



Axis Experience Day



L'evento annuale di Axis si trasforma e torna nel 2020 in un veste nuova, per creare un momento di scambio tra tutti gli attori del mercato: dai nostri partner, integratori, distributori, consulenti e progettisti fino agli utenti finali.

Milano

26 Marzo, 2020

Meet | Share | Connect

Studio Novanta (East End Studios)
in Via Mecenate, 88/a
20138 Milano (MI)

Registrati subito

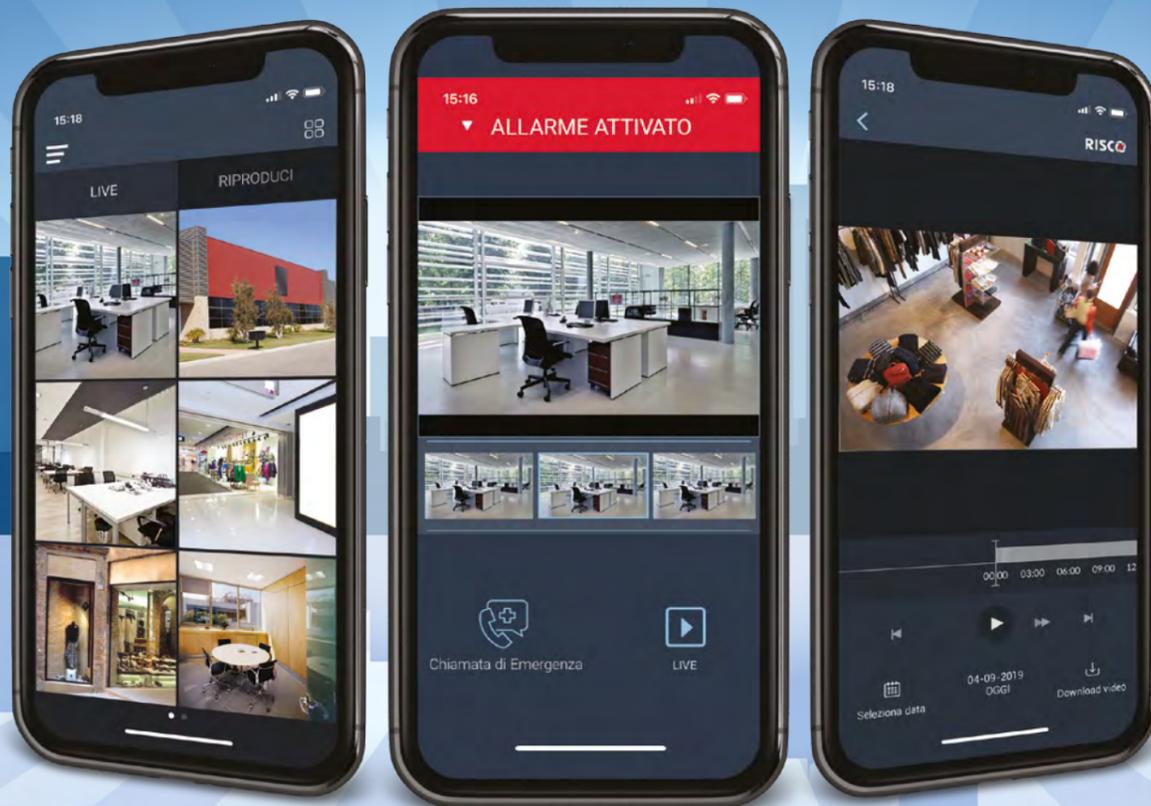


#AxisExperienceDay

#MeetShareConnect

VUpoint NVR

Eleva la Sicurezza integrando Video & Allarme



Live

Video Verifica

Registrazione

Il nuovo VUpoint NVR, un performante sistema di registrazione plug & play, assieme alle telecamere IP VUpoint di RISCO, fornisce una soluzione video unica e completa dall'ineguagliabile capacità di video verifica degli allarmi. Le Soluzioni Integrate di RISCO sono la miglior scelta che potete fare.



Soluzione Video Completa P2P

Ampia gamma di NVR e Telecamere IP per offrire una soluzione personalizzata per ogni applicazione.



Una App. Soluzione Video Integrata

Integrata nelle soluzioni di sicurezza professionali di RISCO per una Verifica degli Allarmi in tempo reale, Live streaming e Registrazione.



Powered by RISCO Cloud

Back Up degli eventi con immagini e clip video, gestione remota da Cloud Installatore ed elevati livelli di Cyber Sicurezza.



Per maggiori informazioni su VUpoint NVR visitate il sito riscogroup.it o scansionate il QRcode

RISCO
GROUP

Sommario Interattivo

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

- 05 Awareness, compliance, security by design: come faranno a sopravvivere le PMI?
- 06 Il Crimine Organizzato nel Retail, un fenomeno in crescita in Italia
- 10 Travel Risk Management, arriverà nel 2021 la ISO 31030 per imprese, università e ONG
- 12 Le tendenze evolutive della sicurezza fisica informatizzata nel 2020. Le convergenze con una recente indagine internazionale
- 15 Video verifica live, registrazione e allarme in un'unica soluzione: VUpoint NVR di RISCO Group
- 16 Premio securindex Installatore Certificato 2019, la parola ai vincitori: Electronic System
- 17 Premio securindex Installatore Certificato 2019, la parola ai vincitori: I.T.S. di Palmisani Marco
- 18 Premio securindex Installatore Certificato 2019, la parola ai vincitori: Tecno Security
- 19 VIGILO4YOU: il "plus" degli Installatori per le abitazioni e lo Small Business
- 20 Varchi automatici Argus: la nuova formula con un design unico e innovativo
- 22 Controllo iniziale e manutenzione dei sistemi di Rilevazione Incendi: pubblicata la Norma UNI:11224
- Redazionali Tecnologie 25



trova il tuo
installatore
certificato

www.securindex.com/installatori

VOLKTEK

Leader mondiale nella produzione di dispositivi di networking per i mercati dell'automazione industriale, della videosorveglianza, della connettività

LAMUNGAN™

Interfaccia semplice e potente per utenti di ogni livello



www.hesa.com

L'editoriale del direttore



Awareness, compliance, security by design: come faranno a sopravvivere le PMI?

Iniziamo il 2020 con una riflessione sul cambio di paradigma della *compliance* (osservanza) delle norme e delle direttive internazionali per la tutela dai rischi (informatici, ambientali, alimentari, ecc), che risulta oggi indirizzata verso criteri di "consapevolezza" e di "responsabilizzazione" e non più all'esecuzione acritica di prescrizioni autoritarie. Come sottolinea Corrado Giustozzi nell'**intervista a essecome**: "Si è passati in modo abbastanza repentino da un approccio interamente prescrittivo, basato su una logica che potremmo definire "dell'adempimento", ad un approccio finalizzato ai risultati e basato su una logica "della responsabilizzazione".

Esaminando le disposizioni più recenti che interessano a vario titolo il mondo della sicurezza, si osserva che norme relative ad ambiti tra loro diversi - come GDPR e Direttiva NIS per la sicurezza delle informazioni, ISO 31030 per la tutela dei lavoratori in missione, Direttiva (UE) 2018/843 sull'antiriciclaggio - condividano in realtà lo stesso approccio impostato su procedure di "analisi dei rischi", "analisi d'impatto" e "progettazione autonoma delle misure di sicurezza" che, almeno in Italia, sono ancora piuttosto sconosciute.

Si starebbe dunque delineando un intrigante salto culturale per l'intero Sistema Paese (aziende pubbliche e private, consulenti, organi di controllo), ma non si possono sottovalutare le conseguenze sul piano pratico, in particolare per le piccole/medie imprese.

Secondo molti osservatori, se le grandi organizzazioni industriali e finanziarie sono già orientate verso questi nuovi approcci o, quanto meno, sono in grado di investire per adeguarsi, le **PMI** possono trovarsi in difficoltà non solo nell'attuare le procedure richieste (magari per un banale motivo di costi) ma, in molti casi, perfino nel sapere dell'esistenza di norme che le riguardano e che devono rispettare.

Sicurezza delle reti e dei dati (per tutti), gestione delle trasferte dei dipendenti (per chiunque lavori all'estero) e procedure antiriciclaggio (per chiunque maneggi denaro contante) potrebbero quindi diventare altrettante occasioni di inadempimento per la galassia delle PMI che, ricordiamo, nel 2017 contava 5,3 milioni di imprese con oltre 15 milioni di addetti (**Prometeia - Sole 24 Ore**).

Inadempimenti che possono comportare non solo alti rischi economici per sanzioni ed eventuali risarcimenti, ma anche danni reputazionali e conseguenze penali per gli amministratori nei casi più gravi.

Per attenuare questi rischi, sarebbe necessario che governo, parti sociali (associazioni di categoria, sindacati dei lavoratori) e gli operatori dell'info/formazione si facessero carico, ognuno per la propria parte, della diffusione della conoscenza delle norme e dei percorsi per la compliance. Purtroppo, il primo problema è il loro livello di informazione e di consapevolezza su questi temi...

In questa situazione, la filiera della sicurezza, per quanto costituita principalmente da PMI esposte agli stessi rischi, potrebbe cogliere l'opportunità di proporsi come *problem solver* per gli ambiti di competenza, offrendo soluzioni efficaci e, soprattutto, sostenibili all'enorme bacino di soggetti che devono mettersi in regola, ma non possono farlo da soli.

In fondo, non sarebbe anche questo un modo per "fare sicurezza"?



Il Crimine Organizzato nel Retail, un fenomeno in crescita in Italia

di Giuseppe Mastromattei – Presidente del Laboratorio per la Sicurezza

Affrontando il tema del Crimine Organizzato nel Retail, mi vengono in mente le sempre più numerose condivisioni di episodi, riconducibili a questo fenomeno, che avvengono quotidianamente tra i colleghi soci del “Laboratorio per la Sicurezza”.

Condivisioni e preoccupazioni alle quali è necessario e improcrastinabile dare un seguito ed avviare delle concrete attività per contrastare una minaccia sempre più preoccupante. Ogni giorno infatti, registriamo efferati attacchi presso numerosi punti vendita e centri commerciali presenti in tutta Italia che, con tutta tranquillità, possiamo affermare siano frutto di attente pianificazioni e analisi da parte di vere e proprie organizzazioni criminali che, dopo aver studiato le vulnerabilità presenti nel sistema e la relativa fattibilità, decidono di colpire catene di negozi con una serialità tipica dei professionisti.

Inoltre, dall’analisi degli eventi registrati, si nota che non vi è più una precisa territorializzazione che contraddistingueva gli episodi negli anni scorsi. Si è passati da attacchi localizzati in determinate regioni di Italia (ben noti sono stati quelli che hanno colpito il nord-est nel 2018) a vere e proprie “serie criminose” (da non confondere con le serie criminali televisive) che si spostano con agilità sull’intero territorio nazionale non curandosi delle distanze geografiche, ma con il solo scopo di accumulare indebitamente e velocemente il maggior profitto una volta individuata una falla o una carenza all’interno di un “processo di vendita” di una catena (pensiamo, ad esempio, ai sistemi di pagamento denominati “self check out”).

“Gruppi di esperti e ben preparati ‘taccheggiatori professionisti’ rubano o ottengono con estrema rapidità, facilità e, soprattutto, fraudolentemente, merci allo scopo di ricollocarle in un mercato alternativo per venderle a privati e rivenditori”



Il crimine organizzato nel Retail, che come sappiamo, comporta il furto su larga scala di beni di consumo quotidiani, ha potenzialmente implicazioni molto più ampie. Gruppi di esperti e ben preparati “taccheggiatori professionisti” rubano o ottengono con estrema rapidità, facilità e, soprattutto, fraudolentemente, merci allo scopo di ricollocarle in un mercato alternativo per venderle a privati e rivenditori attraverso una numerosa ed incontrollabile varietà di metodi. Viviamo d’altronde in una società sempre più globalizzata, dove aumentano le transazioni che avvengono online a discapito di quelle tradizionali “faccia a faccia” che avvengono nei negozi o nei mercati.

Un fattore assolutamente determinante, poiché genera ulteriori opportunità per queste nuove organizzazioni criminali che potremmo definire come una sorta di *Omnicanalità del Crimine* in quanto, oltre a fare affidamento sui mercati di rivendita fisica, le bande hanno oggi a disposizione infiniti e, soprattutto, incontrollati mercati online come mezzo per mettere a profitto la merce acquisita illegalmente. Il tutto con un livello di rischio, ovviamente per loro, ben inferiore a quello che si avrebbe attraverso l’utilizzo di sistemi di rivendita diretta in mercati o simili.

E comunque si parla sempre di un rischio molto basso che viene considerato dagli stessi praticamente trascurabile. Proprio il livello di rischio percepito ci pone davanti ad un particolare sul quale è necessario riflettere con attenzione. Alcune considerazioni:

- il cosiddetto “taccheggio” è una forma di reato con conseguenze trascurabili per gli autori. Spesso sono coinvolti giovanissimi che iniziano per infinite ragioni (non è questa la sede per analizzare i vari contesti sociali e le relative motivazioni) a frequentare negozi e centri commerciali con il solo scopo di prelevare illegalmente la merce, inizialmente con moderazione, magari per gioco o peggio per sfida, e poi, una volta valutata la reazione dei sistemi di sicurezza presenti, aumentando sempre di più l’entità dei furti, con un crescendo che spesso è praticamente incontrollabile, accompagnato da una sorta di impunità percepita.

- inizia quindi a concretizzarsi una vera e propria forma di “confronto con l’Autorità” che porta questi giovani individui alla necessità di andare oltre il gioco e la sfida di cui sopra ed iniziare così, spesso supportati da “criminali adulti”, attività delittuose di diverso tipo, ben diverse dalle forme tradizionali del “taccheggio”; poiché una volta “passata liscia”, può portarli a credere di potersela cavare anche con altri crimini, rafforzando quindi il loro comportamento criminale.

Questo è quindi il rischio che il mondo del Retail oggi vive con preoccupazione e che diventa sempre più determinante nell’analisi delle perdite (c.d. “Differenze inventariali”), ovvero che il taccheggio definisca e promuova la prima identificazione dell’individuo potenzialmente delinquente evidenziando la percezione di sé come criminale.

“Parliamo dunque di un vero e proprio ‘entry level’ nella catena del crimine o, meglio, di un ‘crimine di accesso’ che funge da iniziatore per altre tipologie di crimine”

Parliamo dunque di un vero e proprio “entry level” nella catena del crimine o, meglio, di un “*crimine di accesso*” che funge da iniziatore per altre tipologie di crimine; un metodo, a rischio zero, per avviare delle vere e proprie “start up” criminali e, quindi, ottenere velocemente la disponibilità economica o, meglio, fondi illeciti da investire, ad esempio, nel traffico della droga.



Un punto di partenza di una pericolosa “escalation criminosa”.

Come reagire quindi all’avanzare di questo preoccupante e sottovalutato fenomeno, quali attività devono essere messe in campo per prevenire queste apparentemente poco pericolose attività criminali?

Sicuramente, la condivisione delle informazioni è determinante: condividere ed acquisire dati aumenta la consapevolezza e la conoscenza del fenomeno, ed è, allo stesso tempo, un’efficace forma di organizzazione.

Un’organizzazione che deve vedere il coinvolgimento non solo degli addetti ai lavori, ovvero dei Security Manager e dei Loss Prevention Manager del mondo del Retail, ma anche dei fornitori di servizi, sistemi e tecnologie di sicurezza, del mondo accademico (perché trattasi di un nuovo e preoccupante fenomeno criminale e non più del semplice ladro da supermercato).

Infine, un’organizzazione che preveda la partecipazione proattiva tra sicurezza pubblica e privata.

Proprio la partecipazione tra sicurezza privata e sicurezza pubblica è fondamentale, ma non con l’ottica di delegare alla funzione pubblica l’intera gestione e responsabilità del processo; dovrà essere compito primario degli operatori privati del settore osservare, raccogliere, analizzare e, quindi, fornire all’Autorità Giudiziaria ogni singola e determinante evidenza, affinché le attività investigative possano avviarsi in maniera strutturata per essere più incisive, determinando pertanto una azione penale più decisiva e certa.

Un percorso difficile, di cui l’Associazione “Laboratorio per la Sicurezza” si farà comunque carico per avviare ogni iniziativa finalizzata ad aumentare la consapevolezza del fenomeno e definire, attraverso un confronto aperto a tutti, le migliori e più efficaci azioni di contrasto.

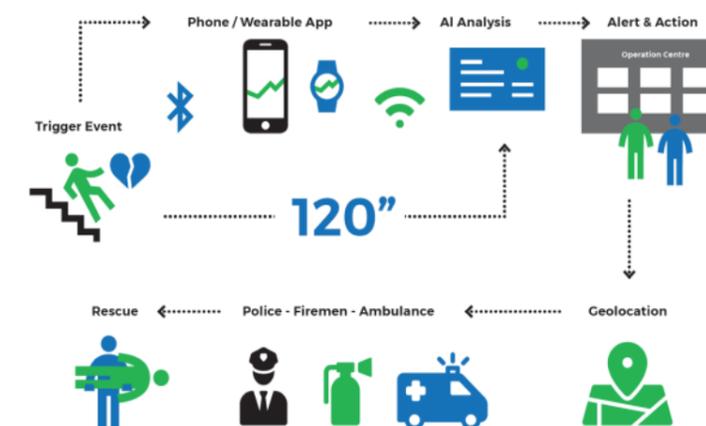
Travel Risk Management

Per la Safety e la Security dei tuoi Asset ovunque nel mondo



Soluzioni tecnologiche

Dashboard
Travel Risk Management
 Country Risk Assessment
 Travel Alerts & Travel News
 Pre-Travel Advisory
 Personal Safety Report
 Vital Signs Monitoring



Centrale Operativa: coordinamento e supporto da remoto H24 365 gg/anno

Umbrella Group Ltd.
 www.umbrella-security.com | info@umbrella-security.com
 A Company of Cittadini dell'Ordine S.p.A. www.cittadinidellordine.com



Il fenomeno ORC negli US secondo la National Retail Federation

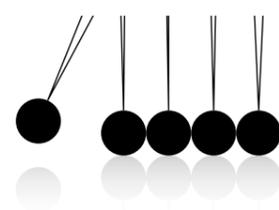
Washington D.C. – Secondo la ricerca annuale sulla Criminalità Organizzata nel Retail (ORC) negli Stati Uniti pubblicata nello scorso novembre dalla **National Retail Federation (NRF)**, nel 2018 oltre due terzi degli operatori intervistati di ogni settore hanno osservato un aumento del fenomeno degli attacchi ORC. *“Il crimine organizzato nel retail continua a costituire una seria minaccia per il sistema”* ha osservato **Bob Moraca**, Loss Prevention Vice President di NRF. *“Queste bande criminali sono evolute e, di conseguenza, lo hanno dovuto fare anche i team per la loss prevention. I retailer stanno dedicando maggiori risorse ed evolvono costantemente le modalità per contrastare questa minaccia incombente”*.



La ricerca ha rilevato che nel 2018 il 97% dei retailer hanno subito attacchi ORC e il 68% ha notato un aumento di queste azioni. La media delle perdite è stata di 703.320 dollari per ogni miliardo di vendite (0,07%), superando per il quarto anno consecutivo il livello di 700.000 dollari. Quasi due terzi dei retailer intervistati (65%) hanno dichiarato che le aziende dedicano maggiore attenzione a questo fenomeno rispetto a cinque anni fa, mentre il 56% sta impiegando risorse tecnologiche aggiuntive per contrastarlo e il 44% sta aumentando i budget per la loss prevention. Tra le misure assunte, il 38% ha cambiato o sta programmando di cambiare le procedure dei resi (delle merci), mentre il 37% sta facendo lo stesso nei punti vendita e il 27% nel controllo dei dipendenti. Il 24% dichiara di intervenire sulle modalità di gestione delle intrusioni nei negozi.

L'ORC si manifesta **sia in forma di furti nei negozi che di furti nelle varie fasi di trasporto delle merci** (73% degli intervistati). Più colpiti i trasferimenti dai centri di distribuzione ai negozi, ma il 33% dei furti avviene all'interno dei centri di distribuzione stessi e il 30% nei trasferimenti tra negozi. La merce rubata viene talvolta riportata nei negozi per avere dei crediti, solitamente in forma di buoni regalo che vengono poi rivenduti. Il 51% degli operatori le ha trovate in vendita su internet e il 17% nei banchi dei pegni.

In genere, le bande ORC rubano un mix di prodotti di design di fascia alta e di articoli di uso quotidiano facili da riciclare. Gli articoli più rubati includono capi di abbigliamento e borse firmate, latte in polvere per neonati, rasoi, detersivi per bucato, pantaloni in denim, bevande energetiche, medicinali anti allergie e liquori di alta gamma. Gli sforzi dei retailer per combattere l'ORC non si limitano a prevenire il furto di merci. Il sondaggio ha rilevato che il 68 per cento dei rivenditori ha affermato che nell'ultimo anno le bande hanno mostrato più aggressività o violenza. Pertanto, molte risorse anti-ORC sono dirette a proteggere la sicurezza dei clienti e dei dipendenti.



**LABORATORIO
 PER LA SICUREZZA**

Travel Risk Management, arriverà nel 2021 la ISO 31030 per imprese, università e ONG

intervista a Roger Warwick, CPP | Esperto designato UNI presso il TC 262/WG 7 "Managing travel risk" | CEO Pyramid Temi Group

Ci può riassumere lo stato di avanzamento dello sviluppo della ISO 31030 dopo l'ultima sessione di lavori del TC internazionale che si è tenuta presso UNI (Ente Italiano di Normazione) a dicembre?

Nel corso dell'ultima sessione di lavori del comitato internazionale ISO/TC 262 "Risk management", WG 7 "Managing travel risk", tenutasi il 10, 11 e 12 Dicembre scorsi a Milano, presso la sede UNI, sono stati esaminati e valutati i commenti ricevuti dai Paesi partecipanti alla seconda bozza dello standard (CD2 - Committee Draft 2). È doveroso sottolineare che, oltre agli iscritti ai comitati internazionali di lavoro ISO, sono state coinvolte anche importanti aziende esportatrici, sia italiane che internazionali, che con la loro esperienza diretta hanno apportato utili commenti e suggerimenti per rendere lo standard maggiormente concreto e applicabile.

A seguito di questa riunione, l'agenda dei lavori ISO prevede a gennaio 2020 la pubblicazione di una nuova bozza del CD, la CD3 che sarà fatta circolare all'interno dei comitati dei Paesi partecipanti e sottoposta per tre mesi al ballottaggio.

Successivamente, nel corso della prossima riunione del WG 7 (che si terrà in Canada dal 26 al 28 Maggio 2020), si metterà a punto la versione DIS (Draft International Standard) che verrà sottoposta per cinque mesi al ballottaggio per raccogliere eventuali nuovi commenti.

Quali sono quindi i tempi ipotizzabili per la sua pubblicazione?

La versione FDIS (Final Draft) del documento è prevista per l'aprile del 2021 e, di conseguenza, la pubblicazione come norma internazionale dovrebbe avvenire nella prima metà dell'anno.

Quali saranno le tappe successive alla pubblicazione e i relativi tempi perché si possa arrivare ad un'applicazione concreta?

Una volta pubblicata, la ISO 31030 rimarrà in vigore per 5 anni, durante i quali non sarà più possibile apportare modifiche. A partire da quel momento, le aziende e tutti gli altri soggetti interessati potranno beneficiare di questa importante norma di linee guida per la gestione dei rischi derivanti da trasferta, che darà loro gli strumenti per dimostrare, eventualmente anche in sede giudiziale, di aver fatto tutto quanto sia ragionevolmente possibile per la tutela dei propri dipendenti e collaboratori. Per arrivare a un'applicazione concreta, occorre considerare i tempi per la strutturazione interna delle organizzazioni (processi, procedure, eventuale Dipartimento Travel Risk Management, ecc) e la messa a disposizione di risorse umane e finanziarie per poter gestire la sicurezza delle trasferte in maniera adeguata rispetto alle esigenze. Un importante supporto è dato dalla consulenza di professionisti della security con specifiche competenze ed esperienza, per assistere le aziende sia nella fase strutturale, sia nella vera e propria gestione della sicurezza delle trasferte, con strutture operative nelle destinazioni a rischio nel caso valutino di operare in outsourcing.

Quali saranno i soggetti direttamente coinvolti e in che modo?

I soggetti direttamente coinvolti sono tutti coloro che, inviando personale in trasferta, devono gestire i rischi derivanti da tali trasferte, specialmente se queste avvengono verso luoghi considerati a rischio. In primo luogo, lo standard ISO 31030 è rivolto alle organizzazioni - di qualsiasi settore e dimensione esse



siano – che devono essere in grado di mettere a punto un programma efficace di gestione dei rischi, relativi alla sicurezza e alla salute, che i propri dipendenti si trovano ad affrontare quando viaggiano in nome e per conto dell'organizzazione stessa. Da sottolineare che si intendono non solo le trasferte in Paesi a rischio ma, in generale, qualsiasi trasferta sia all'estero sia sul territorio nazionale, a breve o lunga permanenza. Lo standard si applica anche ad altri soggetti diversi dalle aziende, ad esempio le università che inviano persone

all'estero per motivi di studio e ricerca, e le ONG i cui volontari partono in missioni umanitarie in aree geografiche considerate a rischio.

Ricordo che anche i legislatori avranno l'opportunità di usufruire dello standard, riconosciuto a livello internazionale, per il giudizio di casi di negligenza del datore di lavoro nei confronti dei propri dipendenti inviati all'estero in trasferta, sui quali la giurisprudenza internazionale, e anche italiana, è ancora carente.



Le tendenze evolutive della sicurezza fisica informatizzata nel 2020. Le convergenze con una recente indagine internazionale

di Nils Fredrik Fazzini, CEO di Citel SpA

Considerato lo spazio che negli anni è stato riservato da essecome-securindex all'evoluzione informatica in chiave PSIM per la gestione della sicurezza fisica in Italia, **Citel** non poteva non cogliere l'opportunità che si è presentata per un confronto con altri Paesi in occasione della pubblicazione di un interessante documento di **Stanley Security** con il titolo **"2020 Industry Trends Report"**. Un'indagine sulle attese, sulle prospettive e sulle criticità, nella vasta platea di utenti ed operatori nel Nord America ed in Europa, tesa soprattutto alla messa a fuoco delle tendenze evolutive tecnico-funzionali in corso nel campo della sicurezza fisica verso nuovi modelli informatizzati

L'occasione per un confronto sull'informatizzazione della sicurezza fisica

Citel si posiziona nel mercato come il produttore di sistemi che ha storicamente lanciato in Italia la struttura in chiave open-PSIM dei sistemi dipartimentali di gestione della sicurezza fisica e che ha poi generato negli anni il più ampio Ecosistema di utenti, di produttori complementari e di integratori in Italia, con un comune riferimento: il modello del *Sistema Informatico Dipartimentale della Sicurezza Fisica*.

L'indagine di Stanley negli USA è pertanto interessante di per sé, considerata la sua ampiezza e profondità, a maggior ragione, nel giudizio di Citel, per il fatto che essa ha portato a risultati fondamentalmente allineati con lo stato dell'arte in Italia e con le tendenze evolutive in corso nel bacino di utenza PSIM di Citel, compresa la naturale convergenza con i moderni modelli dell'informatica gestionale dipartimentale.

Stanley ha focalizzato la rilevazione sulle tecnologie che oggi vengono considerate universalmente rilevanti nell'evoluzione dell'informatica aziendale. Non tutte dello stesso peso ai fini della sicurezza, ma che sono comunque in esercizio oppure oggetto di valutazione anche in Italia e che fanno riferimento alle *innovazioni basate sull'informatizzazione* a tutti gli effetti della gestione della sicurezza fisica, e soprattutto introducendo i moderni modelli orientati alla *dematerializzazione* ed all'*automazione*:

- Remote Services
- Security As A Service (SAAS)
- Monitoring Automation
- Cloud Technology
- Network Security

Ed anche sui modelli tecnici che utilizzano soluzioni ormai correnti nell'informatica gestionale, già applicate al PSIM e basate sulla gestione di tipo *predittivo e intelligente*:

- Big Data
- Customer Experience Transformation
- Machine Learning
- Programmatic Evolution

Infine, rafforzando le pratiche per una gestione più restrittiva della circolazione del personale:

- Stricter Access Control Requirements.

Lo stato dell'arte dell'informatizzazione della sicurezza fisica in Italia

L'indagine di Stanley a livello globale si è presentata come un'occasione particolarmente propizia per Citel per fare un parallelo con lo stato dell'arte nel mercato italiano relativamente ai *singoli paradigmi dell'innovazione* informatica, sempre più frequentemente trattati nel settore.

Va peraltro ricordato preliminarmente che il mercato italiano della sicurezza fisica professionale si è distinto nel quadro internazionale come quello più precoce nell'informatizzazione grazie alla diffusa propensione – a differenza di altri Paesi – per i *sistemi aperti multifornitore* e, quindi, di per sé particolarmente evolutivi dietro la spinta della competizione.

Non è infatti un caso che l'Italia sia il mercato che ha generato precocemente il modello *open-PSIM* di Citel, con un corollario di paradigmi come il *sistema informatico dipartimentale della sicurezza fisica* e del *PSIM come progetto permanente*, a supporto di processi gestionali capaci di far fronte ad esigenze crescenti di *profondità* della protezione in considerazione della crescente dematerializzazione delle minacce. E, in definitiva, con la necessità di allinearsi a criteri mirati generati sull'onda del **Change Management settoriale**, coerente con la *Digital Transformation* generalizzata e diffusa.

Le tecnologie informatiche adottate nel settore della sicurezza fisica e sintesi dello stato dell'arte in Italia

La storia di oltre 20 anni di Citel corrisponde a quella dell'informatizzazione nella fascia critica della sicurezza fisica italiana, comprese le particolari spinte generate da un settore bancario penalizzato dalle rapine e dagli attacchi ai caveau; spinte che hanno portato non solo all'evoluzione accelerata delle piattaforme di telegestione al centro e in campo, ma anche all'accumulo ed alla sedimentazione di esperienza utente, realizzando la *condizione necessaria* per lo sviluppo settoriale di *processi intelligenti* di tipo predittivo ed operativo. E non a caso **Big Data, Customer Experience Transformation, Machine Learning, Monitoring Automation, Network Security, Programmatic Evolution, Cloud**, sono i paradigmi dell'informatica corrente, gestionale e industriale, che con la propria indagine Stanley ha sottoposto al mercato della sicurezza fisica per verificarne aspettative e penetrazione.

Si tratta di paradigmi che in campo PSIM si stanno diffondendo, in linea del progresso generale delle tecnologie informatiche gestionali sulle quali un PSIM professionale si fonda per definizione, sempre che sia *consapevolmente* considerato e gestito come un vero e proprio *sistema informatico dipartimentale*. E sempre a condizione che la sistemistica adottata sia costantemente e tempestivamente adeguata alle *dinamiche evolutive settoriali* di utilizzatori e di partner qualificati e reattivi.

Dinamiche evolutive che in Italia hanno storicamente incluso la **Network Security** (la protezione dei dati di gestione della sicurezza trasmessi in rete) e la **Programmatic Evolution**, termine informatico riconducibile all'evoluzione dei processi di gestione degli eventi, da mantenere *funzionalmente* coerenti con l'andamento dei rischi e *tecnicamente* allineati agli sviluppi della tecnologia.

Così come ci si può aspettare l'utilizzo diffuso del **Cloud** in quanto si tratta di una tendenza *di fondo* in campo informatico per la dematerializzazione dei Server; ma anche perché particolarmente efficace, se non funzionalmente indispensabile, per la fruizione di funzioni software specializzate di gestione video, accessi, di condivisione di basi dati, ecc. Ed anche – e a maggior ragione – per servizi di erogazione di funzionalità *as-a-service*; e in ogni caso per soluzioni tecniche indossabili o portatili che coinvolgono l'uso di telefonia mobile come, ad esempio, lo smartphone combinato a dispositivi IoT.



Più impegnativi sul piano tecnico, ma portatori di un considerevole salto di qualità prestazionali, sono gli sviluppi funzionali legati all'impiego di tecniche come **Big Data, Customer Experience Transformation, Machine Learning, Monitoring Automation**. Sviluppi in cui Citel è pienamente coinvolta perché una gestione PSIM, che è sempre partita dai singoli segnali per pesarli e correlarli per ottenere *eventi e situazioni*, richiede una qualità e profondità delle informazioni indispensabili per generare *funzioni predittive qualificate*. E in tal senso gli sviluppi di Citel in questo campo sono oggetto di collaborazioni già in corso da tempo con specialisti nel settore dell'intelligenza artificiale.

Un peso crescente avrà nel mercato, la **Security As A Service (SAAS)**, vale a dire *servizi di sicurezza da Control Room*, quindi non più i semplici *teleallarmi gestiti dalla vigilanza*. Si tratta di servizi che hanno una storia particolarmente consolidata in Italia rispetto ad altri mercati, grazie ai protocolli di trasmissione pubblici (quindi aperti) *bidirezionali* secondo la normativa pubblicata dal CEI più di 40 anni fa, con servizi *multimediali e interattivi*, combinati con periferiche intelligenti in campo (dati, voce, video). Con quelle logiche e sistemistica che hanno permesso al mercato italiano – ed a Citel come battistrada – di eccellere nell'anticipazione di tendenze evolutive che solo in un secondo momento si sono diffuse sul piano internazionale.



Citel non ha dubbi sul fatto che la diffusione di questa tipologia di servizi farà da acceleratore all'impiego delle *tecnologie IoT* ed all'integrazione funzionale con il mondo della telefonia mobile. A questo punto, con un salto generazionale rispetto ai servizi tradizionali basati su verifiche dell'evento superficiali (da centro) o costose (sul posto) in virtù anche del consolidamento del passaggio in corso dall'attuale *telegestione di eventi al situation management* avanzato, vale a dire la *gestione dell'evento con le sue dinamiche* grazie anche all'uso di funzioni predittive intelligenti generate dall'accumulo e metabolizzazione dell'esperienza.

Stricter Access Control Requirements

In tutte le previsioni di questo periodo il controllo accessi è destinato ad espandersi; anche in un Paese come l'Italia, più refrattario di altri a questa applicazione; ma proprio per questo con spazi più ampi di crescita. In generale si tende a concordare sul fatto che il telefono cellulare come terminale di applicazioni specializzate avrà certamente un ruolo di rilievo nella sistemistica adottata, insieme ad altre tecnologie basate sul riconoscimento di tipo biometrico. E, in ogni caso, come sottosistema di un sistema gestionale complessivo della sicurezza fisica integrata dell'edificio e/o dell'organizzazione nel suo insieme.

Tutela della resilienza aziendale

Indipendentemente dalla ricerca di Stanley ma a completamento della rassegna delle tendenze evolutive, il paradigma più ampio, che contiene tutti i valori-obiettivo fin qui espressi e che spingerà verso una *integrazione sempre più stretta e intelligente* dei processi per la sicurezza, è quello della *resilienza aziendale*, che sempre più spesso viene considerato il valore complessivo più generale e che coinvolge ovviamente anche la sicurezza informatica. E se si parla di resilienza aziendale è naturale che essa venga considerata il presupposto di un obiettivo *vitale*, che è la *Continuità Operativa* dell'impresa.

Mentre, per completare la rassegna dei paradigmi, si dovrà considerare anche la "gestione dell'*inatteso*", con un richiamo nello scorso anno da parte di **Andrea Chittaro** - Presidente di AIPSA - e con conferme, più indirette che dirette, provenienti dal settore industriale.

Per concludere, tutte queste considerazioni non fanno che confermare la possibilità di cogliere con sempre maggiore convinzione le possibilità offerte dall'evoluzione dell'informatica e, in particolare, quelle classificate nella *Digital Transformation*, ormai mature sul piano della tecnologia; ma anche tali da rendere sempre più funzionali con l'accumulazione e la metabolizzazione dei valori di esperienza utente in un ambito di apertura multifunzionale e multifornitore gestita in una visione di progetto permanente.



Contatti:
Citel spa
info@citel.it
www.citel.it

Video verifica live, registrazione e allarme in un'unica soluzione: VUpoint NVR di RISCO Group

a cura della Redazione

VUpoint NVR è la soluzione avanzata di video verifica live di **RISCO Group**, dotata dell'esclusiva tecnologia P2P, che abilita installazioni plug&play ed è pensata per completare i sistemi di sicurezza professionali integrati nel **Cloud RISCO**. Progettato per applicazioni residenziali e per aziende di piccole e medie dimensioni, VUpoint NVR è la prima soluzione video a "triplice azione" nel mercato della sicurezza a integrare **video verifica live, registrazione e allarme**, per permettere agli utenti di agire con tempestività entro i 30 secondi dall'accadere dell'evento, che sono i più importanti.

Mentre le soluzioni TVCC tradizionali supportano funzioni di live view e playback di quanto registrato, VUpoint aggiunge anche le notifiche push in tempo reale con immagini e clip video di 30 secondi inviate direttamente allo smartphone dell'utente o alla vigilanza, al fine di facilitare un intervento il più immediato possibile. Il nuovo VUpoint NVR è quindi un sistema di registrazione performante che, combinato con le telecamere IP VUpoint dell'azienda e facendo leva sulla tecnologia cloud, offre capacità e livelli di video verifica senza eguali.

L'infrastruttura cloud, infatti, trasmette notifiche, clip video e immagini assicurando ridondanza di archiviazione, grazie ad avanzate garanzie di sicurezza e privacy. Inoltre, il cloud offre un doppio livello di protezione che utilizza una cifratura dei dati sofisticata e credenziali di accesso variabile, che esclude la possibilità di accedere alle telecamere se non esplicitamente autorizzati.

Inoltre, gli utenti possono contare su un efficiente back up degli allarmi su Cloud – certificato ISO 27001 per la sicurezza delle informazioni – per non perdere le prove (foto e clip video) in caso di furto o rottura dell'NVR e su elevati livelli di cyber security e video privacy grazie alla tecnologia di sicurezza con token di RISCO.



La soluzione integrata VUpoint NVR di RISCO vanta un'ampia varietà di componenti video e di allarme, offrendo all'installatore la possibilità di personalizzare la soluzione di sicurezza e soddisfare contestualmente le necessità di qualsiasi installazione. Infatti, VUpoint NVR consente di connettere facilmente telecamere ONVIF di terze parti (acquistando licenze video) o la linea professionale **VUpro** di RISCO (licenze fornite gratuitamente) senza alcuna configurazione del router. Inoltre, la nuova soluzione NVR permette ai professionisti della sicurezza di adottare telecamere speciali o di riutilizzare telecamere IP esistenti, anche se non di RISCO.

Gli NVR supportano un hard disk fino a 6 TB (non fornito) e sono disponibili in 4 modelli: 4 canali, 4 canali con 4 porte PoE, 8 canali con 8 porte PoE e 16 canali.

VUpoint NVR è utilizzabile con tutte le centrali dell'azienda connesse al Cloud e può essere gestito dagli utenti attraverso la app iRISCO, disponibile per iOS e Android, che supporta molteplici funzionalità, tra cui live view multi-camera, il playback della registrazione, la video verifica e i controlli PTZ.



Contatti:
RISCO Group
Tel. +39 02 66590054
www.riscogroup.it

Premio securindex Installatore Certificato 2019, la parola ai vincitori: Electronic System

incontro con Gaia Monti | titolare di Electronic System - Lentate sul Seveso (MB)
Vincitore assoluto Premio securindex Installatore Certificato 2019



LA STORIA DELL'AZIENDA

La nostra iniziativa imprenditoriale nasce nei primi anni '80, operando prevalentemente nel settore della sicurezza in ambito bancario, nell'industria automotive, in altri settori industriali e nella Pubblica Amministrazione, con particolare riguardo alla videosorveglianza finalizzata al controllo del territorio.

Con un collaudato team interno composto da ingegneri, progettisti e periti elettronici, la Società si occupa di progettazione e installazione di sistemi di sicurezza nel settore della videosorveglianza e nell'ambito dei sistemi di controllo elettronico degli accessi, antintrusione e antincendio. L'elevata qualità dei nostri servizi è il punto di forza che caratterizza la nostra pluriennale attività, attestato dapprima con la certificazione IMQ/A fin dai primi anni di attività, e poi con le certificazioni ISO 9001:2015 e IMQ AIR VIDEO.

Siamo specializzati in tutte le fasi della realizzazione di un impianto speciale, a partire dall'analisi dei requisiti del Cliente, per arrivare alla progettazione ed alla realizzazione, fino all'assistenza post vendita che, sebbene sia caratterizzata per sua natura da innumerevoli criticità, rappresenta una fase fondamentale per mantenere in efficienza i sistemi progettati e realizzati.

La nostra Società è attiva in tutta Italia, con una presenza più significativa nella Regione Lombardia, in Piemonte, nel Veneto, Friuli Venezia Giulia e nella Regione Campania.

“Come System Integrator, ci aspettiamo di essere supportati dai Produttori e soprattutto dai Distributori in modo coerente alle esigenze del mercato”

LA VISIONE DEL MERCATO

Per ciò che concerne gli sviluppi futuri, confidiamo di poter consolidare la nostra presenza sul territorio nazionale, offrendo

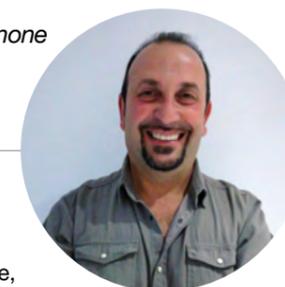
un servizio puntuale ad una Clientela sempre più esigente, non solo da un punto di vista dell'efficienza, ma anche della fruibilità dei sistemi, grazie allo sviluppo e maggior diffusione di funzionalità di analisi video. Presteremo pertanto sempre più attenzione alle problematiche legate alla protezione dei dati personali, che richiede un'accurata progettazione dell'architettura degli impianti e delle reti ad essi connesse per prevenire i rischi relative ad accessi indesiderati fino a episodi di data breach. Nell'ambito della Pubblica Amministrazione, crediamo che il futuro vedrà una sempre maggiore interazione delle tecnologie con l'ambiente circostante in ottica di Smart City, così da consentire uno sviluppo innovativo del territorio, della relativa mobilità e delle infrastrutture. La diffusione dei sistemi automatizzati di analisi del traffico e di lettura delle targhe, con connessione ai database disponibili per applicazione delle logiche interforze, nel rispetto del GDPR, permetteranno un controllo capillare del territorio con conseguente innalzamento del livello di sicurezza reale e percepito.

Crediamo che gli ultimi anni abbiano dimostrato una inversione di tendenza, con crescente interesse verso la qualità del prodotto/servizio a discapito della logica del “minor costo”. Continueremo quindi ad investire in formazione ed aggiornamento, sia dal lato dei requisiti cogenti, sia in termini di prodotti e soluzioni, valutando con attenzione le nuove tecnologie offerte dal mercato.

Ci aspettiamo, come System Integrator, di poter essere supportati dai Produttori e soprattutto dai Distributori in modo coerente alle esigenze del mercato. In tale senso, la conoscenza dei prodotti e il supporto tecnico sono ormai criterio di scelta per noi, come per molte altre aziende del settore che si trovano a dover garantire un servizio efficiente all'utente finale su impianti tecnologicamente sempre più complessi e connessi.

Premio securindex Installatore Certificato 2019, la parola ai vincitori: I.T.S. di Palmisani Marco

incontro con Marco Palmisani | titolare di ITS - Impianti Tecnologici di Sicurezza - Frosinone
Vincitore Premio securindex Installatore Certificato 2019
Cat. Small Installer Centro Italia



LA STORIA DELL'AZIENDA

Dopo aver avuto un'esperienza decennale nel settore della sicurezza, nel 2011 ho deciso di fondare la mia azienda “I.T.S. di Palmisani Marco”, promettendomi di mettere sempre a disposizione dei clienti la professionalità formata in anni di esperienza e di conoscenza dei prodotti presenti nel mercato, entrambi fattori importanti per fornire al cliente finale un prodotto di qualità.

La mia azienda non offre solamente servizi prettamente legati all'installazione di sistemi di allarme ma offre, al contempo, una vasta gamma di servizi come, ad esempio, l'installazione di sistemi di videosorveglianza, di impianti di rilevazione fumi e di domotica.

“I.T.S. di Palmisani Marco” è una piccola impresa composta da due persone, io e un mio collaboratore, che interviene su territorio locale, la provincia di Frosinone, estendendosi fino a Roma e provincia e copre una molteplicità di clienti che spaziano dal singolo privato fino ad arrivare alla pubblica amministrazione e alle strutture sanitarie, passando per le aziende e le industrie.

“Sicurezza e domotica, un mercato in crescita che richiede aggiornamenti continui sulle nuove tecnologie”

LA VISIONE DEL MERCATO

In base alla mia esperienza, l'andamento del mercato nell'ambito della sicurezza è senza dubbio positivo e in crescita. Settori quali l'antincendio, l'antintrusione o la videosorveglianza hanno subito un tasso di sviluppo notevole, come dimostrano le statistiche. Inoltre ci sono altri settori che, negli ultimi anni, si stanno

sviluppano sempre di più all'interno del nostro ambiente, con necessità sempre maggiori del nostro intervento di installatori qualificati. Mi riferisco in particolare ai sistemi di domotica e di automazione della gestione della casa.

Insomma, il futuro del settore sembra alquanto roseo e, personalmente, mi impegnerò al massimo per rimanere sempre aggiornato sulle nuove tecnologie, in modo tale da fornire al cliente finale non solo un prodotto quanto più consono alle sue esigenze, ma anche una maggior professionalità e sicurezza tramite tutti quei servizi di consulenza, verifica e controllo finalizzati al miglioramento della qualità di vita del consumatore.

Collaborazione è la parola chiave che regge tutto il discorso della sicurezza. Per questo, quando mi affido a produttori e distributori cerco sempre coloro che possano affiancarmi e consigliarmi nella scelta del materiale. È, in sostanza, un lavoro di squadra che, se non viene fatto bene, va purtroppo a discapito del cliente finale.

Alla luce di ciò, la richiesta che farei ai produttori e ai distributori è quella di cercare di dialogare di più con noi impiantisti – persone competenti e preparate – per garantire all'utente finale prodotti di qualità e contrastare la distribuzione di prodotti mediocri e molto generici venduti sia online che porta a porta, che ledono la qualità del risultato finale.

Un'altra richiesta, collegata alla precedente, è di fornire a noi installatori una maggior varietà di corsi di aggiornamento durante l'intero anno relativi alle tecnologie più innovative, così da avere una conoscenza a 360 gradi dei prodotti che verranno venduti al cliente finale, presupposto indispensabile per un risultato ottimale.

Premio securindex Installatore Certificato 2019, la parola ai vincitori: Tecno Security

incontro con Federico Piras | Responsabile Tecnico di Tecno Security - Oristano
Vincitore Premio securindex Installatore Certificato 2019
Cat. Small Installer Sud Italia/Isole



LA STORIA DELL'AZIENDA

Tecno Security vuole rappresentare un modello innovativo con solide fondamenta costruite attraverso la conoscenza, prima ancora che del mercato e dei competitor attivi, della storia del settore a partire dalle prime tecnologie che hanno connotato lo sviluppo della Security. Fondamenta costruite anche attraverso la padronanza di discipline, quali l'elettrotecnica, l'elettronica e l'informatica, e del corposo quadro normativo nazionale ed europeo, in costante aggiornamento.

Nel nostro percorso di crescita professionale hanno sempre avuto un ruolo chiave tutti gli attori della filiera: le associazioni di categoria, gli ordini professionali, gli enti di normazione e i costruttori.

In questi anni, abbiamo ricevuto l'apprezzamento da numerosi clienti che, anno dopo anno, ci rinnovano la fiducia. Tra questi musei, istituti scolastici, chiese, gioiellerie, armerie, farmacie, ospedali, complessi alberghieri, campi fotovoltaici, e diversi altri.

Inoltre, a conferma della validità del lavoro sinora svolto, da diverso tempo siamo il riferimento, nel territorio isolano, di importanti aziende produttrici di mezzi forti tradizionali e intelligenti per la gestione del contante all'interno dei punti vendita di importanti realtà della grande distribuzione organizzata e di mercati verticali.

“Sento la necessità di richiamare l'attenzione del Legislatore per regolamentare il settore rendendo obbligatori gli schemi di certificazione volontaria”

LA VISIONE DEL MERCATO

Ritengo che il mercato della sicurezza rappresentato da sistemi d'allarme intrusione, videocontrollo, rivelazione incendi e controllo accessi, non soffra particolarmente dell'attuale congiuntura economica negativa. Il bisogno di sicurezza per chi non ha mai pensato all'implementazione di difese è sempre più elevato, così come la necessità di aggiornare quei sistemi di sicurezza, ormai obsoleti, posti a protezione di imprese ed installazioni vulnerabili. Se pensiamo al solo settore della videosorveglianza, ci rendiamo conto delle enormi potenzialità di crescita per ogni impresa del settore. Verso i costruttori e i distributori non ho particolari richieste, considerata la pluralità dei nostri interlocutori professionali ma sento, invece, la necessità di richiamare l'attenzione del Legislatore allo scopo di regolamentare in modo più puntuale il settore della sicurezza elettronica e, più in generale, dell'impiantistica, ad esempio rendendo obbligatori gli schemi di certificazione volontaria, applicati alle singole persone e all'organizzazione, così da uniformare dei requisiti minimi garantiti, senza limitarci a capacità di carattere generale già previste dal D.M. 37/2008.

Per il futuro il nostro impegno sarà riservato sempre più alla formazione, all'aggiornamento, alla capacità di creare relazioni con gli attori del settore, favorendo la diffusione della cultura della sicurezza. Offriremo soluzioni sempre più integrate, flessibili e robuste, capaci di rendere più sicuri ed efficienti gli edifici nei quali viviamo e lavoriamo. Un occhio di riguardo sarà sempre rivolto a tutti i servizi ad alto valore aggiunto per garantire l'eccellenza di ogni processo.

VIGILO4YOU: il “plus” degli Installatori per le abitazioni e lo Small Business

a cura della Redazione

Cosa è **VIGILO4YOU**? E' il primo servizio di vigilanza “a consumo” per le abitazioni e lo Small Business compatibile con qualsiasi sistema di allarme e con una copertura assicurativa.

Un servizio immediato: basta registrarsi sul sito www.vigilo4you.it, inserire i dati richiesti e acquistare l'intervento di allarme.

Quando il cliente riceve sul suo smartphone l'allarme, effettua la verifica della telecamera anche attraverso l'ascolto ambientale e, solo dopo aver accertato la reale intrusione, attiva l'APP rilasciata gratuitamente da **VIGILO4YOU** per richiedere l'intervento della Guardia Giurata. In caso di avvenuta intrusione, grazie alla copertura assicurativa inclusa nel prepagato vengono rimborsati sia i danni cagionati all'immobile sia il servizio prepagato utilizzato.

Un servizio completo a costo zero!

VIGILO4YOU è la soluzione ideale per le abitazioni e le piccole attività a partita IVA, che completa ed eleva il grado di sicurezza dell'impianto di allarme senza vincolare il Cliente in contratti annuali con canoni mensili, a dispetto di quello che oggi si trova sul mercato.

Qual è la strategia di **VIGILO4YOU** per il 2020? Creare un **Network Nazionale di Installatori** che abbinano al loro impianto di allarme il servizio di pronto intervento di **VIGILO4YOU**, comprensivo della copertura assicurativa.

Il risultato finale è quello di offrire agli Installatori uno strumento facile ed efficace per mantenere, fidelizzare e sviluppare i clienti in essere e, soprattutto, avvicinare nuovi clienti con un pacchetto completo: **tecnologia, servizio, copertura assicurativa**.

Proprio per questo **VIGILO4YOU**, dopo la partecipazione al “Premio securindex Installatore Certificato”, prosegue con nuove iniziative rivolte agli Installatori.



Il **28 febbraio 2020** presso il Salone Eventi di **Vigilanza Group** in via Fura 14 a Brescia, si terrà il primo incontro territoriale con gli Installatori del Nord Italia.

Un evento di approfondimento sulle strategie per acquisire il mercato della sicurezza per il mercato residenziale e lo Small Business in chiave innovativa! **VIGILO4YOU** offrirà a tutti i partecipanti di un piccolo omaggio e un ricco aperitivo che rappresenta un piacevole momento di conoscenza e relazione.

Per chi fosse interessato a partecipare o solo ad avere informazioni aggiuntive è possibile contattare il Call Center **VIGILO4YOU** al n. 800 59 5004



Contatti:
VIGILO 4 YOU
800 59 5004
www.vigilo4you.it

Varchi automatici Argus: la nuova formula con un design unico e innovativo

a cura della Redazione

Un buon design può essere il risultato dello sviluppo di un progetto. Le nuove barriere con sensori **Argus** di **dormakaba** aprono la strada ad una maggiore libertà di forma, colore e funzione. Dalla versione base a soluzioni più raffinate, i nuovi varchi Argus offrono un'ampia gamma di funzioni.

Questa diversità si esprime in modo sostenibile negli elementi di design modulare: con un'ampia gamma di colori e materiali per corrimano, profili, nonché azionamenti e ante, si aprono possibilità di design finora inimmaginabili. I varchi Argus di dormakaba si inseriscono armoniosamente in qualsiasi area reception e non solo: come complemento di un concept, come unità funzionale discreta oppure come elemento distintivo di stile, garantendo alti livelli di security e, allo stesso tempo, rispettando la safety al 100%! Per facilitare qualsiasi requisito di accessibilità, i varchi Argus sono disponibili nelle larghezze di passaggio di 650 mm, 900 mm e 1000 mm. Il sistema di sensori si adatta perfettamente alle rispettive dimensioni. Una guida utente intuitiva con luci di scorrimento opzionali nel corrimano e segnali luminosi colorati del lettore garantiscono un elevato livello di comfort.

La sicurezza resta comunque un aspetto importante nel campo progettuale. Anche per questo, dormakaba ha provveduto a migliorare i suoi varchi. La possibilità di utilizzare ante più alte soddisfa le esigenze di una sicurezza più elevata e di protezione anche contro lo scavalco. Un sistema di sensori adattato alla larghezza e lunghezza del varco, unita alla tecnologia degli azionamenti a basso consumo energetico, garantisce la sicurezza personale.



Un ulteriore aspetto importante in termini di sicurezza passiva è l'utilizzo delle ante in PETG.

In caso di necessità le ante possono essere disponibili anche in vetro temperato di sicurezza.

La semplice installazione di componenti, come i lettori, nelle barriere con sensori Argus ne facilita l'integrazione nei diversi concept di sicurezza e di accesso. Le finiture possono anche essere modificate e quindi, su richiesta, possono adattarsi a qualsiasi cambiamento di stile dell'architettura. I nuovi varchi Argus si basano sul concetto di design XEA e si inseriscono perfettamente nell'attuale portafoglio prodotti di dormakaba. Questo apre una vasta gamma di opzioni per un accesso sempre più elegante e sicuro.

MODELLI DISPONIBILI

Argus 40

Con una lunghezza di soli 1200 mm è adatto anche in situazioni in cui lo spazio è limitato. Un varco automatico ad alto flusso completo, in cui un'estetica puristica soddisfa i regolari requisiti di sicurezza senza compromessi.



Argus 60 e Argus 80

Argus 60 con 1650 mm e Argus 80 con 1660 mm di lunghezza raggiungono il massimo livello di sicurezza: 2 sensori di sicurezza, uno verticale e uno orizzontale sono integrati nella struttura. Dal punto di vista estetico, Argus 60 e 80 offrono una maggiore libertà di scelta, con numerose combinazioni di materiali e colori e illuminazione ambientale.



dormakaba

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

Controllo iniziale e manutenzione dei sistemi di Rilevazione Incendi: pubblicata la Norma UNI:11224

a cura della Redazione

Dal 5 settembre 2019 è stata pubblicata ed è entrata in vigore la nuova versione della **UNI11224:2019** sulla manutenzione e il controllo iniziale dei sistemi di rivelazione incendi.

La nuova Norma si rivolge a tutte le aziende e professionisti che forniscono servizi di manutenzione antincendi, agli imprenditori, ai manager e ai responsabili delle attività che devono pianificare gli interventi di manutenzione sui propri impianti.

Questa revisione prevede il controllo generale dell'impianto al raggiungimento del suo 12° anno di età, introducendo le operazioni da effettuare per i dispositivi in capo, essi siano rivelatori puntiformi di fumo, lineari, ad aspirazione di fiamma, ecc...

Tra le operazioni da effettuare si può scegliere tra:

- **Revisione del rivelatore da parte dell'azienda produttrice**
- **Sostituzione con un rivelatore nuovo**
- **Prova pratica come da UNI 9795 punto 8 per i rivelatori ottici puntiformi e lineari, come da UNI TR 11694 - Appendice C, per i sistemi di aspirazione e come da indicazione del produttore e del progettista per i rivelatori di fiamma.**

Oltre ai punti precedentemente descritti, questo aggiornamento normativo accoglie, tra le novità più importanti, l'introduzione della **figura professionale del tecnico manutentore**, le indicazioni sulla verifica generale



del sistema, l'introduzione dei concetti di "anzianità" e "ciclo" dell'impianto, modifiche sulle modalità e sulle quantità di punti da controllare sull'impianto e le relazioni con la UNI/TR 11607 e la UNI/TR 11694 per le prove e i controlli sui dispositivi di segnalazione ottico/acustica e i sistemi di aspirazione.

A seguito di questa importante revisione, che di fatto sostituisce la UNI 11224:2011, **NSC Italia Srl** ha creato un'iniziativa volta alla sostituzione degli impianti installati in passato che necessitano di manutenzione, con prodotti nuovi, in garanzia, tecnologicamente avanzati, certificati e a norma.

In taluni casi la manutenzione potrebbe risultare infatti anche più onerosa rispetto alla sostituzione con nuove apparecchiature.

I vantaggi nella sostituzione del prodotto installato da tempo che necessita di manutenzione con prodotti nuovi e moderni sono molteplici:

- **Sostituzione di prodotti con sistemi innovativi sotto il profilo tecnologico:** le nostre centrali **Solution F1** e **Solution F2** sono centrali antincendio di nuova generazione, modulari e ultramoderne, sviluppate per soddisfare gli standard e i requisiti internazionali di massimo livello. Le centrali Solution F1 e Solution F2 sono compatibili con i più moderni rilevatori analogici indirizzabili **Hochiki** e **Apollo**, due dei più noti e maggiori produttori di rilevatori al mondo.

- **Tempi ridotti per i test sui sensori:** grazie alla partnership con Hochiki e Apollo, le nostre centrali riescono a comunicare con i punti di campo attraverso protocolli di comunicazione di ultima generazione. Grazie a questo, la velocità per il test di un sensore si riduce ad 1/3 del tempo contribuendo ad una riduzione significativa dei costi inerenti alle manutenzioni ordinarie necessarie per legge.

- **Web Server integrato:** consente di avere un occhio sempre vigile sull'impianto da qualsiasi postazione internet. Il modulo Web server consente la connessione diretta alle centrali Solution F1 e Solution F2 per verificare da remoto il corretto funzionamento dei dispositivi in campo, visualizzare gli allarmi e le eventuali anomalie dell'impianto, consentendo al manutentore di avere in anticipo una valutazione su quello che troverà durante la fase di manutenzione.

- **Certificazioni:** Tutte le nostre centrali e i dispositivi in campo sono certificati EN54 e VdS.

Contattateci per informazioni aggiuntive relative all'iniziativa commerciale volta alla sostituzione dei vecchi prodotti da mantenere con sistemi nuovi, innovativi ad in garanzia.



Contatti:
NSC ITALIA
info@nsc-italia.it
www.nsc-italia.it





GESTIONE, ORGANIZZAZIONE E SERVIZI PER LA SICUREZZA

BW-312, il nuovo contatto magnetico per esterni di Bentel Security

BENTEL SECURITY S.R.L.
(+39) 0861 839060
www.bentelsecurity.com



Bentel Security presenta il nuovo **BW-312**, il nuovo contatto magnetico esterno wireless PowerG della **Serie BW** con ingresso ausiliario, perfetto sia per installazioni in ambito residenziale che per attività commerciali di grandi dimensioni.

Questo robusto dispositivo è stato progettato per la protezione di accessi esterni (inclusi cancelli perimetrali, recinzioni per piscine e giardini, porte per capannoni, finestre e molto altro). Eccezionalmente potente, il **BW-312** è l'unico contatto magnetico esterno con un protocollo di comunicazione bidirezionale capace di offrire prestazioni eccellenti garantite per molti anni grazie alla lunga durata della batteria, assicurando un funzionamento affidabile anche in condizioni meteorologiche avverse.

Il sensore è dotato di funzionalità avanzate (supportate dalle centrali **V20.2** e superiori), come l'anti-mascheramento proprietario che identifica i tentativi di interferenza basati su magnete, il doppio supporto ausiliario di linea che consente allarmi differenziati dai dispositivi cablati collegati e il rilevamento della temperatura locale per un migliore controllo ambientale.

Vantaggi Smart

- Ricetrasmittitore esterno resistente alle intemperie e all'acqua (IP66)
- Ampia distanza di trasmissione wireless
- Anti-Masking e Sensore di temperatura (solo con centrali BW30 BW64 vers. 20.2)
- Prestazioni di sicurezza senza precedenti
- Involucro esterno verniciabile per essere adattabile a ogni superficie
- Facile installazione e manutenzione
- Batterie a lunga durata (fino a 5 anni di funzionamento in condizioni standard)

essecome
ONLINE

n. 01 gennaio 2020
Anno XXXX
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE E COORDINAMENTO EDITORIALE

Raffaello Juvara
editor@securindex.com

HANNO COLLABORATO A QUESTO NUMERO

Nils Fredrik Fazzini, Giuseppe Mastromattei

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

Lilian Visintainer Pinheiro
lilian@lilastudio.it