essecome ONLINE 01/19

Periodico digitale di informazione di security & safety

2019 · ANNO XXXIX

ASSOVALORI

I SEMINARI DI ESSECOME

NORMATIVA ANTIRICICLAGGIO E ISTITUTI DI VIGILANZA COME NUOVI GESTORI DEL CONTANTE

Gli obblighi per i soggetti di cui all'articolo 134 del Testo unico di pubblica sicurezza

27 FEBBRAIO 2019 - ROMA

ROME MARRIOT GRAND HOTEL FLORA

Il Seminario, organizzato da **ASSOVALORI** con il patrocinio di **ANIVP - ASSIV - FEDERSICUREZZA - LEGACOOP** e la collaborazione di **essecome-securindex**, rappresenta un'importante occasione di approfondimento sugli obblighi e gli adempimenti specifici per i soggetti disciplinati dall'art. **134 del TULPS** (istituti di vigilanza privata) e dall'**Albo dei gestori del contante** istituito dalla Banca d'Italia.

ASSOVALORI

ANIVP · ASSIV · FederSicurezza · legacoop PRODUZIONE & SERVIZI

L’editoriale del direttore

Immigrazione, mafie e cosa non si deve dimenticare

1. Nella particolare e delicata fase che il Paese sta attraversando in questi mesi, l’attenzione del pubblico viene indirizzata verso un argomento di portata epocale, collegandolo sapientemente al tema sempre verde della sicurezza: l’immigrazione. Diminuita la spinta emotiva della paura dei furti e delle rapine per la diminuzione dei reati certificata dalle fonti ufficiali (ISTAT, ministero dell’Interno), era necessario per la politica e l’informazione trovare altri argomenti che continuassero a toccare il tasto della “insicurezza percepita” che, come tutti sanno, è un formidabile generatore di like e consensi elettorali in ogni stagione. In particolare, quando serve deviare l’attenzione degli elettori da argomenti forse più banali ma più critici per chi governa, come la possibilità di trovare lavoro, di avere il mutuo per la casa, di contare su ospedali, scuole e trasporti pubblici che funzionino eccetera.
Non a caso, l’immigrazione è da anni al centro di campagne ossessive di quanti vedono nello “straniero”, specie se di pelle nera, un pericolo “a prescindere” per l’ordine pubblico e l’incolumità delle persone a casa nostra.
Pertanto, l’immigrato (meglio se nero) è diventato proprio malgrado un eccellente influencer per il tema della sicurezza, un tema che porta sempre voti.

2. Sono appena cessati gli allarmi per le infiltrazioni di pericolosi terroristi jihadisti tra le persone in arrivo in Europa sui barconi o nei container, dopo che ci si è accorti che tutti gli attentati di matrice islamista avvenuti in Europa negli ultimi anni sono stati commessi da persone nate in Europa o che ci risiedono da anni, non da poveri disgraziati che affrontano pericoli (per noi) inconcepibili per rincorrere una speranza di sopravvivenza.
Ma, dato che l’obiettivo è quello di non avere immigrati (neri) nel nostro cortile, ora si dice che il problema dev’essere affrontato alla radice, investendo nei paesi sub-sahariani per convincere quella gente a non venire in Europa, come se a guerre, fame e siccità si possa rispondere con qualche fabbrichetta che finga di produrre qualcosa in quei paesi e per quelle persone, dimenticando che non si è riusciti e non si riesce farlo nemmeno nelle nostre regioni meridionali.
Dimenticando che le opulente monarchie dei secoli passati, dalle quali sono derivati i moderni Stati europei, hanno deportato milioni di persone (nere) di quegli stessi paesi, riducendole con la forza in schiavitù per sfruttare altri territori oltre mare, di cui si erano nel frattempo impossessate sterminando chi ci era nato.

Dimenticando che dall’inizio dell’era industriale le ricchezze naturali di quei paesi sono state sistematicamente depredate da quegli stessi Stati europei che adesso chiudono porti e frontiere nell’illusione di fermare un esodo di portata biblica e trattano come appestati gli abitanti di quegli stessi paesi che ora vengono a chiederci di lavorare nel nostro cortile per non morire di fame.
Dimenticando ancora che la società europea (ed italiana in particolare) sta invecchiando sempre più e, se non si accolgono e si integrano velocemente nuovi cittadini, l’abbandono di città e campagne che già sta avvenendo nel nostro sud si estenderà alle altre regioni italiane. E allora, nei prossimi anni, chi assisterà i vecchi e gli ammalati e lavorerà nelle fabbriche delle ricche regioni del nostro nord che hanno un PIL che neanche la Baviera?

3. Dimenticando infine (o facendo finta di dimenticare) che le persone (nere, bianche, rosse o gialle) che arrivano in un modo o nell’altro nel nostro paese devono venire accolte nel rispetto della loro dignità umana. Non solo per pulsioni etiche o appartenenze religiose, ma anche per un preciso interesse di sicurezza.
Il Procuratore nazionale antimafia e antiterrorismo Franco Roberti e il fondatore di Abele e di Libera don Luigi Ciotti, che ben conoscono la situazione, stanno lanciando lo stesso allarme in ogni occasione utile: gli immigrati stipati nei centri di accoglienza in condizioni miserabili, senza alcuna prospettiva (e speranza) di integrazione, diventano bacini di reclutamento per le mafie locali e per quelle straniere, interessate non ai piccoli reati predatori che spaventano la gente, ma ai mercati della prostituzione e della droga, ben più lucrosi e meno percepiti come allarme sociale.

4. Allora, invece di trattare gli immigrati come se fossero colpevoli di qualche reato prima ancora che mettano piede nel nostro cortile ed invece di fantasticare su improbabili soluzioni per arrestare un fenomeno epocale, non sarebbe opportuno per la nostra dignità, utile per la nostra sicurezza ed intelligente per il nostro futuro accoglierli in modo decoroso, cercando di integrarli nel modo migliore nella nostra civiltà, lei che millenaria lo è per davvero proprio grazie alle contaminazioni che ha ricevuto nel tempo?

Sommario Interattivo

CLICCA SULL'ICONA PER SCARICARE L'ARTICOLO CHE TI INTERESSA

Le priorità del Governo per la sicurezza del sistema Paese

intervista all'on. Angelo Tofalo - Sottosegretario alla Difesa | a cura di Raffaello Juvara

Al convegno "Mediterraneo. Città e società sicure" del 30 gennaio scorso lei ha confermato la sua attenzione per il mondo della sicurezza privata come partner dello Stato sia per garantire la sicurezza sul territorio nazionale che per contribuire alla tutela delle imprese italiane che operano in scenari internazionali complessi. Quali sono i punti principali che intende realizzare e con quali tempistiche?
Il tema della sicurezza è priorità del Governo. Un argomento di primissima importanza che non coinvolge solo il Ministero della Difesa bensì tutti i Dicasteri impegnati a orientare i propri sforzi verso un'azione comune in grado di rendere più sicuro il Paese. È forte l'esigenza di favorire una integrazione organica tra tutti quei soggetti che, a vario titolo, interagiscono per la sicurezza del sistema Paese. A questo proposito, si sta lavorando allo sviluppo di protocolli per scambi tra gli attori pubblici e privati che operano nel settore della sicurezza. Ci stiamo dirigendo verso la creazione di un'unica rete che operi sinergicamente al fine di prevenire e meglio rispondere alle complesse e numerose minacce che caratterizzano l'odierno scenario nazionale e globale.

Sono stati accennati provvedimenti per la defiscalizzazione dei costi per la sicurezza. Può anticiparci i contenuti?
La sicurezza, a ogni livello e in ogni settore, deve essere considerata un bene comune, un investimento per le aziende, per le amministrazioni pubbliche e per il Paese, non un costo. L'azione del Governo è volta a colmare l'attuale vuoto normativo e promuovere una defiscalizzazione dei costi. La sicurezza cibernetica in primis. Servono provvedimenti specifici che consentano di rafforzare la partnership tra pubblico e privato. A questi progetti sto lavorando con grande impegno, intervenendo su più tavoli e coinvolgendo il settore dell'industria, quello accademico e il mondo istituzionale.

In che modo si potrà formalizzare il ruolo dei responsabili della sicurezza delle imprese che operano in settori sensibili per gli interessi nazionali, per dare maggiore efficacia alla collaborazione tra lo Stato e i privati?
Riconoscendone il ruolo all'interno del Sistema Paese Italia attraverso azioni governative concrete, ossia iniziando un processo di interconnessione fra lo Stato e le strutture di Security aziendali. Condivisione e trasparenza, dunque, dovrebbero essere le parole d'ordine nel nostro futuro. Un ruolo istituzionalmente riconosciuto della figura del Security Manager potrebbe portare al Paese stesso un contributo importante in termini di sicurezza.

In tale ottica, al convegno "Mediterraneo. Città e società sicure" così come in tante altre occasioni, ho voluto lanciare l'appello per un reciproco impegno volto a costruire insieme il Sistema Paese e rafforzare la sicurezza delle nostre comunità. Ho invitato pertanto i Security Manager a operare proposte costruttive e concrete di collaborazione e condivisione informativa, al fine di stimolarne una possibile e rapida discussione parlamentare.

È possibile prevedere provvedimenti per consentire l'attività di soggetti privati organizzati per tutelare le imprese italiane all'estero, sullo schema dei "contractor" stranieri ai quali oggi sono costrette a rivolgersi con costi elevati e talvolta con palesi conflitti di interesse dei rispettivi Paesi di origine con quelli dell'Italia?
E' un tema all'attenzione del Governo. Come ho già detto, in Italia si fa sentire la necessità di mettere mano a un vuoto normativo, quello relativo alla figura dei cosiddetti contractor. Bisogna fare una legge che ne regolamenti il settore. A tal proposito è necessario prestare molta attenzione a scrivere bene il piano normativo. Sono due gli aspetti su cui ragionare: un mercato che potenzialmente si aggira oltre 250 miliardi, dal quale l'Italia è tagliata fuori e dove, a mio avviso, potrebbe e dovrebbe entrare, e dall'altra parte la necessità di tutelare informazioni sensibili per il nostro Paese.

Il ruolo della Security Aziendale nell'ecosistema di sicurezza del Paese. La posizione di AIPSA

intervista ad Andrea Chittaro - presidente AIPSA | a cura di Raffaello Juvara

A che punto è arrivato il progetto di istituzionalizzare la figura dei security manager delle aziende con attività sensibili per la sicurezza del Paese?
La discussione è aperta su diversi fronti ed ha investito direttamente il decisore politico, L'occasione offerta dal recente convegno "Mediterraneo, Società e Città Sicure" di rappresentare nuovamente ai sottosegretari all'interno Stefano Candiani ed alla Difesa Angelo Tofalo un'esigenza che si evidenzia sempre più pressante nel quadro della costruzione dell'ecosistema di sicurezza del paese, è stata puntualmente colta da AIPSA. Le Istituzioni si stanno muovendo e diverse iniziative concrete sono state avviate. Sarà opportuno, ora, riunirle in uno strumento normativo o amministrativo che sancisca la validità di un modello di partenariato pubblico-privato che veda le Direzioni di Security Aziendale come interlocutore formalmente riconosciuto per tutte le tematiche di competenza, a cominciare proprio dalla Cyber Security. Penso alle grandi opportunità che ne deriverebbero, anche in termini occupazionali.

Quali sono i punti cardine del progetto?
Ancora non sono in grado di anticipare termini esatti e struttura, il confronto è in atto ma speriamo di poter presto ottenere qualche primo risultato tangibile.

Secondo lei, come evolveranno nei prossimi anni i compiti dei security manager?
Nella stessa direzione in cui si è da tempo avviata l'evoluzione dei modelli organizzativi e funzionali della sicurezza in azienda. Il termine "manager" prevarrà sempre di più su quello "security" nel quadro di assetti che uniranno domini e competenze verticali sotto un'unica "casa madre". Chi avrà la responsabilità di tali strutture dovrà essere percepito come un abilitatore del business senza, però, mai perdere di vista lo "spirito di servizio" verso tutte le altre funzioni aziendali, che dovrà rimanere un valore fondante.

E come cambieranno i loro profili? La provenienza dalle Forze dell'Ordine continuerà ad essere una credenziale privilegiata o prevarranno altri percorsi formativi?
Come AIPSA abbiamo da poco lanciato un programma denominato "next generation" dedicato agli under 30 della nostra community. Il futuro sono loro, hanno le provenienze accademiche e di studio più disparate, li unisce la passione per la sicurezza aziendale. È dovere di chi, come me, ha qualche anno in più favorire il loro progressivo avvicinamento alla professione e costruire percorsi formativi e di carriera ad hoc. Per ambire ai ruoli di vertice, ci si dovrà confrontare sulle competenze più che sulle provenienze. È un terreno sul quale c'è da lavorare molto. Ma, assieme al tema della diversity, quello dei giovani è in cima alle nostre priorità.

Aumento del PIL, tutela del know-how italiano, impiego degli ex militari: i vantaggi di avere PMSC italiane

intervista a Umberto Saccone - Presidente IFI Advisory | a cura di Raffaello Juvara

Il Sottosegretario alla Difesa on. Tofalo ha confermato, in un'intervista concessa a essecome lo scorso 5 febbraio (leggi) che il Governo è interessato a regolamentare il settore dei contractor per la sicurezza delle nostre aziende all'estero e, quindi, per tutelare informazioni sensibili per l'Italia. Quali sono gli aspetti principali che, secondo lei, dovrebbero venir regolamentati per consentire lo sviluppo di operatori italiani in grado di competere con le grandi organizzazioni internazionali che lavorano da anni in tutto il mondo?

Il sottosegretario Tofalo ha mostrato una particolare sensibilità ai temi della sicurezza. Dobbiamo pertanto dargli atto dell'impegno, con la speranza che riesca coinvolgere quegli attori pubblici e privati che siano in grado di offrire una corretta visione sullo stato delle cose. Una cabina di regia con la quale il governo possa integrare visione, programmazione, coordinamento e azione concreta. Il tema della sicurezza è un tema multiforme, che va esplorato nel suo complesso. La questione dei rischi globali non è solo teorica, ma impatta direttamente sull'economia degli stati, sulle imprese e sul funzionamento del sistema paese ed è in quest'ottica che dobbiamo affrontare il tema.

Le relazioni pubblico privato in Italia non funzionano.

È oramai accertato che la gestione delle questioni geopolitiche planetarie necessita di una profonda sinergia istituzioni-privati per governare eventi eccezionali.

Pertanto, affrontiamo per prima cosa il problema delle relazioni pubblico-privato. Ritengo che il binomio stato-aziende rafforzato da una partnership strutturata possa assicurare una tutela allargata all'intero sistema paese.

Se le imprese vengono danneggiate da atti di terrorismo, attività spionistiche, sabotaggi, frodi, furti, eccetera, non è solo "l'ente economico" ad essere danneggiato, ma l'intera comunità.

In quest'ottica, mettiamo ordine alle nostre riflessioni secondo un programma strutturato che tratti in un unico grande progetto la partnership pubblico privato, la sicurezza dei lavoratori, la vigilanza privata, i contractors, gli oneri per la sicurezza e, ultimo ma non ultimo, il tema dei diritti umani, evitando iniziative a macchia di leopardo che, di fatto, generano solo confusione e non soddisfano il requisito.

In un mercato globale valutato in 250 miliardi di dollari, quanto pagano ogni anno le aziende italiane alle organizzazioni straniere per proteggere i propri dipendenti e le infrastrutture all'estero, in particolare nei teatri con elevati fattori di rischio?

Sono circa 25.000 le imprese controllate da multinazionali italiane presenti in più di 170 paesi, che impiegano quasi 1,8 milioni di addetti. Se lei pensa che, per proteggere in aree critiche le proprie persone e i propri asset, un'azienda multinazionale può spendere qualche decina di milioni l'anno, non ho difficoltà a rispondere che vengano pagati nell'insieme alcuni miliardi di dollari. Soldi che spendiamo a vantaggio di società di sicurezza straniere.

Il paradosso sta nel fatto che il legislatore obbliga le aziende a proteggere le proprie persone (*duty of care*) ma non gli concede gli strumenti per farlo senza doversi avvalere di società straniere, mettendo così a rischio il proprio know-how.

Il 22 giugno 2018 è entrato in vigore il Decreto Legislativo n. 63/2018, che ha attuato in Italia la Direttiva UE n. 943/2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti; è fondamentale però che le aziende siano in grado di dimostrare di aver adottato misure adeguate per proteggere la segretezza delle informazione stesse per poter accedere alle misure previste dal legislatore.

Come si può vedere, è una contraddizione in termini. Nell'ipotesi in cui il datore di lavoro non abbia garantito (anche all'estero, per l'universalità della legge penale) la piena conformità delle proprie misure di sicurezza ai requisiti normativi, in caso di eventi critici si espone a sanzioni amministrative, condanne al risarcimento civile e al danno di immagine che l'azienda può subire, senza contare le responsabilità penali per le figure di vertice coinvolte.

Le conseguenze assumono rilievo penale (senza contare le cause risarcitorie in sede civile) per l'imprenditore, qualora un dipendente muoia o rimanga gravemente ferito a seguito di una negligenza del datore di lavoro nel valutare e mitigare correttamente il rischio di security.

Tra le prime disposizioni in merito di sicurezza si trova l'articolo 2087 del codice civile, che impone all'imprenditore di adottare le misure ritenute necessarie alla tutela dei lavoratori dai rischi per la loro sicurezza. Tale obbligo generale è completato da due norme che rappresentano oggi il paradigma di riferimento in tema di protezione e tutela dei lavoratori: il D.lgs n. 81/2008 (Testo Unico Sicurezza) ed il D.lgs n. 231/2001.

Il Testo Unico all'art. 28 stabilisce che il datore di lavoro, nel Documento di Valutazione dei Rischi, deve considerare tutti i rischi "compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari".

Inoltre, l'art. 30 dello stesso Testo Unico richiama esplicitamente all'implementazione di un modello di organizzazione, gestione e controllo quale esimente ai fini della responsabilità amministrativa di cui al D.Lgs. n. 231/2001, che si va a cumulare con la responsabilità penale delle persone fisiche che materialmente hanno commesso l'illecito, purché quest'ultimo sia stato compiuto nell'interesse o vantaggio dell'ente stesso.

L'art. 25 septies del D.Lgs. 231/01 ha poi esteso la responsabilità amministrativa degli enti anche alle fattispecie di omicidio o lesioni colpose. Tutto questo nel tentativo di dimostrare che il tema deve essere trattato in forma collettivistica, nella

consapevolezza che la proprietà di un sistema non può essere spiegata esclusivamente tramite le sue singole componenti in quanto, dal punto di vista "olistico", la sommatoria funzionale delle parti è sempre maggiore della somma delle prestazioni delle parti prese singolarmente.

Da quali paesi provengono i principali contractor internazionali? Quali sono gli skill individuali degli agenti e come vengono addestrati?

A partire dalla fine della Guerra Fredda il mercato dei servizi militari e di sicurezza erogati da entità private ha sperimentato una crescita senza precedenti, in netta controtendenza rispetto all'andamento economico globale. Analizzando l'andamento della domanda di servizi di sicurezza privati prima e dopo la crisi economico-finanziaria del 2008, è possibile notare come il mercato della sicurezza non solo non abbia risentito degli effetti della recessione, ma sia addirittura cresciuto. Secondo le attuali stime il tasso di crescita spingerà la domanda del mercato della sicurezza a superare i 250 miliardi di dollari nei prossimi anni.

La tendenza a esternalizzare funzioni legate alla sicurezza, fino a questo momento di esclusiva competenza dello Stato, si sta rapidamente diffondendo su scala globale sull'esempio dei Paesi occidentali più sviluppati quali Stati Uniti e Regno Unito, in cui il fenomeno ha avuto origine.

Sebbene le stime prevedano che la domanda più consistente continuerà a provenire dal Nord America, la crescita sarà guidata dai Paesi emergenti di Asia, Europa Orientale, Africa e Medio Oriente, in cui il mercato della sicurezza è ancora relativamente poco sviluppato. In particolare, saranno Cina, India, Russia, Sudafrica e Messico a poter vantare una crescita a due cifre.

Di contro, non vi sono società italiane che operano in questo delicato ed importante settore.

Pertanto, considerando che gran parte delle attività lavorative delle imprese italiane si svolge in tutto o in parte fuori dal territorio nazionale, la maggioranza delle nostre aziende operanti all'estero è costretta a ricorrere a compagnie straniere la cui legislazione nazionale prevede la figura professionale del security contractor.
Sull'ultimo punto le rispondo in maniera sintetica, atteso che un piano di sicurezza ha una sua complessità che difficilmente può essere contenuta in una risposta non strutturata. Una società di contractor deve avere la capacità di rispondere ad attacchi complessi, poter gestire ordigni inesplosi, saper mettere in sicurezza basi ed alloggi secondo i migliori standard internazionali. Deve essere in grado di avere in ogni nazione un sistema di meet and greet valido per la gestione dei clienti dall'arrivo all'aeroporto sino ai luoghi sicuri con un dispositivo di sicurezza idoneo all'intensità della minaccia. Saper effettuare la ricognizione dei luoghi per operare evacuazioni in sicurezza e saper valutare le opzioni di estrazione più efficaci (terra, mare, cielo). Avere idonei piani anti-rapimento ed essere in grado di supportare la società con team di negoziazione in caso di sequestro. Saper gestire unità di crisi e avere le competenze per adeguare i propri piani agli standard HSE (Health, Safety and Environment) della società. Avere una valida politica di sostenibilità delle proprie operazioni con riguardo alle comunità locali. Essere in grado di operare coerentemente alle linee guida relative ai Voluntary Principles on Security and Human Rights (VPs) volte a far sì che l'esigenza di garantire la sicurezza sia sempre soddisfatta in maniera compatibile con il rispetto dei diritti umani e delle libertà fondamentali. Avere una struttura di intelligence in grado di acquisire informazioni sul territorio per prevenire attività ostili.

Quali potrebbero essere i contesti di provenienza dei contractor italiani e dei loro agenti per poter garantire alle aziende utilizzatrici un adeguato livello di efficienza?
La presenza di cittadini italiani tra le fila dei contractor privati è venuta alla luce solo in seguito al rapimento, da parte delle Falangi Verdi di Maometto, di Salvatore Stefio, Maurizio Agliana, Umberto Cupertino ed al brutale assassinio di Fabrizio Quattrocchi.
La stampa italiana bollò frettolosamente i quattro come mercenari, etichettando allo stesso modo anche il resto degli operatori del settore, dimostrando di non avere ancora piena coscienza del ruolo dei contractor e della portata del settore privato. Su questo tema l'AG italiana applicò le previsioni dell'Art. 288 del CP relativo all'arruolamento o armamento non autorizzato a servizio di uno Stato estero, che non trovò riscontro in sede dibattimentale.

Sino ad ora, a parte il disegno di legge d'iniziativa del senatore Mario Mauro nessuna iniziativa è stata presa dal Parlamento.
Oggi, con la trasformazione delle Forze Armate italiane da un esercito di leva ad uno professionale iniziata alla fine degli anni 90, troviamo sul mercato della sicurezza privata ex militari qualificati ai massimi livelli mondiali. Negli ultimi vent'anni, infatti, i nostri uomini e donne con le stellette hanno acquisito esperienze preziose e uniche in tutti i teatri operativi più impegnativi del mondo, riscuotendo ovunque stima e altissima considerazione e inventando nuove e più efficaci dottrine operative, basate sul consenso e sul rispetto dei diritti umani.
Il volontario in ferma prefissata (VFP4) che presta servizio per quattro anni nell'Esercito, Marina, Aeronautica potrebbe, al termine della ferma trovare una giusta collocazione nel mondo della sicurezza. La creazione quindi di una PMSC (Private Military and Security Company) italiana risponderebbe contemporaneamente ad almeno tre sentite ed importanti esigenze.
Una limitazione dell'uscita dall'Italia di ingenti risorse economiche per pagare la sicurezza privata all'estero delle nostre aziende di punta.
Una maggior garanzia per la protezione delle nostre politiche aziendali, dei nostri progetti, delle nostre idee, delle nostre tecnologie che verrebbero tutelate da operatori della sicurezza italiani di provata affidabilità e di grande professionalità.
Infine l'ultima, la più importante, un reimpiego professionale e specialistico di tanti nostri ex militari che, altrimenti, continuerebbero ad ingrossare la già numerosa schiera dei disoccupati. Pertanto sentiamo l'esigenza di proposte innovative in tal senso e, laddove dette proposte si traducessero in norme adeguate, l'Italia potrebbe addirittura ambire ad affermarsi come modello di riferimento a livello europeo.

Una PMSC italiana sarebbe così in grado di fornire prodotti di sicurezza di altissimo profilo in ogni parte del mondo con l'affidabilità, la legittimità e la professionalità garantite da un sistema integrato totalmente italiano in linea con gli interessi strategici nazionali. Allo stato attuale, di fatto, è assente una normativa specifica sulla materia, con l'unica parziale eccezione data dal servizio di antipirateria marittima, svolto da istituti di vigilanza autorizzati, come regolato dall'articolo 5 del decreto-legge 12 luglio 2011, n. 107, convertito, con modificazioni, dalla legge 2 agosto 2011, n. 130.

Ritiene possibile ed opportuno un coinvolgimento degli istituti di vigilanza disciplinati dall'art. 134 del TULPS per sviluppare unità operative con le caratteristiche necessarie?
L'attività di impresa è un'attività economica organizzata e destinata alla produzione di beni o servizi. Non posso quindi escludere che anche gli istituti di vigilanza possano fare un ulteriore passo in avanti assicurando idonee cornici di sicurezza alle imprese private italiane che operano in aree a rischio. Tale possibilità offrirebbe un vantaggio competitivo al nostro «sistema Paese», rispondendo a molteplici e diversificate esigenze.
Innanzitutto, da un punto di vista prettamente economico, incoraggiare lo sviluppo di un mercato della sicurezza privata porterebbe nuove risorse all'erario grazie alla limitazione dell'uscita dal Paese di ingenti risorse economiche utilizzate dalle nostre aziende di punta per pagare la sicurezza privata all'estero.
In secondo luogo, data l'esigenza determinata dalla crisi economica di ridurre le spese militari e quindi il numero delle nostre Forze armate, uno sviluppo in tal senso permetterebbe, come ho detto, l'impiego di quel personale che, già formato a spese dei contribuenti, troverebbe quale naturale sbocco professionale l'impiego in attività di sicurezza privata ad alta qualificazione.
L'impiego di personale italiano costituirebbe, inoltre, una maggiore garanzia di controllo dei flussi informativi ai fini della protezione delle politiche e degli asset aziendali rispetto all'impiego di personale straniero. Il settore della sicurezza ha infatti forti legami con la tutela delle aree strategiche e della protezione degli interessi collettivi. In tale contesto, la contrapposizione fra l'interesse privato della società di sicurezza straniera e l'interesse della tutela della riservatezza degli interessi nazionali delle nostre aziende è un elemento della massima importanza che deve essere tenuto nella dovuta considerazione.
Unica preoccupazione sarebbe la reale capacità di investimento che una società di vigilanza può mettere in campo per soddisfare le richieste di un mercato milionario, dove risorse specializzate, mezzi tecnologici di primario standing (centrali operative, mezzi di comunicazione, macchine blindate, armamento, mezzi di protezione personale) rappresentano costi enormi che necessitano di investimenti importanti.

Antiriciclaggio, gli obiettivi del seminario di Assovalori del 27 febbraio

intervista ad Antonio Staino, presidente Assovalori

Presidente Staino, quali sono gli obiettivi del seminario del 27 febbraio che ha organizzato Assovalori?
Assovalori, associazione che da sempre si occupa delle attività legate al trasporto ed al ricircolo del denaro, ha fortemente voluto questo seminario con l'obiettivo di informare gli operatori degli impegni che li attendono con l'entrata in vigore delle direttive emanate da Banca d'Italia per i gestori del contante, in modo particolare in materia di antiriciclaggio e sulle prossime disposizioni per l'iscrizione e la gestione dell'elenco per gli operatori non finanziari nonché sulla organizzazione, procedure e controlli.

A chi è rivolto?
Senza dubbio alcuno è rivolto agli operatori ex 134 TULPS che svolgono o vorranno svolgere attività di trasporto, scorta, ricircolo del contante e custodia dei valori e all'intera filiera legata a tale attività, quali software house, studi professionali e consulenti per la legge 231, produttori e rivenditori di apparecchiature per il trattamento del denaro, oltre che **Network titolari di 115, Banche e GdO.** Questi ultimi tre soggetti non possono essere esclusi ma dettagliatamente informati e formati sulle norme che cambiano e gli obblighi che avranno nei confronti dei gestori del contante quali puntualità, precisione e rapidità nel fornire informazioni e documenti che vengono loro richiesti per essere conformi. Insomma le richieste rivolte non dovranno essere vissute come invasione nella loro privacy o appesantimento burocratico ma semplicemente quale supporto che gli viene fornito ***(e per il quale dovrà essere riconosciuto il giusto compenso)*** per continuare a loro volta a gestire in tranquillità il loro business.

Cosa chiederete ai rappresentanti delle istituzioni che avete invitato?
I rappresentanti delle Istituzioni non sono stati invitati con la volontà di rivolgere loro delle richieste, ma per far conoscere le difficoltà che abbiamo affrontato, il lavoro e gli sforzi fatti dalla categoria per adempiere agli obblighi che la normativa ci impone, con il conseguente aumento del costo della prestazione erogata al quale l'intero comparto dovrà reclamare e conseguentemente farsi riconoscere dalla clientela.

Qual è il significato dei patrocini delle associazioni della vigilanza, in questo momento?
Rispondo a questa domanda con soddisfazione ed orgoglio, in quanto già nel 2010 auspicavo la piena collaborazione di tutto il comparto, quindi spero sia solo l'inizio del percorso. Il lavoro comune fatto per la redazione delle linee guida sull'adeguata verifica, la sottoscrizione e la presentazione congiunta con tutte le associazioni è stato il primo passo che ci porta oggi ad un evento condiviso e di interesse comune, il solco è tracciato ed auguro quindi si prosegua sugli altri temi.

Come i sistemi di sicurezza partecipano all'evoluzione degli edifici "intelligenti" e alla loro valorizzazione

di Stefano Bellintani, docente Politecnico di Milano e membro della giuria del Premio H'oro

I sistemi di sicurezza partecipano all'evoluzione degli edifici "intelligenti" nella misura in cui sono in grado di correlarsi con le nuove frontiere delle applicazioni digitali, ovvero con il mondo dell'Internet delle cose, meglio conosciuto come IoT o Internet of Things. In altre parole, con il mondo dei Big Data e le varie declinazioni che ne derivano alle diverse scale: dalla cosiddetta "smart city", includendo il tema di grande attualità della città resiliente, fino al singolo edificio e viceversa.

Procedendo con ordine, comincerei col dire che l'Internet delle cose altro non è che una evoluzione dell'uso della Rete, in cui oggetti qualsiasi, ossia le "cose", si rendono riconoscibili e acquisiscono "intelligenza" grazie al fatto di poter comunicare i dati che li riguardano e di accedere a informazioni opportunamente aggregate da parte di altri strumenti "intelligenti".

In un certo senso, si tratta di qualcosa di non molto dissimile da ciò che accade proprio all'interno di un edificio "intelligente": sensori e relativi attuatori che fanno riferimento a un sistema di supervisione e controllo che assicura l'integrazione funzionale. Potremmo dire, in altri termini, che si tratta di una trasposizione concettuale: dall'ambito della Local Area Network a reti territoriali che si spingono fino a quella globale.

Gli IoT rimandano, cioè, a congegni con capacità di rivelazione di dati che vengono inviati con continuità direttamente tramite web e in tempo reale, ad appositi centri di elaborazione.

Questi congegni non si discostano molto dai normali sensori che già conosciamo; la differenza sta nel fatto che, nel caso dell'Internet of Things, il focus si concentra sul valore del dato raccolto; un dato che, utilmente correlato con dati rilevati in contesti apparentemente poco coerenti col primo, può generare informazioni molto utili, ossia fruibili nei campi più disparati.

Nel futuro delle "Cose connesse", i numeri fanno impressione: miliardi di sensori per milioni di miliardi di dati.

Secondo uno studio di Cisco Systems, nel 2020 saranno installati nel mondo fino a 50 trilioni di sensori che collegheranno oggetti di ogni tipo a Internet.

Ancora maggiore, in parallelo, sarà la crescita di dati provenienti da qualsiasi altra fonte e pur sempre riferibili al web; in primis, quelli che giungono dai cosiddetti social. Tutti dati tendenzialmente georeferenziati che, se opportunamente correlati, possono generare informazioni utili per contesti di ogni genere.

Ne deriva che le città e, più in generale, l'ambiente costruito (gli edifici, il loro intorno di dotazioni, le connessioni interne all'urbanizzato e le infrastrutture di collegamento a livello territoriale) non dovrebbero più essere osservati esclusivamente sotto il profilo della loro dimensione reale, ma anche della complessità dei network informativi che esse stesse producono, processano, scambiano, utilizzano e riutilizzano.

Si tratta di un nuovo scenario di riferimento all'interno del quale non è più la città in quanto oggetto fisico ad essere al centro dell'attenzione progettuale ma, piuttosto, la città e suoi edifici in quanto sedi delle dinamiche collegate alle attività che in essi si svolgono.

La possibilità di valutare in tempo reale le dinamiche dei sistemi urbani, con il fine ultimo di comprenderne il funzionamento in relazione all'uso, consente l'individuazione delle criticità, procedendo dall'uso effettivo che delle città, dei suoi edifici e delle sue infrastrutture viene fatto.

D'altro canto, c'è già chi sta realizzando nuove modalità di restituzione dell'Urbanistica: una sorta di nuovo layer da sovrapporre alle consuete rappresentazioni, in cui la città diviene architettura dell'informazione. Esattamente come sta già accadendo nel caso del Comune di Milano, ad esempio, con la definizione dei Piani di resilienza basati su modelli multi-scalari interattivi e relative simulazioni predittive.

La capacità di raccolta di una miriade di dati rimanda a centri di elaborazione, sempre più potenti e veloci che, per l'appunto, vengono chiamati Big Data.

Nello specifico, si tratta dell'insieme di tecnologie e metodologie di analisi di dati massivi che si traduce nella capacità di estrapolare, analizzare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non, per scoprire i legami tra fenomeni diversi e prevedere quelli futuri.

Dal nostro punto di vista, in questo scenario complessivo diviene fondamentale cominciare a comprendere o prefigurare quali possano essere le correlazioni riconducibili alle funzioni tipiche dei sistemi di sicurezza generalmente intesi.

Certamente, a livello di città resiliente, il tema del monitoraggio finalizzato ad un'azione-reazione coerente rispetto all'evento incombente, costituisce un ambito di palese interesse per la possibilità di sviluppo di concrete applicazioni.

La determinazione di un'efficace strategia di prevenzione e di progettazione nei confronti di possibili attacchi alla sicurezza delle persone e delle cose è, in effetti, pienamente coerente con il concetto di resilienza.

Basti pensare all'eventualità di attacchi terroristici piuttosto che a disastri ambientali, in cui risulta fondamentale l'identificazione del rischio in funzione del potenziale impatto che ne consegue a livello specifico e d'insieme o sistemico.

In tal senso, occorre valutare che, pur essendo i sistemi informativi ormai largamente in grado di produrre modelli matematici di previsione dei rischi, il tema centrale su cui concentrare l'attenzione è legato all'affidabilità del dato: solo dati "di qualità" possono alimentare modelli matematico-statistici tali da consegnare ai decisori informazioni affidabili.

In conclusione, vorrei fare riferimento al tema della valorizzazione dell'edificio. In effetti occorre considerare che i dati sulla sicurezza di un determinato contesto possono incidere, non poco, su quello che gli esperti del settore immobiliare definiscono "il più probabile valore di mercato" di un bene immobiliare.

Com'è facile intuire, una zona poco sicura può incidere negativamente sul suo valore. Questo fatto, tuttavia, per quanto di rilievo e per quanto condivisibile o plausibile, fino a poco tempo fa non era stato ancora puntualmente identificato e misurato, in ambito valutativo.

Oggi, al contrario, grazie alle potenzialità di elaborazione dei Big Data, alcuni operatori del settore immobiliare stanno proponendo servizi di stima del valore di mercato, anche in un'ottica prospettica o previsionale.

In estrema sintesi, si tratta di servizi molto utili, ad esempio, per gli istituti bancari nella dismissione dei cosiddetti crediti incagliati con un sottostante immobiliare, per le aste immobiliari, per il finanziamento di operazioni immobiliari in genere. Tali servizi vengono sviluppati attraverso la generazione di algoritmi che al loro interno contengono sempre componenti riconducibili ad indicatori di sicurezza; dal numero di incidenti stradali o di furti nella zona fino alla percezione di sicurezza degli abitanti o alla presenza di telecamere/TVCC nella zona; tutte componenti che all'interno dell'algoritmo, di solito, assumono un peso tutt'altro che secondario.

Ed è d'altra parte chiaro che una zona sicura non può che essere diretta conseguenza di edifici sicuri, con relative dotazioni che comprendono gli spazi esterni annessi, da sommare a strade, parchi, parcheggi, ecc. sicuri.

Rapporto IHS sulla verifica video contro i falsi allarmi negli impianti residenziali

di Anna Sliwon, security analyst, IHS Markit (traduzione a cura di TES - Traduzioni e interpretariato)

Il quadro

• Nel 2017, quasi il 23% degli impianti d'allarme ad uso domestico venduti nel mondo ha incluso qualche forma di **verifica video**, comprendendo impianti installati da professionisti, impianti do-it-yoursel (DIY) e impianti con operatore di sistema multiplo (MSO). Si prevede che entro il 2022 si diffonderanno ulteriormente, arrivando al 32%.

• Nel 2017, in tutto il mondo sono state vendute telecamere a infrarosso passivo ad uso domestico per un valore di 43 milioni di dollari e si prevede che i ricavi di questo mercato aumenteranno a 64 milioni di dollari entro il 2022.

Analisi

I falsi allarmi sono un problema significativo che incide sul settore dei servizi di telesorveglianza e degli impianti d'allarme. Il **90-95% degli allarmi riportati alle centrali operative si rivelano essere falsi** e pertanto costituiscono un costo per i fornitori di servizi, dal momento che devono inviare una squadra di pronto intervento per verificare ogni allarme. Vanno inoltre a sovraccaricare inutilmente le risorse della polizia locale, e potrebbero addirittura causare un aumento dei costi per gli utenti finali, visto che dipendono dalle regolamentazioni locali relative all'intervento per gli allarmi e dalle potenziali multe.

La verifica video risolve questi problemi, dal momento che in breve tempo offre una conferma certa da remoto della natura dell'allarme che aiuta ad accelerare il processo di intervento dell'operatore. Le immagini video possono essere trasferite in tempo reale all'operatore per una valutazione quasi immediata e l'invio sul posto del pronto intervento o della polizia in molto meno tempo.

Il ruolo giocato da DIY, domotica e dalla videosorveglianza residenziale

L'influenza del mercato della sicurezza di DIY, domotica e videosorveglianza residenziale accresce la diffusione delle soluzioni di video verifica, come spiegato di seguito:

• **DIY:** generalmente le telecamere per uso domestico sono over IP ad alta risoluzione e permettono agli utenti di controllare le proprie abitazioni e rivedere se necessario filmati di eventi passati. Tutto ciò può essere fatto attraverso apposite app per smartphone per verificare gli allarmi per intrusione, garantendo maggiore tranquillità agli utenti stessi.

• **Smart Home:** gli impianti di domotica stanno diventando sempre più popolari tra gli utenti finali. Di solito, le telecamere vengono commercializzate insieme ad altre applicazioni, come le prese e le luci intelligenti, che garantiscono agli utenti un ulteriore livello di controllo su ciò che sta avvenendo nella loro abitazione. Alcune telecamere offrono anche applicazioni per rilevare il fumo a supporto dei tradizionali rilevatori, oltre a permettere la sorveglianza con verifica e monitoraggio autonomi. Le centrali operative offrono sempre più spesso servizi di monitoraggio per le case intelligenti dando in questo modo un impulso importante al mercato della verifica video.

• **Videosorveglianza residenziale:** il numero di dispositivi di videosorveglianza per uso domestico disponibili sul mercato sta crescendo rapidamente, fornendo una più ampia scelta di soluzioni a vari prezzi. Gli utenti finali possono aggiungere una telecamera IP ai propri impianti domestici e godere di funzionalità di verifica e monitoraggio in autonomia a basso costo.

I vantaggi per installatori, fornitori e centrali operative

Oggi, molte delle principali centrali operative offrono un servizio di verifica video ad un costo aggiuntivo oltre ai servizi di controllo base. Aggiungere la verifica video al pacchetto di monitoraggio riduce le probabilità che il cliente receda dal contratto o scelga un altro fornitore con servizi più completi. Anche installatori e venditori, desiderosi di offrire una più ampia gamma di servizi, trarranno benefici dalla verifica video. Servizi di cloud hosting e di supporto per il monitoraggio video in autonomia valorizzano l'offerta per l'utente finale. Gli installatori potrebbero trovarsi più vicini ai propri clienti rispetto ad alcune aziende di telesorveglianza e questo rende più semplice sensibilizzare il cliente rispetto alle nuove offerte. In ogni caso, le partnership tra installatori e centrali operative potranno aumentare i ricavi per utente e avere un fatturato annuo più stabile. Le sottoscrizioni procurate dagli installatori potrebbero compensare i tassi di recesso che normalmente riscontrano le aziende di telesorveglianza.

Fattori che ostacolano la diffusione

I maggiori fattori che ostacolano una più ampia adozione della video verifica sono i seguenti:

• **Costi:** sebbene siano evidenti i benefici derivanti dall'includere la verifica video nell'impianto di allarme, molti utenti finali, in particolar modo quelli del settore domestico, potrebbero difficilmente permettersi dispositivi video. I sensori a infrarosso passivo (PIR) con video possono costare a fino a tre volte di più che i sensori PIR senza video.

• **Privacy e sicurezza informatica:** gli utenti privati che fanno uso di telecamere per la verifica video si preoccupano che un hacker possa utilizzare il dispositivo per guardare e ascoltare quanto avviene nella vita privata dei residenti. Dal momento che diverse inchieste hanno riportato casi in cui telecamere IP ad uso domestico sono state attaccate con successo, i potenziali utenti potrebbero fermare l'acquisto di questi dispositivi. Un'ulteriore preoccupazione è che gli operatori delle centrali possano osservare i residenti nelle loro case oltre l'orario autorizzato. I fornitori di soluzioni di verifica video devono pertanto assicurare che i propri impianti includano strumenti di protezione della privacy, consentendo all'utente di limitare l'accesso ai dispositivi video quando desidera.

• **Auto-monitoraggio:** la maggiore disponibilità di dispositivi di videosorveglianza consumer e di impianti di sicurezza DIY che includono nell'offerta prodotti video, hanno portato alla diffusione della verifica e del monitoraggio in autonomia. Tali sistemi sono solitamente preconfigurati per gestire file video, il che facilita l'aggiunta di telecamere e diminuisce la complessità di configurazione dell'impianto, che costituisce un ostacolo all'adozione della verifica video.

Possono i Comuni posare la fibra ottica per realizzare impianti di videosorveglianza?

di Angelo Carpani. Libero professionista, laureato in Ingegneria elettronica presso il Politecnico di Milano, esperto nella progettazione di impianti di videosorveglianza in ambito comunale

Introduzione

Possono i Comuni posare la fibra ottica quale infrastruttura di rete di comunicazione per la realizzazione di impianti di videosorveglianza? La risposta è SI, ma a determinate condizioni.

Il problema è stato sollevato dalla Prefettura di Pordenone nella nota n. 6104 emanata il 6 marzo 2017 dopo una segnalazione del Ministero dello Sviluppo Economico (di seguito abbreviato "MiSE").

Attenzione, qui si parla di "posa" e non di "utilizzo" della fibra ottica!

Data la complessità e la vastità della materia, lo scopo di questo articolo è di fare un po' di chiarezza sull'argomento, richiamando sinteticamente i punti principali della normativa che fa capo al D.Lgs. n.259/2003, noto come "Codice delle comunicazioni elettroniche" (di seguito abbreviato "Codice").

La situazione normativa

Nel precedente articolo *Videosorveglianza e reti Wi-Fi tra "uso privato" e "uso pubblico"* **(essecome online n. 5/2018)** avevamo già chiarito che le reti in **Fibra Ottica** e le reti **Wireless** (operanti in banda Radiolan e Hiperlan), impiegate normalmente quali infrastrutture di rete negli impianti di videosorveglianza, rientrano tra i sistemi di comunicazione elettronica ad **"uso privato"**, intendendo con esso che la rete deve essere utilizzata soltanto per trasmissioni riguardanti attività di propria competenza, con divieto di effettuare traffico per conto terzi (art.101 del Codice).

La materia pertanto è disciplinata dal Titolo III del Codice "Reti e servizi di comunicazione elettronica ad uso privato".

L'art.104 del "Codice" elenca le "attività" soggette alla cosiddetta **"autorizzazione generale"**. È bene precisare che per "attività" si intende "installazione" o "esercizio" di una rete di comunicazione elettronica.

Tra le reti elencate nell'art.104 soggette ad "autorizzazione" generale compaiono (comma 1, lettera b) le reti di comunicazione elettronica su supporto fisico, ad onde convogliate e con sistemi ottici (cioè **fibra ottica**), ad eccezione di quanto previsto dall'art.105, comma 2, lettera a).

Quest'ultimo, rinviando a sua volta all'art.99, comma 5, fa riferimento ai collegamenti realizzati nel proprio fondo o in più fondi dello stesso proprietario, possessore o detentore purché contigui, ovvero nell'ambito dello stesso edificio per collegare una parte di proprietà del privato con altra comune, purché non connessi alle reti di comunicazione elettronica ad uso pubblico.

Quindi, in quest'ultimo caso, la rete di comunicazione è di "libero uso" senza necessità di "autorizzazione generale". Parti dello stesso fondo o più fondi dello stesso proprietario, possessore o detentore si considerano contigui anche se separati, purché collegati da opere permanenti di uso esclusivo del proprietario, che consentano il passaggio pedonale o di mezzi.

Quindi, in quest'ultimo caso, le reti di comunicazione sono di "libero uso" senza necessità di "autorizzazione generale".

Le precisazioni del MiSE

Il MiSE, in risposta alle richieste di chiarimento da parte di alcune Prefetture, ha emanato una nota riguardo al significato giuridico ed alla portata da dare all'espressione "proprio fondo". Sull'argomento si è espressa in particolare la Direzione Generale per le Attività Territoriali di Roma (D.G.A.T.) del MiSE, con *nota DSGCERP – Div.II del 07/11/2017.*

Tale nota ha confermato di **non** ritenere applicabile il concetto di "proprio fondo" alle reti di comunicazione elettronica ad uso privato realizzate su supporto fisico, ad onde convogliate o in **fibra ottica** nello stesso fondo comunale per il collegamento di due o più parti (sedi amministrative) separate da opere permanenti quali le strade, piazze, parcheggi, ecc.

Precisamente, le reti di comunicazione elettronica installate nello stesso fondo comunale per il collegamento di due o più parti (sedi amministrative) separate da opere permanenti quali strade, piazze, parcheggi, ecc., non possono essere di "libero uso", mancando, nel caso più comune e generale, la contiguità tra le parti collegate. Tale contiguità, infatti, si realizzerebbe solo nel caso che le predette opere fossero di uso esclusivo del proprietario e non invece di libero uso da parte di tutti i privati cittadini.

Pertanto dette reti di comunicazione elettronica ad uso privato (reti di videosorveglianza, controllo accessi ztl, ecc.) se realizzate su supporto fisico, ad onde convogliate o in **fibra ottica** sono soggette ad "autorizzazione generale" ai sensi degli artt.99, 104 e 107 del "Codice".

La Segnalazione Certificata di Inizio Attività (SCIA)

Ai sensi dell'art.107, comma 5, del "Codice", il Comune che intende espletare le attività ("installazione" o "esercizio") di cui all'articolo 104, comma 1, lettera b), è tenuto a presentare all'ufficio del MiSE preposto al rilascio del titolo abilitativo (Direzione Generale Servizi di Comunicazione Elettronica, di Radiodiffusione e Postali – Divisione II **dgscerp.div02@pec.mise,gov.it**) una dichiarazione contenente l'intenzione di installare o porre in esercizio una rete di comunicazione ad uso privato conforme al modello riportato nell'**allegato n.17** del "Codice" (art.107, comma 5), nonché tutta la documentazione annessa ivi indicata.

La suddetta dichiarazione costituisce la cosiddetta **SCIA** "Segnalazione Certificata di Inizio Attività" a seguito della quale il soggetto interessato è abilitato ad iniziare la propria attività a decorrere dall'avvenuta presentazione.

In base all'art.116 del "Codice" i contributi inerenti alle autorizzazioni generali, di cui all'articolo 107, sono riportati nell'Allegato 25.

Per il conseguimento di autorizzazioni generali per reti e servizi di comunicazione elettronica ad uso privato, nonché per le richieste di variazione, è dovuto il pagamento di contributi:

a - per l'**istruttoria** delle pratiche;

b - per la **vigilanza**, ivi compresi le verifiche ed i controlli, sull'espletamento del servizio e sulle relative condizioni.

Ai sensi dell'art.32, comma 8, lettera c) dell'Allegato 25, l'entità dei contributi è stabilita nella misura del cinquanta percento relativamente ai servizi di polizia degli enti locali.

Nell'art.102 del Codice sono stabilite le sanzioni (amministrative) per l'installazione o l'esercizio di una rete di comunicazione senza autorizzazione generale (comma 2), commisurate al periodo di esercizio abusivo accertato (comma 3), o in difformità dall'autorizzazione generale rilasciata (comma 4). È prevista anche una eventuale rimozione o sequestro dell'impianto stesso (comma 7) o sospensione, revoca, decadenza dell'autorizzazione generale (art.103 del Codice).

E per le reti wireless?

Anche le reti wireless, nella formulazione originaria del Codice (art.104, comma 1, lettera c), numero 3), rientravano tra le reti soggette ad "autorizzazione" generale quali *sistemi che impiegano bande di frequenze di tipo collettivo senza alcuna protezione, relativi all'installazione o esercizio di reti locali* ***radiolan*** *o* ***hiperlan*** *al di fuori del proprio fondo.*

Il Codice prevedeva diversi allegati per l'ottenimento dell'autorizzazione generale per reti private (come ad es. l'Allegato n.17 per la fibra ottica), ma nel caso degli apparati wireless Radiolan e Hiperlan (art.104, lettera c, numero 3), fra l'altro molto diffusi, non erano stati stabiliti né i contributi, né previsti i moduli/allegati da compilare (anche se alcuni Ispettorati Territoriali avevano rimediato alla "svista" del Legislatore).

Come è stato risolto il problema? Con l'art.69 del D.Lgs. n.70/2012, di modifica del "Codice", è stato soppresso il numero 3) della lettera c) del comma 1 dell'art.104, e in base all'art.70, sempre dello stesso decreto di modifica, le reti in tecnologia radiolan/hiperlan sono di libero uso e pertanto per l'installazione o l'esercizio di tali reti non deve essere più richiesta l'autorizzazione generale!

Gunnebo, un modello vincente anche nell'era digitale

intervista a Marco Depaoli, General Manager di Gunnebo Italia

Qual è il modello organizzativo che ha fatto diventare Gunnebo Italia un fiore all'occhiello del gruppo svedese leader mondiale nella sicurezza?
Il modello organizzativo adottato da Gunnebo Italia è per linee di prodotto. All'interno di ogni linea l'azienda è focalizzata sui segmenti di mercato dove genera valore per i clienti. Questo modello ha contributo ad una crescita del fatturato superiore al 10% annuo con una percentuale del profitto sulle vendite a due cifre.

Quando ha dato inizio al "nuovo corso" che ha prodotto questi risultati e quali obiettivi si è posto per i prossimi anni?
Il nuovo modello è stato implementato in azienda due anni fa. Si è reso necessario introdurre questo nuovo modello organizzativo per essere più orientati e focalizzati sul cliente e poter soddisfare le sue richieste ed aspettative con una struttura di vendita, di progettazione e di assistenza tecnica professionale, competente e capace di rispendere in tempi brevi e creare valore. Questo modello ci permette di essere più competitivi e di aumentare il tasso di successo sulle singole opportunità. L'obiettivo per i prossimi anni è di continuare questo trend di crescita profittevole.

Quali sono le vostre linee di prodotto e quali sono i mercati verticali in fase di sviluppo?
Le linee sono quattro che rappresentano altrettante Business Unit: **sicurezza fisica, sicurezza elettronica, tornelli, cash management**. Per ogni linea sono ben chiari e delineati i mercati in fase di sviluppo dove intendiamo competere e cogliere nuove ed ulteriori opportunità di crescita. Citiamo alcuni esempi: i sistemi di cassette di sicurezza robotizzati per il mercato bancario; le soluzioni di sicurezza elettronica per i siti ad alto rischio; i tornelli per

controllare il flusso di persone in aeroporti, nelle stazioni ferroviarie e nelle metropolitane; il cash management nel retail food e catene specializzate.

Come problem solving, quali soluzioni proponete a settori che stanno dematerializzando il proprio core business, come il bancario e il retail, che devono adeguare la propria organizzazione a nuove esigenze ed a nuovi rischi in materia di sicurezza?
I mercati bancari ed il retail sono mercati maturi per la sicurezza fisica ed elettronica e si rivitalizzano solamente con soluzioni tecnologicamente innovative con la possibilità di centralizzazione degli allarmi tecnologici e della assistenza remota che noi siamo in grado di offrire. Questi mercati, a seguito dei nuovi modelli di business adottati che introducono automazione nei processi no core, diventano e sono estremamente attrattivi ed interessanti per le nostre soluzioni di cassette di sicurezza robotizzate e di cash management che generano un elevato valore aggiunto per chi li installa.

E in che modo la trasformazione digitale impatta sull'organizzazione e sui prodotti di un'azienda che, oltre ai servizi, produce dispositivi tipicamente materiali come tornelli e casseforti?
Per noi la digitalizzazione significa poter offrire prodotti e soluzioni che adottano tecnologie IoT e che portano a modificare i modelli di assistenza tecnica e di manutenzione attuali. Con la tecnologia IoT possiamo diagnosticare in anticipo il degrado di un componente hardware del prodotto ed intervenire preventivamente in sito con il giusto ricambio evitando fermi di macchina e problemi per il cliente. È possibile, se autorizzati, intervenire da remoto per risolvere problemi hardware e software riducendo drasticamente i tempi di intervento e, nel contempo, soddisfare le sempre più stringenti richieste dei clienti in termini di tempo di risoluzione. La tecnologia IoT porta ulteriori vantaggi nel miglioramento continuo dei prodotti e nell'ottimizzazione delle parti di ricambio giacenti a magazzino.

In conclusione, come vede l'evoluzione del mercato della sicurezza, quando giungeranno a compimento i processi di convergenza in atto tra tecnologie e servizi e tra sicurezza fisica e sicurezza informatica, in un mondo completamente interconnesso?
Questo processo è già in essere ed arriveremo alla convergenza molto prima di quanto si possa pensare, dove la tecnologia ed il software giocano un ruolo fondamentale con un ulteriore cambiamento dei modelli di business, dell'organizzazione e dell'arena competitiva.
Trovano posto in organigramma nuove posizioni che prima non erano presenti. Per ricoprire tali posizioni stiamo inserendo risorse (non sempre disponibili sul mercato e comunque di difficile reperimento) con competenze che rispecchiano le convergenze sopra citate e che permettono di affrontare il cambiamento e sostenere la nostra crescita profittevole.

GUNNEBO®
For a safer world

CONTATTI: GUNNEBO ITALIA SPA
Tel. +39 02267101
info.it@gunnebo.com
www.gunnebo.it

Elevare professionalità e formazione degli installatori: la strada di Safe & Lock per competere nel mercato che cambia

intervista a Gaetano Matuozzo, direttore commerciale di Safe & Lock

Ci presenti l'azienda Safe & Lock: la sua storia con le attività svolte e i prodotti trattati, le persone che la dirigono.

Safe & Lock è un'azienda Italiana che opera con successo da oltre 20 anni nel settore della produzione e distribuzione di componenti per sistemi di **Sicurezza, Antincendio, TV.CC, Networking, Domotica e Automazione**; grazie alla professionalità, la competenza, all'esperienza e alla correttezza nei rapporti, ha consolidato legami di partnership e fiducia reciproca con **fornitori di rilievo internazionale**, mettendo a disposizione apparecchiature ad **alto contenuto tecnologico** con caratteristiche **innovative** in modo da anticipare le tendenze e le esigenze del mercato. Sensibile come pochi alla **qualità**, effettua costantemente severe selezioni: prima di adottare una linea, viene analizzato il produttore, testati scrupolosamente i prodotti e solo dopo aver superato i test inseriti a catalogo; oltre ad investire continuamente risorse economiche dedicate allo sviluppo di nuovi progetti al fine di garantire prodotti aggiornati con **tecnologie di ultima generazione**.

Siamo un team di persone giovani, intraprendenti, preparate e dinamiche, che ci permette di competere sul territorio da protagonisti.

Oltre ad avvalersi della pluriennale esperienza di Alessandro Brogi, nel ns. team è presente con l'incarico di direttore Tecnico Marcello Ditommaso, già certificato fin dalla prima sessione di esame IMQ Air e AIRVIDEO sia come tecnico installatore che progettista, ed è a disposizione della clientela.

Qual è la vostra visione del mercato della sicurezza allo stato attuale e come si evolverà nei prossimi anni?

Il mercato della sicurezza è in continua evoluzione, e di conseguenza cambiano le esigenze. Dove prima era prioritaria la protezione dei beni materiali, ora si predilige la salvaguardia della persona. Ciò comporta uno spostamento del primo anello di rilevazione sempre più distante dalle mura domestiche, in grado di intercettare un intruso prima che lo stesso possa mettere a repentaglio l'incolumità della propria famiglia; per ottenere questo occorre realizzare sistemi di protezione esterna capaci di intercettare precocemente un intruso e a loro volta essere affidabili sopportando impervie problematiche ambientali. Le ns. competenze a tale riguardo sono di alto livello e a disposizione con progetti personalizzabili in affiancamento ai ns. clienti.

Per quali motivi ha proposto ai suoi clienti di intraprendere il percorso di formazione e certificazione IMQ AIR e AIRVIDEO?

La professionalità è sempre più un requisito necessario per il lavoro di oggi e di domani perciò Safe & Lock è impegnata a contribuire alla formazione degli installatori rendendoli consapevoli degli obblighi, vincoli, e norme che regolamentano il settore al fine di limitargli responsabilità ed esposizioni e rischi inaspettati.

La formazione dei nostri clienti per noi è talmente importante che ci ha spinto oltre a organizzare corsi propedeutici alla certificazione IMQ AIR e AIRVIDEO a creare Safe & Lock Academy inFORATION tecnology, un vero e proprio nuovo ramo aziendale, con un brand ed un logo esclusivo, dedicato alla formazione periodica e costante di installatori e progettisti, finalizzata ad una maggiore specializzazione per un'attività efficiente, veloce e remunerativa.

S&L Academy non ha un solo scopo ma molteplici, ovvero: fornire un'adeguata analisi del rischio di ogni singola realtà valutata in conformità con le normative CEI/EN che la regolamentano, analizzare le diverse soluzioni progettuali di un sistema, far conoscere le effettive caratteristiche tecniche e i principi di funzionamento dei prodotti per protezioni esterne, interne e wireless; informare su come eseguire una corretta installazione e il relativo cablaggio dei vari sistemi di Security e Domotica, al fine di ottenere un'armoniosa interazione tra loro.

Quali sono i vostri obiettivi per il futuro?

Stiamo sviluppando diverse iniziative esclusive, alcune di esse integrate con S&L Academy che offriranno ai nostri clienti delle opportunità nuove ed inesplorate nel nostro settore.

Il nostro team è sempre alla ricerca di soluzioni innovative e all'avanguardia per fronteggiare le attuali e future sfide a cui va incontro un settore come il nostro in costante evoluzione.

Grazie anche alla collaborazione con nuovi partner ci stiamo sempre più specializzando per dare forma, solidità ed efficacia ad una realtà volta a restare sempre ai massimi livelli in termini di presenza e competitività in un settore dove la corsa alle proposte low cost sta sgretolando il mercato, la professionalità e l'eccellenza; valori questi fondamentali e imprescindibili sui quali puntiamo per essere competitivi e creare mercato.

DIAS presenta lares 4.0 di KSENIA SECURITY, la più innovativa piattaforma IoT ibrida per sicurezza e home automation

a cura della Redazione

Semplicemente unica nel settore della sicurezza fisica (antintrusione, controllo accessi e videosorveglianza) come pure nella Home & Building Automation, la prestigiosa proposta tutta italiana di **KSENIA Security** è riconosciuta ed apprezzata in Europa e nel mondo per la capacità di offrire un livello di innovazione e design senza precedenti unitamente a soluzioni progettate e realizzate per essere eco-sostenibili.

Tale successo è possibile grazie alla lunga esperienza maturata nel settore, alla convergenza dinamica di idee e competenze eterogenee, all'impegno e passione profuse nel desiderio di realizzare qualcosa di veramente unico, nuovo ma solido, a misura delle esigenze sempre maggiori degli installatori e degli utenti finali - anche in termini di aspettative future - guidandole in una logica di integrazione totale.

La **Open Platform 'lares'**, nelle sue diverse declinazioni **IoT, ibrida** e **wireless**, da 16 a 644 zone e uscite, rappresenta la massima espressione in termini di potenza, integrazione e connettività: componentistica di ultima generazione, un grado elevatissimo di qualità e affidabilità certificata, espandibilità e completa programmabilità da remoto, anche da smartphone mediante APP dedicate sia all'Installatore professionale sia al cliente finale. Su un'unica centrale di dimensioni quanto mai contenute, si accentrano sia le funzioni domotiche che quelle di sicurezza antintrusione, connettività IP/Ethernet e 3G quale back-up o viceversa.

La nuova piattaforma di centrali ibride della **serie lares 4.0** di KSENIA rappresenta la più innovativa soluzione IoT per la sicurezza e la Home & Building Automation.

Grazie all'accordo di partnership appena siglato con **KSENIA, DIAS** è lieta di offrire ai propri clienti questa gamma di centrali di qualità eccellente, di produzione nazionale e appositamente progettate per rispondere alle specifiche esigenze del mercato italiano.

Carlo Hruby, Amministratore Unico di DIAS, sottolinea: *"Siamo molto soddisfatti dell'accordo di collaborazione siglato con KSENIA Security, che Raffaele Di Crosta ha fondato e portato all'eccellenza con serietà e lungimiranza. Le caratteristiche di queste centrali sono assolutamente in linea con la naturale evoluzione che sta interessando il nostro settore e che fa sì che un sistema, per essere completo e per rispondere alle esigenze della società contemporanea, debba integrare le funzioni di sicurezza con quelle di automazione domestica e di building automation: sono certo che verranno apprezzate dalla nostra rete di distributori, dai loro clienti e dagli utenti finali".*

Tutte le nuove centrali lares 4.0 sono la soluzione perfetta e più avanzata nell'era della digitalizzazione (IoT) per quanto riguarda la sicurezza e la Home&Building Automation. Esse dispongono infatti di un numero di uscite uguale al numero degli ingressi per la gestione delle luci, del clima, dell'irrigazione e delle tapparelle, insomma di qualsiasi tipo di automazione o elettrodomestico: sia le funzioni destinate alla sicurezza che quelle per la smart home possono essere ora gestite da un'unica APP utente (lares4.0) e programmate dall'installatore da qualsiasi terminale mobile (KSENIA Pro). Indipendentemente dalla dimensione, la scheda di centrale nasce con già a bordo la porta Ethernet e il transceiver wireless bidirezionale 868 MHz, compatibile con tutte le periferiche wls esistenti KSENIA; esse sono dotate anche di doppio BUS e di terminali di connessione estraibili. Tutte le schede sono predisposte per accogliere direttamente a bordo (senza BUS di comunicazione per aumentare al massimo la velocità di transito delle informazioni e dei dati) sia il modulo 3G (e presto il 4G-LTE) sia, ove necessario, il modulo PSTN.

In ogni caso è garantito l'invio di messaggi vocali, email, Contact ID e protocollo SIA DC-09 livello III alle Centrali di Sorveglianza. L'APP installatore consente poi di centralizzare e geo-localizzare tutte le centrali installate e pertanto di offrire il massimo dell'assistenza al cliente finale mediante la ricezione di notifiche push anche per alert tecnologici (ciò vale per tutte le centrali IoT - lares 4.0 e lares wls 96 IP).

I modelli di centrale disponibili sono i seguenti:

lares 4.0 wls 96

Gestisce fino a 32 periferiche radio e fino a 96 zone wireless. Possibile espansione cablata su BUS: fino a 3 interfacce utente (a scelta tra tastiera ergo e lettori di prossimità volo e volo-in), 1 sirena su BUS (imago o radius), 1 domus per gestire le funzioni cronotermostato. Certificata EN50131-GRADO 2

lares 4.0- 16

Gestisce fino a 16 IN + 16 OUT con 6 partizioni
nativa con interfaccia Ethernet (senza wireless a bordo - necessita di ricetrasmettitore duo)
Incluse le APP Installatore (KSENIA Pro) e Utente (lares 4.0)
Certificata EN 50131-GRADO 3

lares 4.0- 40

Gestisce fino a 40 IN + 40 OUT con 12 partizioni
nativa con interfaccia Ethernet (senza wireless a bordo - necessita di ricetrasmettitore duo)
Incluse le APP Installatore (KSENIA Pro) e Utente (lares 4.0)
Certificata EN 50131-GRADO 3

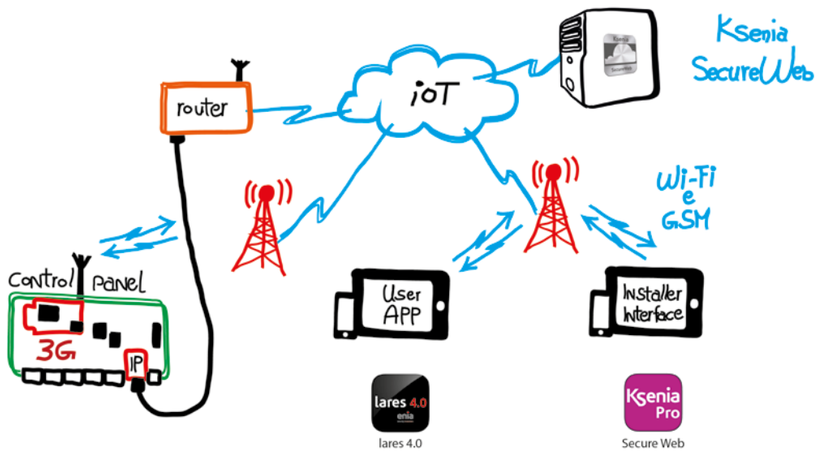
lares 4.0- 40 wls

Gestisce fino a 40 IN + 40 OUT con 12 partizioni
nativa con interfaccia Ethernet e wireless bidirezionale 868 MHz (in tecnologia DPMS - Dynamic Power Management System) e doppio BUS di serie.
Incluse le APP Installatore (KSENIA Pro) e Utente (lares 4.0)
Certificata EN 50131-GRADO 3

lares 4.0 - 140 wls
Gestisce fino a 140 IN +140 OUT con 20 partizioni
nativa con interfaccia Ethernet e wireless bidirezionale 868 MHz (in tecnologia DPMS - Dynamic Power Management System) e doppio BUS di serie.
Incluse le APP Installatore (KSENIA Pro) e Utente (lares 4.0)
Certificata EN 50131-GRADO 3

lares 4.0 - 644 wls
Gestisce fino a 644 IN + 644 OUT con 30 partizioni (e oltre su progetto specifico)
nativa con interfaccia Ethernet e wireless bidirezionale 868 MHz (in tecnologia DPMS - Dynamic Power Management System) e doppio BUS di serie.
Incluse le APP Installatore (KSENIA Pro) e Utente (lares 4.0)
Certificata EN 50131-GRADO 3

Per maggiori informazioni:



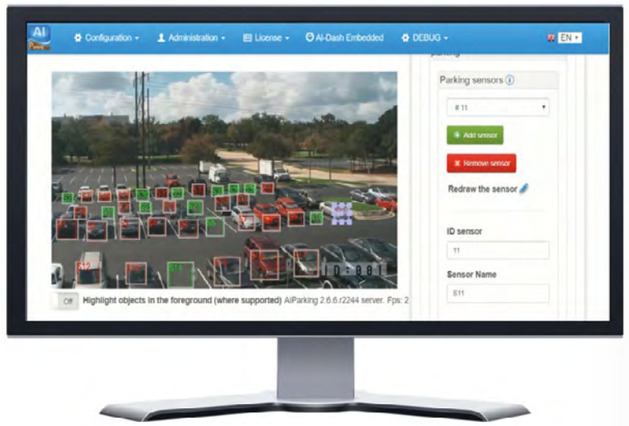
dias

CONTATTI: DIAS SRL
Tel. +39 02 38036901
www.dias.it

A.I. Tech presenta la soluzione di analisi video per il monitoraggio dei parcheggi

a cura della Redazione

Una recente analisi dell'ISTAT conferma che tra le principali preoccupazioni del cittadino italiano vi è quella legata alla ricerca del parcheggio, che si attesta al secondo posto dopo la problematica legata al traffico e prima ancora di quella relativa all'inquinamento. Diventa pertanto di fondamentale importanza disporre di uno strumento per il monitoraggio dei parcheggi che possa supportare il cittadino e il gestore dei parcheggi, sia questo privato o pubblico.



La soluzione di analisi video di **A.I. Tech**, **AI- Parking**, si colloca proprio in questo contesto. AI-Parking consente infatti di analizzare in tempo reale le immagini acquisite da una telecamera che inquadra il parcheggio, di analizzare i singoli posti di un parcheggio e valutarne lo stato di occupazione, ossia di comprendere in tempo reale se quel posto sia libero o occupato. AI-Parking è uno dei tre prodotti della linea **DEEP-VISION**, la nuova linea di casa A.I. Tech che combina l'esperienza dell'azienda sulla visione artificiale con i più avanzati algoritmi di deep learning.

Tutto ciò grazie all'impiego di algoritmi avanzati di detection e classificazione dei veicoli basati appunto su deep networks, progettate e sviluppate dal team di A.I. Tech e ottimizzate per funzionare direttamente a bordo camera. AI-Parking non necessita di una inizializzazione del sistema "scarico", ossia non necessita di essere configurato in situazioni in cui il parcheggio non presenta veicoli. Inoltre, è in grado di valutare lo stato di occupazione di un posto anche nel caso in cui il veicolo sia solo parzialmente visibile. Due caratteristiche fondamentali per la messa in opera di un sistema per il monitoraggio dei parcheggi.

Accanto all'elevata efficienza e affidabilità della soluzione di casa A.I. Tech, numerosi sono i vantaggi offerti dalla soluzione AI-Parking, unici nel suo genere. Scopriamoli insieme.

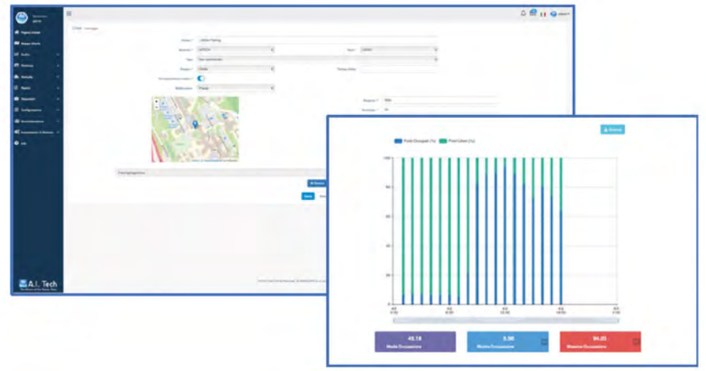
La soluzione di A.I. Tech è **multipiattaforma**. Questa infatti può essere installata in versione edge, embedded e server.

Versione edge:
AI-Parking può essere installato direttamente a bordo di specifici modelli di camere, senza alcuna necessità di un server esterno (si suggerisce di contattare il team di A.I. Tech per l'elenco delle camere compatibili). Questa è in assoluto la prima soluzione per lo smart parking presente sul mercato e basata su deep learning capace di funzionare direttamente a bordo camera.

Versione server:
il plugin è fornito come una distribuzione Linux customizzata su cui i plugin sono già caricati. Pertanto, nessuna applicazione da installare e nessun ulteriore costo di sistema operativo da aggiungere. Nel caso in cui sia già presente una macchina Windows, la distribuzione fornita da A.I. Tech può essere gestita attraverso l'impiego di macchine virtuali.

Versione embedded:
AI-Appliance contiene in un piccolo box sia la componente hardware che quella software. Soluzione plug and play, accessibile tramite semplice ed intuitiva interfaccia web, AI-Appliance consente il funzionamento in parallelo di fino a 4 differenti funzionalità di analisi video di tipo AI- Parking. Grande soli 9 cm x 7.1 cm x 6.2 cm, certificato CE/RoHS, AI-Appliance è dotato di power supply (9-28 Vdc) e contenitore da guida DIN; relays e open collector attivabili tramite gli allarmi generati da AI-Parking; input analogici e digitali capaci di attivare e disattivare dinamicamente i plugin di analisi video. Qualcuno lo ha definito "il server in una mano".

Smart parking in casa, A.I.Tech non significa solo analisi video. La soluzione infatti si completa con un cruscotto web estremamente intuitivo e user-friendly per la gestione e la visualizzazione avanzata su mappa dei dati raccolti dai vari plugin di analisi video: **SMART PARKING**.

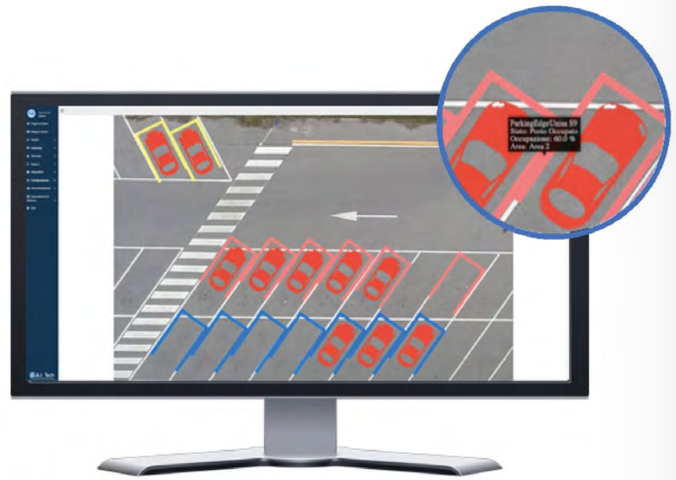


SMART-PARKING è il vertical di **AI-DASH-PRO** che consente di effettuare il monitoraggio dei parcheggi, sia perimetrati che non perimetrati (su strada). Vediamo insieme quali sono le differenze in termini di gestione.

I **parcheggi su strada** (o non perimetrati) sono quei parcheggi in cui non esiste un varco di ingresso o di uscita; in tal caso, l'esigenza è quella di monitorare, grazie all'impiego di una camera di sorveglianza su cui è installato il plugin AI-Parking, i posti delimitati da strisce, ciascuno dei quali può essere associato ad un sensore di parcheggio che può assumere due stati: libero (se non è presente alcun veicolo) e occupato (se è invece presente il veicolo).

In tal caso sarà possibile effettuare la gestione dei parcheggi su più livelli, sulla base delle specifiche esigenze: sarà infatti possibile visualizzare le informazioni relative a sensori (il singolo posto), aree di parcheggio (intese come aggregazioni di sensori, anche se inquadrati da telecamere differenti) e infine parcheggi (ossia aggregazioni di sensori e di aree). Per ciascun livello sarà quindi possibile effettuare un monitoraggio in tempo reale, valutando il numero di posti

liberi e occupati in aree e parcheggi, con riferimento allo specifico posto; tutto ciò attraverso una mappa su cui è possibile visualizzare lo stato dei parcheggi oppure grazie all'impiego di grafici e report.



I **parcheggi perimetrati** sono invece quei parcheggi dotati di un punto di ingresso e un punto di uscita, tipicamente (ma non necessariamente) provvisti di sbarra. Tali parcheggi possono essere monitorati in due modi: come nel caso dei parcheggi su strada (per ottenere informazioni sui singoli posti all'interno del parcheggio, oltre che sullo stato complessivo del parcheggio) o utilizzando delle camere di lettura targa (LPR) poste ai varchi di ingresso e uscita, al fine di ottenere delle informazioni complessive sul parcheggio. In questo scenario, il Vertical SMART PARKING consente di gestire white list e black list in tempo reale, con la possibilità di attivare automaticamente un sistema esterno in caso di veicolo con targa in white list attraverso CGI (es: apertura automatica sbarra di accesso in caso di veicolo noto); è inoltre possibile effettuare una valutazione dello stato del parcheggio, in termini di numero posti liberi/occupati sia in uno specifico momento che nel tempo attraverso dei grafici di supporto.

A.I. Tech: L'esperienza di oltre 30 anni di ricerca e trasferimento tecnologico nei settori dell'Intelligenza Artificiale e della Visione Artificiale, coniugata con competenze di ingegnerizzazione di soluzioni hardware, software e di progettazione su sistemi embedded, consentono ad A.I. Tech di proporre soluzioni innovative e all'avanguardia nel settore della analisi video intelligente. Il suo team giovane e dinamico, guidato da menti brillanti ed esperte, è capace di ideare, progettare e realizzare sistemi in grado di rendere intelligente una normale telecamera di sorveglianza. Grazie ai prodotti di A.I. Tech, la telecamera non si limita alla semplice osservazione della scena, ma diventa capace di comprendere cosa sta avvenendo attraverso il riconoscimento degli oggetti e l'analisi del loro comportamento. I prodotti di A.I. Tech possono essere utilizzati nei più svariati mercati verticali: dal retail alla business intelligence, dal monitoraggio del traffico all'ambient assisted living, dallo smart road alle smart city, dallo smart parking alla video sorveglianza intelligente.

A.I. Tech
The Vision of the future. Now.

CONTATTI: A.I. Tech srl
Tel. +39 393 8384253
www.aitech.vision

Il primo convegno per Security Manager italiani sulla Digital Transformation della gestione informatizzata della sicurezza fisica

di Nils Fredrik Fazzini - Amministratore delegato di Citel spa

Il Convegno costituisce una prima occasione per mettere a fuoco le tendenze della ***Digital Transformation*** in corso nel campo dell'informatica generale, per approfondirne l'applicabilità e lo stato dell'arte rispetto alla gestione informatizzata della Sicurezza Fisica aziendale; ma anche per attivare un confronto sul coinvolgimento del Security Manager riguardo al governo della tecnologia secondo modelli moderni, all'altezza di quelli correnti nell'ICT aziendale.

A tale proposito, dal proprio punto di osservazione Citel ritiene di poter segnalare che l'evoluzione, già in corso in Italia, ha portato in diversi casi al consolidamento nei fatti di un ***Sistema Informatico Dipartimentale della Sicurezza Fisica*** secondo un modello evoluto anche rispetto ai principali mercati esteri.

Con valenze particolari sotto l'aspetto dell'apertura multi-fornitore secondo il modello "open-PSIM", un paradigma evolutivo che Citel ha consolidato e diffuso negli anni nel mercato nazionale convergendo con le preferenze e le politiche prevalenti degli utilizzatori professionali di riferimento.

La Digital Transformation ed il Sistema Informatico Dipartimentale della Sicurezza

In un contesto esigente ed innovativo come quello italiano della sicurezza fisica, con una storia evolutiva che già nel 2009 consentiva a Citel di rendere pubblico in sede Associazione Bancaria Italiana l'*open-PSIM*, la ***Digital Transformation*** ha trovato non solo un terreno fertile ma processi già maturi riguardo ai ***sei pilastri*** che la definiscono e che, applicati alla gestione informatizzata della sicurezza fisica, possono essere sintetizzati come segue:

1. Automazione della gestione delle segnalazioni mediante *processi programmati* a fronte di segnali, eventi o situazioni;

2. Informatizzazione dei processi di gestione, direzionali o da Control-Room, valorizzati dall'impiego di applicazioni di tipo *Analytics*; anche con la flessibilità e l'articolazione favorita dalle soluzioni di *Cloud Computing* come alternativa od a complemento di Server fisici per i processi operativi primari o secondari o complementari;

3. Dematerializzazione dell'interazione tra gli addetti in campo come naturale effetto di tutti i processi che permettono la *riduzione al minimo degli spostamenti fisici*;

4.Virtualizzazione della strumentazione, dei comandi operativi, del feed-back, del reporting;

5. Edge computing con l'*impiego di dispositivi periferici intelligenti e comunicanti*, compresa la telefonia mobile, l'IOT, le soluzioni in genere di messaggistica per l'interazione informativa ed operativa tra il sistema di gestione e l'addetto in campo;

6. System of Engagement con *processi focalizzati sui comportamenti* delle persone e *contestualizzati* in tempo reale ai fini di un loro efficace coinvolgimento.

La qualificazione del mercato italiano e dell'Ecosistema open-PSIM

L'Italia ha avuto un incontestabile ruolo di innovatore riguardo al tema dell'informatizzazione della sicurezza fisica: la grande e media utenza nazionale è sempre stata in prima linea nell'evoluzione in proposito, anche rispetto al quadro internazionale, grazie in particolare al ruolo ed al peso dei Security Manager, indipendentemente dal fatto che fossero di estrazione informatica o provenienti dalla sicurezza nazionale.

È stato il mercato italiano ad imboccare per primo la strada dei protocolli pubblici di telegestione su rete dati condivisa ed anche il primo a consolidare modelli di progetto in chiave di **apertura multifornitor**e, un requisito oggi ben radicato nel settore in Italia, ma non altrettanto nei Paesi con una prevalenza di grandi produttori multinazionali, portati comprensibilmente a difendere la vendita di prodotti propri a catalogo integrati nel sistema.

In Italia si sono quindi verificate precocemente le condizioni di apertura per far crescere negli anni **un *Ecosistema* aperto del paradigma PSIM che, in nome dell'informatizzazione dipartimentale della sicurezza fisica, ha prodotto evoluzione tecnico-applicativa, economie di scopo e di scala, specializzazione e qualificazione di Terze Parti di integrazione, installazione e manutenzione.**

L'utenza di Citel ed i terzi appartenenti all'Ecosistema sono arrivati già da tempo ad essere **la comunità più numerosa del settore italiano del open-PSIM**, ma, soprattutto, quella che ha contribuito maggiormente all'evoluzione funzionale dei processi, se non altro per il fatto che l'Ecosistema di Citel è arrivato a consolidare una comunità di oltre 100 sistemi grandi e medi, con un catalogo di quasi 150 moduli di integrazione per prodotti e sistemi di terzi produttori a fini di interoperabilità e un numero in proporzione di integratori ed installatori via via scelti dagli stessi utenti finali e supportati da Citel nella trasformazione digitale del loro ruolo.

I SEMINARI DI ESSECOME

DIGITAL TRANSFORMATION DELLA GESTIONE INFORMATIZZATA DELLA SICUREZZA FISICA

16 APRILE 2019
Hotel Hilton Garden Inn - Via Columella, 36

Nella mattina del 16 e del 17 aprile sarà possibile partecipare a dimostrazioni di Centrax SM (Situation Manager), la nuova generazione dell'open-PSIM più diffuso in Italia predisposto per l'utilizzo delle innovazioni della Digital Transformation, a cominciare dalla gestione eventi supportata da funzioni di Artificial Intelligence.

Per informazioni e richiesta di partecipazione scrivere a segreteria@securindex.com

Il quadro attuale del settore della sicurezza fisica informatizzata e le tendenze di fondo in corso dimostrano a distanza di anni che un vero Sistema Informatico dipartimentale potrà essere costruito solo su basi fondate su progetti dichiaratamente aperti ed evolutivi, su scelte basate sui fatti e sull'appartenenza ad un comunità di utilizzatori e di Terze Parti di servizio, su referenze storiche a garanzia di affidabilità e professionalità. Tutti requisiti fondamentali per una prospettiva – insita nella natura del sistema informatico – *di un **life-long project supportato da una software factory** specializzata e dedicata al PSIM ed all'interoperabilità sostenibile.*

Si tratta di condizioni irrinunciabili, verificabili nella storia del settore della sicurezza e ovviamente dei Sistemi Informatici gestionali, dove si sono consolidati nel tempo soltanto i modelli multifunzionali e multifornitore, strutturati non solo sul piano tecnico ma anche della valorizzazione dell'Ecosistema di comunità di produttori complementari e terze parti operanti secondo principi di sinergia naturale incanalati in un contesto organico di tipo ERP.

Controllo accessi semplice dormakaba exivo per il B&B Bonalberti di Verona

a cura della Redazione

Il B&B Bonalberti di Verona nasce a seguito della ristrutturazione di un appartamento a cura dello studio di architettura Giurato-Fabri, con una solida esperienza trentennale nella progettazione architettonica attenta alle esigenze del committente. Il progetto prevedeva l'adeguamento dell'appartamento in una struttura B&B con la creazione di due miniappartamenti.

Esigenza del cliente

L'esigenza del cliente, proprietario della struttura, era quella di poter monitorare, modificare e assegnare le autorizzazioni di accesso per gli ospiti in modo semplice e sicuro anche a distanza, senza la necessità di presidiare fisicamente la struttura. Inoltre, il cliente richiedeva una soluzione di controllo accessi "smart", che non prevedesse l'utilizzo di tessere o chiavi per accedere alle stanze.

Soluzione implementata

La soluzione scelta è stata quella di **dormakaba exivo**. **exivo** è, infatti, un sistema di controllo accessi semplice da installare ed utilizzare che si adatta perfettamente alla gestione, anche a distanza, di una piccola struttura ricettiva.

La piattaforma exivo è accessibile e gestibile via browser in qualsiasi momento, da qualsiasi luogo e dispositivo (pc, tablet, smartphone).

Attraverso exivo, l'utente può inviare facilmente le credenziali di accesso al visitatore, rappresentate da un codice PIN utilizzabile per aprire la porta di ingresso esterna, quella blindata del B&B e quella dei singoli miniappartamenti prenotati. Le porte sono state dotate di un'antenna dormakaba 90 02 con tastiera per inserimento PIN. In alternativa, l'ospite può comodamente aprire le porte con il suo smartphone cliccando l'icona che compare sullo schermo del proprio telefono, contenuta in un messaggio sicuro in formato HTTPS.

Con la funzionalità "Visitatore" dell'applicazione exivo, il proprietario della struttura può inviare quindi il codice di accesso all'ospite specificando le porte a lui autorizzate all'accesso e le finestre temporali di validità del codice in funzione del tempo di soggiorno da lui prenotato.

dormakaba

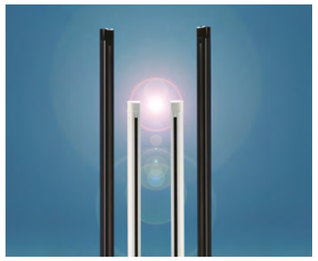
CONTATTI: DORMAKABA ITALIA
Tel. +39 051 41 78311
Tel. +39 02 494842
info.it@dormakaba.com
www.dormakaba.it

L’eccellenza nella protezione per esterno firmata HESA

a cura della Redazione

HESA offre una gamma completa di protezioni perimetrali per esterno, diverse per applicazioni e campi di utilizzo, in grado di soddisfare ogni specifica esigenza di sicurezza: barriere elettroniche, a microonde o infrarossi attivi, rivelatori volumetrici per esterno, scanner laser, sensori per recinzione, telecamere termiche e software di analisi video per la rilevazione di persone e oggetti in movimento.
All’interno della gamma, entriamo qui nel dettaglio delle caratteristiche e delle prestazioni delle barriere a raggi infrarossi per esterno **HESA Serie 5000, 7000, 8000, 8000A, 7000** e delle colonne **Serie 6000, 4498 e 4598**, che consentono di proteggere con efficacia gli ambienti esterni adattandosi a diversi contesti.

Serie 5000 - Barriere a raggi infrarossi codificati per porte, finestre e lucernari



Le barriere **HESA Serie 5000** rappresentano la soluzione completa, affidabile e conveniente per la protezione discreta di porte, finestre e lucernari, consentendo all’utente di lasciare porte e finestre aperte. Ogni fascio è costituito da 2 raggi indipendenti e separati, per evitare che gli insetti possano interrompere il fascio e attivare l’allarme. L’interruzione di un singolo raggio, infatti, non provoca alcun allarme. Il design discreto e la cura di tutti i dettagli rendono queste barriere le più idonee a soddisfare ogni esigenza. La disponibilità della prolunga di raccordo permette di completare l’installazione fino all’altezza del serramento, per un migliore risultato estetico.

Serie 8000, 8000A e 7000 - Barriere a raggi infrarossi per esterno per la protezione di perimetri e di facciate di edifici

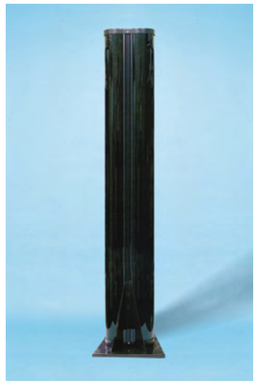
Le barriere **HESA Serie 8000** risolvono il problema dell’affidabilità in esterno e permettono una semplice e veloce installazione. Fornite pre-cablate e già comprese di basamento in acciaio, con una portata di 60 metri sono la soluzione ideale per la protezione di un ambiente esterno quale il perimetro di un edificio. Una molteplicità di fasci assicura la massima stabilità anche nelle più avverse condizioni atmosferiche e l’impostazione in AND di fasci adiacenti elimina i falsi allarmi.
Le barriere Serie 8000 hanno ottiche ruotabili a triplo raggio infrarosso codificato per eliminare interferenze reciproche, con compensazione automatica della luce solare e dispongono del relè di disqualifica ambientale che interviene quando il segnale scende gradatamente, come in caso di nebbia, neve o pioggia fitta.
La disponibilità di 4 modelli da 2 a 5 fasci a seconda dell’altezza da 1 a 2.5 metri della colonna, che può essere integrata con una lampada, permette all’installatore di scegliere il modello più idoneo alle esigen**ze del cliente.**
La Serie 8000 è affiancata dalla Serie 8000A, che mantiene le stesse caratteristiche e prestazioni e che si differenzia per avere le ottiche impostate a 90° per il montaggio ad angolo.

La Serie 8000 è inoltre affiancata dalla **Serie 7000** per installazione a parete, per la protezione esterna di facciate di edifici, dotata delle stesse caratteristiche tecniche che ne garantiscono affidabilità e facilità di installazione. Una sola barriera protegge un’intera facciata fino ad una distanza di 60 metri e, come la Serie 8000, dispone di termostato e di riscaldatore integrati, di uscita per l’allineamento strumentale e di una morsettiera di connessione, oltre alle staffe per il fissaggio.

Serie 6000 - Colonne GARDIAN cilindriche per barriere a raggi infrarossi

Dotate di forma cilindrica di diametro contenuto, le colonne **GARDIAN Serie 6000** rappresentano la soluzione ideale per la protezione degli spazi esterni integrandosi perfettamente all’ambiente mantenendo un livello estetico elevato, grazie alla possibilità di essere utilizzate come lampada o lampione da giardino, in un unico apparecchio. All’interno della colonna è possibile alloggiare barriere a raggi infrarossi o a microonde che possono essere orientate lungo un arco di 180°, mentre lo schermo nero trasparente ai raggi infrarossi consente di mascherare la dislocazione dei gruppi ottici per impedirne l’esatta individuazione. Il robusto profilato in alluminio anodizzato e lo schermo in policarbonato resistente agli urti consentono installazioni solide e durature nel tempo anche in condizioni ambientali e atmosferiche avverse. L’installazione richiede il fissaggio al suolo mediante basamento opzionale da fissare a una base in cemento di facile realizzazione. Sono disponibili in altezze standard di 1, 1.5, 2, 2.5 e 3 metri.

Serie 4498 e Serie 4598 - Colonne GARDIAN semicilindriche monofacciali e bifacciali per barriere a raggi infrarossi



La forma semicilindrica delle colonne **Serie 4498**, con una larghezza di mm 178 e una profondità di mm 156, permette di orientare i fasci delle barriere o della microonda sull’intero arco di 180°. Lo schermo nero trasparente solo ai raggi infrarossi non consente di individuare la dislocazione e l’orientamento dei gruppi ottici. Il robusto profilato in alluminio consente il fissaggio della colonna a parete, su basamento o l’abbinamento con un’altra colonna per una protezione a 360°. Il coperchio in alluminio è provvisto di fessure di areazione per evitare la condensa di vapore acqueo. Alla Serie 4498 si affianca la Serie 4598, che permette di orientare i fasci delle barriere o della microonda sull’intero arco di 360°. Queste barriere sono particolarmente adatte alla protezione di lunghi perimetri e nei contesti dove è richiesto un elevato livello di sicurezza.

Nel sito web di HESA è possibile approfondire l’intera proposta delle protezioni per esterno offerte dall’azienda.

CONTATTI: HESA SPA
Tel. +39 02 380361
www.hesa.com

RISCO Group rinnova e potenzia Agility™4, il sistema di sicurezza radio bidirezionale

a cura della Redazione

Agility™4 è il sistema di sicurezza radio bidirezionale di ultima generazione di **RISCO Group** – società indipendente leader a livello globale specializzata nello sviluppo, nella produzione e nella commercializzazione di un'ampia gamma di soluzioni di sicurezza integrate – di cui è disponibile una nuova versione, potenziata in termini di sicurezza, affidabilità e rinnovata nel design rispetto alle versioni precedenti.

Agility™4 integra, grazie alla tecnologia cloud, le funzionalità di Video Verifica di **VUpoint** – progettato per installazioni residenziali e aziende di piccole e medie dimensioni – ed è in grado di garantire livelli di sicurezza e praticità senza eguali, oltre a proteggere da pericoli quali incendi, allagamenti o fughe di gas, indirizzando le esigenze in continua evoluzione del mercato in termini di soluzioni radio, cloud-based e integrate con applicazioni di gestione, controllo e video verifica live plug&play.
Infatti, tramite VUpoint, Agility™4 abilita la video verifica in tempo reale e live streaming, nonchè la ricezione di immagini in alta definizione in caso di allarme in corso o su richiesta, tramite **PIR CAM radio** e/o **VUpoint P2P**. Infine, è possibile gestire il nuovo sistema di RISCO in modo semplice e intuitivo tramite l'app per smartphone iRISCO e web browser, grazie alla possibilità di inviare agli utenti finali e alle vigilanze notifiche push, immagini e video sia di giorno che di notte. Offre anche la possibilità di controllare i sistemi installati ovunque ci si trovi, assicurando un livello di sicurezza senza precedenti.

Agility, grazie alla tastiera LCD, risponde alle esigenze del mercato, che, per la quasi totalità dell'attuale offerta prevede centrali di allarme con tastiere integrate a bordo che, per essere sfruttate, richiedono l'installazione della centrale in prossimità dell'ingresso, risultando quindi facilmente attaccabili da parte di malintenzionati: distruggendo e/o rimuovendo la centrale, vengono disabilitate le chiamate di soccorso e cancellata qualsiasi prova di quanto accaduto.
La tastiera LCD di Agility è remota – e non integrata – e permette quindi di posizionare la centrale in un luogo sicuro e lasciare la tastiera in prossimità dell'ingresso: in questo caso, la distruzione e/o rimozione della tastiera non impedirà alla centrale di effettuare le chiamate di soccorso e al cloud RISCO di tenere memoria di quanto accaduto.
Proprio per questo motivo, arricchito con la nuova tastiera wireless **Panda** e l'elegante telecomando – oltre a un'ampia gamma di accessori radio bidirezionali, contatti e sensori per interni ed esterni – il sistema Agility™4 è in grado di garantire una portata radio sensibilmente incrementata per prestazioni ancora più elevate.

Agility™4 offre la possibilità di gestire fino a 32 zone, include 8 PIR con fotocamera e offre il supporto a tutte le più avanzate tecnologie di comunicazione disponibili – tra cui PSTN, IP, GSM 2G & 3G e GPRS – per poter configurare più canali contemporaneamente, assicurando la massima ridondanza e resilienza nel sistema di comunicazione.

Completa l'offerta di Agility™4 anche una gamma completa di accessori per la sicurezza delle persone, per l'antintrusione e supporta la Smart Home, che può essere integrata come componente aggiuntiva su tutti i sistemi

di sicurezza RISCO purchè collegati al Cloud e gestita tramite iRISCO. L'utente finale può così gestire in maniera smart la propria abitazione, inclusi consumi energetici, tapparelle, elettrodomestici e accessi, migliorandone contestualmente comfort e sicurezza direttamente dal proprio smartphone.

"La scelta di sistemi di sicurezza integrati con Smart Home e video verifica è un trend in forte crescita tra gli utenti residenziali e le piccole e medie imprese. Proprio per indirizzare le esigenze in continua evoluzione del mercato, RISCO Group ha progettato il nuovo Agility™4, la risposta puntuale ed efficace dell'azienda nata dalla combinazione vincente di sicurezza, protezione, video verifica e smart home. Anche in questo caso, il Cloud di RISCO – che rappresenta un paradigma comune a tutte le soluzioni dell'azienda – ci ha permesso di differenziarci sul mercato integrando in una sola applicazione antintrusione, video verifica e smart home, oltre a garantire a utenti e sistemi di vigilanza l'accessibilità dei dati, la stabilità e la continua disponibilità del sistema," ha dichiarato **Ivan Castellan**, Branch Manager di **RISCO Group Italia**.

Scopri online Agility™4!

RISCO GROUP

CONTATTI: RISCO GROUP
Tel. +39 02 66590054
www.riscogroup.it

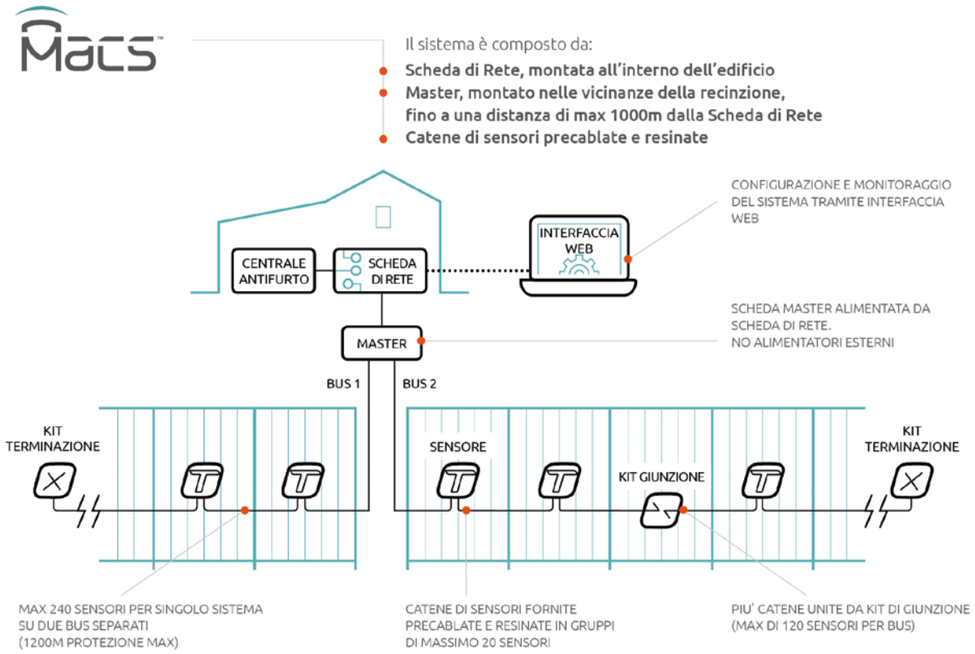
Macs, la protezione perimetrale evoluta

a cura della Redazione

MACS è il sistema di anti-intrusione perimetrale studiato da **TSec** per recinzioni metalliche rigide e semirigide.
Sfruttando la tecnologia **MEMS** e grazie ad un sofisticato algoritmo studiato e testato da **TSec**, MACS è in grado di segnalare tentativi di scavalcamento, minimizzando al tempo stesso rilevazioni improprie dovute a pioggia e vento, alla presenza di strade, ferrovie o macchinari situati nelle vicinanze della recinzione e persino ad azioni umane non assimilabili allo scavalcamento.
MACS è altresì in grado di riconoscere tentativi di manomissione eseguiti sulle schede di controllo, sui sensori o sul cavo, nonché tentativi di taglio, sfondamento e/o rimozione del pannello della recinzione.
È inoltre possibile identificare in maniera univoca ciascun sensore sia in fase di programmazione che di monitoring, fornendo una precisa indicazione del sensore che ha generato l'allarme.
La progettazione partita dalla ricerca di una soluzione perimetrale per grandi estensioni non ha trascurato la flessibilità e l'adattabilità ad impianti residenziali di dimensioni più contenute.

Il sistema è composto da:
- catene di sensori collegati tra loro attraverso bus proprietario
- una scheda master posta sul campo, nella quale convergono le catene di sensori
- una scheda di rete, posta in interno, che alimenta tutto il sistema e si interfaccia con la centrale di allarme e il mondo IP.

La configurazione e la gestione del sistema avviene attraverso una semplice ed intuitiva interfaccia web.



Sensori:
Il sensore è racchiuso in un contenitore in tecnopolimero rinforzato con fibra di vetro dal design compatto ed elegante, che si sposa con le esigenze estetiche senza tralasciare quelle pratiche. La speciale forma consente infatti l'installazione rapida dei sensori con singola vite centrale e contropiastra sulle diverse tipologie di recinzione.
I sensori sono precablati e completamente resinati in fabbrica, garantendo la protezione IP68 ed il minimo tempo di installazione.
Lo speciale design interno del contenitore del sensore fornisce grande resistenza allo strappo del cavo, garantendo robustezza ed affidabilità al sistema stesso.
Il sistema prevede il collegamento di massimo due linee di sensori, fino ad un massimo di 120 sensori per linea.
Ogni sensore può essere montato (a seconda della grandezza dei pannelli della recinzione) tipicamente ogni due pannelli o ad una distanza massima uno dall'altro di 5 metri. La distanza massima di copertura di un singolo sistema può arrivare fino a 1200 metri di recinzione.
È possibile installare i sensori anche sui pali di supporto dei pannelli.

Scheda Master:
La scheda di controllo, denominata Master, è in grado di gestire fino ad un massimo di due catene su bus di comunicazione indipendenti, per un totale di 240 sensori.
Il Master è contenuto in una scatola stagna di dimensioni ridotte, viene installato in esterno ed è alimentato attraverso il cavo che lo collega alla scheda di rete, posta all'interno della struttura. Il cavo può avere una lunghezza fino a 1 chilometro.

Questa configurazione permette all'installatore di non dover portare all'esterno alimentazione 220V e non dover installare armadi contenenti alimentatori e batterie tampone dedicate.

Scheda di rete:
La scheda di rete ha a bordo 8 relè di uscita configurabili + 1 relè di tamper per poter interfacciare il sistema MACS con una centrale di allarme. Viene altresì connessa alla rete attraverso la porta ethernet per permettere la programmazione e gestione del sistema sia in locale che in remoto attraverso l' interfaccia web.
La scheda di rete, pensata quindi per essere installata in prossimità della centrale di allarme o di un concentratore, permette di alimentare tutto il sistema grazie ad un ingresso 12V DC. Il consumo massimo di un sistema completo è di 3A.
È possibile acquistare la scheda di rete comprensiva di alimentatore in un comodo e robusto contenitore metallico.

Interfaccia web:
L'interfaccia di programmazione fornisce all'installatore una grande flessibilità nella programmazione, con la possibilità di impostare tutti i parametri di sistema, delle uscite, delle zone e di ogni singolo sensore.
I sensori si auto-inizializzano alla prima installazione o su richiesta dell'installatore stesso ed il Master assegna in automatico un indirizzo univoco a ciascun sensore, che verrà poi utilizzato per la programmazione ed il monitoraggio puntuali.
È possibile abilitare un pop-up degli allarmi sull'interfaccia, per permettere a vigilanza o guardie a presidio del sito protetto di visualizzare in tempo reale eventuali allarmi ed individuarne in modo tempestivo il punto esatto. Tutte queste attività sono possibili anche da remoto.
È possibile consultare il log degli ultimi 10.000 eventi del sistema con i relativi dati rilevati sul sensore che ha generato l'allarme.

Per le sue peculiarità di rilevazione e per la semplicità di installazione e configurazione, il sistema MACS rappresenta oggi una soluzione straordinaria per efficacia e affidabilità con le tecnologie di analisi piu' innovative presenti sul mercato.

MACS è:

• **Sicuro e affidabile:** la tecnologia di rilevazione Mems e i sofisticati algoritmi di analisi proprietari permettono al sistema una rilevazione certa dello scavalcamento e una elevatissima capacità di discriminazione di tutti gli eventi ambientali di disturbo.

• **Intelligente:** la funzione di calibrazione di MACS permette al sistema di apprendere la tipologia di recinzione su cui è installato, memorizzandone le frequenze di risonanza e i modi di vibrare. Questo permette di analizzare la vibrazione e riconoscere con precisione l'evento.

• **Puntuale:** il bus di collegamento dei sensori permette di individuare, in caso di allarme, il punto preciso che lo ha generato e permette all'installatore una taratura fine di sensibilità e ritardo che può arrivare fino al singolo sensore.

• **Flessibile:** l'nterfaccia web permette la gestione dei sensori e l'associazione alle zone senza nessun vincolo di posizione. La calibrazione e la taratura puntuale dei sensori permettono l'utilizzo del sistema su tipologie diverse di recinzione nella stessa installazione.

• **Rapido:** l'installazione dei sensori con singola vite e la configurazione con interfaccia web flessibile garantiscono un tempo di installazione e programmazione estremamente rapido, grazie anche all'assenza di alimentazione 230v in esterno.

TSec
TECHNOLOGY FOR SECURITY

CONTATTI: TSec SpA
Tel. +39 030 5785302
www.tsec.it

Macs

La recinzione diventa intelligente.

MACS. Sistema antintrusione perimetrale per recinzioni metalliche rigide e semirigide.

SOFTWARE DI GESTIONE | SCHEDA DI RETE | MASTER | 2 CATENE DA MAX 120 SENSORI CIASCUNA

TSec
TECHNOLOGY FOR SECURITY

www.tsec.it

3P Elettronica presenta le Centrali EOS, vera novità nel settore della sicurezza

intervista a Saverio Parisi, responsabile commerciale di 3P Elettronica

Ci può presentare 3P Elettronica, le linee di prodotto e i progetti?
Siamo una azienda che costruisce apparecchiature elettroniche per la sicurezza. Le nostre linee di prodotti sono sensori da interno a doppia tecnologia, combinatori telefonici GSM, centrali da 6 a 128 zone con GSM integrati, schede chiavi universali, sirene e schede accessori varie come schede relè ecc.
Le nostre prime esperienze di costruzione risalgono alla centrale G6 realizzata per conto di GUARDALL e al combinatore SEKURVOX, uno dei primi combinatori telefonici su linea GSM con guida vocale.
Sulla base dell'esperienza acquisita, abbiamo man mano espanso la linea prodotti con la costruzione del nuovo combinatore telefonico ALICE VOX e le nuove centrali della linea INFINITY.
Le centrali serie INFINITY sono molto apprezzate dagli installatori in quanto abbinano una grande versatilità ad una programmazione semplice e intuitiva.
Le centrali INFINITY sono sempre corredate di GSM modulo vocale e tastiera touch screen capacitiva. Grazie all'ottimo rapporto qualità/prezzo, le vendite delle centrali si assestano intorno a 5.000 unità annue.
In funzione delle nuove esigenze di mercato, tra cui web server e video verifica integrata, con uno sforzo notevole in termini di progettazione, risorse ed investimenti, abbiamo sviluppato nel 2018 una nuova linea di centrali chiamata EOS, che risponde alle crescenti richieste di mercato e esula dalle classiche concezioni delle centrali di sicurezza presenti sul mercato.

Parliamo di questa novità. Quali sono le caratteristiche di EOS?
La nuova centrale EOS esce dai canoni tradizionali di una centrale di allarme. EOS si sviluppa su 4 piattaforme principali: Sicurezza, Videocontrollo, Domotica e GPS.

Sicurezza: le centrali EOS riprendono la filosofia di programmazione delle centrali INFINITY, quindi grandi performance con programmazioni intuitive con un web server integrato ed una tastiera touch screen grafica. Sempre come INFINITY sono realizzate in due versioni: 8/32 zone e 8/128 zone.
Il web server permette di programmare la centrale con un PC, con un tablet o semplicemente con uno smartphone, perché il software di programmazione non è installato sul PC ma è integrato in ogni singola unità di centrale.
La centrale inoltre si connette automaticamente al nostro server con funzioni di cloud. L'installatore può, quindi, connettersi anche da remoto previa autorizzazione dell'utente ed effettuare tutte le operazioni di programmazione. Tutte le centrali, oltre al GSM, al modulo LAN e alla sintesi vocale da remoto, hanno integrato un modulo radio bidirezionale 868 MHz con molteplici accessori radio tra cui:
- un tripla tecnologia da esterno
- doppia tecnologia da interno
- sensori a tenda
- un nuovissimo contatto magnetico che include 5 tecnologie: reed magnetico, sensore tapparelle, sismico, accelerometro e tamper sulla manomissione del magnete
- telecomando bidirezionale a 4 tasti.

Infine la tastiera touch screen grafica permette all'utente di effettuare operazioni tipo inserimento/disinserimento, esclusioni zona, cambio pin, ecc in maniera intuitiva.
Nella tastiera touch screen è alloggiato un sensore rfid per la gestione con chiave elettronica.
Mini espansioni d'ingresso e di uscita e attivatori esterni completano la gamma relativa alla sicurezza.
Ulteriore novità per la sezione sicurezza sono le EEPROM estraibili. Una contiene tutta la programmazione e può essere trasferita da una centrale all'altra; l'altra tutta la memoria eventi - circa 1200 - che può essere anche stampata.
È importante accennare qualcosa del nostro server. Ogni centrale all'accensione si connette automaticamente al server, il quale monitorizza perennemente le centrali e, in caso di attacco Jammer sul GSM o taglio della linea telefonica, informa immediatamente l'utente con un messaggio di testo.
Il server effettua ogni ora un backup su un server esterno.
La centrale può connettersi a qualsiasi istituto di vigilanza utilizzando il SIA IP DC09 sia con linea LAN che con GPRS

Videocontrollo: Altra piattaforma sono le telecamere IP. La centrale gestisce fino ad un massimo di 16 telecamere IP dedicate. Sono disponibili sia telecamere da interno che da esterno, tutte da 2MP e con la possibilità di gestire il "parla-ascolta".

Domotica: la centrale EOS gestisce inoltre 60 moduli domotici per luci e tapparelle, controllo carichi e sensori di temperatura, tutti WI-FI e gestibili anche con Google Home. Gestisce inoltre ad apparati domotici per la gestione delle temperature e dei carichi. Ulteriore novità nell'ambito domotico è il ricevitore IR smart WiFi per trasferire ogni comando del telecomando (condizionatore, TV, apparati audio, ecc.) e renderli parte integrante del sistema domotico. Quindi qualsiasi condizionatore può essere attivato da remoto e regolato in temperatura.

GPS: ultima piattaforma è il GPS che per la prima volta entra a far parte dei sistemi di sicurezza. Praticamente, l'auto può diventare una zona remota della centrale che si allarma se viene aperta o spostata ed è possibile individuarla tramite una APP dedicata La centrale controlla anche anziani che possono allontanarsi da casa e smarrirsi.

Ecco perché affermiamo che EOS è la centrale di "seconda generazione". La centrale multipiattaforma, tutta gestibile dall'utente con una unica APP suddivisa in quattro categorie: Centrale Allarme – Domotica – TVCC – GPS. Tramite questa APP l'utente ha il completo controllo della sua abitazione e della sua attività.
Ultima, ma non trascurabile osservazione è l'impatto costo/prestazioni. Abbiamo fatto uno sforzo di carattere tecnico per riuscire a concentrare tutte queste tecnologie e la gestione della tastiera touch su un microprocessore ARM di ultima generazione, quindi allineati dal punto di vista economico con le centrali tradizionali.

Quali sono le tipologie di utilizzatori finali cui è rivolta?
La centrale EOS è indicata, a seconda dei tagli, nell'ambito residenziale, commerciale e industriale. Le sue prestazioni la rendono molto versatile soprattutto in ambito industriale. Infatti la centrale è dotata di 8 timer indipendenti, per inserimenti automatici, blocco di utenti a determinate ore, festività e controllo ronda della vigilanza. La centrale gestisce inoltre un piccolo controllo accessi integrato con una memoria eventi differenziata.

Quali sono i vostri partner di canale per la distribuzione sul territorio?
Noi ci rivolgiamo esclusivamente a distributori di sistemi di sicurezza. Da sempre abbiamo utilizzato i distributori come nostri unici interlocutori. Tramite loro riusciamo a far confluire tutte le novità tecniche e a organizzare corsi specifici con gli installatori. Poniamo i nostri distributori nella condizione di completa autonomia sia dal punto di vista tecnico che commerciale.

ERMES presenta un nuovo gateway over IP per la diffusione sonora nelle aree urbane

a cura della Redazione

ERMES ha introdotto una nuova versione dell'amplificatore audio Over IP da 40W che si differenzia dalle precedenti per essere alimentata direttamente a 230Vac e per essere realizzata in un contenitore in poliestere caricato vetro, quindi adatto anche all'installazione in ambienti con atmosfera corrosiva, come avviene in prossimità del mare. Questo gateway amplificato Over IP, utilizzato in unione a una coppia di trombe da 20W, si presta in maniera ottimale per essere installato direttamente sui pali dell'illuminazione pubblica, come spesso viene richiesto nella sonorizzazione di aree urbane.

Una tipica applicazione per questa soluzione è la sonorizzazione delle passeggiate prospicienti i lungomari di cittadine a vocazione turistica e, in generale, di strade, viali, piazze o parchi pubblici.

Il collegamento di rete può essere realizzato in rame o in fibra, ma può essere adottato anche un collegamento dati in WiFi.

Questo sistema consente sia la diffusione di musica di sottofondo sia la diffusione di annunci che possono essere effettuati dal vivo utilizzando una console microfonica anche in maniera automatica, installando su un PC un apposito software che, sulla base di una programmazione oraria preimpostata, trasmette ai gateway annunci memorizzati in precedenza.

Gli annunci possono essere effettuati non solo da una postazione fissa ma anche in mobilità completando il sistema con un gateway GSM che, grazie ad una apposita applicazione, consente di effettuare annunci da un qualsiasi smartphone.

Quest'ultima caratteristica rende il sistema particolarmente adatto ad essere utilizzato anche in occasione di manifestazioni che richiamano un elevato numero di persone quando non è semplice disporre di una postazione fissa per la diffusione di annunci. In questo caso è possibile effettuare delle installazioni provvisorie grazie alla semplicità di installazione e configurazione degli apparati.

CONTATTI: ERMES ELETTRONICA SRL
Tel. +39 0438 308470
www.ermes-cctv.com

Straordinaria qualità di immagine per la gestione del traffico con AXIS Q1785-LE

AXIS COMMUNICATIONS
(+39) 02 8424 5762
www.axis.com

AXIS Q1785-LE è una telecamera di rete con risoluzione HDTV 1080p fino a 60 IPS, progettata soprattutto per applicazioni di monitoraggio del traffico, con zoom ottico 32x per un'alta qualità di immagine anche a distanze rilevanti, catturando con estrema nitidezza dettagli come le targhe delle auto o il loro colore.

Con un grado di resistenza agli urti IK 10, la classe di protezione IP66, IP67 e NEMA 4X, l'intervallo di temperatura da -40°C a + 60°C, lo sbrinamento automatico della finestra anteriore e la membrana integrata per la deumidificazione, permette di ottenere alte prestazioni anche in condizioni climatiche estreme e un utilizzo ottimale anche nell'oscurità più totale, grazie a illuminatori LED con portata fino a 80 metri e la funzionalità **OptimizedIR**.

È dotata di tecnologie uniche come **AXIS WDR – Forensic Capture**, per dettagli chiari e definiti in situazioni di forte controluce, **AXIS Lightfinder** per immagini estremamente luminose anche nel buio più profondo, stabilizzazione elettronica dell'immagine per compensare eventuali vibrazioni e le modalità predefinite Forensic, Vivid e Traffic che ne rendono l'utilizzo più semplice.

Inoltre, **Axis Zipstream** riduce la larghezza di banda e lo spazio di archiviazione senza compromettere la qualità delle immagini e gli algoritmi di analisi **AXIS Motion Guard, AXIS Fence Guard** e **AXIS Loitering Guard** integrati a bordo consentono una videosorveglianza proattiva di interni ed esterni. Infine, **Axis Corridor Format** adatta facilmente l'area di visualizzazione alle varie situazioni aumentando l'efficienza in tutte le applicazioni.

TM70 touchscreen di PARADOX: connubio di design e semplicità di utilizzo

DIAS SRL
(+39) 02 38036901
www.dias.it

La tastiera **TM70** touchscreen di **PARADOX**, distribuita da **DIAS**, presenta una forma sottile ed elegante, in linea con le più attuali tendenze dell'arredamento e consente di gestire l'impianto di allarme in modo intuitivo grazie a un menù guidato e interattivo, con la possibilità di personalizzare le etichette zone, le aree, i codici utenti e le uscite programmabili.

TM70 permette all'utente di caricare fino a 32 planimetrie e foto a colori dei locali protetti, consentendogli di vedere in tempo reale l'intero sistema su un unico display con lo stato delle singole zone.

L'ampio schermo da 7 pollici permette di visualizzare meglio tutte le informazioni del sistema e, attraverso la funzione di cornice digitale, di vedere immagini e foto con un'elevata risoluzione.

La forma compatta e sottile permette un semplice fissaggio a parete.

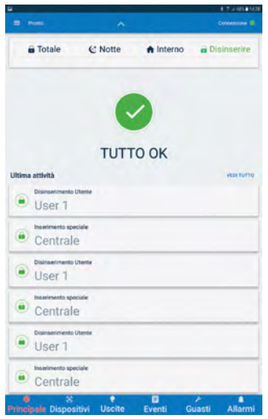
La tastiera garantisce l'attivazione e disattivazione fino ad otto uscite programmabili in modo semplice e intuitivo. Tra le funzioni utili per gli utenti finali, evidenziamo la possibilità di visualizzare la temperatura, di regolare la retroilluminazione, il volume e la sensibilità del touchscreen.

La tastiera TM70, che si affianca al modello **TM50** con schermo da 5 pollici, è compatibile con i sistemi **Spectra, EVO e Magellan MG5000/MG5050.**

Inoltre, supporta il server **Swan** di nuova generazione, il bus RS-485 veloce e criptato, permette la programmazione completa del sistema tramite menù, aggiornamento locale firmware tastiera, immagini screen saver scaricabili tramite scheda SD.

HESA presenta la nuova app ConnectAlarm per le centrai Serie PowerNeo di DSC

HESA SPA
(+39) 02 380361
www.hesa.com



La **Serie PowerNeo** distribuita da **HES**A soddisfa ogni esigenza di protezione, sia in ambito residenziale che in ambito commerciale.
Con un ottimo rapporto prezzo-prestazioni e interfacce di comunicazione moderne e di facile utilizzo, queste centrali coniugano affidabilità e semplicità di gestione, di manutenzione e di programmazione. Consentono la verifica video degli eventi che generano allarme grazie ai rivelatori per interno e per esterno con telecamera a colori integrata.
Le centrali **Serie PowerNeo** rispondono a tutte le esigenze di sicurezza e comfort degli utenti, con la possibilità di gestione del sistema tramite app dedicata per sistemi iOS e Android, che è oggi al centro dell'attenzione.
È infatti appena uscita la nuova app gratuita **ConnectAlarm** in lingua italiana compatibile con le centrali serie **PowerNeo Versione 1.3** o superiore utilizzate con i comunicatori **3G2080, TL2803G e TL280** Versione 5.03 o superiore. Questa nuova app, che affiancherà per diverso tempo l'attuale app PowerSeries Neo, dispone di queste principali novità:

- grafica completamente nuova
- l'installatore tramite l'app ConnectAlarm Activation, dopo la registrazione deve abilitare la centrale per il cloud
- l'utente può ora selezionare le notifiche che desidera ricevere, allarmi, guasti, inserimenti disinserimenti ripristini, ecc.
- in caso di allarme, i rivelatori senza fili con telecamera a colori PG8934 e PG8944 forniscono, oltre ai 10 fotogrammi, anche un filmato di 5 secondi.

La versione 5.0 del Cloud di RISCO Group

RISCO Group
(+39) 02 66590054
www.riscogroup.it

RISCO Group ha implementato la propria piattaforma Cloud con diverse novità e opportunità di business per i suoi clienti. Ad oggi sono 260.000 le utenze che utilizzano il Cloud di RISCO Group per la gestione dei propri impianti, con un trend in forte crescita. Centralizzando risorse ed intelligenza, la piattaforma Cloud semplifica notevolmente l'installazione e la configurazione delle apparecchiature remote presenti presso i siti degli utenti, garantendo servizi di sicurezza e Smart Home professionali a costi sostenibili.
Inoltre, la piattaforma garantisce sicurezza e privacy grazie all'infrastruttura cloud **Azure** di **Microsof**t.
La versione 5.0 del Cloud di RISCO ha un'interfaccia grafica completamente rinnovata, con funzionalità aggiuntive che vanno dall'anagrafica all'utilizzo di mappe che permettono di gestire al meglio gli interventi per la manutenzione e l'installazione degli apparati.
Le società di installazione che oggi usano il prodotto RISCO godono di un accesso privilegiato e gratuito alla piattaforma che consente un controllo tecnico professionale dei sistemi installati e sempre nuove ed interessanti opportunità per ampliare il proprio business acquisendo nuovi clienti e soddisfacendo le nuove esigenze di quelli attuali.
Il Cloud 5.0 è il punto di partenza di una piattaforma scalabile multifunzione che pone la figura dell'utente finale e della società di installazione al centro della progettazione e dello sviluppo di nuove caratteristiche sempre più sicure, affidabili e performanti.

TSec presenta i contatti magnetici CLH- 201

TSEC SPA
(+39) 030 5785302
www.tsec.it

I contatti magnetici **CLH-201** prodotti da **TSec**, certificati di Grado 3 secondo la norma EN 50131-2-6, offrono la sicurezza della tecnologia antimascheramento brevettata **Magnasphere®** in un robusto involucro di alluminio anodizzato. Non è pertanto possibile inibire l'apertura del contatto con influenze magnetiche dall'esterno del perimetro protetto.
Il sistema modulare per il cablaggio consente l'utilizzo con uscita diretta del cavo, con la guaina armata inox (disponibile come accessorio) o altre guaine con diametro interno di 8mm.
Il sistema anti-rimozione magnetico è più affidabile dei tradizionali meccanismi a micro-interruttori e un livello superiore di sicurezza, senza complicazioni in fase di installazione.
E' possibile montarli in linea o ad angolo retto senza staffe accessorie, per una flessibilità e rapidità di montaggio senza precedenti.
I CLH-201 hanno la resinatura completa sia per l'uso interno che esterno e sono certificati in classe ambientale IV.
La gamma CLH-201 è composta da alcune varianti:
CLH-201-D con il doppio contatto chiuso con magnete presente, per installazioni dove sia richiesto il controllo di due sistemi, ad esempio anti-intrusione e controllo accessi, senza dover installare relais accessori in centrale.
CLH-201-DS con il doppio contatto in scambio
Sono disponibili la versioni a morsetto: in questo caso i contatti sono certificati in classe ambientale II.

essecome ONLINE

n. 01 gennaio 2019
Anno XXXIX
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Angelo Carpani,
Nils Fredrik

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
essecome editore srls
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

REGISTRAZIONE
Tribunale di Milano n. 21
del 31 gennaio 2018

GRAFICA/IMPAGINAZIONE
contatto@lilastudio.it