Grado V.

Particolare attenzione viene inoltre posta a una convinzione talvolta diffusa nel mercato, secondo la quale l'inserimento all'interno della camera corazzata di ulteriori mezzi di custodia ad alta sicurezza potrebbe incrementare la classificazione dell'intero sistema. Anche su questo punto il documento di ANIMA SICUREZZA è estremamente chiaro precisando che la presenza di casseforti certificate o di altri mezzi forti collocati all'interno dello spazio protetto non produce alcun effetto sul

grado della camera corazzata.

Al riguardo non è superfluo ricordare che la norma prevede che la valutazione della resistenza sia riferita esclusivamente all'involucro esterno costituito dalle pareti e dalla porta, indipendentemente da ciò che viene successivamente installato al suo interno.

Il documento associativo ribadisce infine il principio fondamentale secondo cui affinché una classificazione possa essere considerata valida e affidabile, le prove devono essere necessariamente eseguite da laboratori accreditati per l'esecuzione dei test previsti dalla UNI EN 1143-1:2019.

Solo l'analisi tecnica della documentazione progettuale, la verifica dei materiali impiegati, il campionamento delle strutture e l'esecuzione delle prove sui punti critici consentono di ottenere quei dati oggettivi sui quali un organismo di certificazione può fondare il rilascio di un certificato credibile e riconosciuto dal mercato.

Attraverso attività di divulgazione tecnica, programmi di formazione specialistica, iniziative di sensibilizzazione e occasioni di confronto tra operatori del settore, ANIMA SICUREZZA promuove la conoscenza delle normative, delle tecnologie disponibili e delle migliori pratiche applicabili alla sicurezza fisica.

L'obiettivo è favorire una maggiore consapevolezza sull'importanza di adottare soluzioni certificate e correttamente dimensionate rispetto alle specifiche esigenze di protezione. Solo attraverso una corretta analisi del rischio e una piena comprensione delle caratteristiche dei sistemi disponibili è infatti possibile sviluppare strategie di difesa realmente efficaci, contribuendo all'innalzamento degli standard di sicurezza e alla diffusione di una cultura della prevenzione basata su competenza, responsabilità e qualità verificata.

Un contributo significativo che si aggiunge al documento "Linee guida per la prevenzione del rischio furto" (edizione 2024), frutto della proficua collaborazione tra ANIMA SICUREZZA e ANIA nell'ambito delle attività volte alla definizione e alla diffusione di linee guida destinate agli operatori del settore, alle compagnie assicurative e ai consumatori.

In effetti, l'iniziativa si inserisce in un più ampio percorso finalizzato a promuovere una maggiore consapevolezza sui temi della protezione fisica e della gestione del rischio, favorendo da un lato la diffusione di una solida cultura della sicurezza attraverso la divulgazione di conoscenze tecniche, normative e operative riguardanti le più efficaci misure di prevenzione e contenimento del rischio furto e dall'altro la collaborazione tra associazioni di settore, organismi tecnici e operatori professionali, fattore fondamentale per contribuire all'innalzamento degli standard di sicurezza e alla diffusione di pratiche basate su competenza, trasparenza e qualità certificata.

Vigilanza come ti vorrei. La parola al sindacato – Silvia Avanzini (EBIVER)

intervista a Silvia Avanzini, Presidente EBIVER

Partiamo dalla ricerca che EBIVER ha fatto realizzare sullo stato di salute della V.P. vista da chi ci lavora dentro. Quale fotografia esce?

Volendo dare voce alle lavoratrici e ai lavoratori della vigilanza privata e dei servizi di sicurezza, questo rapporto raccoglie e analizza soggettività e condizioni di lavoro. Il risultato si declina tra la soddisfazione, il suo necessario ma tuttora irrealizzato riconoscimento economico e il senso di utilità sociale. Da rilevare che su quest'ultimo aspetto l'indagine non rileva una contrapposizione tra "senso civico" e "visione securitaria" ma, anzi, le due matrici valoriali sembrano convivere senza negarsi reciprocamente.

Un elemento questo che permette una lettura e un approccio al settore con minor pregiudizio, fuori dai cliché un po' periferici e marginali in cui si è persa anche un po' di novellistica e di produzione cinematografica.

L'aspetto cruciale emerso è il riconoscimento sul lavoro, tanto da far pensare ad una ricostruzione dell'immagine del settore. Chi lavora nel settore ha infatti evidenziato di sentirsi poco riconosciuto sia dalla società evidenziando una bassa rappresentazione sociale del lavoro, sia dall'azienda per cui lavora, intendendosi la dimensione contrattuale e, quindi, il valore attribuito alla professione. Da qui, la fotografia netta prosegue con la principale preoccupazione di non disporre di risorse economiche adeguate per riuscire a vivere dignitosamente e la necessità di una migliore conciliazione dei tempi di vita e dei tempi di lavoro.

Una sintesi solo all'apparenza banale e scontata, dal momento che la ricerca conferma anche che flessibilità e disponibilità risultano la principale richiesta da parte aziendale.

Un altro aspetto importante evidenziato dalla ricerca è il ruolo attribuito alla contrattazione collettiva, sia essa



di primo o secondo livello, come momento di sintesi per evitare la conflittualità tra le parti.

Ritengo che una ricerca così mirata e significativa, condotta su un campione di quasi 600 rispondenti, restituisca risultati non solo da prendere seriamente in considerazione ma confermi e rafforzi il ruolo dell'ente bilaterale.

Uno dei punti dolenti e, appunto, scontati è l'aspetto salariale che vede la categoria in fondo alla scala, pur essendo fortemente sindacalizzata. Cosa è successo?

È una domanda molto diretta e quindi dovrei forse ricordare a tutti noi quanto pesano i mancati rinnovi alle giuste scadenze nelle tasche delle lavoratrici e dei lavoratori.

Il contratto della vigilanza privata e dei servizi fiduciari - oggi servizi di sicurezza - nonostante una notevole ed articolata mobilitazione con manifestazioni molto partecipate, è arrivato al rinnovo dopo oltre 8 anni. Ricordiamo anche il periodo covid, con il mondo sospeso e fermo, che ha visto le donne e gli uomini della sicurezza lavorare senza risparmio fino ad essere da invisibili a essenziali come buona parte dei cosiddetti "lavoratori in appalto", con tutta la retorica utile in quel momento che nulla ha poi prodotto. Si aggiunga infine ai mancati rinnovi la spirale inflattiva 2019-2023 e si ottiene la risposta al perché oggi la categoria

necessiti di relazioni sindacali mature e responsabili da entrambe le parti se davvero si vuole ricostruire l'immagine del settore come chiedono le lavoratrici e i lavoratori.

Il rinnovo del maggio 2023 con l'addendum del febbraio 2024 - oltre a chiudere la parte salariale - definisce anche le norme per avviare la contrattazione del settore in tempi certi, restituendo alla contrattazione collettiva gli elementi di garanzia salariale per tempi e recuperi.

Cosa ha "distratto" il sindacato tanto da dover far intervenire le procure a difendere i diritti dei lavoratori?

Ut supra: il sindacato confederale non si è mai "distratto" dai diritti dei lavoratori ma ha gestito e accompagnato l'intervento delle procure per quello che di necessario era da imporre alle aziende sotto controllo giudiziario. La "distrazione" dai diritti è piuttosto di chi dequalifica lavoratori e imprese in processi che hanno contribuito ad abbassare diritti e tutele alimentando concorrenza sleale e dumping. È bene ricordare che le forme di "sfruttamento" negli appalti (con l'abrogazione della l.1369/60 con d.lgs. 276/2003), con subappalti, distacchi, partita iva, false cooperative e quant'altro, spesso nel silenzio della committenza, sono le più difficili da individuare.

Come si può ridare appeal a questo mestiere, che potrebbe avere un ruolo chiave in una società sempre meno assistita dallo Stato? il sindacato è pronto adesso a recuperare un ruolo guida nel cambiamento?

"Adesso" è un avverbio di tempo errato. Il sindacato di categoria - Filcams, Fisascat e Uiltucs - in un contesto di involuzione legislativa e di moltiplicazione di forme contrattuali precarie, si è distinto "sempre" - il giusto avverbio di tempo - come guida per il contrasto e la riconquista di alcune tutele

tipiche della precedente normativa (aspetti relativi al Codice degli Appalti Pubblici) tra contrattazione d'anticipo, genuinità dell'appalto, ccnl leader e contrasto al dumping contrattuale. Al CNEL sono depositati più di 1000 contratti e al repertorio nazionale sono iscritti enti di sigle non rappresentative. Dal Tribunale di Milano, però, una sentenza innovativa su appalti privati e contratto leader dà ragione al sindacato ricorrente (Filcams CGIL di Milano - 4 dicembre 2025) e condanna per comportamento antisindacale due aziende imponendo la disapplicazione del contratto di altra sigla non confederale e non comparativamente più rappresentativa, guarda caso nella vasta area del lavoro dei servizi di sicurezza in fortissima espansione.

Questo è l'argine che stiamo costruendo quotidianamente, ad esempio nei cambi appalto come nella contrattazione d'anticipo con le stazioni appaltanti.

E poi c'è il fronte del rinnovo contrattuale. La ripresa con l'invio della piattaforma unitaria a novembre e un calendario già definito e avviato con la presenza delle delegazioni non è un semplice rituale ma il rinnovo di un sano protagonismo delle lavoratrici e dei lavoratori.

Come abbiamo detto sopra, la ricerca lo conferma: la contrattazione collettiva è considerata dai lavoratori cruciale per il miglioramento delle condizioni ancor più della rivendicazione conflittuale.

Concludendo, l'attrattività del settore - ci ripetiamo - va di pari passo con il suo riconoscimento che passa attraverso condizioni di lavoro e salariali dignitose perché non prevalga quel cliché marginale e non attuale oltretutto ingiusto e non pertinente per cui si lavora nella vigilanza privata solo come ultima e unica occasione, trascinando verso il basso competenze e professionalità.

Guerra al caporalato, arriva la blockchain per certificare le retribuzioni

intervista a Vito Mastrominico, CEO di TMT Innovation

Da dove parte l'idea di certificare le retribuzioni dei servizi in appalto con la blockchain?

L'idea nasce dal nostro osservatorio di azienda specializzata in cybersicurezza e soluzioni tecnologiche avanzate che segue diverse entità, in particolare nel mondo dei servizi di sicurezza nel Centro-Sud. È un settore complesso, caratterizzato storicamente da una concorrenza sleale fortissima, dove gli operatori "virtuosi" che applicano i contratti di lavoro leader, formano il personale e investono nella legalità, devono combattere una guerra spietata sui prezzi, dove viene usato ogni mezzo per abbassare il costo del lavoro sulla pelle dei lavoratori.

È una situazione limite, fatta anche di turni massacranti registrati "fuori busta" o camuffati sotto voci di rimborso fittizie o non retribuiti affatto; di controlli troppo lenti e rari da parte delle Autorità tutorie, spesso impossibilitate a intervenire per mancanza di personale; del "buio informativo" in cui si trovano i committenti che devono pagare le fatture basandosi su autocertificazioni cartacee che non garantiscono alcun controllo sulle ore realmente prestate sul campo. Committenti che spesso ignorano i rischi ai quali si espongono per la responsabilità solidale nei confronti dei dipendenti degli appaltatori.

Da qui l'idea di impiegare tecnologie avanzate ma ampiamente consolidate come la blockchain per mettere a disposizione di questo comparto (ma non solo) un sistema che permetta di certificare le presenze e la relativa retribuzione.

Quali sono i soggetti più interessati alla vostra idea?

Di fatto, la nostra piattaforma si rivolge a tutte le filiere di servizi nelle tre figure chiave: il fornitore, il committente privato e pubblico, i lavoratori.

I vantaggi si declinano in modo specifico per ciascuno di questi soggetti, creando un vero e proprio ecosistema di fiducia:

1. Fornitori di servizi – lealtà competitiva: si rivolge ai soggetti che scelgono la strada dell'onestà e della legalità



certificata. Il vantaggio principale è di tipo commerciale e competitivo: la piattaforma diventa un bollino di eccellenza e trasparenza in un mercato inquinato dal dumping. Il fornitore può finalmente dimostrare il proprio valore con certezza e trasparenza, disarmando la concorrenza sleale e proporsi ai grandi clienti come partner qualificato e affidabile.

2. Committenti – schermatura legale e reputazionale: si propone principalmente alle aziende che usufruiscono in modo continuativo di servizi acquistati con la formula "ora/uomo" attraverso gare di appalto. La piattaforma offre una vera e propria "schermatura legale" permanente, in quanto il committente disporrà di un accesso indipendente e verificato per il controllo continuo dell'attività espletata dal fornitore.

3. Lavoratori – trasparenza retributiva: non sono coinvolti in modo diretto nel sistema di certificazione tramite piattaforma ma grazie ad essa hanno la garanzia che le ore di servizio siano registrate in modo inalterabile, eliminando le aree grigie che molto spesso si vengono a creare. Questo genera un clima di "pace sindacale" all'interno dell'organizzazione, in quanto i dati inseriti sono oggettivi e incontestabili. Per

questo motivo, la piattaforma può fungere da garante naturale per i sindacati.

Un'azienda potrebbe sottoporre al controllo dell'applicazione solo una parte, ad esempio un singolo appalto il cui committente ha richiesto la certificazione?

La risposta è chiaramente sì, la logica generale di funzionamento della piattaforma lo permette. L'azienda non deve per forza utilizzarla per l'intera organizzazione ma potrebbe farlo anche per una singola commessa che richiede un modello di certificazione più trasparente.

Tuttavia, un utilizzo parziale lascia sempre il dubbio di zone grigie, ad esempio sull'impiego degli stessi lavoratori per svolgere anche altri turni di lavoro, magari non retribuiti in maniera corretta.

E invece con una singola utenza si potrebbero monitorare e certificare più aziende, ad esempio un'associazione oppure una rete d'impresa?

Una caratteristica chiave della piattaforma è proprio l'architettura "multi-tenant", pensata per gestire organizzazioni complesse con più aziende sotto la stessa proprietà o consorzi di imprese indipendenti, con le dovute precisazioni sul tema privacy e segreto industriale.

Se parliamo di un gruppo societario con più aziende o di un consorzio di imprese indipendenti che lavorano per la stessa committente, la condivisione di informazioni segue logiche molto semplici. Nel primo caso, la sola capogruppo avrà visione totale di turni e documenti caricati per i clienti da tutte le sue aziende che, invece, avranno visibilità solo di ciò faranno loro con i propri clienti; nel secondo caso, sarà la committente ad avere visione totale delle informazioni caricate dalle aziende che per essa svolgono i servizi e queste, invece, avranno visione solo del proprio operato. Più complesso il caso di un'associazione di categoria, dove le aziende associate sono autonome e in diretta concorrenza tra loro sul mercato. In questo scenario, la tutela del segreto industriale e della privacy è rispettata se l'associazione si assume l'onere di essere "garante" del caricamento dei dati in piattaforma.

In conclusione, ci può descrivere in sintesi come funziona?

La nostra intuizione risiede nel superare il paradigma basato sul "dover fidarsi", sostituendolo con il "poter verificare" attraverso il valore unico della notarizzazione digitale. L'idea non è quella di stravolgere i sistemi gestionali già in uso o di creare un database centralizzato, ma di sfruttare i vantaggi offerti dalla tecnologia blockchain relativi alla trasparenza, alla tracciabilità e all'immutabilità dei dati, senza trascurare il delicato tema della privacy.

Il processo si articola in tre passaggi:

1. Generazione del dato ed estrazione dell'hash (impronta digitale): l'azienda carica i turni dei propri operatori con tutte le informazioni necessarie da dover mostrare al committente o alle Autorità (identificativo operatore, tipologia di contratto di lavoro, ore di lavoro effettuate, cliente), i documenti sensibili (LUL e DURC) ed eventuali documenti di comunicazione. Questi sono, quindi, sintetizzati in un "hash", ovvero un'impronta digitale univoca di quella informazione.

2. Notarizzazione in blockchain: esclusivamente l'hash viene caricato e registrato in blockchain pubblica, in modo da non caricare i dati sensibili in chiaro. A questo punto si riceve il "timestamp", ovvero la marca temporale che certifica che in un dato giorno e ad una data ora è stata scritta un'informazione in blockchain con quel contenuto (hash). Da questo momento non può più essere cancellata o alterata la registrazione dalla blockchain pubblica, è visibile a tutti.

3. Verifica istantanea: il committente o l'Autorità può verificare la veridicità delle informazioni sia attraverso la piattaforma, con un sistema di controllo che rilascia un feedback positivo o negativo relativo all'avvenuta notarizzazione, sia in modo indipendente attraverso la modalità di accesso autonomo verificato.

In tal modo, se necessario il committente potrà ammonire il fornitore immediatamente e, nei casi più gravi, potrà informare gli organi preposti dimostrando di aver esercitato i controlli dovuti sul comportamento del fornitore.



n. 03/2026
Anno XLVI
Periodico fondato da Paolo Tura

**DIRETTORE RESPONSABILE E
COORDINAMENTO EDITORIALE**

Raffaello Juvara
editor@securindex.com

HANNO COLLABORATO

Marco Albanese e Giovanni Taccori

SEGRETERIA DI REDAZIONE

redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI

marketing@securindex.com

EDITORE

essecome editore srls
Piazza Gae Aulenti 1, torre B - 20154 Milano
Tel. +39 02 3675 7931

REGISTRAZIONE

- Tribunale di Milano n. 21 del 31 gennaio 2018
- Registro pubblico Operatori di Comunicazione (ROC) n. 34727

GRAFICA/IMPAGINAZIONE

Lilian Visintainer Pinheiro
lilian@lilastudio.it



PrimeX InVista

Sicurezza totale, controllo assoluto.

Le telecamere **InVista** di Inim, integrate con una centrale **Prime X**, sfruttano l'AI per analizzare la scena in tempo reale. Creando **aree o linee virtuali**, è possibile attivare scenari domotici al loro attraversamento, come la dimmerazione delle luci, la chiusura delle tapparelle o l'attivazione di dispositivi domotici.

L'app **Inim Home** integra perfettamente sicurezza, videosorveglianza e domotica in un'unica interfaccia intuitiva, permettendo di ricevere notifiche in tempo reale su smartphone o smartwatch.