

securindex.com

IA AL LAVORO

PER LA COMPLIANCE DELLE ORGANIZZAZIONI

**Il Decreto Controlli e le
responsabilità della committenza**

6 ottobre 2026

 aisma

AISMA

Dove tecnologia
e umanità
si incontrano,
nasce la sanità
del futuro



CITTADINI DELL'ORDINE
1870

INNOVAZIONE E PROTEZIONE: LA SOLUZIONE COMPLETA PER IL TUO BUSINESS

Sicurezza e Vigilanza

Presidio fisso armato e disarmato
per la protezione del patrimonio

Consulenza Tecnologica

Supporto nella scelta delle migliori
tecnologie per la sicurezza

Fornitura e Installazione di Impianti di Sicurezza

Soluzioni personalizzate per
garantire la massima protezione

Sistemi Antincendio

Soluzioni integrate per la
prevenzione e gestione dei rischi da
incendio

Monitoraggio H24 dei Sistemi Sicurezza e Antincendio

Supervisione continua da parte della
nostra centrale operativa

Cybersecurity

Consulenza e difesa avanzata
contro le minacce digitali



GRUPPO CITTADINI DELL'ORDINE

Fondata nel 1870 con l'obiettivo di garantire la sicurezza delle persone e dei beni, Cittadini dell'Ordine opera nel settore da oltre 155 anni. Offriamo soluzioni tecnologiche avanzate per affrontare le sfide moderne della sicurezza, mettendo a disposizione delle aziende la nostra esperienza e la nostra competenza, che ci rendono partner ideali per ogni esigenza di protezione.

www.cittadinidellordine.com

 800 010 298



SENZA CUBE SERVICE

- ❌ Planning su fogli e calendari separati
- ❌ Siti e interventi senza visione geografica
- ❌ Ticket dispersi tra email e telefonate
- ❌ Registri e scadenze gestiti manualmente
- ❌ Dati da documenti e immagini inseriti manualmente

CON CUBE SERVICE

- ✅ Planning condiviso e sempre aggiornato
- ✅ Manutenzioni localizzate sulla mappa
- ✅ Ticket tracciati fino alla chiusura
- ✅ Compliance e registri digitali
- ✅ AI per leggere documenti esterni e immagini degli estintori, popolando il database

L'editoriale del direttore



Manutentori sistemi antincendio, una storia di ordinaria burocrazia

Come ben sanno gli addetti ai lavori (ma solo loro perché nessuno si è mai occupato della questione), il 25 settembre 2026 è scaduto l'ultimo termine per la presentazione delle istanze ai Comandi regionali dei Vigili del Fuoco per la valutazione dei requisiti stabiliti dal [DM 1 settembre 2021](#), il cosiddetto "Decreto Controlli", per i tecnici manutentori dei sistemi di sicurezza antincendio.

Con questo decreto, l'Italia si era dotata di una normativa all'avanguardia con specifiche ben dettagliate delle tecnologie, delle procedure per il mantenimento e dei requisiti dei tecnici manutentori, figure chiave per garantire il funzionamento dei sistemi in caso di necessità. Sono circa 15.000 le ditte identificate dai codici Ateco di riferimento con la stima di almeno 100.000 tecnici da esaminare da parte dei Comandi Regionali dei Vigili del Fuoco.

Il DM sarebbe dovuto entrare in vigore un anno dopo la sua pubblicazione in G.U. avvenuta il 25 settembre 2021 ma i ritardi nella messa a punto del sistema hanno costretto per quattro anni consecutivi a prorogare i termini fino all'ultima scadenza del 25 settembre 2026, una dead line oltre la quale chi non ha sostenuto l'esame da parte dei VV.FF non potrebbe più lavorare sui sistemi dei propri clienti.

La sera del 25 settembre, nel sito dei Vigili del Fuoco risultavano 11.126 tecnici esaminati dai Comandi Regionali (dal massimo di 2281 in Veneto al minimo di 14 in Molise) ma, considerando che la maggior parte dei manutentori deve sostenere più esami (uno per ogni categoria di dispositivi che intende gestire), il numero di persone fisiche effettivamente valutate potrebbe essere molto inferiore.

A fronte di una situazione che potrebbe diventare drammatica, con migliaia di tecnici che si trovano senza lavoro e una quantità ancora maggiore di impianti senza manutenzione, è stato deciso in extremis che i soggetti che hanno presentato l'istanza entro il 25 settembre ma non hanno ancora sostenuto l'esame "possano continuare a eseguire gli interventi di manutenzione e i controlli sugli impianti, sulle attrezzature e sugli altri sistemi di sicurezza antincendio rientranti nelle tipologie oggetto dell'istanza". ([DM 22 settembre 2026 - G.U. n. 222 del 24 settembre 2026](#)). Come corollario del DM, la [circolare del Direttore del Dipartimento dei Vigili del Fuoco del 24 settembre](#) ha precisato che chi presentato l'istanza entro il 25 settembre potrà continuare a lavorare anche senza pre-accordo sottoscritto con il soggetto formatore/sede d'esame.

A questo punto ci si chiede inevitabilmente:

1. i tecnici che dal 26 settembre non possono più lavorare (presumibilmente la maggioranza) cosa devono fare per mettersi in regola, dal momento che nulla viene detto in proposito dal DM né dalla circolare del 24 settembre? E quali sarebbero i tempi?
2. parimenti, un'azienda che volesse assumere e formare nuovi tecnici dopo la dead line, oppure dei giovani che volessero avvicinarsi alla mansione, cosa dovranno fare?
3. dal momento che era evidente da tempo che si sarebbe arrivati al 25 settembre 2026 con solo una frazione di tecnici abilitati, perché i provvedimenti di proroga che stabiliscono chi può lavorare e chi no sono stati emessi solamente il giorno prima della scadenza impedendo a molti di regolarizzarsi?

È solo l'ennesima, triste storia di ordinaria burocrazia?

Ultima ma non meno importante questione: dal momento che tra gli esclusi post 25 settembre è prevedibile che più di uno continui a lavorare sugli impianti senza qualificazione, i responsabili delle organizzazioni che devono controllare la compliance dei propri fornitori sono informati del problema? E in caso di sinistro, come si comporteranno le assicurazioni?



Sommario

- 08 Compliance, perché interessa alle Procure della Repubblica
- 10 Perché la compliance è un fattore di sicurezza per le imprese
- 12 Shadow risk management: i rischi che non compaiono nell'organigramma aziendale
- 14 Governare l'intelligenza artificiale prima di usarla: la compliance comincia dall'architettura
- 16 Cyberloop, il partner per la compliance delle organizzazioni
- 18 Come gestire in modo strutturato e tracciabile la manutenzione dei presidi antincendio
- 20 Dal varco al flusso: la gamma Magnetic® trasforma la sicurezza degli accessi
- 22 L'esperienza Vivaldi Group al servizio della sicurezza

Una nuova visione della sicurezza



**VIDEOSORVEGLIANZA
E VIDEORONDA
CON AI**



**LOCALIZZAZIONE
SATELLITARE
GPS**



**ANTINTRUSIONE E
ANTINCENDIO**



**ROBOT
TERRESTRI**



**VIGILANZA
ARMATA E
DISARMATA**

IA AL LAVORO

PER LA COMPLIANCE DELLE ORGANIZZAZIONI

Il Decreto Controlli e le responsabilità della committenza

6 ottobre 2026

Palazzo Cusani, Milano

Questa edizione del ciclo di workshop "IA al lavoro" che esamina le applicazioni di IA per la sicurezza, è divisa in due parti: la prima è dedicata alla compliance delle organizzazioni alle normative comunitarie sulla sicurezza dei dati con un approfondimento sulle responsabilità del committente negli appalti; la seconda è riservata alla scadenza del 25 settembre per la qualificazione dei tecnici manutentori dei sistemi di rilevamento incendi (DM 1 settembre 2021)

La quantità e la complessità delle norme che le organizzazioni pubbliche e private di ogni dimensione devono rispettare rende oggi indispensabile l'utilizzo di sistemi intelligenti che permettano alle funzioni responsabili di mantenere il costante controllo della situazione per intervenire tempestivamente con le opportune azioni correttive.

L'entità della sanzioni e dei possibili risvolti risarcitori è tale da compromettere la stessa continuità, in particolare per le imprese minori, al punto di considerare la compliance come un vero fattore di protezione dell'azienda.

Verrà affrontato il tema delle responsabilità del committente negli appalti, con un approfondimento in merito ai rischi di caporalato nella supply chain; a seguire verranno esaminate situazioni diverse di criticità e possibili soluzioni con IA per il rispetto della compliance.

Nella seconda parte si affronterà uno dei temi più critici sul piano delle responsabilità dei committenti e delle proprietà del Real Estate: la manutenzione dei sistemi di rilevamento incendi.

La scadenza del 25 settembre per la messa in regola dei tecnici manutentori sarà motivo per fare il punto sul DM 1 settembre 2021 "Decreto Controlli" con rappresentanti dei Vigili del Fuoco.

PROGRAMMA

- 9.30 Registrazione partecipanti
- 10.00 Inizio lavori
- 10.10 **Compliance: consapevolezza e responsabilizzazione del committente**
invitati: avv. Riccardo Rossotto (Studio RPLT), dott. Ciro Santoriello Procuratore Aggiunto Procura Cuneo
- 11.00 **IA al lavoro per la compliance delle organizzazioni. Il confronto con le risorse umane**
Silvia Avanzini (EBIVER), Alessandro Manfredini (AIPSA), Martino Mogavero (ASIS Italy), Pasquale Mundo (BNL BNP Paribas), Luca Pacitti (Istituto Vigilanza Coopservice), Marco Stratta (Segretario Generale A.N.I.V.P.), avv. Alberto Ziliani (UNIV)
- 12.30 **Strumenti e buone pratiche**
invitati: Luca Camerino (Compass), Francesco Hemmeler (CEO di AISEC), Vito Mastrominico (TMT Innovation), Sidney Mathoux (Studio RPLT), Alessandro Molari (Cyberloop Gruppo CdO), Stefano Moretto (Life3), Amir Topalovic (AISMA)
- 13.30 Light lunch
- 14.30 **Decreto controlli, il punto della situazione**
keynote speech di Paolo Massimi (Corpo dei Vigili del Fuoco)
- 15.00 **La compliance del manutentore dei sistemi antincendio**
conversazione con: Antonio Avolio (AIPS), Paolo Galiazzo (EL.MO. spa), Stefano Moretto (Life3), Ferruccio Ravelli (Sparim Bolzano)
- 16.15 Fine lavori

Evento in presenza con rilascio dell'Attestato di Partecipanza su richiesta.

Per informazioni: segreteria@securindex.com

Partner



Patrocino



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?

Sì 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.

ATE
urmet

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.

**Siamo presenti a MIBA Levante,
18-19 novembre
Nuovo Padiglione. Stand 100,
ingresso Agricoltura.**



Perché la compliance è un fattore di sicurezza per le imprese

intervista all'Avv. Riccardo Rossotto, partner Studio RPLT

Compliance come fattore di sicurezza per le organizzazioni. È possibile stimare quali sono i rischi e i costi del mancato rispetto delle norme per un'organizzazione?

Sì, è possibile ma per inquadrare questo tema mi permetto di fare un passo indietro: in Italia il tema della compliance è un tema vissuto come un nuovo costo che si aggiunge ai tanti, troppi "lacci e laccioli" che già opprimono i conti economici delle nostre PMI.

Soprattutto in momenti di crisi, sia economica sia geopolitica, gli imprenditori sono portati a concentrarsi sul business cercando di salvaguardare fatturati e redditività dell'azienda. In questo modo tutti quei costi che sono in apparenza non direttamente collegati al business, vengono derubricati o non inseriti nei piani di investimento. Questo va ovviamente a detrimento di una corretta ottemperanza dell'imprenditore e dell'impresa ai vincoli normativi. Ormai la normativa italiana e la giurisprudenza che si sta consolidando nel tempo, sono concentrate nel responsabilizzare l'imprenditore e l'impresa, a strutturare la propria azienda con degli assetti organizzativi adeguati alle dimensioni e alla complessità del ciclo produttivo. Assistiamo con frequenza a decisioni della magistratura italiana che sanzionano condotte imprenditoriali non adeguate a quella che viene ormai definita "la responsabilità organizzativa". L'imprenditore deve vigilare sull'adeguatezza dei propri assetti organizzativi controllando la correttezza dei processi produttivi, mettendo in atto tutte quelle azioni necessarie per cercare di evitare il verificarsi di sinistri e cioè di illeciti sanzionati dall'ordinamento. Per rispondere quindi alla domanda se sia stimabile e quantificabile il rischio di una non ottemperanza ai vincoli della compliance, tenendo conto di questo contesto culturale e industriale del nostro paese, siamo orientati a rispondere positivamente, facendo però presente all'imprenditore che quel tipo di investimenti necessari per rispettare la normativa non deve essere considerato un semplice costo; sono, in realtà, un



investimento mirato a tutelare il patrimonio aziendale e quindi a valorizzarlo anche nel caso di operazioni straordinarie. Oggi una impresa vale di più se ha un sistema di compliance corretto ed efficiente: questa è la miglior dimostrazione che tutti i costi necessari per adeguare la propria organizzazione alla normativa, sono in realtà degli investimenti che da un lato salvaguardano l'azienda e la proprietà e dall'altro contribuiscono a dare una maggior valorizzazione all'azienda medesima. Quindi la stima preventiva degli investimenti necessari per essere compliant è un passaggio fondamentale, e possibile, nella creazione di valore di un'impresa.

Come valuta i livelli di awareness e di accountability in materia da parte dei vertici aziendali delle imprese italiane?

Mi ricollego a cosa ho appena accennato nella prima risposta. Salvo le grandi aziende che ovviamente hanno una cultura aziendale e un management capace, idoneo ed esperto in questa materia, il grande mondo delle PMI, che costituiscono la spina dorsale del nostro modello industriale, sconta ancora un deficit culturale nell'approcciare il tema della compliance. Ci sono segnali di miglioramento che ogni tanto derivano, però, da situazioni in cui l'imprenditore si è trovato con

un avviso di garanzia notificatogli per un reato rilevante ai fini della 231 e da quel momento ha capito l'importanza di attrezzarsi con una compliance adeguata al suo modello di business. Bisognerebbe fare prevenzione e invece ho la sensazione che siamo ancora in una fase in cui regna la battuta "a me non succede" o, peggio, "sono tutti costi quelli della compliance non recuperabili: burocrazia pura"!

Quali misure si potrebbero adottare per divulgare una più attenta cultura della compliance?

Non stancarsi mai di suggerire agli imprenditori di adeguarsi al perimetro degli obblighi che ormai la normativa e la giurisprudenza impongono a chi sceglie di fare quel mestiere. Oggi, se sceglie di fare l'imprenditore, devi avere come priorità, dopo ovviamente la profittevolezza del business (combinazione, non dimentichiamocelo mai, di capitale economico e di capitale umano, soprattutto), quella di adeguare la tua azienda alle norme vigenti, soprattutto in materia di controlli e di vigilanza sulla correttezza delle condotte di tutte le risorse umane impiegate nel processo produttivo. Un ruolo fondamentale lo hanno sicuramente le associazioni di categoria ma gli stessi professionisti hanno la responsabilità di trasferire questa cultura ai loro clienti. Ho constatato, per esempio, che è molto importante organizzare degli eventi in cui gli imprenditori possano percepire il pensiero dei magistrati in materia, l'approccio organizzativo degli aziendalisti, i vincoli di legge e gli indirizzi giurisprudenziali degli avvocati. Insomma, la cultura della compliance si sviluppa attraverso una formazione multidisciplinare e oggi, durante la rivoluzione digitale che stiamo vivendo, deve essere anche arricchita di quella parte di tecnologie che servono a semplificare e rendere più efficienti i controlli aziendali e quindi in generale i contenuti della compliance.

Ci sono strumenti (ovvero quali caratteristiche devono avere) che permettano ai committenti di monitorare il livello di compliance dei propri fornitori in modo legittimamente utilizzabile per tutelare se stessi?

L'innovazione tecnologica sta fornendo agli operatori tutta una serie di nuovi prodotti, maggiormente nel campo informatico, che agevolano l'imprenditore ad assolvere ai doveri di compliance in modo più efficiente e meno costoso. Esistono strumenti "ad hoc", per esempio nella prevenzione del rischio di illeciti nelle filiere, che permettono al capo filiera di obbligare i membri ad adottare delle misure di informazione e di controllo che favoriscono una meno complessa vigilanza da parte del capo filiera. L'esperienza per esempio del "cruscotto di legalità" (un software che serve per l'appunto a controllare in modo più efficiente la regolarità e conformità alla legge delle condotte di aziende facenti parte di filiere) sta dando risultati molto positivi anche in termini di creazione di una specifica cultura imprenditoriale in questa materia. Spesso gli imprenditori, attraverso questi necessari monitoraggi e controlli sulle proprie condotte ma anche su quelle dei propri subfornitori e subappaltatori, si rendono conto di conoscere meglio la propria azienda, di presidiare meglio i vari processi decisionali, di interagire in modo più trasparente e costruttivo con i propri fornitori. L'innovazione tecnologica, oggi, toglie da un lato molti alibi di chi non voleva ottemperare alla compliance ma, dall'altro lato, aumenta le responsabilità degli imprenditori non solo di adottare i nuovi tools creati dalla rivoluzione digitale ma di utilizzarli in maniera tale da poter dimostrare in caso di ispezione di terzi (audit del capo filiera o ispezioni delle autorità preposte), di aver fatto tutto quanto possibile per aumentare i controlli ed evitare la commissione di reati.

Shadow risk management: i rischi che non compaiono nell'organigramma aziendale

di Francesco Hemmeler, senior executive partner di AISEC, Security Advisor Company

“Per anni abbiamo cercato il nemico all'interno. Oggi rischiamo di non vedere quello che entra ogni giorno dalla porta dei fornitori. Caporalato, infiltrazioni criminali, frodi, violazioni normative, incidenti cyber e danni reputazionali hanno sempre più spesso un elemento in comune: nascono all'esterno dell'organizzazione, ma ne colpiscono direttamente il business. In un contesto in cui NIS2, CER e GDPR richiedono una crescente capacità di controllo della filiera, continuare a considerare il rischio delle terze parti come un problema contrattuale significa osservare il mondo attraverso uno specchietto retrovisore”.



Le aziende investono milioni per proteggere sedi, dati, infrastrutture e persone. Eppure le crisi più gravi continuano spesso ad arrivare da soggetti che non compaiono nell'organigramma aziendale: i fornitori

Per troppo tempo abbiamo considerato il fornitore come un soggetto da qualificare e contrattualizzare. Oggi dobbiamo iniziare a considerarlo per ciò che potrebbe essere: un potenziale vettore di rischio capace di influenzare la sicurezza, la continuità operativa e la reputazione dell'organizzazione.

Nel nuovo scenario normativo e geopolitico, caratterizzato da supply chain frammentate, esternalizzazioni pervasive e crescente pressione criminale sulle filiere produttive, il fornitore è diventato parte integrante del perimetro di rischio aziendale. La domanda che un Consiglio di Amministrazione dovrebbe porsi non è più se un fornitore sia economicamente affidabile, ma se possa rappresentare una minaccia per l'organizzazione, potenzialmente in grado di generare impatti superiori a quelli di molti rischi interni monitorati quotidianamente.

La filiera come superficie di attacco

È ormai evidente dal verificarsi di tanti eventi che la sicurezza ha progressivamente abbandonato una visione centrata sul perimetro fisico o informatico dell'organizzazione. Le recenti inchieste sulla supply chain nei settori della logistica, della moda e della distribuzione hanno evidenziato come fenomeni di sfruttamento del lavoro, frodi fiscali e possibili infiltrazioni criminali possano svilupparsi all'interno delle reti di fornitori e subfornitori, coinvolgendo indirettamente anche grandi aziende committenti, chiamate a rispondere ad una forma di “agevolazione colposa” di attività illecite, arrivando a vedersi attribuite misure di amministrazione giudiziaria anche se non direttamente coinvolte nei reati ma ritenute incapaci di governare i rischi presenti nella propria supply chain. Anche sul fronte cyber sono numerosi i casi di compromissione di reti informatiche di clienti per causa di fornitori “meno protetti”. La crescente interdipendenza tra aziende ha reso le filiere uno dei principali vettori di vulnerabilità, un po' come una catena che se ha un anello debole, rischia di vanificare l'intera sua funzionalità.

Formalmente il problema appartiene a un soggetto terzo, ma nella realtà operativa, mediatica e reputazionale, il danno ricade inevitabilmente sull'organizzazione committente ed è per questo che i clienti, gli investitori, le autorità e in generale l'opinione pubblica non fanno più alcuna distinzione tra l'azienda e il suo ecosistema di fornitori.

NIS2 e CER: la fine dell'alibi del “non lo sapevamo”

L'evoluzione del quadro regolatorio europeo sta segnando un passaggio culturale prima ancora che normativo. La Direttiva NIS2 impone alle organizzazioni soggette di considerare esplicitamente i rischi provenienti dalla supply chain e dai fornitori di servizi, introducendo obblighi di gestione e controllo che trasformano il monitoraggio delle terze parti in un requisito di governance. Similmente la Direttiva CER porta questa logica sul piano della resilienza delle infrastrutture e dei servizi essenziali, richiedendo di comprendere e gestire le dipendenze critiche che possono compromettere la continuità operativa, soprattutto quando questa si riflette direttamente sulle funzioni critiche dello stato e della società (salute, pubblica sicurezza, economia nazionale, energia, ecc.). Anche il GDPR, attraverso il principio di accountability e gli obblighi connessi ai rapporti con i fornitori che operano come responsabili del trattamento, ha da tempo stabilito che non basta scegliere un partner: occorre dimostrare di averne valutato il rischio, l'affidabilità e le garanzie offerte, monitorandone nel tempo la conformità.

Il caporalato è anche un problema di security

Esiste poi un tema che raramente viene affrontato nei

dibattiti sulla sicurezza aziendale e che apparentemente sembrerebbe non interessare chi si occupa di security: il caporalato.

Troppo spesso viene considerato esclusivamente un problema sociale, giuslavoristico o sindacale, ma esso rappresenta anche un rischio di security e reputazionale. Le organizzazioni che si avvalgono di reti complesse di appaltatori e subappaltatori possono inconsapevolmente esporsi a fenomeni di sfruttamento della manodopera, falsificazione documentale, evasione contributiva, infiltrazioni criminali o altre pratiche illecite. Quando queste situazioni emergono, la domanda che inevitabilmente viene rivolta all'azienda committente è sempre la stessa: cosa è stato fatto per prevenire questo rischio? Avete adottato dei controlli per monitorarlo?

L'Intelligenza Artificiale come strumento di controllo preventivo

Le tradizionali attività di qualificazione dei fornitori, basate su questionari, audit e verifiche periodiche, non sono più sufficienti per intercettare rischi che evolvono rapidamente. La vera sfida non è qualificare il fornitore, ma monitorarlo nel tempo. In questo contesto l'Intelligenza Artificiale può supportare l'analisi continua di informazioni e segnali di anomalia provenienti da fonti diverse, aumentando la capacità di individuare tempestivamente potenziali vulnerabilità. Tuttavia, la tecnologia da sola non basta: servono competenze specialistiche e una stretta collaborazione tra Security, Risk Management, Compliance e Procurement per trasformare i dati in reale capacità di prevenzione.

Governare l'intelligenza artificiale prima di usarla: la compliance comincia dall'architettura

intervista a Amir Topalovic, CEO di AISMA

Il workshop "IA al lavoro" del 6 ottobre a Palazzo Cusani parla di responsabilità del committente, supply chain e Decreto Controlli. Che cosa c'entra la governance dell'intelligenza artificiale?

C'entra perché il principio è lo stesso. Il committente risponde anche di ciò che non esegue direttamente: dei fornitori, dei subappalti, delle condizioni di lavoro lungo la filiera, della manutenzione degli impianti affidata a terzi. Con l'intelligenza artificiale accade qualcosa di analogo. Un'organizzazione risponde delle decisioni prese con il supporto di strumenti di cui spesso non conosce il funzionamento, che elaborano dati di cui non sempre controlla la provenienza. Oggi l'adozione dell'AI procede più velocemente della sua governance, e il rischio non è più soltanto tecnologico: è organizzativo, reputazionale e regolamentare. Proprio per questo gli strumenti di monitoraggio della compliance, se basati sull'AI, devono essere a loro volta governati. Pensiamo al Decreto Controlli: un sistema che monitora scadenze di manutenzione e qualifiche dei tecnici è utile solo se le sue segnalazioni sono affidabili e ricostruibili. Una segnalazione mancata o non documentata non riduce il rischio del committente: lo sposta, rendendolo meno visibile.

Che cosa significa, concretamente, governare un progetto di intelligenza artificiale?

Significa poter rispondere in ogni momento a una domanda precisa: chi ha l'autorità di applicare una determinata conoscenza, in quale versione, con quali vincoli e con quale tracciabilità? Non basta sapere quali documenti l'AI ha consultato. Occorre sapere se quella conoscenza poteva essere usata per quella decisione, da quella persona, con quella autorizzazione. È la distinzione



tra governance della conoscenza e governance della decisione. In pratica servono una mappa strutturata della conoscenza aziendale, confini espliciti entro cui l'AI può operare, regole di business applicate direttamente al livello dell'AI, permessi granulari su utenti e dati e un punto di controllo unico per tutte le applicazioni. Senza queste condizioni un'AI può produrre risposte convincenti ma non verificabili, e nessuno è in grado di ricostruire a posteriori perché una decisione sia stata presa. La governance non è un documento da allegare al progetto: è un'infrastruttura.

Quali riferimenti normativi deve tenere presenti chi avvia un progetto oggi?

Come sottolinea l'avv. Francesca Niola, responsabile legal e compliance di AISMA, AI Act, NIS2 e DORA non vanno letti come tre percorsi paralleli, perché si intersecano sulla stessa infrastruttura tecnologica. Una soluzione basata sull'AI svolge inoltre due funzioni giuridiche insieme. È uno strumento di conformità, perché genera log, report e tracciabilità utili a dimostrare l'adempimento degli obblighi. Può però essere anche oggetto di conformità: se ricade tra

i sistemi ad alto rischio dell'AI Act, deve rispettarne a sua volta i requisiti. È il caso, ad esempio, dei sistemi impiegati nella selezione e nella gestione del personale: qui l'AI Act chiede al datore di lavoro di informare preventivamente i rappresentanti dei lavoratori e i lavoratori interessati, e la legge 132/2025 affianca obblighi informativi specifici sull'uso dell'AI nel rapporto di lavoro. Il Regolamento (UE) 2026/1744 ha spostato al 2 dicembre 2027 gli obblighi per questi sistemi, ma il tempo guadagnato serve a progettare, non ad attendere. Anche la supply chain è coinvolta: NIS2 include la sicurezza della catena di fornitura tra le misure di gestione del rischio, e DORA disciplina in modo dettagliato i fornitori ICT degli enti finanziari.

Dalla norma all'architettura: quali caratteristiche deve avere una soluzione governata?

Alcune caratteristiche devono esserci di serie. La prima è un audit trail generato automaticamente. Il log che l'AI Act richiede per i sistemi ad alto rischio è lo stesso che un'ispezione NIS2 o DORA chiede di esibire: progettato bene, un obbligo diventa una prova già pronta. La seconda è la provenienza verificabile, cioè la possibilità di sapere per ogni risposta da quali fonti deriva, in quale versione e con quali citazioni. La terza, per noi decisiva, è che quando manca un riscontro fattuale il sistema non produca comunque una risposta verosimile, ma si fermi e dichiari l'assenza di evidenza. Servono poi una sorveglianza umana

configurabile, con ruoli e soglie di intervento definiti, e permessi assegnati per singola azione, non soltanto per profilo. Infine l'indipendenza dal modello: poter sostituire il modello linguistico senza ricostruire la conoscenza accumulata riduce la dipendenza dal fornitore e tutela il know-how. Su questi principi abbiamo costruito Cogniss, il Cognitive Control Plane di AISMA: un'infrastruttura di governo su cui far operare le applicazioni di intelligenza artificiale, non l'ennesimo strumento di reportistica.

Quale consiglio darebbe a una PMI o a un committente che vuole iniziare?

Di partire da un perimetro circoscritto e di seguire un metodo. Primo, classificare la soluzione in base alla finalità e al settore di impiego. Secondo, mappare gli obblighi applicabili incrociando AI Act, NIS2 e DORA. Terzo, verificare il fornitore: documentazione tecnica, log disponibili, clausole contrattuali. Quarto, definire chi sorveglia, con quali soglie e con quali responsabilità interne. Quinto, monitorare nel tempo, perché la conformità di un sistema che apprende non è una fotografia. Per le imprese minori il punto è ancora più rilevante: l'entità delle sanzioni e dei possibili risarcimenti può comprometterne la continuità. Una governance progettata prima, e non aggiunta a posteriori, costa meno, protegge l'azienda e trasforma un obbligo in un elemento di fiducia verso clienti, autorità e lavoratori.



Contatti:
AISMA Srl
info@aisma.it
<https://aismasrl.it/>

Cyberloop, il partner per la compliance delle organizzazioni

Intervista a Alessandro Molari, CEO di Cyberloop – Gruppo Cittadini dell'Ordine

Il concetto di compliance è stato introdotto sostanzialmente dalle direttive europee in materia di cybersecurity. Può spiegare la relazione tra il rispetto delle norme e la sicurezza informatica?

Le direttive non hanno inventato la sicurezza: hanno introdotto l'obbligo di dimostrarla. NIS2, CER, DORA e Cyber Resilience Act chiedono tre cose — misure proporzionate al rischio, evidenza che siano operative e un titolare che ne risponda, cioè l'organo di gestione e non il responsabile IT.

Conformità e sicurezza però non coincidono. Un'organizzazione può avere politiche approvate, registri aggiornati e nessuna capacità reale di accorgersi di un'intrusione. Il 70% delle organizzazioni europee cita la conformità come primo motore di spesa (ENISA, 2025), ma in Italia l'83% delle grandi imprese dichiara di gestire attivamente il rischio cyber e solo il 28% risulta altamente resiliente (Osservatorio del Politecnico di Milano). La norma ha portato però ciò che il mercato da solo non produceva: una data, un perimetro e un responsabile con nome e cognome. Letta così è un buon punto di partenza — il pavimento, non il soffitto. Il rischio è l'uso opposto: adempiere per la scadenza, con documenti che descrivono misure che nessuno ha mai provato.

Qual è la proposta di Cyberloop ai soggetti che rientrano nelle categorie disciplinate dalle direttive europee, al fine di renderle compliant?

Nessun fornitore rende conforme un'organizzazione: la conformità è uno stato che si mantiene. Possiamo accompagnare il percorso, in cinque tempi.

Si comincia misurando: un assessment sui requisiti della Direttiva, funzione per funzione, che restituisce i divari in ordine rispetto alla data.

Segue l'adeguamento — politiche, procedure, analisi del rischio, piani di continuità e di risposta — che serve a qualcosa solo se descrive ciò che l'organizzazione fa davvero.



Il terzo tempo è il presidio dell'indirizzo: il servizio vCISO mette a disposizione un professionista con attività, frequenze e indicatori dichiarati, e una rendicontazione periodica all'organo di gestione.

Il quarto è il monitoraggio, su due perimetri: l'infrastruttura, presidiata dal SOC MDR CYLOS ventiquattro ore su ventiquattro, che produce la tracciabilità di che cosa è successo e quando; e la filiera dei fornitori, presidiata da Chain Zero — il tema della domanda successiva.

Il quinto è la notifica. I termini verso il CSIRT Italia — ventiquattro ore, settantadue ore, relazione finale entro un mese — decorrono mentre l'incidente è ancora in corso. Il nostro servizio di Referente CSIRT mantiene il punto di contatto e predispose le notifiche; la trasmissione parte solo dopo conferma scritta del Cliente, perché l'obbligo resta suo.

Cyberloop opera un CSIRT riconosciuto da Trusted Introducer, con maturità ENISA Advanced secondo il modello SIM3.

Attraversa tutti i tempi la formazione: la determinazione ACN chiede formazione documentata, non generica sensibilizzazione.

Qual è il livello di consapevolezza da parte dei responsabili di questi soggetti?

Va distinto su tre piani.

Sapere di essere in perimetro. Consapevolezza alta e cresciuta in fretta: il 57% delle organizzazioni segnala maggiore attenzione del consiglio di amministrazione per effetto della NIS2 (Osservatorio del Politecnico di Milano).

Sapere che cosa comporta. Qui il divario si apre. Molti leggono la Direttiva come un adempimento documentale delegabile all'IT, quando la responsabilità è dell'organo di gestione e riguarda misure operative. Il 30% delle organizzazioni europee non ha condotto alcun assessment negli ultimi dodici mesi (ENISA).

Sapere a che punto si è. È il piano più debole, e riguarda soprattutto la fascia media. Il Cyber Index PMI colloca le imprese sotto i 250 dipendenti a 55 su 100, con il vulnerability management all'11% e gli assessment al 44%: sanno che cosa hanno, non in che stato è.

Dietro c'è un dato di sistema: la spesa italiana in cybersecurity resta allo 0,13-0,14% del PIL contro una media G7 dello 0,3%. La consapevolezza è cresciuta più in fretta delle competenze disponibili.

In che modo si potrebbe migliorare la situazione?

Quattro mosse, in ordine.

Misurare prima di comprare. Scegliere lo strumento e poi cercargli un problema è il modo più rapido per spendere senza ridurre il rischio. La sequenza corretta parte dal contesto e arriva al controllo passando per rischio, evidenza e priorità.

Assegnare la titolarità e una cadenza. La NIS2 chiede un responsabile, non un referente. Un riporto periodico all'organo di gestione, con pochi indicatori stabili, cambia più di molti strumenti.

Provare i percorsi prima che servano. Un piano di risposta mai simulato e una notifica mai provata sono documenti, non capacità. Una simulazione da tavolo dice in una giornata quello che un audit documentale non vede.

Colmare il divario di competenze con il presidio. Nell'Unione Europea mancano 299.000 professionisti di sicurezza (ENISA): per la maggior parte delle organizzazioni

italiane una funzione interna dedicata non è realistica, e la strada praticabile è un presidio esterno continuativo con attività e frequenze dichiarate.

Un'avvertenza, infine: il calendario non finisce il 31 ottobre. Novembre porta l'avvio dell'attività ispettiva, il 2027 la direttiva CER e il Cyber Resilience Act. Chi organizza il lavoro per scadenze singole lo rifarà da capo ogni volta.

La NIS2 estende la responsabilità alla catena di fornitura, e le FAQ dell'ACN chiedono di valutare la singola fornitura. Come si governa in concreto il rischio dei fornitori?

È l'obbligo più sottovalutato, ed è già pienamente in vigore: valutare il rischio della singola fornitura, inserire requisiti proporzionati in contratto e verificarli nel tempo con report, audit, test e log. Dal 31 maggio 2026 i soggetti in perimetro elencano i fornitori rilevanti sulla piattaforma dell'Agenzia. Lo stato dell'arte è un elenco su un foglio di calcolo e una campagna di questionari annuale che nessuno rilegge: costa poco e non regge davanti a chi chiede evidenza. Il mercato offre due metà del percorso — le piattaforme di intelligence danno il segnale esterno, gli strumenti di governance danno il processo. Ricucirle resta un lavoro del cliente.

Chain Zero è la piattaforma che Cyberloop ha sviluppato per tenere insieme le due metà. Censisce le terze parti a perimetro, ne osserva la postura dall'esterno in continuo e assegna a ciascuna un punteggio che si può aprire fino ai fattori che lo generano e alle evidenze da cui viene. Sopra il punteggio ci sono le campagne di questionario, l'indice di coerenza fra quanto la terza parte dichiara e quanto è rilevabile dall'esterno, e i piani di rientro con un responsabile e una scadenza. Il presidio prosegue anche sul fornitore che non risponde. Contano poi tre scelte di progetto: dati ed evidenze trattati e conservati nell'Unione Europea, modelli linguistici che operano su infrastruttura Cyberloop, rapporto contrattuale retto dalla legge italiana. Per chi deve rispondere a un'autorità europea non è un dettaglio.

Resta il punto vero, che è il perimetro: la domanda decisiva non è quanto costa, è quante terze parti contano davvero.



Contatto:
Cyberloop – Gruppo Cittadini dell'Ordine
info@cyberloop.it
www.cyberloop.it
www.cittadinidellordine.com

Come gestire in modo strutturato e tracciabile la manutenzione dei presidi antincendio

intervista a Stefano Moretto, CEO di Life3

Ci può descrivere in sintesi Cube Service, cosa fa e chi lo dovrebbe utilizzare?

Cube Service è una piattaforma digitale sviluppata per gestire in modo strutturato e tracciabile le attività di manutenzione degli impianti di sicurezza e dei presidi antincendio. Nasce dall'esperienza maturata nel settore e dalla necessità di rispondere a un contesto normativo sempre più rigoroso, nel quale non è sufficiente eseguire le manutenzioni: occorre anche pianificarle, documentarle, renderle verificabili e conservarne le evidenze nel tempo. La piattaforma consente di programmare visite e interventi attraverso un calendario condiviso, organizzare clienti, siti e squadre tecniche e localizzare le manutenzioni direttamente su una mappa geografica interattiva. In questo modo l'ufficio può avere una visione immediata delle attività previste e della loro distribuzione sul territorio, agevolando il coordinamento operativo e l'ottimizzazione degli spostamenti.

Cube Service guida inoltre i tecnici nelle attività sul campo mediante procedure e checklist, permette di registrare anomalie, archiviare la documentazione tecnica e produrre rapporti digitali firmabili e condivisibili. Integra anche la gestione dei ticket, che possono essere aperti sia dal cliente sia dal manutentore e seguiti lungo l'intero processo, dalla presa in carico fino alla chiusura. Le funzionalità sono sviluppate per supportare la conformità alle normative specifiche applicabili alle diverse tipologie di impianto e presidio.

È una soluzione pensata innanzitutto per le aziende che effettuano manutenzione antincendio e manutenzione di impianti speciali, ma coinvolge un ecosistema più ampio: tecnici, responsabili operativi, service manager, responsabili della sicurezza e proprietari o gestori degli immobili. L'obiettivo è trasformare la manutenzione da semplice adempimento operativo a processo digitale governato, misurabile e documentato.



In relazione all'esigenza dei diversi soggetti interessati all'efficienza dei sistemi antincendio di dimostrare di aver "fatto il possibile", qual è la risposta di Cube Service?

Oggi uno dei temi più sentiti nel settore è la cosiddetta "dimostrabilità". In caso di guasto, malfunzionamento o evento critico, non basta affermare che i controlli siano stati eseguiti: occorre poter dimostrare quando sono stati svolti, da chi, secondo quali procedure e con quali risultati. La risposta di Cube Service è una tracciabilità strutturata dell'intero processo manutentivo. Visite e interventi vengono pianificati nel calendario condiviso, assegnati agli operatori, eseguiti e registrati digitalmente. Le attività sul campo possono essere guidate da procedure e checklist coerenti con le norme tecniche e con le disposizioni applicabili alla specifica tipologia di impianto o presidio.

A questo si aggiungono strumenti quali i QR Code, la registrazione delle anomalie, l'archiviazione della documentazione tecnica e la generazione di rapporti digitali. Anche le richieste e le criticità possono essere gestite tramite ticket, aperti dal cliente o dal manutentore e tracciati dalla presa in carico fino alla risoluzione e alla chiusura. Ne deriva uno storico organico e consultabile dell'intero ciclo manutentivo.

Per il manutentore ciò significa disporre delle evidenze necessarie a documentare le attività svolte. Per il responsabile della sicurezza rappresenta uno strumento di controllo e verifica. Per il proprietario o il gestore dell'immobile costituisce una tutela concreta, perché rende visibili lo stato delle manutenzioni, le scadenze, le anomalie rilevate e le azioni intraprese per gestirle.

In un contesto influenzato dal Decreto Controlli e da norme tecniche sempre più dettagliate, Cube Service supporta quindi la compliance organizzando attività, controlli ed evidenze in modo coerente con i requisiti applicabili. Il software non sostituisce la competenza del manutentore né certifica da solo la conformità, ma rende il processo più controllabile e fornisce elementi oggettivi utili alla gestione del rischio e delle responsabilità.

Può venire utilizzato solo dai manutentori di sistemi antincendio o anche dai proprietari/gestori di parchi immobiliari?

Da entrambi.

Sebbene Cube Service sia nato per rispondere alle esigenze operative delle aziende di manutenzione, la sua architettura lo rende particolarmente utile anche per proprietari, asset manager, facility manager e gestori di patrimoni immobiliari distribuiti sul territorio.

Dal punto di vista del manutentore, la piattaforma consente di governare il planning di visite e interventi mediante un calendario condiviso, coordinare le squadre tecniche, consultare su mappa geografica la distribuzione dei siti e delle attività e controllare documentazione, scadenze e stato di avanzamento. Dal punto di vista del committente, offre visibilità e trasparenza sui servizi ricevuti.

Il proprietario o gestore può verificare lo stato delle manutenzioni, accedere alla documentazione aggiornata, consultare i rapporti di intervento e monitorare anomalie e ticket. Può inoltre aprire direttamente una richiesta, seguirne la presa in carico e verificarne la chiusura. Questo approccio rende più efficace la collaborazione tra fornitore e cliente, perché le informazioni rilevanti sono raccolte in un unico ambiente digitale e condiviso.

Cube Service non è quindi soltanto uno strumento operativo per il tecnico manutentore, ma una piattaforma di governo dell'intero processo: dalla pianificazione alla gestione delle richieste, dall'esecuzione dei controlli alla produzione delle evidenze necessarie per supportare la compliance e la sicurezza del patrimonio immobiliare.

In che modo lo proponete sul mercato? In vendita o SaaS?

Attualmente Cube Service è venduto in formula on-premise, con possibilità di installazione anche in cloud. Il client è web e consente agli utenti di accedere alla piattaforma tramite browser.

Questa configurazione permette alle aziende di scegliere l'ambiente di installazione in base alle proprie esigenze informatiche e organizzative, mantenendo un'interfaccia di utilizzo accessibile via web.

Il valore di Cube Service non risiede soltanto nel software, ma nella disponibilità di un ecosistema digitale in continua evoluzione, capace di collegare ufficio, operatori sul campo e cliente e di supportare le esigenze operative, documentali e normative delle aziende del settore antincendio e della sicurezza.

Il rilascio della soluzione SaaS, che si aggiungerà alla proposta attuale, è previsto entro la fine del 2026.

Life₃

Contatto:
Life3 Srl
Tel. 045 485 25 29
info@life3.it

Dal varco al flusso: la gamma Magnetic® trasforma la sicurezza degli accessi

comunicato aziendale

Ci sono soluzioni che fanno della presenza fisica il loro principale punto di forza e altri che, al contrario, cercano quasi di scomparire nell'architettura. Alcuni devono resistere a milioni di passaggi e alle condizioni atmosferiche, altri devono accompagnare migliaia di passeggeri attraverso un aeroporto senza rallentare il percorso. È proprio questa varietà di situazioni a raccontare i prodotti **Magnetic®**, uno dei marchi di eccellenza del **gruppo FAAC Technologies**: una realtà specializzata nel controllo degli accessi con una gamma di soluzioni per gestire il passaggio delle persone in contesti molto diversi.

Entrata nel 2012 a far parte del **gruppo FAAC Technologies**, **Magnetic®** ha portato una competenza maturata in Germania nelle tecnologie per il controllo degli accessi. La sua gamma comprende soluzioni per la protezione perimetrale, il controllo degli accessi pedonali e la gestione dei flussi in contesti ad alta intensità di passaggio. Una proposta che trova applicazione nella logistica e nell'industria, negli aeroporti, negli edifici direzionali e nelle strutture aperte al pubblico.

Tornelli a tutta altezza: il primo filtro per l'accesso al perimetro

All'esterno degli edifici, il primo requisito è spesso la capacità di creare un filtro fisico efficace senza rallentare inutilmente chi è autorizzato a entrare. I **tornelli a tutta altezza MPT Magnetic®** rispondono a questa esigenza con una struttura pensata per il controllo degli accessi in spazi esterni e perimetri aziendali, anche in contesti caratterizzati da un'elevata frequenza di passaggio e condizioni ambientali impegnative.

Realizzati in acciaio zincato o, su richiesta, in acciaio inox, gli MPT sono disponibili in versione singola o doppia e sono progettati per arrivare a 10 milioni di cicli. A questa soluzione si affiancano: **MPG**, con anta battente e maggiore larghezza di passaggio, facilita l'accesso a persone con mobilità ridotta, il transito con materiali o bagagli; **MPB** è dedicato al passaggio di persone con biciclette, grazie a un varco specifico integrato nel tornello.



Sono soluzioni particolarmente adatte a perimetri aziendali, industriali e logistici, dove il tornello non rappresenta semplicemente un punto di passaggio, ma costituisce il primo livello di controllo tra l'area esterna e quella riservata.

Momentum®: la sicurezza che accompagna il viaggio

Se nel perimetro di un'azienda il varco deve soprattutto proteggere, in aeroporto deve anche accompagnare. È per questo scenario che **Magnetic®** ha sviluppato **Momentum®**, una famiglia di varchi per il controllo accessi nata per il settore aeroportuale e pensati per seguire il passeggero nelle diverse fasi del percorso: dai controlli pre-security alla dogana, fino all'imbarco e all'accesso alle lounge.

La gamma comprende **mPass**, per la verifica delle carte d'imbarco e dei dati biometrici nell'accesso alle aree di sicurezza; **mBorder**, sistema ABC per la verifica dell'identità attraverso documenti e dati biometrici; e **mGo**, varco di imbarco per la verifica del passeggero prima dell'accesso all'aeromobile.

La modularità è uno dei tratti distintivi del sistema **Momentum®**: i varchi possono essere configurati con lettori, sistemi biometrici e altri dispositivi, integrandosi con le architetture digitali e di sicurezza già presenti.

La famiglia **Momentum®** unisce quindi sicurezza, velocità e gestione dei flussi.



Un esempio concreto arriva dall'**Aeroporto d'Abruzzo**, dove la crescita del traffico passeggeri ha portato alla necessità di superare le verifiche manuali delle carte d'imbarco. I varchi **mPass Momentum®**, integrati con il Security Checkpoint di A-ICE, hanno automatizzato la validazione e introdotto regole precise per il controllo degli accessi all'area imbarchi. Il sistema verifica la carta, il passeggero e il volo, impedisce i duplicati e blocca automaticamente i tentativi fuori dalla finestra temporale prevista.

Anche all'**Aeroporto "Falcone e Borsellino" di Palermo** i **varchi ABC EasyGate**, sviluppati attraverso l'integrazione tra la tecnologia di accesso **Magnetic®** e il software biometrico **Secunet**, consentono di automatizzare il processo di verifica dell'identità del viaggiatore attraverso il controllo del documento elettronico e il riconoscimento biometrico del volto.

Il caso dei due scali italiani mostra bene una caratteristica della gamma **Momentum®**: la sicurezza non viene affidata a un singolo dispositivo, ma nasce dall'integrazione tra il varco, i sistemi informatici e le procedure operative dell'aeroporto.

FlowMotion®: quando il controllo accessi diventa parte dell'architettura

Negli edifici civili il rapporto tra sicurezza e accesso cambia ancora. Qui il varco deve controllare chi entra, ma anche inserirsi in spazi nei quali estetica, comfort e semplicità di utilizzo sono valori che vengono sempre più considerati. In questi casi entra in gioco **FlowMotion®**, la gamma di varchi pedonali motorizzati **Magnetic®**.

mTripod, **mWing** e **mSwing** condividono un'impostazione precisa: design essenziale, dimensioni contenute, illuminazione integrata, materiali resistenti e personalizzabili e in tutti i casi sicurezza e affidabilità garantite.

mTripod è un tornello a tripode progettato per il controllo degli accessi pedonali; **mWing** è il varco rapido con ante in vetro, pensato per garantire elevati flussi di passaggio e un'esperienza di transito veloce e senza contatto; **mSwing** disponibile con porta singola o doppia, è progettato per il passaggio di visitatori con bagagli, il trasporto di materiali e l'accesso di utenti a mobilità ridotta.

Dietro la leggerezza estetica c'è però una soluzione progettata per un utilizzo intensivo. I tre modelli possono raggiungere **10 milioni di cicli di apertura e chiusura**, utilizzano un'unica unità di controllo e possono essere collegati ai sistemi di supervisione dell'edificio. È inoltre possibile integrare tecnologie di terze parti, permettendo al varco di inserirsi nelle infrastrutture di sicurezza e building management già esistenti.

Alcune applicazioni raccontano bene questa filosofia. In contesti direzionali, ricettivi e pubblici, la gamma **FlowMotion®** consente di combinare il controllo degli accessi con un inserimento discreto e allo stesso tempo di impatto nell'architettura. È il caso, tra gli altri, del **Park Gallanti Holiday Village**, dell'accesso riservato al personale di due stabilimenti dell'azienda **IMA** e della residenza universitaria **Laude Living a Bologna**: esempi in cui i varchi **FlowMotion®** sono stati scelti per gestire gli ingressi integrando la tecnologia nel contesto architettonico.

FAAC

Contatti:
FAAC
www.faac.it

L'esperienza Vivaldi Group al servizio della sicurezza

comunicato aziendale

Quando si parla di sicurezza in caso di emergenza, la rapidità e la chiarezza delle comunicazioni possono fare la differenza. Per questo motivo i sistemi di evacuazione vocale EVAC hanno progressivamente sostituito i tradizionali impianti di allarme.

Un messaggio vocale chiaro, comprensibile ed immediato è infatti in grado di guidare le persone verso il comportamento corretto da adottare, riducendo il rischio di panico e aumentando l'efficacia delle procedure di evacuazione. Tuttavia, progettare un sistema EVAC realmente efficiente non significa semplicemente installare altoparlanti conformi alla normativa EN54. Per garantire che ogni messaggio venga compreso in modo chiaro e intelligibile, è necessario considerare numerosi fattori tecnici, tra cui la propagazione del suono, l'acustica degli ambienti, il rumore di fondo e le caratteristiche specifiche della struttura.

L'importanza dell'acustica nella progettazione EVAC

Uno degli errori più frequenti nella progettazione dei sistemi EVAC è sottovalutare la fisica del suono. Nella pratica progettuale si tende spesso a concentrarsi sul numero dei diffusori installati e sulla conformità dei componenti, trascurando l'effettiva intelligibilità dei messaggi vocali nelle aree servite.

Ogni ambiente presenta infatti caratteristiche acustiche differenti: spazi industriali, centri commerciali, edifici direzionali, strutture sanitarie, stazioni o aeroporti richiedono approcci progettuali specifici.

Un sistema correttamente dimensionato deve garantire che il messaggio di emergenza sia percepito e compreso in ogni punto dell'impianto, anche nelle condizioni più critiche.



L'esperienza Vivaldi al servizio della sicurezza

Da oltre cinquant'anni Vivaldi Group progetta e sviluppa soluzioni audio professionali, un know-how che rappresenta oggi un valore aggiunto nel settore dei sistemi EVAC. Le competenze aziendali non riguardano solamente la produzione di elettroniche e diffusori certificati, ma si estendono alla progettazione completa di impianti di evacuazione vocale per strutture di ogni dimensione, dai piccoli edifici fino ai grandi complessi multi-sito.

Soluzioni EVAC progettate per crescere nel tempo

Le esigenze di una struttura possono evolversi nel corso degli anni. Per questo motivo i sistemi EVAC Vivaldi sono pensati per offrire la massima flessibilità e scalabilità. La gamma comprende sia soluzioni compatte all-in-one sia sistemi modulari a rack, entrambi progettati per essere ampliate successivamente all'installazione iniziale.

Funzionalità di networking

Più sistemi possono essere collegati e integrati tra loro, tramite la rete, anello aperto o anello chiuso.

Espandibilità

I sistemi Vivaldi sono espandibili, linkando più centrali, fino a 32, consentendo una crescita graduale dell'impianto. Un ulteriore vantaggio è rappresentato dalla possibilità di integrare sorgenti audio multimediali esterne (55.000 web radio, Spotify, Airplay, Bluetooth...), gestibili tramite App e configurabili in modo indipendente per ciascuna zona. Ciò permette di utilizzare l'impianto non solo per le comunicazioni di emergenza, ma anche per la diffusione

sonora, la musica di sottofondo e gli annunci di servizio, mantenendo sempre la massima priorità alle funzioni di sicurezza.

Molto più di un sistema EVAC

Scegliere Vivaldi significa affidarsi a un partner che conosce il mondo dell'audio a 360 gradi. Perché la sicurezza non dipende soltanto dalla presenza di un impianto, ma dalla certezza che il messaggio giusto venga ascoltato e compreso nel momento più importante. Vivaldi mette questa competenza al servizio di ogni progetto, trasformando l'evacuazione vocale in un vero strumento di protezione delle persone e delle strutture, da oltre 50 anni.

VIVALDI

Contatti:
Vivaldi srl
Tel. +39 0421 307825
info@vivaldigroup.it

Partner

AIMA
www.aismasrl.it
Il copertina, 14-15

COOPSERVICE
www.vigilanzacoopservice.it
5

CYBERLOOP BY CITTADINI DELL'ORDINE
https://cyberloop.it - www.cittadinidellordine.com
I romana, 16-17

ERMES S.R.L.
www.ermes-online.it
25

FAAC
www.faac.it
20-21

INIM ELECTRONICS S.R.L.
www.inim.biz
IV copertina

LIFE 3 S.R.L.
www.life3.it
2, 18-19

URMET-ATE S.R.L.
www.urmet-ate.it
9

VIVALDI S.R.L.
www.vivaldigroup.it
22-23

essecome
ONLINE

n. 04/2026
Anno XLVI
Periodico fondato da Paolo Tura

**DIRETTORE RESPONSABILE E
COORDINAMENTO EDITORIALE**
Raffaello Juvara
editor@securindex.com

**HA COLLABORATO
A QUESTO NUMERO**
Francesco Hemmeler

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

ERMES: L'EVOLUZIONE DELLA SICUREZZA FISICA E LOGICA IN AZIENDA

Proteggi i tuoi dati fino alla fine. Compliance GDPR garantita.



La sicurezza aziendale non si ferma agli accessi. Elimina in modo definitivo e irrecuperabile i dati sensibili a fine ciclo di vita.



DISTRUZIONE FISICA

Distruggi documenti professionali Depei ad alta sicurezza, progettati per tritare carta, card in PVC e supporti ottici.



CANCELLAZIONE MAGNETICA

Degausser certificati in grado di smagnetizzare istantaneamente hard disk e nastri, rendendo i dati completamente illeggibili.



CONFORMITÀ TOTALE

Soluzioni hardware essenziali per garantire il pieno rispetto delle normative GDPR e proteggersi da potenziali data-breach.

info@ermes-online.it

www.ermes-online.it

051 757040





PrimeX InVista

Sicurezza totale, controllo assoluto.

Con l'ecosistema Inim puoi offrire ai tuoi clienti una soluzione completa per la gestione intelligente e integrata dei loro spazi.

La centrale di allarme **PrimeX** combina antintrusione e domotica in un'unica centrale evoluta, mentre **InVista** completa il sistema con una videosorveglianza affidabile e intelligente.

Attraverso l'app **Inim Home**, l'utente può gestire la sicurezza, visualizzare le telecamere e controllare le automazioni, anche da remoto. **Allarme, videosorveglianza e domotica: un unico ecosistema da installare, configurare e proporre ai tuoi clienti.**