essecome ONLINE 05/18

Periodico digitale di informazione di security & safety

2018 · ANNO XXXVIII

RISCO Group.

Più di 180.000 famiglie italiane hanno affidato la propria serenità e sicurezza a soluzioni RISCO, negli ultimi 10 anni.

RISCO GROUP

Diventa un installatore RISCO e offri ai tuoi clienti una soluzione basata su Cloud che integra Sicurezza, Video e Smart Home.

Scopri le soluzioni RISCO e trova l'installatore professionista a te più vicino, scansionando il QR code

MIX COMUNICAZIONE - MI

INXPECT
The sense of motion.

Vedere senza guardare.

Sensore di movimento MSK-101:
il radar diventa intelligente.

Tsec
TECHNOLOGY FOR SECURITY

www.tsec.it

L'editoriale

Frammento da un vecchio pc abbandonato in un self-storage

"Nell'estate del 2018 la Digital Transformation aveva ormai normalizzato qualsiasi attività produttiva e culturale, riconducendo ogni transazione ad un passaggio di dati in rete, controllabili (e rigorosamente controllati) dalle centrali della Federazione delle cinque Major globali dell'Information Technology (GAFMA in codice). Il PIL aggregato della Federazione l'avrebbe collocata di diritto nel G5, ma il suo potere era infinitamente superiore a qualsiasi nazione politica, non solo perché del tutto esente dai condizionamenti democratici di parlamenti, governi e opposizioni degli stati normali. La vera potenza della Federazione era data dal possesso dei dati più intimi di ogni essere umano, raccolti negli anni da ognuna delle Major nel proprio core business.

Non era stata necessaria alcuna attività illegale, di spionaggio o violenta. Era bastato catalogare pazientemente le informazioni che ognuno lasciava volontariamente sui social o in quanto consumatore, navigante di internet, sportivo, musicista ecc ecc. Mettere insieme le informazioni per profilare perfettamente ogni essere umano, anche se viveva nelle lande più sperdute, era stato un gioco da ragazzi per chi disponeva di battaglioni di informatici come le Major.

Così come sviluppare software di analisi video per il riconoscimento facciale, in grado di individuare all'istante una persona in mezzo alla folla. Era stato fin troppo facile far credere che serviva ad accendere lo smartphone o fare la spesa al supermercato senza fare la coda alla cassa. Ci cascavano tutti come grulli e così potevano venire tracciati passo dopo passo dalle telecamere disseminate in ogni angolo delle città. E quanto erano contenti di entrare in un negozio e trovare il personal shopper che gli offriva la maglietta proprio del colore che volevano e della taglia giusta, grazie ai software predittivi che avevano "intuito" le loro intenzioni di acquisto!

("*Privacy? What's privacy?* - si chiedevano ridendo i CEO delle Major nei loro comitati planetari - *roba da governi*…!")

Non c'erano proclami, raduni oceanici o altre manifestazioni di forza, la Federazione non aveva bisogno di mostrare i muscoli, non aveva nemici o antagonisti. Tutti volevano venir solo riconosciuti come consumatori, lavoravano alacremente per avere la carta di credito e poter sottoscrivere decine di contratti d'uso (auto, casa, smartphone, impianto di sicurezza, netflix, tv, palestra ecc) e non far la fatica di pensare come spendere i soldi da un mese all'altro.

Gruppi etnici tra loro avversari da secoli convergevano pacificamente sotto gli ologrammi delle 5 Major digitali, importava solamente farsi classificare in gruppi omogenei di acquirenti transnazionali pronti ad essere accuditi da una premurosa Federazione, attenta solamente ad anticipare ed esaudire i loro desideri. Mica era un Grande Fratello con la paranoia dei dissidenti..."

(Questo frammento è stato scaricato da un arcaico computer portatile trovato miracolosamente intatto nell'estate del 2084 in un self storage box in disuso da una pattuglia di droni alla ricerca di CAI (Consumatori Anarchici Irriducibili), pericolosi nemici della Federazione perché vivevano in clandestinità, coltivavano orti e si cucivano i vestiti per non lasciar traccia di acquisti, mettendo così in discussione alla radice il sistema grazie al quale i padroni delle Major governavano il mondo ormai da quasi 70 anni).

Sommario Interattivo

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

02 Frammento da un vecchio pc abbandonato in un self-storage

05 Sicurezza convergente e GDPR: quali effetti sulle organizzazioni pubbliche e private?

07 Le categorie SOA da richiedere negli appalti di Videosorveglianza

09 Security Director Forum 2018, come cambia la sicurezza

11 Travel security, un altro fronte operativo per i security manager

13 Certificazione installatori: IMQ presenta lo schema IMQ AIR VIDEO

14 Cosa cambia nei corsi propedeutici alla certificazione IMQ AIR VIDEO

17 Progetto Installatore Sicuro

21 RISCO Group presenta il Programma Partner RISCO Stars

23 Le 8 migliori video analitiche e i principali trend nelle banche per la sicurezza fisica e la Branch Transformation

25 Senator, protezione da furti e incendi firmata ChubbSafes

27 La Digital Transformation e il modello ERP per sicurezza fisica aziendale

31 Le comunicazione audio in IP nelle carceri

35 Hanwha Techwin presenta la telecamera multidirezionale con doppio obiettivo serie Wisenet P

37 Integrare un rivelatore a tenda in un sistema di sicurezza e di videosorveglianza su rete IP: l'esperienza diretta di OPTEX

39 Prime e la dinamica dell'Installatore Identificato Inim

41 MACS: quando il sensore fa la differenza, anche nelle recinzioni. Ecco la Linea MACS di Nuova Defim Orsogrill

43 lares 4.0: la soluzione IoT più innovativa per Sicurezza Fisica e Home & Building Automation

47 CST- Coded Sensor Technology la piattaforma di TSec contro l'insider attack

49 Case study: soluzioni integrate Axis per il controllo degli accessi e la sicurezza del Caruso Place Boutique & Wellness Suites

51 Arriva in Italia DoorTek,la linea di porte e partizioni di sicurezza Gunnebo

55 Premio H d'oro 2017 Centro Sportivo FC Internazionale

Redazionali Tecnologie

57 - 58 - 59

Cover Story

iRISCO: L'APP ALLEATA DELLE FAMIGLIE PER GARANTIRE UNA CASA SICURA E SMART!

La vita quotidiana di oggi, che si tratti della normale routine o delle vacanze, vede sempre più protagoniste le nuove tecnologie: la soluzione di **RISCO Group** – che incarna la filosofia dell'azienda di casa sicura e intelligente perfettamente integrata e connessa – è l'esempio di come le nuove tecnologie possano migliorare e semplificare la vita delle persone. Combinando sicurezza e verifica video professionale **VUpoint** ad accessori intelligenti completamente integrati nel sistema purchè connessi al Cloud di RISCO, i sistemi di sicurezza RISCO consentono agli utenti di gestire la protezione della propria abitazione in maniera semplice e immediata direttamente dal proprio smartphone grazie all'app iRISCO disponibile per iOS e Android, oltre ad abilitare la gestione smart dei consumi energetici, di tapparelle, elettrodomestici e accessi.

Inoltre, l'integrazione di soluzioni Smart Home nel sistema di sicurezza RISCO con video verifica, permette di automatizzare alcune attività attraverso la creazione di scenari personalizzati sulla base delle proprie abitudini, per godere sempre del massimo comfort potenziando la sicurezza, al centro di questa rivoluzione che digitalizza il quotidiano.

Semplicemente dal palmo della propria mano con un solo click dall'app iRISCO è infatti possibile gestire in toto la propria dimora, sia localmente che da remoto, impostando azioni manualmente, come ad esempio lo scenario "Uscendo da casa": basta selezionare gli elementi da attivare la mattina quando si parte alla volta dell'ufficio – spegnimento delle luci, inserimento del sistema di sicurezza o il controllo della temperatura – e il gioco è fatto!

Si può andare in vacanza senza la preoccupazione di aver scordato qualcosa nella fretta e senza pensieri, potendo contare sul proprio sistema di sicurezza, e su una casa intelligente che svolge in maniera regolare attività che simulano la presenza in casa (accensione/spegnimento delle luci, alzamento/abbassamento delle tapparelle e così via), dissuadendo così potenziali malintenzionati. Da non sottovalutare l'aspetto relativo al risparmio energetico, sia per quanto riguarda il rispetto ambientale sia il contenimento dei costi in ambito domestico. Smart Home, infatti, oltre a favorire un risparmio in termini di tempo – grazie all'automazione o alla gestione da remoto di alcune azioni – permette di ottimizzare i consumi e controllare i costi attraverso una gestione e un impiego smart dell'energia, che viene sfruttata e utilizzata solo quando serve. Ad esempio, grazie a un termostato intelligente e ai sensori presenti in casa è possibile programmare la temperatura quando ci si sveglia o quando si rientra in casa. Un controllo intelligente delle diverse fonti energetiche permette di limitare gli sprechi e migliorare le performance degli impianti, riducendo così anche l'impatto ambientale.

Nell'ottica di indirizzare al meglio i bisogni in continua evoluzione dei consumatori e le richieste del mercato, RISCO Group lavora costantemente per arricchire Smart Home di nuove funzionalità accettando la sfida di rendere le case degli italiani ancora più intelligenti e connesse. Per avvicinare ulteriormente i propri utenti al mondo smart home e più in generale a quello della sicurezza e ai migliori professionisti che vi operano, l'azienda ha recentemente sviluppato un nuovo **sito** ad hoc, più user-friendly e a portata dei consumatori. Sul sito sono presenti i riferimenti degli Installatori, su base geografica, che hanno conseguito certificazioni sui prodotti RISCO.

Sicurezza convergente e GDPR: quali effetti sulle organizzazioni pubbliche e private?

a colloquio con Luisa Franchina, Presidente AIIC
a cura di Raffaello Juvara

Quali sono gli effetti per la sicurezza delle IC determinati dalla convergenza tra sicurezza fisica e quella logica?
Il concetto di *cyber-physical system* può essere considerato uno degli elementi chiave del processo di digitalizzazione del settore industriale – e in particolare del manifatturiero – nell'ambito della cosiddetta Industria 4.0.
Protagoniste di questa quarta rivoluzione industriale sono infatti tutte quelle tecnologie abilitanti in grado di creare dei sistemi "intelligenti", interconnessi e intercomunicanti, in grado non solo di acquisire ed elaborare enormi quantità di dati, ma anche di sfruttare questa capacità computazionale e di comunicazione reciproca per migliorare i processi, non soltanto produttivi, ma anche decisionali.
Questa convergenza pone altresì una serie di questioni relative alla sicurezza che non vanno assolutamente sottovalutate: pensiamo ai sistemi ICS (Industrial Control Systems), altrimenti detti SCADA (Supervisory Control And Data Acquisition), che vengono impiegati anche per la gestione dei processi che garantiscono il funzionamento delle infrastrutture critiche, la cui continuità operativa risulta essenziale per il mantenimento del benessere della popolazione.
I dati statistici e i report redatti dalle maggiori compagnie di sicurezza informatica e dalle principali agenzie nazionali e sovranazionali (come il CLUSIT e l'ENISA) ci mostrano un trend molto chiaro: gli attacchi informatici sofisticati in grado di determinare un impatto materiale, sfruttando la convergenza tra il dominio cyber e quello fisico, sono sempre più diffusi e rappresentano ormai una realtà.

Le organizzazioni sono pronte ai cambiamenti?
In Italia notiamo diversi segnali positivi: la Legge di Bilancio 2018 ha dato un notevole input al piano Industria 4.0, presentato nel biennio precedente, incoraggiando il rilancio degli investimenti da parte delle imprese, la costruzione di competenze, la governance.
La principale sfida della "trasformazione digitale" delle organizzazioni è legata a una questione culturale, di mentalità. Il principale ostacolo al processo di digitalizzazione delle imprese, ma anche del settore pubblico, è costituito dalla difficoltà di sganciarsi da una visione che, da un lato, considera la spesa in nuove tecnologie come una dispersione di risorse anziché un investimento; dall'altro, considera il mondo del "cyber" come qualcosa di poco gestibile se non addirittura pericoloso.

Tuttavia, per essere competitivi sullo scenario internazionale, oggi, investire sulle tecnologie digitali e sulle soluzioni di sicurezza atte a tutelare i propri asset materiali e immateriali è diventato un imperativo. Parlando di sicurezza, è necessario in primis ripensare la visione dell'intero ecosistema difensivo, privilegiando un approccio più «agile» e trasversale, in grado di operare su più domini.

E le competenze delle persone preposte sono all'altezza della situazione?
Uno dei pilastri del piano Industria 4.0 è proprio la creazione di competenze, attraverso iniziative atte a finanziare centri di eccellenza e la creazione di competence center, in cui è previsto un forte coinvolgimento sia di istituzioni universitarie che di realtà private, con il supporto di altri centri di competenza a livello europeo. Tutte queste realtà sono accomunate da un focus su ambiti tecnologici specifici e da una vision in ottica Industria 4.0.
È importante, in futuro, puntare sempre di più su un'attività formativa adeguata alle nuove competenze richieste dal mercato del digitale: Internet of Things, cybersecurity, data science e Intelligenza artificiale saranno i settori con cui le imprese dovranno necessariamente interfacciarsi nei prossimi anni e in cui i nuovi professionisti del digitale dovranno sviluppare le proprie competenze.

Come valuta la risposta delle Pubbliche Amministrazioni?
Secondo la fotografia scattata dall'Osservatorio Agenda Digitale del POLIMI, in collaborazione con l'AgId, negli ultimi quattro anni lo slancio dell'Italia per allinearsi all'Europa nella "corsa al digitale" è stato notevole, ed è necessario continuare su questa linea evitando battute d'arresto o ulteriori ritardi per non vanificare gli sforzi fatti sino ad ora.
Sempre secondo l'Osservatorio, dal 2013 al 2015 la spesa in tecnologie digitali da parte della PA italiana ammontava a circa 5,6 miliardi di euro l'anno. Con la diminuzione della spesa pubblica in digitale (come previsto dalla Finanziaria del 2016), entro la fine del 2018 sarà possibile liberare risorse per gli investimenti relativi al Piano Triennale per l'Informatica nella Pubblica amministrazione, grazie all'adesione delle PA a sistemi come PagoPA, il sistema nazionale per i pagamenti a favore della Pubblica Amministrazione, o il Sistema pubblico di identità digitale (SPID), portando a un'ottimizzazione e a un significativo risparmio dei costi di acquisto e della gestione delle soluzioni digitali adottate all'interno delle PA.

GDPR, solo adempimenti o anche opportunità per le organizzazioni?
ndubbiamente la nuova normativa in materia di privacy richiede alle aziende alcuni sforzi di adeguamento, in particolare per le piccole e medie imprese e soprattutto dal punto di vista delle misure di sicurezza richieste per la protezione dei dati personali. Tuttavia, si tratta di investimenti che possono rappresentare un'opportunità di sviluppo per le piccole realtà italiane che sono ancora restie all'adozione di tecnologie digitali.

Le categorie SOA da richiedere negli appalti di Videosorveglianza

di Angelo Carpani, libero professionista, laureato in Ingegneria elettronica esperto nella progettazione di impianti di videosorveglianza in ambito comunale

1. Introduzione

La Certificazione SOA (acronimo di "Società Organismo di Attestazione") è una attestazione di qualificazione che comprova la capacità economica e tecnica di una impresa di qualificarsi per l'esecuzione di appalti pubblici di "lavori" di importo maggiore a 150.000 euro e conferma, inoltre, che il soggetto certificato sia in possesso di tutti i requisiti necessari alla contrattazione pubblica.

I requisiti per lavori pubblici di importo pari o inferiore a 150.000 euro sono invece disciplinati dall'art. 90 del DPR n.207/2010 ("Regolamento"), articolo rimasto ancora in vigore in via transitoria ai sensi degli articoli 216 e 217 del D.Lgs. n.50/2016 ("Codice dei contratti").

L'art. 60 del "Regolamento" prevede che le stazioni appaltanti non possano richiedere ai concorrenti la dimostrazione della qualificazione con modalità e contenuti diversi.

Scopo di questo articolo non è quello di trattare in modo esaustivo e completo il sistema di qualificazione e i requisiti necessari per gli esecutori di lavori, argomento vasto e complesso, ma di dare indicazioni precise alle stazioni appaltanti su quali siano le categorie SOA da richiedere e quale requisito tecnico ed economico alle imprese che intendono partecipare agli appalti "lavori" per la realizzazione di impianti di videosorveglianza. Necessità, quest'ultima, che scaturisce dal fatto che capita spesso di vedere pubblicate delle gare d'appalto "lavori" in cui vengono richieste delle categorie SOA non in linea con i pronunciamenti dell'Autorità di Vigilanza (AVCP), ora ANAC.

Prima di entrare nel merito, viene fatto di seguito qualche breve richiamo sulla normativa.

Le categorie di opere previste dalla normativa sono le seguenti:

- 13 riguardanti **opere generali**, individuate con l'acronimo **"OG"**;
- 35 riguardanti **opere specializzate**, individuate con l'acronimo **"OS"**.

Le categorie SOA sono definite nell'Allegato A del "Regolamento" e richiamiamo di seguito quelle di nostro interesse:

OS5 – Impianti pneumatici e antintrusione

Riguarda la fornitura, il montaggio e la manutenzione o ristrutturazione di impianti pneumatici e di impianti antintrusione, completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi in opere generali che siano state già realizzate o siano in corso di costruzione.

OS19 – Impianti di reti di telecomunicazione e di trasmissione dati

Riguarda la fornitura, il montaggio e la manutenzione o ristrutturazione di impianti di commutazione per reti pubbliche o private, locali o interurbane, di telecomunicazione per telefonia, telex, dati e video su cavi in rame, su cavi in fibra ottica, su mezzi radioelettrici, su satelliti telefonici, radiotelefonici, televisivi e reti di trasmissione dati e simili, qualsiasi sia il loro grado di importanza, completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi, separatamente dalla esecuzione di altri impianti, in opere generali che siano state già realizzate o siano in corso di costruzione.

OS30 – Impianti interni elettrici, telefonici, radiotelefonici e televisivi

Riguarda la fornitura, il montaggio e la manutenzione o ristrutturazione di impianti elettrici, telefonici, radiotelefonici, televisivi, nonché reti di trasmissioni dati e simili, completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi in opere generali che siano state già realizzate o siano in corso di costruzione.

Di seguito vengono richiamati "sinteticamente" due interventi dell'Autorità di Vigilanza in materia di categorie SOA richieste per la realizzazione di impianti di videosorveglianza.

2. La Determinazione n.19 del 27/09/2001

Nel 2001 l'allora Autorità di Vigilanza sui Contratti Pubblici (AVCP), ora ANAC, intervenne sull'argomento a fronte di un quesito posto dalle Federazione Imprese Elettriche ed Elettroniche inerente l'inquadramento dei lavori relativi all'installazione dei sistemi di videosorveglianza nella declaratoria di cui all'allegato A del DPR 34/2000 (quest'ultimo poi abrogato dal DPR. n.207 del 2010 dall'8 giugno 2011).

L'ANIE, aderente alla Federazione suddetta, evidenziò che tali impianti potevano rientrare nella categoria OS5, in qualità di impianti antintrusione ma, nello stesso tempo, anche nella categoria OS19 per la loro connotazione, più propria, di impianti di telecomunicazione.

L'AVCP si pronunciò affermando che *"i lavori relativi all'istallazione dei sistemi di video sorveglianza, essendo finalizzati al controllo della sicurezza di edifici, di strade ecc.., e, pertanto, ad impedire l'accesso alle opere di soggetti non autorizzati, sono da considerarsi come impianti antintrusione e, quindi, rientranti nella declaratoria della* ***categoria OS5*** *di cui all'allegato A del DPR 34/2000".*

Nonostante la "determinazione" dell'Autorità, si assiste ancora oggi alla pubblicazione di molte gare di appalti lavori per la realizzazione di impianti di videosorveglianza in cui viene richiesta erroneamente la sola categoria SOA OS19.

3. Il Parere n.89 del 19/05/2011

Nel 2011 ci fu un ulteriore intervento dell'AVCP a fronte di una istanza di "parere" con cui una impresa contestava la scelta della stazione appaltante di indicare la categoria OS19 per la realizzazione di un sistema di videosorveglianza in fibra ottica quale categoria prevalente dei lavori da affidare, ritenendo più idonea la categoria OS30.

La stazione appaltante, a riscontro dell'istruttoria procedimentale dell'Autorità, evidenziava come la scelta della categoria da inserire nel bando di gara fosse frutto di una valutazione tecnica, non ritenendo congruo scegliere la categoria OS30, in quanto questa si riferisce ad impianti "interni" ad edifici, mentre il progetto in appalto riguardava impianti "esterni".

Il "parere" dell'Autorità fu il seguente: *"Orbene, non appare censurabile negli invocati termini la qualificazione scelta della stazione appaltante, sia a fronte della indicata destinazione all'esterno degli impianti da realizzare (come reso evidente altresì dalla finalità perseguita di sicurezza urbana), sia dal fatto che la diversa categoria OS30 concerne il differente caso di interventi accessori ad opere di costruzione più ampie, confermandosi, così, il carattere interno non rilevante nella specie".*

L'Autorità ritenne allora, nei limiti di cui in motivazione, che la previsione di bando in contestazione non era contraria ai principi in tema di evidenza pubblica.

Va precisato che il "parere" si esprime riguardo la categoria "prevalente". Nell'intervento in progetto, era prevista anche la realizzazione della rete di comunicazione in fibra ottica. E' noto, per gli operatori del settore, che generalmente costa di più realizzare la rete in fibra ottica che non installare le telecamere. E' ovvio quindi che la categoria prevalente riguardasse la realizzazione della rete in fibra ottica la quale, trattandosi di una "rete di telecomunicazione e di trasmissione dati", non poteva che ricadere nella declaratoria della categoria OS19.

4. Quali categorie SOA dunque richiedere?

Va innanzitutto osservato che gli interventi dell'Autorità rispondono a quesiti e a casi particolari. Dagli interventi dell'Autorità sopra richiamati, a parere di chi scrive, si possono comunque trarne delle conclusioni di carattere "generale" riguardo la realizzazione di impianti di videosorveglianza e che sono le seguenti:

- per la parte di impianto relativa alle telecamere ("video"), deve essere richiesta la categoria OS5;
- per la parte di impianto relativa alla rete di comunicazione, deve essere richiesta la categoria OS19.

Quale sarà poi la categoria "prevalente", dipenderà dagli importi riferiti alle categorie richieste nel bando di gara: in qualche caso sarà l'OS5 se sarà prevalente in termini economici la parte "video", e in qualche altro caso sarà l'OS19 se sarà prevalente in termini economici la parte "rete".

CONTATTO:
angelo.carpani@tiscali.it

Security Director Forum 2018, come cambia la sicurezza

a cura della Redazione

Si è tenuto il 18 e 19 giugno nella splendida cornice dell'Hotel Capuccini di Gubbio il **Security Director Forum 2018** organizzato da **Richmond**. Due giorni di meeting, seminari, workshop, gruppi di lavoro, incontri mirati per una full immersion nel mercato security, al fine di confrontarsi, trovare soluzioni e incrementare i contatti business.

Oltre 60 responsabili della sicurezza di imprese pubbliche e private di ogni settore si sono confrontati sul cambiamento in atto della sicurezza fisica con il contributo di esperti e fornitori qualificati. Ha partecipato per la prima volta il **Laboratorio per la Sicurezza** con uno speech di **Jerome Bertrume** e **Gabriele Venuti** sui nuovi rischi per le imprese derivanti dalla digitalizzazione dei processi, che sottolineano la centralità della formazione e della consapevolezza delle persone.

In particolare, Bertrume ha affrontato il tema di GDPR: *"La migrazione degli asset critici dal mondo fisico al mondo digitale porta imprese e persone a un finto sentimento di sicurezza e di controllo. GDPR costituisce un'opportunità (l'ultima!) per integrare la dimensione cyber nel piano di sicurezza, nella consapevolezza che la mancata formazione delle persone costituisce spesso l'anello più debole della catena di protezione. Come per altri problemi di sicurezza e furti, il Security Manager deve essere la pietra angolare che aiuterà a proteggere davvero le infrastrutture pattando dalle persone e sviluppando una sana consapevolezza del rischio cyber."*

Venuti si è soffermato sugli effetti dei data breach: *"Con l'avvento della digital trasformation anche i rischi sono cambiati, basti pensare al danno reputazionale ed economico che un data breach può causare ad un'azienda. Il vero problema nasce quando gli individui - dipendenti o clienti - non percepiscono la facilità con cui si può essere vittime di frodi o altri eventi criminosi; ad oggi la maggior parte dei cyberattacks sfruttano le vulnerabilità dell'essere umano come superficialità, negligenza, disattenzione, buona fede, nulla di diverso dalle classiche frodi del mondo reale. Perciò, a seguito di installazione di adeguate tecnologie cybersecurity, il lavoro più importante non potrà che essere la sensibilizzazione dell'individuo per aumentare la percezione del rischio e riconoscere le minacce che il mondo digital presenta"*

Luisa Franchina, presidente AIIC, che ha partecipato al Security Director Forum, ha commentato: *"L'evento è stato particolarmente interessante grazie ad una organizzazione non convenzionale ed estremamente attenta ai dettagli e alla coerenza logica degli interventi. Un evento dedicato a una professionalità delicata e importante per tutte le aziende in ogni settore".*

Claudio Honegger, Amministratore unico di Richmond Italia, ha dichiarato: *"Un evento che costituisce un acceleratore di formazione e innovazione e permette di fare il punto sulla sicurezza aziendale e sul contesto normativo in continua evoluzione. Anche quest'anno l'offerta formativa è stata ampia e variegata e i partecipanti hanno potuto condividere tra di loro esperienze, idee, buone prassi e testimonianze lavorative. Un ringraziamento va quindi a tutti i relatori che hanno permesso la buona riuscita del forum e a tutti gli exhibitor e i responsabili della sicurezza che ci supportano e che tornano a casa entusiasti di questa esperienza" .*

securindex
formazione

CORSI DI FORMAZIONE PER
PROFESSIONISTI DELLA SICUREZZA

per informazioni sui programmi e date scrivere a:
segreteria@securindex.com

Travel security, un altro fronte operativo per i security manager

a colloquio con Matteo Tassoni, Country Security Manager (Italy, Greece, Croatia, Serbia & Israel) at ABB
a cura di Raffaello Juvara

Rischi sanitari, rischi naturali o accidentali, criminalità comune e terrorismo sono i rischi principali che minacciano le persone in viaggio per lavoro. Qual è la scala di importanza, anche in relazione alle aree geografiche di viaggio?
Innanzitutto vorrei sottolineare, prima di scendere nei dettagli, quanto sia importante per le Aziende avere uno strumento di Travel Security. Si è sempre discusso di quanto sia strategico, ed ora è diventato prassi comune, fare un'analisi dei rischi ed avere una qualsivoglia misura di security quando si parla di Sicurezza Fisica ma, a tutt'oggi, la sicurezza del personale viaggiante è ancora molto, troppo, sottostimata. Dall'altra parte, sia a livello giuridico che di sensibilità dei singoli, viene sempre più visto come inconcepibile che nel 2018 qualcuno possa correre rischi evitabili mentre sta svolgendo la propria attività lavorativa. Da questo punto di vista, non vi è alcuna differenza fra i rischi sul luogo di lavoro (di cui tanto si parla e sui quali la Security riveste una parte marginale) ed i rischi sul lavoro dovuti a trasferte, sui quali invece siamo competenti noi Security Manager. Avere quindi uno strumento per la valutazione, la gestione e la prevenzione di questo tipo di rischi è, nel 2018, di vitale importanza per una reale protezione dell'Azienda nel suo insieme.
Quando poi lo si ha, e qui vengo alla domanda, ci si accorge di alcuni luoghi comuni e credenze.
La maggior parte delle Aziende ha iniziato ad avere strumenti di Travel Security legati ai rischi terrorismo e per proteggere il personale mandato in nazioni a rischio guerra. Nel corso del tempo ci si è accorti (come nel nostro caso) che il 95,7% delle emergenze erano di tipo medico (anche banali: un ascesso ad un dente), di piccola criminalità (all'ordine del giorno le rapine/sequestri col "sequestrato"

costretto a girare di bancomat in bancomat e poi lasciato nelle periferie) o emergenze operative (aver perso i documenti, essere fermati dalla Polizia e non capire la lingua locale).
La verità è, dunque, che gli interventi di emergenza per problematiche terroristiche e di rischio guerra sono minimali rispetto alle altre. Attraverso una Travel Security è possibile proteggere il viaggiatore (e l'Azienda) a 360°. La Travel Security, quindi, è il campo in cui lo spettro di intervento di un Security Manager viene maggiormente ampliato, ponendolo a contatto con tanti altri clienti interni, fra cui Sales, HR, HSE e Operation.

In che modo devono venire affrontati i diversi rischi per dare risposte adeguate alle esigenze di sicurezza delle persone e assicurare, di conseguenza, la protezione del patrimonio aziendale?
Bisogna innanzitutto che i dipendenti dell'Azienda abbiano chiari due concetti chiave sui quali puntiamo tutta la nostra campagna informativa:
• La prevenzione e la formazione pre-viaggio sono il 99% della Travel Security: quando sei già partito è tardi;
• Se tu sei il primo che trascuri la tua sicurezza, c'è veramente poco che gli altri possano fare per te quando sei in pericolo.

Magari sono concetti molto crudi ma servono per risvegliare le coscienze sul tema. La maggior parte dei problemi incontrati dai viaggiatori si potevano evitare alla partenza: tipici esempi sono quelli legati ai rischi di malaria e febbre gialla oppure ai rischi dei trasporti locali. Ancora adesso trovo incredibile quante persone contraggono banali infezioni intestinali perché usano ghiaccio o si lavano i denti con l'acqua del rubinetto in paesi in cui è risaputo, e noi diamo per scontato, che certe cose non vadano fatte. Ovviamente l'aspetto più importante è quello legato alla tracciatura dei viaggi dei dipendenti: sapere dove si trovano è il primo passo per poterli proteggere. Un secondo aspetto fondamentale è quello, una volta saputo dove sono, di avere chi possa operare in quei posti in caso di emergenza. Fortunatamente, ci sono società che offrono eccellenti servizi in entrambi i punti di cui sopra.

Possiamo dare una definizione univoca di Travel Security, delle figure aziendali coinvolte, degli obiettivi da perseguire?
Credo sia un concetto che inevitabilmente varia di Azienda in Azienda ma con alcuni comuni denominatori legati a "tutte quelle attività che vengono fatte per la protezione del personale viaggiante".
Per la mia Azienda (ABB), la Travel Security viene definita come lo strumento per la prevenzione dei comportamenti a rischio da parte dei dipendenti, per la protezione e la gestione delle aree a rischio di instabilità politica e sociale, per la gestione dei protocolli sanitari, MEDEVAC e di evacuazione in generale.

Quali sono le competenze tipiche del security manager (p.e. analisi del rischio, gestione delle crisi) che trovano applicazione nella Travel Security? E quali nuove competenze deve acquisire?
Nel mio ruolo mi sono dovuto sicuramente dovuto imbattere in nuovi skills e in nuove metodologie per poter essere efficiente in questo campo. Di sicuro, il problema maggiore è quello di non poter seguire con un'analisi del rischio pre-viaggio tutti i dipendenti che sono considerati "frequent travellers" e che, nel 2017, hanno viaggiato in 152 diversi Paesi. L'analisi del rischio quindi diventa non più la survey fisica (impossibile da gestire e troppo onerosa) ma la validazione delle informazioni disponibili sulle singole aree o sulla documentazione del sito.
Bisogna poi avere una mente molto aperta che lasci fuori ogni pregiudizio e ogni luogo comune, ma che analizzi solo i dati verificati. Un caso specifico - in negativo - è quello dell'Egitto, nazione a fortissimo rischio che, come italiani, facciamo fatica a percepire e ad accettare; al contrario, percepiamo ancora Israele come una nazione con la guerra civile fra le strade di Tel Aviv e consideriamo pericoloso andarci anche per turismo… Anche se questo aspetto sembra semplice, in realtà è forse la cosa più difficile da affrontare correttamente.

Quali sono gli obiettivi, gli strumenti e gli indicatori per un'adeguata gestione della travel security?
Prima di tutto, credo non ci possa essere una valida Travel Security senza un sistema coordinato di Crisis Management con chiare responsabilità. In secondo luogo, è basilare una gestione centralizzata delle prenotazioni dei viaggi che alimenti il portale di Travel Tracker: banalmente, il responsabile della sicurezza del personale viaggiante deve sapere dov'è per poterlo proteggerre…!
Inoltre sono necessari momenti di formazioni face-to-face e di e-learning, schede Paese sempre aggiornate, sistemi di comunicazione mail/sms/telefono in caso di emergenza, eccetera. Affidarsi ad un buon provider di protezione medica e di rimpatrio internazionale è infine fondamentale per una riuscita del tutto.

Certificazione installatori: IMQ presenta lo schema IMQ AIR VIDEO

a cura della Redazione

Dal 1° luglio 2018 si affianca allo schema **IMQ AIR**, in vigore dal 2017, il nuovo schema **IMQ AIR VIDEO** per la qualificazione delle figure professionali di Responsabile Tecnico (Progettista) e Esperto Tecnico (Installatore) per **sistemi di Allarme Intrusione-Rapina e Videosorveglianza.** Rimane in vigore lo schema **IMQ AIR** per Responsabili Tecnici (Progettisti) e Esperti Tecnici (Installatori) relativo ai soli impianti di allarme intrusione e rapina, per il quale l'esame riguarderà la conoscenza della **Norma CEI 79.3:2012** e, per la parte legale, le **responsabilità del fornitore e la tutela dei dati personali (GDPR)**. I Responsabili Tecnici (Progettisti) affronteranno anche un'esercitazione pratica su un progetto di impianto antintrusione. Tra i requisiti richiesti per l'ammissione all'esame c'è la frequentazione di un corso, qualificato da IMQ, di almeno **12 ore** sulle materie d'esame.

Il nuovo schema **IMQ AIR VIDEO** si estende alle competenze dei Responsabili Tecnici (Progettisti) e degli Esperti Tecnici (Installatori) di impianti di videosorveglianza, diventati parte integrante dei sistemi di allarme intrusione e rapina. Oltre ai test previsti dallo schema IMQ AIR, l'esame per la certificazione IMQ AIR VIDEO riguarderà anche la conoscenza dei sistemi di videosorveglianza e delle reti IP, mentre i Responsabili Tecnici (Progettisti) affronteranno anche un'esercitazione pratica su un progetto di impianto di videosorveglianza. Tra i requisiti richiesti per l'ammissione all'esame c'è la frequentazione di un corso, qualificato da IMQ, di almeno **20 ore** sulle materie d'esame.

E' possibile ottenere la certificazione per entrambe le figure di Responsabile Tecnico (Progettista) ed Esperto Tecnico ((installatore) IMQ AIR VIDEO con un'unica sessione di esame.

IMQ

Schema di certificazione IMQ AIR

I Progettisti e Installatori in possesso della certificazione IMQ AIR rilasciata entro il 30 giugno 2018 potranno sostenere un esame integrativo per ottenere la certificazione IMQ AIR VIDEO.

IMQ prevede inoltre un percorso specifico per la certificazione delle persone, secondo i suddetti schemi, che lavorano presso le imprese installatrici già in possesso della certificazione IMQ.

Francesco Sperandini, Direttore della B.U. Machinery, In-Service Inspections & Certification of Persons di IMQ, ha dichiarato: *"Con lo schema IMQ AIR VIDEO vogliamo rispondere ad una specifica domanda del mercato: qualificare le competenze degli esperti in impianti di videosorveglianza e, al tempo stesso, predisporre gli operatori del settore al recepimento degli Standard Europei in materia di Qualifica e Certificazione delle imprese che erogano servizi di progettazione, installazione e manutenzione di impianti antintrusione e rapina, videosorveglianza e antincendio. Il tutto in un quadro di tutela dell'utilizzatore finale, in linea con i principi stabiliti dall'UE".*

Cosa cambia nei corsi propedeutici alla certificazione IMQ AIR VIDEO

a colloquio con Roberto Dalla Torre, coordinatore corsi di securindex formazione

Dal 1° luglio è entrato in vigore il nuovo schema IMQ AIR VIDEO per la qualificazione delle diverse figure di Esperti in impianti di allarme intrusione, rapina e videosorveglianza. Come cambiano i corsi propedeutici alla certificazione organizzati da securindex formazione e qualificati da IMQ?

Per il nuovo schema IMQ AIR VIDEO per la qualificazione delle figure professionali di Esperto di Impianti nelle due specialità di Responsabile Tecnico (Progettista) e Esperto Tecnico (Installatore) per sistemi di Allarme Intrusione-Rapina e Videosorveglianza, securindex formazione ha preparato uno specifico percorso formativo che prevede 8 ore di corso sulle reti IP e videosorveglianza, 8 ore sulla norma CEI 79-3:2012 (con esercitazione di applicazione del modello matematico) e 4 ore sulla parte legale/contrattuale. Naturalmente vengono mantenuti anche i corsi propedeutici all'ottenimento della certificazione IMQ AIR, ovvero per la qualificazione delle figure professionali di Esperto di Impianti - Responsabile Tecnico (Progettista) e Esperto Tecnico (Installatore) - per sistemi di Allarme Intrusione-Rapina che non si occupano di Videosorveglianza. In questo caso, il corso prevede 8 ore sulla norma CEI 79-3:2012 (con esercitazione di applicazione del modello matematico) e 4 ore sulla parte legale/contrattuale.

Possiamo fare un bilancio dello schema IMQ AIR, entrato in vigore all'inizio del 2017? Come hanno risposto gli operatori del settore, le aziende produttrici, i clienti finali?

Il bilancio è assolutamente positivo: abbiamo erogato al 30 giugno 12 corsi con la partecipazione di oltre 150 discenti, 135 dei quali hanno ottenuto la Certificazione IMQ AIR tra Esperti di Impianti ovvero in grado di progettare gli impianti antintrusione, ed Esperti di Installazione ovvero addetti all'installazione e manutenzione degli impianti antintrusione.

Siamo partiti con un corso pilota nel gennaio 2017 con 10 partecipanti che ci ha permesso di mettere a punto il percorso formativo ed il materiale didattico. Quindi, sempre nel 2017 abbiamo erogato tre corsi open a Milano presso la sede di IMQ e quattro corsi presso aziende produttrici di apparecchiature antintrusione e aziende distributrici.

Nel 2018 abbiamo erogato fino ad oggi 5 corsi, tre dei quali presso aziende del settore (due aziende distributrici ed una che fornisce servizi).

Gli operatori del settore hanno risposto con molto interesse, trovando nella certificazione IMQ AIR una risposta concreta e attendibile alla crescente esigenza di qualificazione dei professionisti della sicurezza, in un mercato sempre più invaso da offerte di ogni genere basate esclusivamente sul fattore prezzo, che poco o nulla hanno a che vedere con la sicurezza, ma che generano confusione tra gli utilizzatori finali.

Dev'essere anche evidenziato che ai nostri corsi hanno partecipato diversi addetti alla sicurezza di primari Istituti di credito che hanno superato l'esame IMQ ed hanno ottenuto il Certificato IMQ AIR come progettisti.

Proprio questa settimana erogheremo un corso presso una primaria azienda costruttrice nella sede di Padova, che ci è stato richiesto con l'intento di qualificare e quindi certificare le figure tecnico/commerciali dell'azienda che dovranno assistere i propri clienti (anche installatori) nella scelta dei sistemi di sicurezza più idonei in conformità alle norme CEI 79-3.

Quali sono i programmi per securindex formazione per la seconda parte del 2018?

Visto il successo fin qui ottenuto e gli importanti sviluppi che avrà il nuovo schema IMQ AIR VIDEO, prevedo una seconda parte del 2018 particolarmente impegnativa per tutto lo staff securindex formazione, del quale mi pregio di far parte sia in qualità di docente che di coordinatore.

Metteremo in calendario a partire da settembre il nuovo corso open che verrà erogato a Milano, finalizzato all'ottenimento della certificazione IMQ AIR VIDEO che affiancherà la proposta formativa per l'ottenimento della certificazione IMQ AIR ovvero per le figure che non realizzano impianti di videosorveglianza ma solamente impianti antintrusione.

Sicuramente metteremo in calendario alcuni proposte formative riguardanti una materia d'attualità come il Regolamento europeo sul trattamento dei dati (GDPR).

Proporremo inoltre un corso di due giorni rivolto agli installatori, che li aiuterà ad affrontare le tematiche legate alla vendita dei sistemi di sicurezza.

Stiamo mettendo infine a punto dei corsi di aggiornamento su varie tematiche, rivolti alle figure già certificate IMQ AIR.

Il programma dei corsi autunnali verrà pubblicato prossimamente sul sito **www.securindex.com**

PER INFORMAZIONI:
segreteria@securindex.com
fabrizio.sisto@imq.it

HammerADV

sol®

DOPO L'ESTATE, DENTRO LA NUVOLA SPLENDERÀ UN
NUOVO SOL.
IL SISTEMA ALL-IN-ONE
DI INIM 100% WIRELESS.
SEMPLICE, POTENTE, SENZA LIMITI.
SOLO PER PROFESSIONISTI!

inim ELECTRONICS
inim.biz

PROGETTO INSTALLATORE SICURO
dalla parte del professionista della sicurezza

Il **Progetto Installatore Sicuro** offre ai professionisti della sicurezza - **progettisti, installatori, integratori, manutentori** - un esclusivo percorso di qualificazione personale attraverso l'accrescimento e la certificazione delle competenze, con l'obiettivo di tutelare l'attività svolta e di poterla sviluppare su basi consolidate.

Corsi di formazione, certificazioni IMQ, assicurazioni professionali sono i pilastri fondamentali del **Progetto Installatore Sicuro**, che accompagnerà nel tempo i partecipanti con corsi avanzati e seminari di aggiornamento per la formazione continua. Verranno sviluppate iniziative riservate di marketing digitale per conoscere e farsi riconoscere da clienti consapevoli di dover affidare la propria sicurezza solo a professionisti qualificati.

DIVENTA UN INSTALLATORE SICURO:
UN PROFESSIONISTA SICURO DELLE SUE COMPETENZE PER DARE SICUREZZA AI SUOI CLIENTI

Per informazioni:
02.36757931
segreteria@securindex.com

FORMAZIONE

securindex formazione

Le attività di formazione sono curate da **securindex formazione** che organizza corsi e seminari specialistici nei settori **Sicurezza Fisica, Sicurezza delle Reti, Tutela dei Dati Personali.**

securindex formazione si avvale per la docenza di noti professionisti di comprovata esperienza nelle materie previste nei corsi. I corsi propedeutici alle certificazioni sono riconosciuti dagli Organismi di Certificazione di riferimento.

I corsi vengono organizzati con lezioni frontali in modalità open o riservata per aziende.
Ai partecipanti viene rilasciato l'Attestato di Partecipazione valido al fine dell'ottenimento dei crediti formativi previsti per ciascun modulo formativo ai fini del mantenimento della certificazione.

PROGRAMMA CORSI 2018

1. **Corso Propedeutico alla Certificazione IMQ AIR per Progettisti e Installatori Impianti Allarme:**
Modulo unico di 16 ore + 4 ore ripasso ed esercitazioni di calcolo pre-esame IMQ in tre giornate consecutive.
Sessione open a Milano presso IMQ.

2. **Corso Introduttivo al GDPR 679/2016:**
Modulo unico di 4 ore con test di autovalutazione.
Sessioni open a Milano.

3. **Corso Introduttivo alla Progettazione Impianti Videosorveglianza:**
Modulo unico di 4 ore con test di autovalutazione.
Sessioni open a Milano.

4. **Corsi di Vendita Sistemi di Sicurezza Professional Base:**
Moduli di 8 + 8 ore in due giornate separate.
Sessioni open a Milano.

essecome security&safety · AON Empower Results® · IMQ · MARINTEC · securindex.com

CERTIFICAZIONE

CERTIFICAZIONE ESPERTI IMPIANTI DI ALLARME INTRUSIONE-RAPINA E VIDEOSORVEGLIANZA IMQ AIR/IMQ AIR VIDEO

Il mondo della sicurezza sta evolvendo rapidamente: le nuove tecnologie, l'integrazione con la domotica e gli edifici intelligenti, le richieste di un mercato sempre più esigente e preparato, le responsabilità in caso di malfunzionamento del sistema venduto sono solamente alcuni dei fattori di cambiamento. Un'evoluzione rapida, che richiede figure professionali sempre più preparate e affidabili, in particolare installatori qualificati che possano garantire, da una parte, i produttori e i distributori sul corretto utilizzo dei loro prodotti; dall'altra, i committenti, offrendo loro l'evidenza di essersi rivolti a professionisti competenti e sempre aggiornati sulle nuove tecnologie.

Per rispondere a queste esigenze, **IMQ**, ente italiano leader nella valutazione della conformità, ha dato vita nel 2017 a **IMQ AIR**, uno schema di qualificazione per Esperti di Impianti di Allarme Intrusione e Rapina, strutturato su due livelli: Progettista e Installatore.

Dal 1° luglio 2018 si affianca il nuovo schema **IMQ AIR VIDEO** per la qualificazione delle figure professionali di Responsabile Tecnico (Progettista) e Esperto Tecnico (Installatore) per **sistemi di Allarme Intrusione-Rapina e Videosorveglianza.**

Rimane in vigore lo schema **IMQ AIR** per Responsabili Tecnici (Progettisti) e Esperti Tecnici (Installatori) relativo ai soli impianti di allarme intrusione e rapina, per il quale l'esame riguarderà la conoscenza della **Norma CEI 79.3:2012** e, per la parte legale, le **responsabilità del fornitore e la tutela dei dati personali (GDPR)**. I Responsabili Tecnici (Progettisti) affronteranno anche un'esercitazione pratica su un progetto di impianto antintrusione. Tra i requisiti richiesti per l'ammissione all'esame c'è la frequentazione di un corso, qualificato da IMQ, di almeno **12 ore** sulle materie d'esame.

Il nuovo schema **IMQ AIR VIDEO** si estende alle competenze dei Responsabili Tecnici (Progettisti) e degli Esperti Tecnici (Installatori) di impianti di videosorveglianza, diventati parte integrante dei sistemi di allarme intrusione e rapina. Oltre ai test previsti dallo schema IMQ AIR, l'esame per la certificazione IMQ AIR VIDEO riguarderà anche la conoscenza dei sistemi di videosorveglianza e delle reti IP, mentre i Responsabili Tecnici (Progettisti) affronteranno anche un'esercitazione pratica su un progetto di impianto di videosorveglianza. Tra i requisiti richiesti per l'ammissione all'esame c'è la frequentazione di un corso, qualificato da IMQ, di almeno **20 ore** sulle materie d'esame.

È possibile ottenere la certificazione per entrambe le figure di Responsabile Tecnico (Progettista) ed Esperto Tecnico ((installatore) IMQ AIR VIDEO con un'unica sessione di esame.

I Progettisti e Installatori in possesso della certificazione IMQ AIR rilasciata entro il 30 giugno 2018 potranno sostenere un esame integrativo per ottenere la certificazione IMQ AIR VIDEO.

IMQ prevede inoltre un percorso specifico per la certificazione delle persone, secondo i suddetti schemi, che lavorano presso le imprese installatrici già in possesso della certificazione IMQ.

ASSICURAZIONE

Dalla collaborazione tra **Aon Benfield Italia**, società appartenente al più grande gruppo di brokeraggio assicurativo nel mondo, **Marintec**, agenzia corrispondente dei **Lloyd's**, ed **essecome/securindex**, è nata la prima polizza contro i rischi professionali riservata ai **progettisti e installatori di impianti di allarme**, sviluppata in esclusiva da alcuni sottoscrittori dei **Lloyd's di Londra**.

La polizza copre i rischi di **Responsabilità Civile verso Terzi (RCT), verso Prestatori d'Opera (RCO) e Contrattuale (RCC)** per gli importi che l'installatore di impianti di allarme intrusione e rapina possa venir chiamato a risarcire per i danni causati a terzi esercitando la propria attività ed è **riservata agli installatori in possesso della certificazione IMQ AIR.**

Estratto dalle tabelle premi R.C.T. – R.C.C. - R.C.O. comprensivi di Accessori 15% e Imposte 22,5%.

N.B. I premi indicati sono per polizze a massimale unico. I massimali possono essere diversi per ogni Rischio.

Progettista (Fig. A): Esperto di impianti di allarme intrusione e rapina, intendendosi per tale il Soggetto che ha le conoscenze, l'esperienza e le capacità necessarie per svolgere le attività di valutazione dei rischio, progettazione dell'impianto e validazione del progetto in possesso della certificazione IMQ AIR.

Massimale / Fatturato	500.000	1.500.000	2.500.000	5.000.000
100.000	557	584	597	657
500.000	1824	1878	1933	2127
1.000.000	3644	3754	3865	4351
5.000.000	18213	18759	19321	21254

Installatore (Fig. B): Esperto di impianti di allarme intrusione e rapina, intendendosi per tale il Soggetto che ha le conoscenze, l'esperienza e le capacità necessarie per svolgere le attività di pianificazione, installazione, manutenzione e riparazione dell'impianto, in possesso della certificazione IMQ AIR.

Massimale / Fatturato	500.000	1.500.000	2.500.000	5.000.000
100.000	494	535	547	602
500.000	1675	1725	1778	1954
1.000.000	3348	3448	3553	3907
5.000.000	16735	17237	17753	19528

N.B. Il presente Estratto non rappresenta in alcun modo una proposta contrattuale, ma solo una sintesi a titolo esclusivamente informativo delle Condizioni Particolari e delle Tabelle della Polizza RC Professionale Installatori dei Lloyd's riservata ai Progettisti , Installatori e Manutentori di Impianti di Allarme Intrusione e Rapina in possesso della certificazione IMQ AIR.

RISCO Group presenta il Programma Partner RISCO Stars

a cura della Redazione

RISCO Stars è il programma di **RISCO Group** pensato per supportare la crescita di distributori e installatori attraverso formazione online e fornendo gli strumenti necessari per aumentare la propria visibilità nel mercato. Lanciato nel 2016, ha visto lo scorso anno più che raddoppiare il **numero di partner Gold** (da **12** a **26** in soli dodici mesi) e conta anche **1 partner Platinum**.

Il programma include tre livelli di partecipazione – **Silver, Gold e Platinum** – caratterizzati da vantaggi esclusivi e requisiti pensati per incentivare la crescita, la competenza e la formazione degli installatori. Il livello di adesione – Silver – si consegue attraverso la semplice registrazione gratuita al programma, quelli **Gold** e **Platinum** raggiungendo rispettivamente 25.000 o 80.000 punti Stars e 2 o 4 certificazioni.

I tre livelli permettono di riconoscere la competenza e la fedeltà, nonché promuovere la presenza di una rete di installatori professionisti di qualità che utilizzano RISCO sul territorio italiano. Inoltre, la premiazione favorisce la loro crescita, promuovendone il potenziale di vendita attraverso vantaggi appositamente studiati e assegnati a seconda del livello di programma raggiunto.

Tutti i clienti hanno inoltre la possibilità di accedere gratuitamente a corsi di formazione professionali online per migliorare le competenze sulle soluzioni RISCO anche con il rilascio di certificati online, elemento chiave per garantire elevata qualità, competenza e professionalità all'interno dell'intero circuito professionale.

Tutti i partner elencati sul sito RISCO Group dedicato agli utenti finali hanno conseguito le certificazioni sulle centrali **Agility™** e **LightSYS™2**, ovvero le più specifiche per le applicazioni nel mercato residenziale, garanzia di professionalità anche per gli utenti finali. La possibilità di inserire il proprio nome all'interno della pagina è un riconoscimento importante per gli installatori, considerato che da gennaio 2018 ad oggi RISCO ha registrato più di 17.000 visite uniche. Inoltre, a conferma della validità dell'attività di sensibilizzazione dei partner sull'importanza del continuo aggiornamento professionale tramite le certificazioni, RISCO conta ad ora oltre 1.100 certificazioni conseguite da circa 570 aziende.

RISCO GROUP

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

Le 8 migliori video analitiche e i principali trend nelle banche per la sicurezza fisica e la Branch Transformation

di Pietro Tonussi Business development manager, Southern Europe, in Axis Communications

Non c'è dubbio che nel corso degli ultimi anni le tecnologie emergenti hanno aperto la strada alle più innovative applicazioni di sicurezza fisica. L'evoluzione delle filiali bancarie è un argomento di cui si parla con sempre maggiore frequenza, soprattutto facendo riferimento alla capacità di sfruttare le nuove tecnologie per migliorare le operazioni di business, pur mantenendo un focus sulla sicurezza.
La varietà di applicazioni di analisi video è piuttosto ampia e continua ad espandersi con l'introduzione sul mercato di ulteriori soluzioni. Ad oggi nel retail banking, le video analitiche più utilizzate sono:

Per quanto riguarda le sfide di sicurezza

1. Protezione delle aree sensibili
Cross Line Detection è un'applicazione che rileva soggetti in movimento che attraversano una linea virtuale generando un evento. Se l'evento si verifica in un luogo specifico e fuori dal normale orario di ufficio il software appositamente programmato genera degli avvisi che segnalano una presenza indesiderata.

2. Prevenire lo stazionamento prolungato di persone in specifiche aree
È possibile utilizzare l'analisi video per individuare persone che entrano in una specifica area ed inviare un avviso se rimangono in tale area per un determinato periodo di tempo troppo lungo. Ad esempio, nelle aree self dei Bancomat, possono aiutare ad impedire alle persone di fermarsi in queste aree in modo tale da non correre il rischio di creare un ambiente potenzialmente pericoloso o indesiderato per i clienti.

3. Gestione dei parcheggi
Strutture senza efficaci misure per il controllo accessi dei propri parcheggi sono vulnerabili ai criminali. Le soluzioni di controllo accessi dei veicoli aiutano a gestire l'entrata di clienti e dipendenti, attraverso la lettura della targa e con un controllo in tempo reale della white&black list è possibile gestire in modo appropriato l'ingresso delle persone autorizzate e prendere le dovute contromisure in caso contrario e possono inoltre lavorare con un sistema di controllo accessi o interfono.

4. Rilevamento di specifici suoni e conseguente invio di avvisi
Un sistema audio IP si integra perfettamente con un'installazione di sicurezza video, oltre ad aiutare a prevenire un'intrusione attraverso messaggi audio di avvertimento, può anche rilevare suoni in situazioni potenzialmente pericolose: aggressioni, allarmi, colpi di pistola, vetri rotti, rumori insoliti possono significare un possibile incidente in arrivo: la possibilità di ottenere avvisi per queste situazioni, grazie all'analisi analitica di Sound Detection, consente la gestione proattiva degli eventi da parte del personale di sicurezza.

Ottimizzazione delle filiali per migliorare la Customer Experience

5. Determinare gli orari di apertura ottimali ed esigenze del personale
Conoscere il numero di persone che frequentano la filiale – e in quali orari – permette l'ottimizzazione del personale di staff nelle fasce orarie desiderate e le migliori ore di apertura: l'analisi di People Counter monitora il flusso dei clienti durante la giornata, contando automaticamente in tempo reale il numero di persone e la direzione in cui si muovono , consentendo di migliorare l'esperienza del cliente.

6. Scegliere quanti cassieri e dirigenti avere in filiale in determinati giorni e orari
Acquisire in tempo reale statistiche su quanto tempo I clienti aspettano in fila, potrebbe migliorare notevolmente l'esperienza del cliente: un'analisi intelligente di gestione delle code, tiene traccia della durata e dei cambiamenti nel corso di una giornata, consentendo alle banche di gestire al meglio l'apertura degli sportelli in funzione del numero delle persone. In questo modo diminuisce il tempo di attesa dei clienti, creando un'esperienza più positiva.

7. Marketing canalizzato alla clientela
Grazie alle statistiche, raccolte dalle varie agenzie, basate sul gender e l'età presunta dei clienti è possibile gestire e allineare le attività di marketing nelle specifiche aree o in specifiche fasce orarie. Le analisi per l'identificazione demografica consentono, ad esempio, di adattare automaticamente e in tempo reale l'annuncio su un display digitale al sesso e/o all'età della persona davanti allo schermo e di valutare il successo di campagne specifiche.

8. Far sentire i clienti a proprio agio
Per migliorare ulteriormente l'esperienza dei clienti è possibile integrare l'audio. Quando parliamo dei sensi, tendiamo a pensare prima battuta alla vista, ma in realtà rispondiamo con la stessa intensità anche con l'udito: la musica di sottofondo è una delle componenti più utili in un'efficace strategia di business in un qualsiasi negozio, in quanto è importante creare connessioni emotive in grado di scatenare il comportamento desiderato… Siete mai stati in un negozio tra novembre e dicembre? ci sono canzoni natalizie, giusto?

Migliorare l'innovazione della filiale

Le analitiche sono strumenti che aiutano notevolmente le banche a massimizzare il loro valore attraverso sistemi video IP ed ottenere una visione più approfondita del loro business. In alcuni casi, queste soluzioni esistono già ma non vengono utilizzate al massimo delle loro potenzialità. E' importante per i responsabili della sicurezza fisica, condividere con il proprio team operativo come anche loro possano trarre profitto da questi strumenti. Per le banche che puntano sull'innovazione, la raccolta di preziosi dati in tempo reale sulle performance sarà fondamentale per ottimizzare il proprio business.

CONTATTI: AXIS COMMUNICATIONS
Tel. +39 02 8424 5762
www.axis.com

Senator, protezione da furti e incendi firmata ChubbSafes

a cura della Redazione

Una nuova cassaforte certificata ideale per la casa e per l'ufficio: Senator, griffata ChubbSafes, marchio storico nel settore dei mezzi forti. In un'unica cassaforte si ritrovano numerosi pregi, dal design elegante all'ottima protezione dal fuoco e dai furti.

Furti e rapine in Italia diminuiscono, secondo il Ministero dell'Interno, ma partono pur sempre da una base abbastanza elevata: con oltre 20.000 furti per milione di abitanti, il dato, seppure in calo, è tra i più alti fra i principali Paesi europei.

Un altro poco invidiabile primato del nostro Paese riguarda gli incendi: anche in questo caso, con oltre 700 grandi incendi nel 2017 siamo al primo posto in Europa. Anche se questo fenomeno riguarda prevalentemente aree boschive, la percezione del rischio di incendi presso il pubblico risulta in aumento.

Visto l'insieme dei dati disponibili, è facilmente comprensibile che la domanda di protezione da eventi esterni sia in crescita: il settore della sicurezza nel suo complesso riflette questa tendenza con un andamento piuttosto dinamico.

Sicurezza, la domanda è in aumento

Il segmento dei mezzi forti è in linea con questa situazione: la percezione di insicurezza porta a voler proteggere i beni al meglio. La cassaforte è sempre una soluzione pratica, sia dal punto di vista della funzione come deterrente per i furti, sia per quanto riguarda le qualità di protezione dalle fiamme offerte dal mezzo forte.

Da un lato, aumentando di molto il tempo necessario perché i malintenzionati accedano al suo contenuto, la cassaforte fa crescere la probabilità che un intervento esterno interrompa il loro operato; dall'altro, i materiali con cui è realizzata possono minimizzare la possibilità che un incendio prima di essere domato riesca a danneggiare il contenuto.

Quale mezzo forte scegliere? La varietà disponibile sul mercato è ampia: per essere sicuri di non scegliere una soluzione sovra o sotto dimensionata, il consiglio di chi è esperto in materia è un valido aiuto. Il personale tecnico e commerciale di Gunnebo è a disposizione per spiegare le caratteristiche dei vari modelli e suggerire il più adatto a ogni esigenza.

Una cassaforte contro furti e fuoco

Ed è proprio per rispondere alle aspettative di utenti sempre più attenti ed esigenti, che **Gunnebo** ha sviluppato la cassaforte **SENATOR**. La nuova gamma, articolata in quattro modelli, consente di conciliare le doti di sicurezza con un design accattivante ad un prezzo competitivo.

Può così trovare idonea collocazione all'interno della maggior parte di abitazioni ed uffici, oltre che di piccole e medie attività commerciali.

Per offrire una protezione completa contro entrambe le minacce più temute: i furti ed il fuoco, l'intera gamma Senator è certificata EN 1143-1 Grado 1 per quanto riguarda la resistenza all'effrazione e EN 15659, LFS 30P fino a 30 minuti per la resistenza al fuoco da ECB•S (European Certification Board of Security).

Anche le serrature di Senator rispondono a stringenti requisiti qualitativi: la serratura a chiave Classe A e la serratura elettronica Classe B ad alta sicurezza sono entrambe certificate EN 1300.

La feritoia per l'introduzione della chiave include un copritoppa, che fornisce una protezione aggiuntiva.

Una soluzione pratica dal design accurato

I pregi di Senator sono evidenti dal punto di vista estetico e funzionale: l'elegante colore grigio antracite e la maniglia ergonomica ne sottolineano il design moderno, mentre il battente removibile rende più agevole la movimentazione, grazie ad una riduzione del peso complessivo di oltre il 20%, di grande aiuto per installazioni in posizioni difficilmente accessibili.

Ogni cassaforte Senator è dotata di un ripiano amovibile e di robusti catenacci rettangolari da 25 x 15 mm. Le casseforti della gamma Senator sono già pronte per l'uso al momento della consegna e possono essere fissate al pavimento con un kit di ancoraggio incluso nella fornitura.

Senator è disponibile in diversi modelli con capienze che vanno dai 32 a 190 litri, per soddisfare qualsiasi necessità di custodia. A partire dal modello da 46 litri è disponibile una doppia serratura opzionale: la serratura principale può essere integrata da una combinazione a 3 dischi (Classe B EN 1300) o da una serratura elettronica (Classe B EN 1300).

Senator, come tutti i mezzi forti **Chubbsafes**, è prodotta e distribuita da **Gunnebo**, leader nel fornire soluzioni su misura per la protezione valori e per ogni altra esigenza di sicurezza.

Per ulteriori informazioni sulle casseforti **Chubbsafes** e su tutte le soluzioni di sicurezza offerte da **Gunnebo**, potete contattare l'azienda telefonicamente allo 02267101, scrivere all'indirizzo info.it@gunnebo.com o visitare il sito www.cassefortilipsvago.it

GUNNEBO®
For a safer world

CONTATTI: GUNNEBO ITALIA SPA
Tel. +39 02 267101
www.gunnebo.it

Applicazioni per Centri Commerciali

COMUNICAZIONI AUDIO **OVER IP**

ermes
freedom to communicate

P2P Peer To Peer | PoE Power over Ethernet | VoIP Voice over IP | No Server

www.ermes-cctv.com ermes@ermes-cctv.com Tel. +39 0438 308470 Via Treviso, 36 - 31020 San Vendemiano (TV) - Italy

La Digital Transformation e il modello ERP per sicurezza fisica aziendale

di Nils Fredrik Fazzini, CEO di CITEL spa

Nell'onda lunga della *digital transformation*, Citel ha segnato in un ventennio dei passaggi significativi nell'evoluzione della sicurezza fisica: dall'uso condiviso di reti dati aziendali degli anni '90, alla messa in discussione dei protocolli proprietari e chiusi che vincolavano l'utente al fornitore, precludendo l'adozione delle piattaforme di correlazione aperte, alla gestione multimediale degli eventi, fino al **PSIM**; un paradigma di successo che è ora maturo per un consolidamento mettendolo al centro di un ***ERP della sicurezza fisica e della resilienza aziendale*** secondo un modello preannunciato all'inizio del 2018 da CITEL proprio da queste colonne.

La classificazione in categoria "ERP" di un PSIM e del suo Ecosistema di utenti e costruttori complementari potrà sembrare un salto di paradigma ambizioso agli occhi di chi sta ancora utilizzando soluzioni tradizionali di gestione della sicurezza, eventualmente ancora ferme alla pura gestione centralizzata degli allarmi in un contesto monofornitore.

Al contrario, l'ERP non è altro che una categoria nel settore informatico basata su un modello soprattutto pratico di interazione tra fornitori, utenti e terze parti, che ha influenzato positivamente il mondo dell'informatica gestionale contribuendo a smantellare i vincoli costrittivi che si istituivano in passato tra cliente e fornitore, quasi sempre a danno dell'utente. E che si sposa perfettamente con l'indirizzo in atto verso l'interoperabilità.

Pertanto, per Citel semplicemente non c'era ragione per non adottare il termine ERP quando esso è già da anni un dato di fatto nelle proprie politiche e nell'assetto del proprio mercato; con una storia di informatizzazione della sicurezza fisica secondo il paradigma di un PSIM al centro di un vero e proprio Ecosistema composto da utilizzatori, terze parti di servizio, produttori complementari.

I meccanismi generali degli Ecosistemi (composti da comunità di stakeholder che generano spinte sinergiche per l'evoluzione), che sono alla base di un ERP, hanno funzionato realmente nel percorso di Citel, non solo perché coerenti con la sua strategia basata sulle architetture aperte multifornitore e multi-applicazione, ma anche per il fatto che quelle spinte hanno avuto a disposizione quasi due decenni per produrre effetti positivi di selezione naturale per sistemi, prodotti e processi di gestione. E per trasferire all'utenza i benefici della competizione meritocratica nel settore.

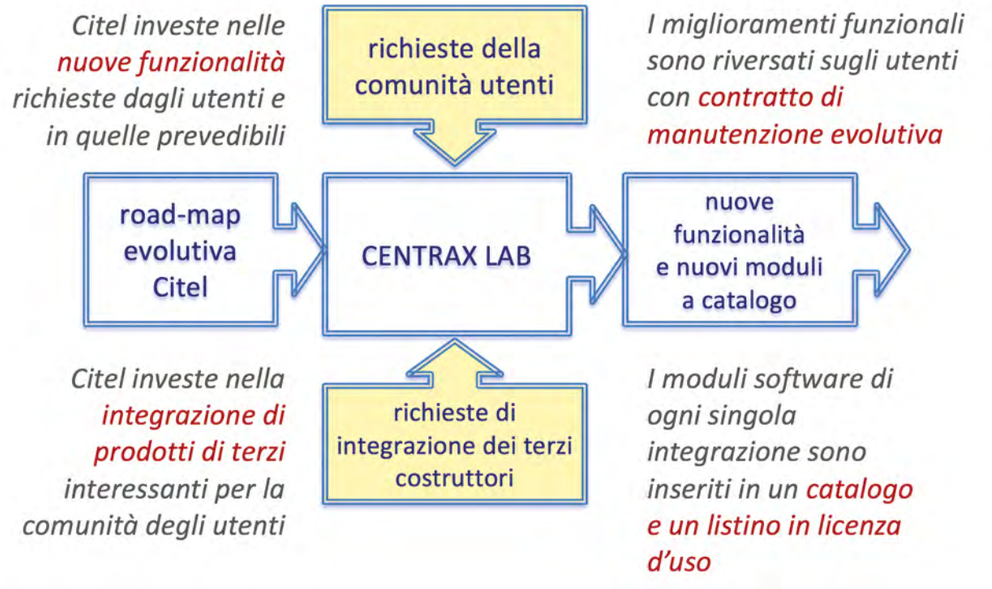
Come si materializza un ERP della sicurezza aziendale

Nel campo della gestione aziendale, un ERP canonico viene definito dalla letteratura informatica come:

- un insieme di software applicativi che, facendo riferimento ad una unica base dati, permettono di ottenere la migliore interazione possibile tra i processi di gestione dell'azienda, ovvero vendite, produzione, amministrazione; con il risultato di generare valore aggiunto per l'utilizzatore in termini di semplificazione, correttezza, tempestività, efficienza;
- l'apertura dei software suddetti all'integrazione di altri processi informatici complementari con modalità codificate a garanzia dell'integrità dei dati e della normalizzazione tecnico-applicativa;
- una serie di servizi informatici di consulenza, implementazione, sviluppo, personalizzazione, integrazione, installazione e manutenzione forniti da una comunità di terze parti, professionalmente qualificate e abilitate riguardo al software ed ai sistemi coinvolti, selezionate e referenziate nella comunità.

Le origini del paradigma "ERP" e le valenze generali

Forse è il caso di precisare che ERP è un modello collaborativo informatizzato concepito in Black & Decker negli USA negli anni '60 come MRP (Material Resource Planning), successivamente esteso all'intera attività dell'Impresa e quindi ribattezzato ERP



(Enterprise Resource Planning), sempre negli USA nel 1990.

Si tratta di una storia che porta a precisare che il paradigma ERP:

- è slegato da un qualsiasi specifico produttore di software;
- ha un carattere polivalente nell'ambito dell'informatizzazione dei processi aziendali;
- quindi, può essere utilmente impiegato anche nelle applicazioni dipartimentali della sicurezza fisica informatizzata, quelle che in realtà producono livelli più elevati di sicurezza aziendale, safety, resilienza aziendale in genere.

Per una maggiore chiarezza dei paradigmi della sicurezza

In quanto produttore di sistemi aperti, Citel ha valutato che l'adozione del modello ERP favorisce indubbiamente l'organizzazione e la valorizzazione delle interazioni collaborative tra ruoli e specializzazioni di più stakeholder, che siano produttori complementari, o fornitori di servizi.

Lo stesso vale per l'utente che, aiutato dalla collocazione dei diversi soggetti nel modello ERP, ha la possibilità di percepire più facilmente e utilmente i ruoli e le relazioni tra il fornitore principale, quelli secondari, le terze parti coinvolte, indicate dal fornitore oppure preferibili per il committente se scelte liberamente.

In definitiva, al di là delle sinergie più strette che possono nascere dall'appartenenza ad un ERP, la consapevolezza agli occhi dell'utente delle relazioni tra le varie parti del quadro complessivo ha – secondo Citel - una valenza positiva di per sé.

Il modello che Citel ha codificato in proposito consiste in un ERP basato:

- sul Centrax open-PSIM leader dello specifico mercato;
- sulla valorizzazione organica di una massa di user experience, unica nel mercato per varietà settoriale e dimensionale;
- sullo sviluppo continuativo di moduli di integrazione di apparati di terzi per espandere la libertà di scelta dell'utente di apparati di campo e sistemi gestionali di mercato e/o prodotti da terzi;
- su una software factory interna che ha dato prova in circa 20 anni di saper passare – senza creare criticità per gli utilizzatori – per tutti i salti evolutivi delle piattaforme e dello sviluppo di software base ed applicativo in una logica di life-long project, indispensabile per un sistema informatico, sia aziendale che settoriale.

I fatti del ERP di Citel

In quanto collegato ad una grande comunità che si è costituita negli anni, composta da stakeholders collaborativi, anche perché coinvolti in un lifelong project:

- **l'Ecosistema** delle comunità degli *stakeholder* dinamici;
- la valorizzazione della ***user-experience***;
- la centralità della **Software Factory** specializzata e dedicata ai processi operativi ed alle soluzioni per l'interoperabilità.

L'ERP di Citel si basa solo su entità che vengono classificate di seguito secondo il loro ruolo naturale, ai fini di come possono contribuire e di ciò che possono ricevere. Secondo un processo che vede Citel nel ruolo di investitore in nuovi processi gestionali ed integrazioni da catalogo, con un ritorno che può essere adeguato solo in presenza di una molteplicità di soggetti nella comunità degli utenti.
Una politica che si è rivelata utile – se non indispensabile – per quegli utenti che percepiscono consapevolmente il fatto che il PSIM è un *lifelong project*, ovvero un progetto destinato ad essere continuamente soggetto ad evoluzione intervenendo I meno possibile sull'esistente.

A - L'Ecosistema del PSIM è composto da **tre comunità di fatto:**

1. una ***comunità di oltre 100 utenti***, *composita per dimensioni e settore di attività*, caratterizzata da una dinamica di spinte evolutive per l'allargamento dell'orizzonte applicativo, per la profondità dei processi gestionali dipartimentali nella sicurezza fisica e le sue implicazioni nella resilienza aziendale;
2. una ***comunità di produttori di oltre 140 sistemi***, *sotto sistemi, moduli applicativi, apparati specializzati*, predisposti all'interoperabilità ed alla correlazione con il PSIM accomunati da una base dati unificata, ovvero accessi, incendio, gestione portinerie, allarmi e segnalazioni tecniche, gestione ronde, ecc.;
3. una ***comunità di circa 150 terze parti di servizio*** in rapporti diretti con l'utente per attività di progettazione, sviluppo commerciale, manutenzione, ecc.; anche nel ruolo di main-contractor. Che si rapportano organicamene a vario titolo con Citel in quanto coinvolti presso gli utenti come installazione, manutenzione, sviluppi, progettazione. E che diventano oltre 400 considerando anche le terze parti che si rapportano con Citel non organicamente.

In realtà sono circa 400 le imprese che hanno a che fare in un modo o nell'altro con il PSIM al centro del ERP. Sono soggetti che hanno ben chiaro – avendolo vissuto per esperienza – che il contesto ERP è un mercato più meritocratico, veloce e reattivo di quello dei sistemi diversamente inquadrati.

B - **La Software Factory** di Citel con le sue articolazioni specialistiche, organizzata internamente e per partnership è una missione basata:

- sulla valorizzazione della *user experience* di qualità e della sua metabolizzazione finalizzata al continuo affinamento di piattaforme e processi gestionali efficienti e sostenibili;
- sulla gestione dei processi della sicurezza fisica in quanto inseriti in un ***progetto permanente***, secondo i canoni del *life-long project*;
- su un catalogo completo di applicazioni complementari e strettamente integrante, anche di terzi, compresi quelli che riguardano il software gestionale e di chi lo produce e lo supporta; e la conseguente necessità di affidarsi (esattamente come si usa nell'informatica gestionale) ad una reale *software factory* con una specializzazione effettivamente maturata nel tempo e una storia di progetti di successo e di customer satisfaction; strutturata con uno staff interno stabilizzato ed una organizzazione preparata a supportare il cliente in un'ottica di lungo periodo.

CITEL

CONTATTI: CITEL SPA
info@citel.it
www.citel.it

Le comunicazione audio in IP nelle carceri

a cura di Filippo Gambino, CEO di ERMES Elettronica srl

Introduzione

Non vi è alcun dubbio che l'utilizzo di efficienti sistemi di comunicazione all'interno delle carceri e di altri luoghi di detenzione come le caserme dei carabinieri o di altri organi di polizia costituisca un importantissimo ausilio per la gestione di tali strutture.

L'utilizzo di affidabili sistemi di comunicazione contribuisce ad elevare in modo significativo la sicurezza di tali strutture sia i termini di security sia in termini di safety; è evidente, infatti, come il disporre di un affidabile sistema di comunicazione tra il personale di sorveglianza o tra questo e i detenuti all'interno delle celle contribuisca a ridurre in maniera considerevole le conseguenze di episodi critici che, se gestiti tempestivamente e nella maniera più adeguata, possono risolversi il più delle volte in maniera priva di conseguenze.

Diversi studi, ad esempio, hanno dimostrato come l'installazione di un sistema di citofoni all'interno delle celle contribuisca a ridurre in maniera considerevole le conseguenze più pericolose dei tentativi di suicidio grazie al tempestivo intervento del personale di sorveglianza allertato con immediatezza dai compagni di cella.

Il sistema di comunicazione con le celle

Una struttura carceraria solitamente richiede l'installazione di sistemi di interfonia e di diffusione sonora nelle singole celle, nei locali comuni e in corrispondenza dei varchi critici; tutti questi apparati fanno capo sia al posto di guardia locale, sia alla sala controllo che gestisce la sicurezza dell'intero edificio.

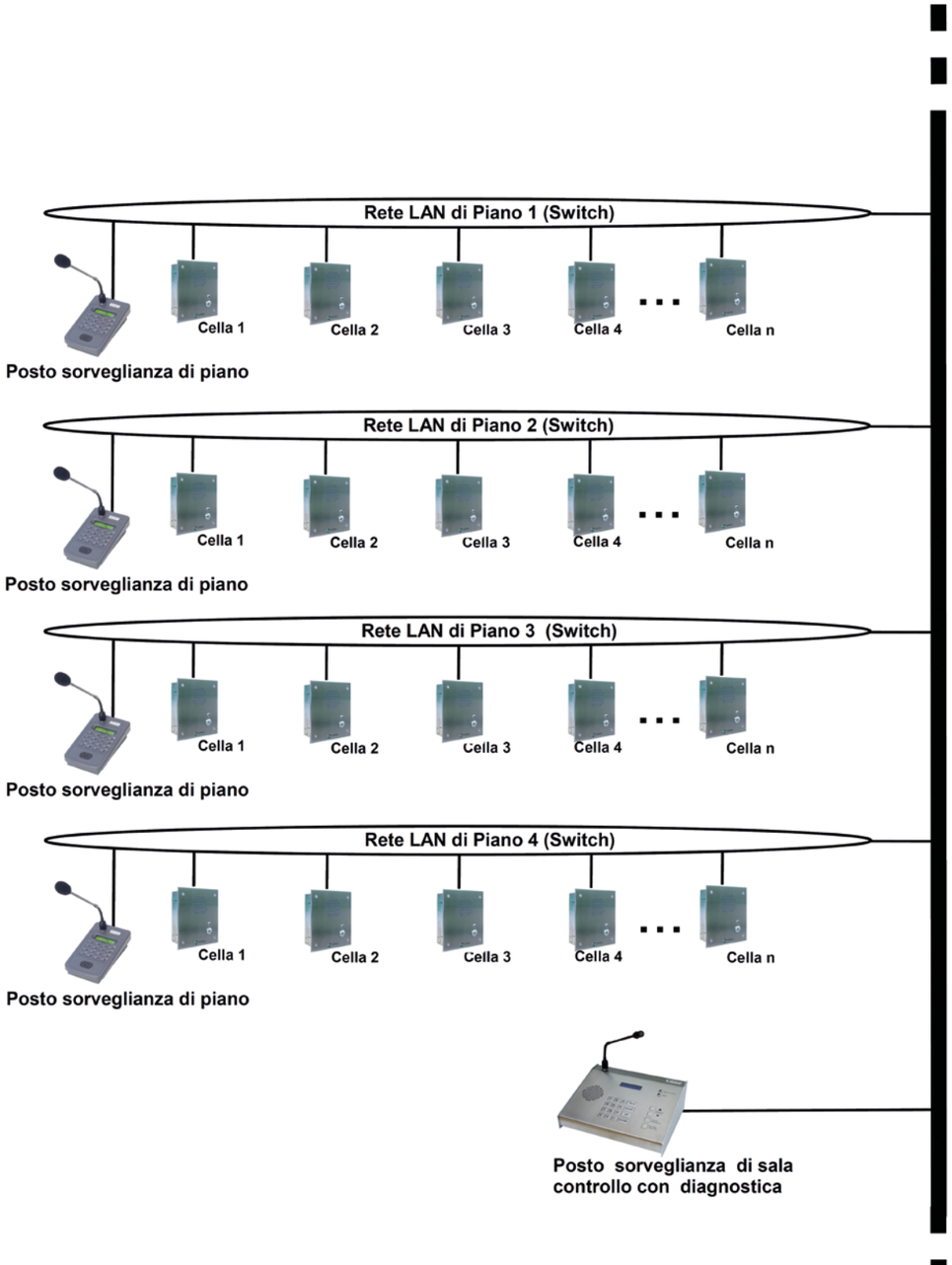
In queste note focalizzeremo l'attenzione sui sistemi di citofonia per la comunicazione tra l'interno delle celle e le postazioni del personale di sorveglianza, tralasciando gli altri sistemi come la diffusione sonora degli annunci o l'interfonia associata al controllo degli accessi o dei varchi in genere.

La soluzione Over IP è certamente quella più adatta per la realizzazione di questi impianti in quanto riduce significativamente i tempi ed i costi di installazione grazie alla possibilità di condividere la rete ETHERNET con altri sistemi come, ad esempio, la videosorveglianza.

Lo schema a blocchi mostra un simile impianto dove le comunicazioni attivate dall'interfono di ciascuna cella fanno capo al posto di guardia che sovraintende alla sicurezza dello specifico settore ed, eventualmente, possono essere deviate verso la sala di supervisione e controllo.

Il sistema consente anche la diffusione di annunci effettuati sia dal posto di guardia sia dal posto centrale di controllo verso il singolo interfono, verso un gruppo di interfoni (annuncio di gruppo) o verso la totalità degli interfoni (annuncio generale). In questo caso gli interfoni assumono la funzione di cassa acustica amplificata.

Gli apparati sono alimentati in modalità Power Over Ethernet (PoE) e utilizzano un protocollo di comunicazione Peer-To-Peer basato su apparati stand alone che consente l'eliminazione del server o di altre unità di gestione centralizzate.



Sistema Chiamata per celle nelle carceri

Gli interfoni per le celle

Nelle celle e nei locali comuni è previsto l'utilizzo di interfoni da incasso ad un pulsante con pannello frontale in acciaio inox, esecuzione anti-vandalo e grado di protezione IP65; sul pannello frontale trovano inoltre posto un led di segnalazione, un microfono ed un altoparlante.
La scatola da incasso è realizzata in lamiera di acciaio di spessore 15/10 con alette antistrappo che, cementate nella parete, ne contrastano la rimozione forzata. Il pannello frontale è realizzato in acciaio inox con spessore di 30/10 ed è fissato alla scatola da incasso con viti anti-manomissione con testa sigillata.

Questo interfono consente di:
• effettuare una chiamata verso il posto di guardia di competenza;
• deviare automaticamente a cascata la chiamata verso un massimo di altre 4 postazioni, compreso il posto di controllo centrale, qualora la chiamata non sia presa in carico entro un tempo prefissato;
• ricevere automaticamente le chiamate provenienti da un posto di guardia o dal posto di controllo centrale senza la necessità di intervento da parte del detenuto attivando la comunicazione in viva voce;
• diffondere gli annunci effettuati da un posto di guardia o dal posto di controllo centrale utilizzando l'apparato come altoparlante Over IP;
• consentire l'ascolto ambientale silenzioso.

Gli interfoni per il posto di guardia

Si tratta di una console in materiale plastico con altoparlante, microfono, tastiera numerica e display LCD che, secondo le esigenze, può essere dotata di microfono a collo d'oca o di cornetta telefonica e, se necessario, può essere fornita in versione interamente metallica.
La console del posto di guardia consente all'agente di gestire le comunicazioni con un numero illimitato di interfoni periferici che può chiamare, selezionando il corrispondente identificativo sulla tastiera, o da cui può ricevere la chiamata; in ogni caso sarà l'operatore del posto di guardia che potrà chiudere la conversazione con apposito comando.

Altre funzioni implementate dalle console sono:
• la possibilità di effettuare l'ascolto silenzioso dei suoni all'interno della cella;
• la gestione delle code di chiamata e delle chiamate perse;
• la possibilità di effettuare la diffusione di annunci sul singolo interfono di cella, su gruppi di interfoni o sull'intera rete di interfoni; inoltre è possibile inserire nel sistema dei gateway amplificati (amplificatori audio Over IP) con i relativi altoparlanti per implementare la diffusione sonora nelle aree comuni;
• la possibilità di effettuare chiamate tra le diverse console dei posti di guardia e tra queste ed il posto di controllo centrale implementando così un sistema di intercomunicante di servizio.

ermes
freedom to communicate

Il posto di controllo centrale

Il posto di controllo centrale può essere attrezzato con una console analoga a quella utilizzata per i posti di guardia, ma che rispetto a questa implementa anche una funzione di supervisione degli interfoni installati nelle celle segnalando immediatamente eventuali guasti sia degli apparati o del collegamento di rete.
In alternativa è possibile utilizzare una postazione computerizzata basata su un PC con relativo software sul cui schermo è visualizzata in forma schematica la mappa dell'intera installazione con la localizzazione dei singoli apparati ed i pulsanti di comando attivati dal mouse. In caso di strutture complesse il sistema è essere in grado di gestire più mappe organizzate in una struttura gerarchica.

Questo sistema, oltre a consentire le medesime funzioni della console stand alone, è in grado di:
• gestire l'abilitazione al servizio di più operatori che potranno abilitarsi e disabilitarsi con una password personale;
• tenere traccia su un LOG esportabile in formati standard degli eventi significativi legati alla gestione del sistema (abilitazione e disabilitazione al servizio dei diversi operatori, anomalie di connessione/guasti, chiamate ricevute);
• registrare le conversazioni tra gli operatori e le celle.

In definitiva questa soluzione, grazie alla sua flessibilità ed alla facile scalabilità, è la soluzione più adatta per la gestione delle comunicazioni all'interno delle strutture di detenzione.

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

Nuovi dissuasori Hörmann:
ora la sicurezza è più elevata

• Dispositivi di protezione contro veicoli con un peso fino a 7,5 t e una velocità di 80 km/h
• Ampia gamma di soluzioni: dissuasori automatici, semiautomatici, fissi o amovibili
• Funzione rapida per situazioni di emergenza che attiva i sistemi in soli 1,5 secondi

SECURITY
HIGH SECURITY
Partner KlimaHaus CasaClima
www.hormann.it
info@hormann.it

HÖRMANN
Porte • Portoni • Sistemi di chiusura

Hanwha Techwin presenta la telecamera multidirezionale con doppio obiettivo serie Wisenet P

a cura della Redazione

In seguito al successo riscosso lo scorso anno dalla PNM-9081VQ, una telecamera multidirezionale a quattro canali che consente una sorveglianza a 360°, **Hanwha Techwin** ha lanciato una nuova telecamera multidirezionale che ospita due obiettivi in un unico alloggiamento.

Il punto di forza della nuova telecamera è la capacità di monitorare simultaneamente due aree da diverse angolazioni, installando un unico corpo camera che racchiude due telecamere di videosorveglianza. Questo consente la massima copertura dello spazio monitorato, flessibilità ed ottima qualità dell'immagine.

Grazie ai suoi due obiettivi indipendenti, la telecamera **PNM-7000VD** è in grado di catturare immagini Full HD da 2MP di due aree contigue.

A seconda del campo visivo da monitorare è possibile scegliere tra quattro diversi obiettivi da 2,4 fino a 6mm per una copertura fino a 270°, rendendo la **PNM-7000VD** una soluzione ideale per il monitoraggio di ampi spazi aperti come parcheggi, centri commerciali e magazzini.

"È comprensibile che gli utenti finali cerchino di ottenere il massimo valore dal proprio sistema di videosorveglianza. La nuova telecamera multidirezionale con doppio obiettivo riduce sensibilmente i costi normalmente associati all'installazione di due telecamere diverse, ad esempio agli angoli di un edificio o di un sito, senza scendere a compromessi in quanto alla qualità dell'immagine" ha affermato **Bob (H.Y.) Hwang Ph.D.**, Managing Director di **Hanwha Techwin**.

"È un perfetto esempio della nostra filosofia 'We MOVE with trust', secondo la quale introduciamo soluzioni innovative che offrono vantaggi tangibili e apprezzabili nella vita di tutti i giorni."

Ricca di funzioni

La **PNM-7000VD** è dotata delle tecnologie all'avanguardia come il **Wide Dynamic Range** (WDR) da 150 dB, la correzione della distorsione ottica e la stabilizzazione digitale dell'immagine per offrire immagini ottimizzate in qualsiasi condizione ambientale.

Inoltre, ha integrate una lunga serie di funzioni utili tra cui il mascheramento privacy e numerose funzioni di video analisi come rilevamento direzione, face detection, defog, linea virtuale, comparsa/scomparsa, stazionamento e manomissione.

I due ingressi per schede di memoria **SD/SDHC/SDXC** permettono di archiviare video direttamente a bordo anche in caso di interruzione della connettività di rete garantendo la continuità del servizio.

WiseStream II

La **PNM-7000VD** supporta la compressione H.264 e MJPEG, ma l'efficienza di questi formati di codifica può essere migliorata fino al 99% combinando la compressione H.265 a **WiseStream II**, una tecnologia di compressione complementare che controlla dinamicamente la codifica dei dati, bilanciando qualità e livello di compressione in base alla quantità di movimento presente nella ripresa.

CONTATTI: HANWHA TECHWIN EUROPE LTD
Tel. +39 02 38608228
www.hanwha-security.eu

Integrare un rivelatore a tenda in un sistema di sicurezza e di videosorveglianza su rete IP: l'esperienza diretta di OPTEX

a cura della Redazione

Recentemente gli uffici di **OPTEX Europe** sono stati trasferiti in una nuova sede. Il trasloco ha fornito al team tecnico di OPTEX l'opportunità di progettare e installare un sistema antintrusione, TVCC e controllo accessi per proteggere il nuovo ufficio e il magazzino ad esso collegato.

I tecnici hanno progettato l'installazione di rivelatori per esterno a lunga portata e di sensori a scansione laser intorno all'edificio, identificando un'area piccola e stretta ubicata sul retro dello stabile che non sarebbe stata coperta dai sensori a lungo raggio. La soluzione più efficace per proteggere quest'area stretta si è rivelata il nuovo sensore a tenda per esterno **BX Shield.**

Per aggiungere **BX Shield** **(https://shop.hesa.com/it/oxbxsst.html)** al sistema di sicurezza su rete IP, il team ha collegato il sensore all'encoder **IP PIE-1** **(https://shop.hesa.com/it/oxzpie1.html)**. La scatola da incasso opzionale per i moduli BX-Shield cablati si è dimostrata delle dimensioni perfette per adattarsi al modulo PIE-1. Aggiungendo PIE-1 ai sensori BX Shield è stato possibile collegare il sensore con tutte le piattaforme VMS che hanno integrato il codice evento **OPTEX Redwall**.

Essere in grado di collegare i sensori esterni a media portata OPTEX, come BX Shield, al resto del sistema IP ha permesso al team OPTEX di creare una soluzione di sicurezza completa su misura per il layout specifico del sito.

Tutti i sensori esterni cablati OPTEX possono essere collegati all'encoder PIE-1.

Grazie all'encoder PIE-1 il segnale di uscite relè viene convertito in un codice ASCII e i rivelatori possono essere collegati a piattaforme VMS (Video Management Software) di gestione video per comandare telecamere IP.

PIE-1 genera il Codice Eventi usando gli ingressi di allarme analogici. Il software di gestione video riceve il codice evento e invia un comando di posizionamento al brandeggio preimpostato della telecamera e/o di avvio di registrazione con una telecamera.

PIE-1 può essere alimentato anche in Power-over-Ethernet (PoE) ed è conforme **IEEE802.3** mediante il collegamento, tramite un solo cavo LAN, con un concentratore o uno switch PoE.

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

Prime e la dinamica dell'Installatore Identificato Inim

a cura della Redazione

Prime, la nuova centrale antintrusione di **Inim** è nativamente connessa ad **Inim Cloud** e alle sue potenzialità. E' quindi la scelta migliore per tutte le installazioni che richiedono connettività IP e, in particolare, connettività Cloud.
La connettività IP a bordo della scheda principale garantisce grande rapidità di risposta nell'uso dell'**App AlienMobile** e nell'uso dell'interfaccia web di **Inim Cloud**. Tempi di risposta estremamente rapidi per un'esperienza d'uso davvero gratificante. Tramite l'App AlienMobile, tramite l'interfaccia web del Cloud o tramite il web-server disponibile sulla scheda **PrimeLAN**, l'utente ha tutto sotto controllo. Inserimenti e disinserimenti, accensioni e spegnimenti, gestione dell'illuminazione, gestione degli scenari domotici, gestione dei cronotermostati ambientali e notifiche in tempo reale di tutto quanto accade.
Tramite l'**App InimTech Security** l'installatore può gestire gli impianti installati e connessi al Cloud, ricevere notifiche, contattare i clienti ed avviare il navigatore direttamente dal suo smartphone. Tutto in punta di dita sullo schermo touch del dispositivo mobile o del PC.
La piattaforma Prime, grazie alla scheda **PrimeLAN**, è in grado di gestire i protocolli **KNX** e **ONVIF** che consentono al sistema Prime di interagire con i più diffusi sistemi domotici e con ogni sistema di videosorveglianza IP che sia ONVIF compatibile.
Prime è un sistema ibrido (cablato + via radio bidirezionale). La centrale nasce cablata ma la semplice aggiunta del ricetrasmettitore bidirezionale BS200 la trasforma in una potente centrale via radio ai massimi livelli di prestazione ed affidabilità. La comunicazione bidirezionale, la supervisione e la protezione delle informazioni trasmesse fa del sottosistema via radio di Prime un prezioso ausilio all'installatore professionista.
Grazie al software Prime/STUDIO, inoltre, è possibile effettuare la completa programmazione dell'impianto tramite connessione Cloud.

Perché nasce Prime?
INIM è da sempre convinta che la professionalità, la competenza e la preparazione di tutti gli attori della filiera della sicurezza (produttori, distributori, installatori) sia una necessità non derogabile per poter offrire all'utente il livello di sicurezza ed i servizi che si aspetta. INIM fa la sua parte, fornendo al mercato prodotti di alto profilo tecnologico, con i più alti standard di sicurezza ed affidabilità e certificati secondo le norme più stringenti del settore.
In questo contesto, ed al fine di proteggere la professionalità dei propri installatori, INIM propone la figura dell'**Installatore Identificato**. L'istituzione di questa figura si propone di rimuovere quei fenomeni che sviliscono la professionalità degli installatori oltre che svilire la professionalità e la qualità del prodotto INIM.
INIM, attraverso l'introduzione di questa figura, vuole quindi proteggere il ruolo dell'installatore. Vuole proteggere la professionalità e la competenza dell'installatore da fenomeni di concorrenza scorretta come, ad esempio, il fenomeno delle vendite on-line di apparecchiature di sicurezza o da altri fenomeni anche più gravi, come quello delle installazioni effettuate da chi non ha alcun titolo per effettuarle e, quindi, opera non solo contro le corrette politiche commerciali, ma addirittura contro la legge.
Tali canali di vendita non garantiscono un'adeguata e controllata conoscenza dei prodotti, delle norme di prodotto, delle norme di installazione e manutenzione.
Non garantiscono un adeguato supporto nelle fasi pre-vendita (formazione, progettazione) così come nelle fasi di post-vendita (programmazione, assistenza tecnica, manutenzione, riparazione). Inoltre, i canali di vendita non autorizzati operano una concorrenza sostanzialmente scorretta quando si limitano alla mera vendita senza fornire i servizi necessari a corredo delle apparecchiature di sicurezza.
Dalla formazione alla progettazione, dall'assistenza alla programmazione: questi servizi sono sempre disponibili presso i distributori autorizzati INIM che, per tali servizi, investono risorse a volte ingenti. L'istituzione della figura dell'installatore identificato è quindi volta, da un lato, a proteggere il lavoro e la professionalità dell'installatore e, dall'altro, a identificare in maniera chiara i distributori autorizzati INIM dove poter trovare tutti i servizi di cui un installatore ha bisogno e dove trovare un'adeguata conoscenza del territorio nel quale l'installatore opera e delle sue necessità.
L'**Installatore Identificato** è un sistema "premiante", cioè un sistema che offre all'installatore dei vantaggi e servizi aggiuntivi se sono soddisfatte talune condizioni.
Condizioni, da sottolineare, che non sono volte a limitare ma, piuttosto, sono volte a proteggere l'installatore stesso e la sua professionalità.
Una di queste condizioni è la selezione e l'affidamento per l'acquisto ad un distributore INIM autorizzato nella propria zona, ossia nella provincia in cui ha sede la società dell'installatore. I distributori disponibili nella propria area saranno mostrati durante la procedura di attivazione del profilo Installatore Identificato.
Un'altra condizione è quella di utilizzare le centrali acquistate dal distributore selezionato per realizzare installazioni e non per effettuare rivendita. INIM vuole premiare gli installatori e la loro professionalità. I prodotti coinvolti nel programma "Installatore Identificato" sono le centrali antintrusione INIM Prime.
L'installatore deve avere già attivo un account INIM-Cloud. In caso contrario dovrà attivare un account INIM-Cloud e già la semplice richiesta di attivazione del profilo Installatore Identificato, una volta portata a termine con successo, permette di ottenere 1GB di spazio nel cloud INIM per il salvataggio delle soluzioni.
Se il prodotto è stato acquistato dal distributore selezionato, sarà possibile utilizzare il software di programmazione Prime/STUDIO con un menù di programmazione testuale e l'installatore avrà la disponibilità dell'assistenza tecnica remota INIM per la centrale, oltre che l'estensione della garanzia per la centrale a 5 anni.
All'installatore sarà erogato inoltre un "Welcome kit" una volta che si sia utilizzato il software Prime/STUDIO per programmare le centrali Prime su 20 diverse centrali.

Diventa Installatore Identificato Inim!

Ecco il riepilogo dei vantaggi:
- Garanzia estesa: la garanzia sulle centrali Prime per gli Installatori Identificati è di 5 anni;
- Più spazio di storage: per gli installatori identificati raddoppia lo spazio di storage per il backup in Inim Cloud fino a 1GB;
- Software di programmazione: l'Installatore Identificato ha il libero utilizzo del software di programmazione per le centrali Prime;
- Assistenza tecnica esclusiva: solo l'Installatore Identificato può usufruire dell'assistenza tecnica per le centrali Prime;
- Welcome kit: abbigliamento Inim composto da polo, felpa e gilet da lavoro;
- Corsi gratuiti: possibilità di accesso a corsi gratuiti organizzati da Inim in via esclusiva per gli Installatori Identificati. I corsi potranno dare anche accesso a certificazioni Inim e certificazioni IMQ;
- Offerte dedicate esclusive, omaggi, eventi, materiali promozionali e tanto altro;
- Controllo sulla filiera distributiva: l'Installatore Identificato sarà maggiormente protetto dal fenomeno delle vendite online che danneggia i professionisti della sicurezza. Non sarà più confrontato nelle sue offerte con le offerte presenti online;
- Legame con un **distributore ufficiale Inim**: un valore aggiunto al prodotto. Formazione, promozione, assistenza, magazzino, presenza sul territorio, sono i vantaggi del contatto diretto tra installatore e distributore ufficiale.

CONTATTI: INIM ELECTRONICS SRL
Tel. +39 0735 705007
www.inim.biz

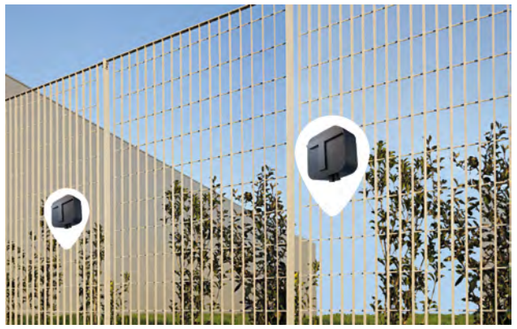
MACS: quando il sensore fa la differenza, anche nelle recinzioni. Ecco la Linea MACS di Nuova Defim Orsogrill

a colloquio con Tiziano Gatti, coordinatore commerciale Italia|Estero Nuova Defim spa
a cura della Redazione

Quali sono le applicazioni più avanzate di sensoristica attiva alle recinzioni di protezione che avete in produzione?
L'idea è nata nel momento in cui abbiamo iniziato a pensare che le recinzioni, per quanto robuste e anche gradevoli esteticamente, potessero avere una funzione superiore a quella semplicemente delimitativa o dissuasiva. O, meglio, potevano farlo in "versione 4.0", sfruttando i vantaggi che la tecnologia metteva a disposizione. Qui è entrata in gioco la sensoristica più avanzata e lo ha fatto mettendo in campo tutte le potenzialità di cui dispone, definendo un nuovo standard di massima sicurezza perimetrale capace di superare i limiti che in passato le vecchie recinzioni allarmate imponevano. Tra questi, giusto per ricordane alcuni, costi elevati, facilità di manomissione e scarsa efficacia in caso di effrazione. Senza parlare dei falsi allarmi, un punto debole che le rendeva poco attrattive, soprattutto per chi ha l'obiettivo di proteggere perimetri estesi o aree di particolare importanza. Grazie alla stretta collaborazione esclusiva con un partner tecnologico avanzato come T-Sec, che ha messo a disposizione di Nuova Defim Orsogril conoscenze e tecnologie "su misura" per le nostre recinzioni, abbiamo dato vita al sistema MACS. Con il sistema MACS (MEMS-based anticlimbing system) si rilevano in maniera puntuale i tentativi di effrazione e scavalcamento, discriminando con grande precisione eventi naturali o accidentali. Grazie alla facilità di installazione e alla possibilità di monitoraggio da remoto, è un importante passo avanti verso la ricerca di soluzioni efficaci per la sicurezza perimetrale.
MACS è una tecnologia unica e innovativa che reinterpreta gli acceleratori MEMS già presenti negli smartphone in chiave di sicurezza. Dalla collaborazione tra i leader nelle recinzioni

e nella sensoristica elettronica sono stati sviluppati speciali algoritmi elaborati ad hoc per i modelli della linea Recintha e per le recinzioni in grigliato a marchio Orsogril.
Il sistema si compone di una catena di sensori ed un master. La catena è precablata e composta da 120 sensori. L'installazione avviene lungo la recinzione fino a coprire un perimetro massimo di 1,2 chilometri per singolo master.

Quali sono i vantaggi che rendono MACS unico nel panorama delle recinzioni allarmate?
Prima di tutto è un sistema inflessibile e affidabile perché il sofisticato algoritmo rileva ogni tentativo di scavalcamento. Non è influenzabile da eventi climatici (pioggia, vento), dalla presenza di vegetazione o da azioni umane diverse dallo scavalcamento. È anche estremamente intelligente e preciso. Infatti, la tecnologia applicata consente di identificare in modo univoco ciascun sensore, fornendo una precisa indicazione del punto in allarme. Il sistema riconosce inoltre i tentativi di manomissione, segnalando anche azioni di taglio o rimozione del pannello di recinzione.



Il Sistema MACS è veloce e adattabile, due caratteristiche che lo rendono adatto all'integrazione con sistemi di allarme già presenti. La facilità di installazione e di programmazione del sistema lo rendono perfettamente adattabile a ogni progetto di qualsiasi dimensione e complessità. La tecnologia MACS è progettata per integrarsi a qualunque sistema di allarme con la massima compatibilità.
Poiché compatibilità implica una capacità di aggiornarsi nel tempo, Nuova Defim Orsogril è impegnata a migliorare costantemente il sistema MACS. Gli sviluppi futuri saranno garantiti da aggiornamenti firmware di sensori e master.
In ogni caso, MACS è sempre programmabile e proattivo. Il sistema, grazie a una tecnologia di autoapprendimento, si auto-adatta alla recinzione su cui è installato. Inoltre, con la possibilità di impostare parametri di sistema, di zona e addirittura di singolo sensore, raggiunge la massima efficacia con minimi costi di installazione.

Quindi si adatta a diverse recinzioni di Nuova Defim Orsogril? In che modo?
MACS si declina nelle nostre recinzioni secondo due modalità: sia totalmente integrato, sia esternamente, a seconda dei modelli. Per esempio, il sistema è predisposto per essere associato alla recinzione Recintha N/L che è da sempre sinonimo di soluzione elegante, flessibile e colorata. Oggi, grazie all'elettronica, diventa ancora più sicura. Con Recintha N/L MACS la recinzione intelligente amplia il suo utilizzo, dal grande sito industriale alla dimensione familiare. Inoltre c'è la recinzione Sterope MACS, realizzate in grigliato. Inventate da Orsogril per l'ambito industriale, hanno trovato applicazione anche in ambito commerciale e residenziale.

Cosa proponete agli integratori che devono realizzare sistemi di sicurezza di siti dove si trovano server o archivi informatici, in termini di compliance al GDPR?
Per chi ha l'obiettivo di proteggere aree così sensibili che richiedono una massima sicurezza sia fisica sia elettronica, le soluzioni ideali sono Recintha Safety MACS ed Elettra MACS, dove la sicurezza raggiunge i massimi livelli. Recintha Safety è l'emblema stesso della sicurezza. La maglia antiscavalcamento e antitaglio, il sistema di fissaggio antistrappo e le elevate caratteristiche di solidità e robustezza ne fanno già una barriera invalicabile. Ora, con la forza dell'elettronica unita all'acciaio, si offre un sistema con sensori e cavi invisibili e inaccessibili. Il sistema è pre-tarato su Recintha Safety con modalità di auto-apprendimento. Individua esattamente il punto esatto di intrusione o manomissione ed elimina i falsi allarmi. Chi deve proteggere grandi aree, comprese le tecnologie e i dati che custodiscono, potrà farlo usando un solo master per 1,2 chilometri. Offriamo inoltre la possibilità di collegamento da remoto direttamente su master per programmare e monitorare gli eventi. E per facilitare l'installazione c'è un software dedicato.

In generale, quali sono i programmi del Gruppo per il prossimo futuro?
Siamo convinti che il settore delle recinzioni sia tutt'altro che maturo. Il connubio virtuoso tra la forza dell'acciaio, che ci deriva anche dall'appartenenza ad uno dei principali player siderurgici europei come il Gruppo Feralpi, e l'intelligenza elettronica riserveranno nuovi sviluppi in futuro. Noi ci crediamo. Siamo i primi e gli unici ad offrire un sistema così evoluto come MACS, ma non vogliamo fermarci qui.

CONTATTI: NUOVA DEFIM S.P.A.
Tel. +39 031 33521
www.nuovadefim.com

lares 4.0: la soluzione IoT più innovativa per Sicurezza Fisica e Home & Building Automation

a cura della Redazione

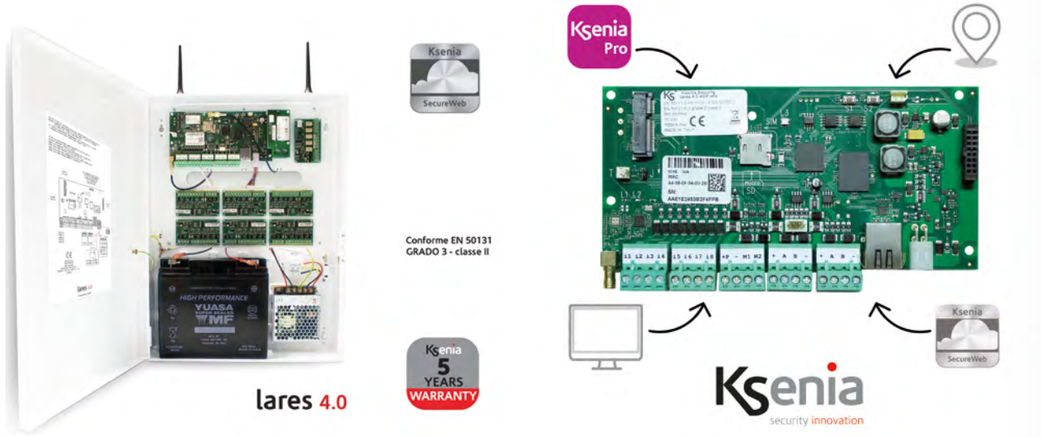
---

lares 4.0 è il nome evocativo della nuova piattaforma IoT ibrida di **Ksenia Security**.
Tutte le nuove centrali **lares 4.0** sono la soluzione perfetta e più avanzata nell'era della digitalizzazione (IoT) per quanto riguarda sia la Sicurezza Fisica (Antintrusione, Videosorveglianza, Controllo accessi) che la Home & Building Automation e rappresentano una importante innovazione tecnologica per la possibilità di programmazione e gestione del sistema mediante **Ksenia SecureWeb**, in aggiunta alle consuete modalità standard via PC.

Nell'era digitale, Ksenia SecureWeb è un servizio **Cloud SICURO** che si appoggia ad AWS permettendo quindi di sviluppare applicazioni complesse caratterizzate da maggiore flessibilità, scalabilità e affidabilità.

Le centrali lares 4.0 sono tutte ibride (sistema filare e wireless) e dispongono 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.

Assieme alla Sicurezza nelle sue accezioni di cui sopra, anche la SMART HOME possono essere ora gestite da un'unica APP utente (lares 4.0) e programmate dall'Installatore ora anche da qualsiasi terminale mobile **(Ksenia Pro)**. Indipendentemente dal taglio della centrale scelto, la scheda madre nasce con già a bordo la porta Ethernet, 8 morsetti di ingresso e 2 morsetti che possono essere configurati come ingresso o uscita.



La centrale è disponibile in 2 versioni diverse: per i tagli più piccoli la centrale dispone di un solo BUS (compatibile a parte alcune eccezioni con tutte le periferiche BUS esistenti che possono essere aggiornate dalla centrale), mentre per tutti gli altri integra già il doppio BUS e il transceiver wireless bidirezionale 868MHz (compatibile con tutte le periferiche wireless esistenti Ksenia).

Particolare attenzione viene sempre posta alla facilità di installazione e per questo tutti i terminali di connessione sono estraibili. Su tutte le versioni ed indipendentemente dal taglio di centrale, le schede dispongono di uno slot per SD card per espandere la memoria disponibile, oltre ad 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, sms, notifiche push, Contact ID e protocollo SIA DC-09 livello III alle Centrali di Sorveglianza.

lares 4.0 è disponibile e perfettamente scalabile nelle taglie 16, 40, 140 e 644 o addirittura customizzabile per esigenze di zone e/o di uscite ancora superiori. La scheda della centrale può essere installata dentro ai contenitori metallici esistenti utilizzati per 'lares-IP'. Inoltre è disponibile un nuovo contenitore metallico per installazioni medio-grandi: di dimensioni 435x325x90mm; esso consente di allocare oltre che la scheda madre della centrale con i relativi moduli add-on, fino a 7 moduli di espansione, la batteria di back-up da 18Ah e dispone di un alimentatore switching da 50W.

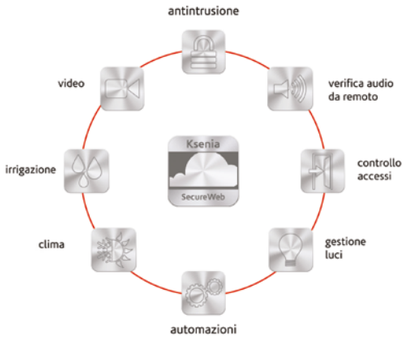
La piattaforma lares 4.0 è dotata di una serie di nuove periferiche sia per Sicurezza Fisica sia anche per quella che oggi viene definita in senso lato Domotica o SMART HOME - SMART BUILDING (cioè gestione di automazioni, luci, temperature, elettrodomestici, irrigazione, eccetera).

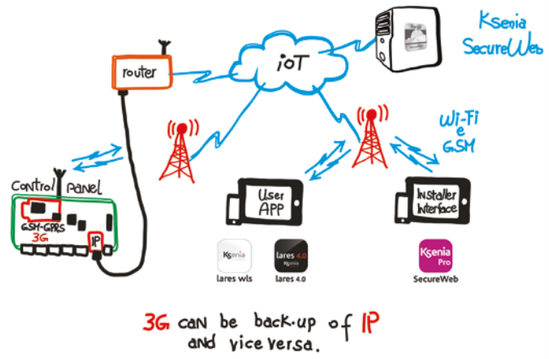
ergo-T come 'TOUCHSCREEN' è la tastiera capacitiva multi-touch di ultima generazione con un contrasto ed una risoluzione estremamente elevate. Ideale interfaccia di comando e controllo della nuova centrale lares 4.0, l'ultima nata dalla serie delle tastiere 'ergo', a differenza di tutti i numerosi tablets presenti sul mercato, è stata progettata quale MULTIMEDIA CENTER da cui gestire e programmare tutte le numerose funzioni.

auxi-H è un modulo utilizzabile non solo in ambito sicurezza, ma anche per l'automazione domestica. Tramite un apposito ponticello a bordo scheda è possibile impostare due modalità di funzionamento:
1. auxi-HT: per la completa gestione di finestre munite di avvolgibili motorizzati.
2. auxi-HL: per la gestione delle luci.

Nel primo caso (auxi-HT) le 2 uscite relé (8A-250V) diventano interbloccate per il controllo diretto del motore avvolgibile. Dagli scenari configurati su lares 4.0, non solo è possibile aprire o chiudere completamente gli avvolgibili, ma anche posizionarle in 4 diverse posizioni di apertura (apertura a 2/3, apertura a metà, apertura ad 1/3, solo passaggio aria). Con i pulsanti locali è possibile gestire la classica movimentazione ad uomo presente, ma anche gestire la completa apertura e chiusura con un semplice doppio-clic. Nel secondo caso (auxi-HL), le due uscite relé possono invece essere comandate liberamente dagli scenari di lares 4.0, oltre che gestite localmente con i pulsanti collegati agli ingressi locali. In entrambe le modalità di funzionamento, dispone infatti di 2 ingressi liberamente configurabili, e di un ingresso di allarme dedicato al collegamento di sensori di tipo tapparella.

auxi-L è una scheda di espansione con 5 uscite relé da 250V-8A (10A di picco), con uno scambio in comune, ideale per la gestione delle luci e per la disconnessone dei carichi.





domus è un modulo da incasso che , sfruttando l'apertura Keystone (di dimensione identica su qualsiasi serie di placche di interruttori), permette, per ogni locale, di avere in un solo dispositivo un sensore di movimento, un sensore di temperatura, di umidità relativa e di intensità luminosa. Ideale in ambito domotico permette, in combinazione con il modulo **auxi-L**, di accendere e spegnere le luci in funzione della luminosità interna, ogni volta che qualcuno si trova nel locale. Dispone, inoltre, di un sensore di temperatura ed umidità, prodotto dalla Sensirion (leader mondiale nella produzione di questi dispositivi) in grado di pilotare e gestire al meglio il proprio impianto di condizionamento e deumidificazione, per ottenere il reale grado di comfort desiderato.

Esso diventa indispensabile per ambienti d'ufficio e per la corretta umidificazione necessaria nei musei per la migliore conservazione delle opere d'arte. **domus** è il dispositivo ideale per il controllo della temperatura in ambito residenziale e non solo: esso può essere comodamente installato in ogni ambiente. Mediante il cronotermostato disponibile sulla centrale lares 4.0 è possibile regolare quindi la temperatura comodamente ovunque, adattando il livello di comfort all'uso dell'ambiente con anche importanti risparmi energetici. Grazie alla flessibilità della centrale lares 4.0 esso può comandare sia dispositivi di riscaldamento che di condizionamento.

Ksenia security innovation

CONTATTI: KSENIA SECURITY
Tel. +39 0735 751646
www.kseniasecurity.com

securindex.com
IL PORTALE ITALIANO DELLA SICUREZZA

MIX COMUNICAZIONE - MI

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

CST- Coded Sensor Technology la piattaforma di TSec contro l'insider attack

a cura della Redazione

La progettazione dei sistemi anti-intrusione o, più correttamente, di allarme antifurto, prevede sempre una definizione di rischio basata sulla divisione dello spazio in zone d'azione. Ad alto livello, tali zone sono l'area da proteggere (zona interna), e la zona ad essa complementare, ovvero quella esterna, con un perimetro a fungere da confine tra le due.

Nei casi più semplici, ad esempio negli impianti residenziali medio/piccoli, questo tipo di architettura è già sufficiente per definire la struttura dell'impianto, con dispositivi funzionali alla protezione perimetrale (barriere, contatti magnetici, sensori inerziali, ecc.), spesso coadiuvati, almeno negli impianti più importanti, da dispositivi complementari che proteggono la zona interna (sensori volumetrici, ecc.).

L'architettura degli impianti più complessi, come quelli dedicati alla protezione dei centri commerciali, delle residenze prestigiose o degli edifici bancari, è certamente più articolata, e spesso prevede ulteriori suddivisioni degli spazi in sottoinsiemi omogenei per funzione, livello di accesso e rischio. Rimane comunque valida, anche in questi impianti complessi, la nozione di divisione dello spazio in due macro zone: quella interna al perimetro protetto e quella esterna. Mentre negli impianti residenziali piccoli il rischio di intrusione avviene esclusivamente dall'esterno del perimetro protetto, nel caso di impianti più complessi il rischio principale può arrivare dall'interno del perimetro protetto: il vettore primario del rischio diviene l'**insider attack**.

L'insider attack rappresenta uno dei fattori di rischio più significativi per i sistemi di sicurezza moderni. Molto spesso, infatti, gli attacchi avvengono dall'interno del perimetro, sia da parte del personale che dei visitatori, soprattutto quando i sistemi di sicurezza devono supervisionare varchi temporizzati (bussole, uffici cassa, ecc.) o uscite di sicurezza. Un insider attack porta l'attaccante ad aver accesso alle parti vitali del sistema di sicurezza, facendo quindi in modo che le sue azioni possano avere una efficacia molto superiore al caso dell'outsider attack. E' per questo che anche i dispositivi di protezione utilizzati devono essere progettati appositamente per la difesa da questo tipo di attacco.

I contatti magnetici sono uno dei dispositivi più usati negli impianti d'allarme da oltre quarant'anni. Lo switch Reed è stato il cuore tecnologico incontrastato di questo tipo di dispositivi fino a pochissimo tempo fa.

Il livello di sicurezza ottenibile da un dispositivo basato su singolo Reed è tuttavia molto basso: il singolo switch Reed ha infatti una capacità pressoché nulla di discernere tra il campo magnetico generato dal proprio magnete di riferimento e un magnete esterno usato da un attaccante per mascherare l'assenza del magnete di riferimento. In questo modo risulta molto semplice ingannare il sensore con un magnete esterno, e aprire il varco senza che il contatto lo segnali alla centrale.

Con la piattaforma **CST** sviluppata da **TSec**, questi problemi possono essere risolti per la prima volta con una tecnologia completamente passiva.

Coded Sensor Technology (CST) è più di una linea di contatti: è la prima piattaforma ad alta sicurezza al mondo per la realizzazione di sensori magnetici su misura con tecnologia Magnasphere®.

Sulla base di un cuore tecnologico comune, TSec può personalizzare le funzionalità dei sensori in modo da soddisfare anche le più stringenti esigenze di alta sicurezza.

A partire dalla possibilità di realizzare tamper anti-rimozione su parte sensore e parte magnete, fino all'integrabilità di contatto magnetico e sensore inerziale in un unico dispositivo: le possibilità sono semplicemente infinite.

Il contatto riconosce il proprio magnete: la Coded Sensor Technology, esclusivo brevetto TSec, permette di realizzare coppie di sensori e magneti codificate.

Tentativi di utilizzare un magnete diverso da quello codificato causano l'apertura di un circuito di tamper 24h indipendente dal contatto primario. Questo avviene principalmente se il tentativo di bypass è effettuato tra sensore e magnete. Proprio perché il codice magnetico è monitorato attraverso una linea tamper separata dall'allarme, tutta la linea CST è in grado di proteggersi da attacchi magnetici anche a porta aperta e impianto di allarme disinserito.

Per le loro caratteristiche di sicurezza uniche sul mercato i sensori CST rappresentano un'ottima applicazione per la protezione di varchi di zone ad altissima sicurezza e di porte interbloccate.

I sensori CST, nonostante la loro tecnologia avanzata, si presentano alle centrali come comuni contatti passivi: compatibilità completa con ogni marca di centrale.

Sono disponibili nelle versioni con cavo o a morsetti nelle configurazioni:

- **CST-15** contatto magnetico di allarme codificato, linea separata di codice magnetico errato e linea separata di tamper antirimozione.

Sono disponibili nella versione **CST-15** completamente resinata oppure **CST-15-M** con terminali a morsetto.

- **CST-16V** contatto magnetico di allarme codificato, linea separata di codice magnetico errato, linea separata di tamper antirimozione e sensore inerziale integrato.

E' il sensore di punta della gamma di contatti magnetici a quadruplo bilanciamento CST (Coded Sensor Technology).

I modelli **CST-16V** integrano un sensore inerziale passivo TSec per garantire anche la massima sicurezza antiscasso. Sono particolarmente indicati per applicazioni legate alle problematiche di Insider Attack (ad esempio contro la disabilitazione di porzioni del sistema di sicurezza dall'interno del perimetro protetto).

Sono disponibili nella versione **CST-16V** completamente resinata con cavetto da 3 mt oppure **CST-16V-M** con terminali a morsetto.

- **CST-03** contatto magnetico codificato ad alta tolleranza e linea separata di codice magnetico errato.

I modelli **CST-03** aggiungono alla codifica una grande tolleranza, e sono quindi adatti per portoni industriali, porte a libro e cancelli.

Sono disponibili nella versione **CST-03** completamente resinata con cavetto da 3 mt, che garantisce installazioni in esterno sicure nel tempo, oppure nella versione **CST-03-M** con terminali a morsetto.

Tutti i sensori della gamma CST hanno la caratteristica di poter essere montati in linea o ad angolo retto senza necessità di staffe accessorie.

Possono essere forniti con resistenze di bilanciamento integrate dei valori richiesti.

Sono garantiti 10 anni e sono prodotti interamente in Italia.

TSec
TECHNOLOGY FOR SECURITY

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

Case study: soluzioni integrate Axis per il controllo degli accessi e la sicurezza del Caruso Place Boutique & Wellness Suites

a cura della Redazione

Missione

Caruso Place Boutique & Wellness Suites si trova nel cuore di Napoli, all'interno dello storico Palazzo Berio in via Toledo. Per offrire uno standard di servizio sempre più elevato ai propri clienti e gestire al meglio l'investimento, i proprietari necessitavano di una soluzione semplice e pratica che garantisse il passaggio dalla prenotazione all'abilitazione della camera senza intervento di personale e consentisse l'identificazione di eventuali anomalie del sistema in modo autonomo, senza dover ricorrere a interventi esterni.

Soluzione

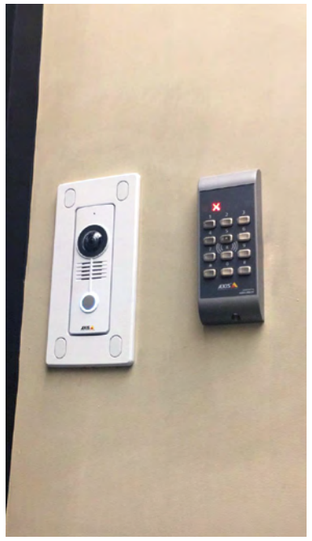
La soluzione proposta da **Smartnet**, Partner di **Axis Communications**, ha permesso di realizzare un sistema di controllo accessi automatizzato basato su piattaforma aperta Axis con integrazione di videocitofonia e telecamere Axis, completamente gestito via IP da personale alberghiero anche in remoto grazie alla piattaforma **ConsolONE**. Integrato con il software alberghiero **"Hotel4"**, sviluppato da **Ericsoft**, consente l'associazione dinamica dei codici di apertura porte e la rimozione automatica al termine del periodo di prenotazione della stanza.

Risultato

Questa soluzione ha permesso di realizzare un sistema di controllo accessi pratico e funzionale per la gestione degli accessi tramite utilizzo di badge per il personale e con l'inserimento di codice PIN per i clienti. Grazie alla piattaforma aperta Axis, la tecnologia basata su IP ha permesso al Caruso Place Boutique & Wellness Suites di ridurre l'eventuale necessità di manutenzione, grazie a un sistema controllabile da remoto, e di garantire ai clienti un soggiorno più confortevole, potendo contare su qualità e sicurezza ai massimi livelli.

Caruso Place Boutique & Wellness Suites accoglie i suoi ospiti in una atmosfera di charme con servizi di alto livello nel cuore di Napoli, a pochi passi dalle attrazioni più celebri della città come Piazza del Plebiscito, Palazzo Reale, Teatro San Carlo, situato proprio di fronte alla celebre Galleria Umberto I. I proprietari di questo angolo di relax e accoglienza turistica, in cui convivono materiali raffinati e dettagli di stile iconici del gusto napoletano, hanno considerato tutte le esigenze dei viaggiatori dando vita ad un hotel di design, in cui tradizione e tecnologia sono al servizio dei clienti che scelgono di trascorre un periodo di vacanza o semplicemente di relax in una delle 10 camere dell'hotel situato nelle antiche mura dello storico palazzo Berio.

"L'uso della chiave o del badge elettronico in hotel è ormai un vecchio concetto per l'apertura delle camere. In un mondo sempre più basato su nuove tecnologie ci è sembrato opportuno dare un ulteriore servizio ai nostri clienti," dichiara la proprietaria **Manuela Aloschi**. *"I clienti ricevono via sms il loro codice di accesso alla camera personale che permette a tutti i componenti di poter accedere alla propria stanza in qualsiasi momento senza doversi ricordare di portare con sé nessun badge magnetico. Abbiamo notato che questo servizio è stato fin da subito molto apprezzato dai nostri clienti e quindi siamo molto contenti della scelta fatta".*



La soluzione installata può contare sulle migliori tecnologie **Axis Communications**, che permettono un'integrazione completa e semplice, grazie allo standard IP aperto, con i software sviluppati da terze parti. In particolare questa installazione è caratterizzata da 7 **Network Door Controller AXIS A1001**, una soluzione che garantisce i vantaggi dell'IP ad architettura aperta in un sistema di controllo degli accessi fisico; i 2 videocitofoni **AXIS A8105-E** svolgono la funzione di videocamera di sicurezza completa, potente strumento di comunicazione e comodo apriporta, tutto in un unico dispositivo per l'ingresso principale e quello posteriore.
Complemento perfetto della soluzione di sorveglianza in uso, inoltre contribuiscono alla sicurezza dei locali con un'identificazione attendibile 24 ore al giorno e, unite alle telecamere AXIS della serie M, garantiscono massimi standard di sicurezza all'interno dello stabile e agli ingressi. L'integrazione tra il sistema telefonico Voip e la security con i videocitofoni che svolgono entrambe le funzioni, ha consentito all'hotel di ottimizzare gli investimenti e di raggiungere pienamente i propri obiettivi.

Marco Pirone, Networking Engineer di Smartnet Srl, Partner di Axis, ha aggiunto: *"Lo standard aperto delle soluzioni Axis ci ha permesso di realizzare un sistema funzionale e semplice allo stesso tempo, in grado di rispondere in pieno alla richieste dell'utente finale. La soluzione è stata apprezzata anche dai fornitori del software per alberghi, che hanno valutato in maniera particolarmente positiva la semplicità di integrazione del sistema sottolineando come non abbiano mai avuto a che fare, prima d'ora, con sistemi così sofisticati e all'avanguardia".*

AXIS COMMUNICATIONS

CONTATTI: AXIS COMMUNICATIONS
Tel. +39 02 8424 5762
www.axis.com

Arriva in Italia DoorTek, la linea di porte e partizioni di sicurezza Gunnebo

a cura della Redazione

Già apprezzate sui mercati internazionali, arrivano anche in Italia le porte e le partizioni DoorTek di Gunnebo, dalle molteplici possibilità di personalizzazione .

DoorTek, nuova linea di porte e pareti certificate di sicurezza, si affaccia sul mercato italiano, dopo aver riscosso interesse nei mercati d'oltralpe con numerose installazioni di successo.
Si tratta di una linea firmata **Gunnebo**: la multinazionale svedese leader nel settore della sicurezza non ha mai infatti smesso di considerare le opportunità di acquisto di aziende del settore, rendendo così sempre più completa la sua gamma di soluzioni integrabili per ogni esigenza di sicurezza. Con l'acquisizione di diverse aziende in Francia, compresa l'alsaziana **Ritzenthaler**, specializzata in serramenti, porte e bussole di sicurezza, l'offerta Gunnebo di prodotti di questo tipo è diventata la più completa del segmento. L'azienda è così pronta a soddisfare il crescente interesse da parte del mercato italiano per porte, serramenti e pareti modulari di sicurezza.

Flussi continui, protezione elevata

Sono numerosi i contesti nei quali un'elevata protezione da eventi dannosi, fortuiti o intenzionali, va abbinata alla capacità di gestione di flussi continui nel tempo di numerose persone, che si tratti di dipendenti o esterni. Oltre a banche e gioiellerie, che per la natura dei beni presenti costituiscono da sempre una forte tentazione per i malintenzionati, al mercato potenziale di queste soluzioni si sono aggiunte altre realtà, come i siti dove sono conservati materiali di valore, dai metalli preziosi a minerali e terre rare, utilizzati in misura crescente dall'industria, ai farmaci particolarmente costosi o ricercati presenti nei centri di produzione e distribuzione farmaceutica. Non solo nelle nuove costruzioni ma anche nelle ristrutturazioni, il progetista accorto sente l'esigenza di dotare di protezione adeguata le parti con accesso al pubblico e i locali interni nevralgici che devono fornire protezione in caso di attacco o di crisi.

Non solo furti

Oltre ai tipici fruitori di questi mezzi di protezione, quali siti militari, aeroporti, centri di detenzione, sono da annoverarsi anche realtà che finora non avevano considerato di essere a rischio, ma che le cronache hanno portato a ricredersi. Reception "simboliche" di aziende private, centrali di produzione e distribuzione di energia, data center, punti di accredito e guardianie di ambasciate e consolati e sempre più spesso di edifici sensibili quali grattacieli e centri commerciali, debbono consentire il passaggio frequente di clienti e dipendenti, ospiti e visitatori e allo stesso tempo garantire un'efficace protezione da effrazioni, sparatorie, esplosioni e dall'azione del fuoco. E non è solo il terrorismo a destare preoccupazioni: anche incidenti del tutto imprevisti, come quelli che si possono verificare in impianti chimici, raffinerie, nell'industria estrattiva, nelle centrali energetiche o in altri contesti con presenza di materiali infiammabili e rischio di esplosioni, possono avere conseguenze devastanti per i dipendenti, che una prudente progettazione di porte e barriere può contribuire a prevenire.

Protezione modulare

La protezione desiderata può riguardare uno o più di questi ambiti, o anche tutti e quattro. Consapevole di questa varietà di esigenze, Gunnebo ha strutturato l'offerta **DoorTek** in modo modulare e personalizzabile, oltre che – come è logico attendersi – dal punto di vista di dimensioni e finiture di porte e pareti, che sono realizzate su misura, anche con riferimento al tipo di protezione richiesta. Il cliente può infatti richiedere una barriera antieffrazione, antiproiettile, anti-esplosione o antincendio, oppure una qualsiasi combinazione delle resistenze all'effrazione **(MagTek)**, balistica **(DarTek)**, esplosioni **(BlasTek)** e fuoco **(VulTek)**. Permangono naturalmente le possibilità di personalizzazione anche all'interno delle singole tipologie: la protezione balistica può ad esempio essere integrata con trattamenti per prevenire la proiezione di schegge verso gli occupanti del sito protetto.

Certificazione completa

Molti fornitori, che si limitano ad assemblare componenti certificati, non sono in grado di assicurare che il prodotto risultato di tale processo sia nella sua interezza conforme alla classe di resistenza desiderata dal Cliente. Gunnebo pone la linea **DoorTek** ad un livello di sicurezza superiore e soprattutto verificato: è il prodotto completo, assemblato, che viene infatti sottoposto ai severi test che ne attestano le performance dichiarate in ogni suo componente, in modo che la certificazione riguardi proprio ciò che il cliente acquista, validato nella sua interezza. Nessun rischio che alcuni dettagli, come i cardini, la serratura o le giunture fra diversi materiali, possano costituire anelli deboli, fornendo all'intero una resistenza minore di quella delle sue parti: con la certificazione del prodotto finito **DoorTek** si pone come una soluzione assolutamente garantita.
Chi acquista porte e partizioni **DoorTek** tipicamente è soggetto a controlli di terze parti, come le assicurazioni o enti certificatori: l'attestazione unica di classe di resistenza fornita da Gunnebo è un valido aiuto per superare tutti i controlli previsti senza problemi. In materia di sicurezza le garanzie di qualità sono vitali: la tranquillità che deriva dal rivolgersi a un fornitore come Gunnebo è decisamente apprezzata dai grandi committenti.

Una gamma ampia per ogni esigenza

L'offerta **DoorTek** comprende diverse proposte per ogni situazione:

- porte di sicurezza, certificate da laboratori indipendenti in conformità con le normative europee. La gamma comprende le linee MagTek IA e DarTek IA, che offrono prestazioni di isolamento termico conformi alla Normativa 2012/27 riguardo alla riduzione dei consumi energetici;
- porte interbloccate: la gamma SkySas rileva passaggi singoli o masse metalliche, offre un'elevata resistenza ai tentativi di effrazione e agli attacchi balistici e si presenta con un design essenziale e accattivante;
- pareti e vetri di sicurezza: una vasta selezione di pannelli, pareti e soffitti modulari, certificati e garantiti per offrire un perimetro sicuro in aree dalle elevate esigenze di sicurezza;

- sistemi sicuri di trasferimento: dispositivi per punti cassa e cassetti per trasferire in modo sicuro banconote, biglietti e plichi, integrabili in pareti di vetro ad alta sicurezza offrendo protezione da attacchi fisici, balistici e batteriologici.

Protezione per edifici e persone

La gamma **DoorTek** offre una valida protezione da attacchi vandalici, manuali, esplosivi o di altro tipo, attuati singolarmente o in combinazione, senza però compromettere la libertà di movimento di dipendenti, clienti e visitatori o pregiudicare il corretto svolgimento delle operazioni nell'edificio; il design elegante e personalizzabile di queste soluzioni permette loro di integrarsi in ogni contesto architettonico, anche il più prestigioso, valorizzandolo.

Pur avendo un catalogo ricchissimo, Gunnebo è in grado di andare anche oltre alla sua ampia offerta per soddisfare le esigenze dei clienti: grazie al controllo sugli stabilimenti produttivi di proprietà, può fornire anche versioni dei propri prodotti personalizzate in base alle specifiche richieste dei clienti, in tempi decisamente rapidi.

Per ulteriori informazioni sulle soluzioni Gunnebo per il controllo degli accessi e in generale per tutti gli aspetti della sicurezza, potete contattare l'azienda all'indirizzo **entrancecontrol.it@gunnebo.com**, telefonare al numero **0461/248914** o visitare il sito **www.gunnebo.it**

Hygiaphone

Fra i brevetti internazionali acquisiti da Gunnebo nel suo programma di espansione rientra **Hygiaphone**, un'invenzione rivoluzionaria per i suoi tempi: si tratta di un sistema a membrane integrato in pareti di sicurezza in vetro, studiato per proteggere i dipendenti delle ferrovie francesi **SNCF** dal contagio durante l'epidemia di Spagnola del 1945. Il contatto con il pubblico era necessario per questi operatori, ma poteva essere pericoloso: come mantenere un servizio accurato, ponendosi in vista e all'ascolto delle persone e rimanendo allo stesso tempo protetti dal contagio? **Hygiaphone** risolse il problema con eleganza, superando i sistemi spesso gracchianti di riproduzione vocale mediante microfoni. La membrana amplifica le vibrazioni della conversazione consentendo un ottimo ascolto, isolando nel contempo le voci dal rumore di fondo, spesso elevato nelle stazioni.

Il moderno concetto di servizio senza barriere e di sportello aperto, per favorire un miglior contatto e un rapporto più personale con il cliente, ha chiaramente diminuito la richiesta per questo tipo di barriera; resta però di grande utilità in contesti, ospedalieri o ad alto rischio di attacchi terroristici anche batteriologici, dove la prevenzione del contagio è fondamentale.

GUNNEBO®
For a safer world

CONTATTI: GUNNEBO ITALIA SPA
info.it@gunnebo.com
www.gunnebo.it

Protecting people
protecting you

CDO
CITTADINI DELL'ORDINE
Sicurezza dal 1870

IN ITALIA E ALL'ESTERO
Analisi rischi e prevenzione
Portierato
Vigilanza armata
Vigilanza ispettiva
Tecnologie
Servizio antitaccheggio
Pronto intervento
Gestione network

www.agenziaimage.com

Premio H d'oro 2017
Centro Sportivo FC Internazionale

a cura della Redazione

Categoria: **INFRASTRUTTURE E SERVIZI**

Azienda installatrice: **ZOIS**

Denominazione e località dell'impianto: **Centro Sportivo FC Internazionale**

Committente: **FC Internazionale**

Tipologia di impianto realizzata: **Impianto antintrusione, videosorveglianza e controllo accessi**

Data di ultimazione lavori: **febbraio 2017**

Lo scorso 27 novembre al Museo Egizio di Torino si è svolta la premiazione dei vincitori e dei finalisti della dodicesima edizione del Premio H d'oro, il concorso organizzato dalla **Fondazione Enzo Hruby** per premiare le migliori realizzazioni di sicurezza e con esse la professionalità dei più qualificati operatori del settore. La società **ZOIS** di Solaro (MI) è arrivata in finale con un avanzato sistema antintrusione, di videosorveglianza e controllo accessi dedicato al **Centro Sportivo FC Internazionale.**

Descrizione dell'impianto

Presso la società FC internazionale, l'azienda ZOIS ha realizzato un nuovo sistema antintrusione, di videosorveglianza e controllo accessi. I sistemi sono installati e gestiti su quattro livelli, corrispondenti al piano interrato e al terzo, quarto e quinto piano.

La gestione degli accessi avviene tramite un lettore d'impronte interfacciato ad una scheda su centrale a 512 zone che comanda la porta automatica. Fuori dalla fascia oraria impostata, il lettore d'impronte necessita dell'inserimento di codice sulla tastiera antintrusione e di successiva lettura biometrica. Tutte queste logiche sono gestite dalla macro della centrale antintrusione.

Il software di gestione gestisce tutti i siti di FC Internazionale, ovvero la sede di **Milano, Interello, La Pinetina e il magazzino.**

Nel centro sportivo più significativo, **La Pinetina**, è stato realizzato un sistema antintrusione e TVCC per tutti i siti che sorgono al suo interno. Alla garritta d'ingresso c'è il presidio h24 dove viene gestito il sistema antintrusione tramite software proprietari.

Tutte le telecamere sono di tipo 2 Megapixel per i tre campi di allenamento. Il sistema è cablato in fibra ottica, per un network complesso e diramato.

Grado di difficoltà, problemi e soluzioni

L'impegno maggiore per eseguire questo impianto è stato il dimensionamento per la parte network per le grandi distanze e la creazione in molteplici punti di quadri di smistamento per fornire connettività alle telecamere dislocate in magazzino, nel centro benessere, nello spogliatoio, nel ristorante, nella sala stampa campi, e agli accessi perimetrali.

La difficoltà maggiore riscontrata è stata la necessità di lavorare rapidamente, spesso in contemporanea con altri lavoratori in determinate fasce orarie e zone. Questo per non ostacolare e disturbare la concentrazione dei preparatori tecnici e dei calciatori.

Caratteristiche particolari dell'opera

Il risultato è un sistema unificato per tutte le sedi, in modo tale che dalla postazione di gestione remota, tramite rete lan virtuale, è possibile avere tutto sotto controllo. Tramite APP è possibile gestire immagini, accessi, comandi, inserimenti e gestione memoria eventi. Si tratta di un sistema complesso, esteso e nello stesso tempo snello, stabile e affidabile.

Staff e tempo impiegati per la realizzazione

Il sistema è stato realizzato in diversi step per un totale di circa 70 giorni lavorativi.

Con AXIS Audio Manager C7050 Server un controllo totale dell'audio di rete

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

Per sfruttare al massimo i vantaggi dell'audio di rete con l'obiettivo di aumentare la sicurezza e offrire la migliore esperienza possibile al pubblico, **Axis Communications** presenta **AXIS Audio Manager C7050 Server**, un punto singolo di gestione audio che include hardware e software e, utilizzando una sola interfaccia, consente di gestire e controllare tutti i dispositivi audio di rete Axis tra cui altoparlanti, bridge audio, microfoni e altoparlanti a tromba.
Facile da installare e utilizzare, **AXIS Audio Manager C7050 Server** è una soluzione ideale per garantire una semplice ed efficiente gestione centralizzata dei contenuti e della programmazione audio all'interno di sistemi più grandi e avanzati, ad esempio in catene di negozi oppure scuole.
Con **AXIS Audio Manager C7050 Server** è possibile definire zone diverse in base alla posizione geografica e alle specifiche aree, permettendo così di programmare e trasmettere annunci, spot e musica di sottofondo personalizzabili secondo le più diverse esigenze e occasioni.
Inoltre, la gestione dei contenuti dalla sede centrale o dai singoli siti o punti vendita consente di controllare l'intero sistema audio di rete con un computer, un tablet o uno smartphone, ad esempio programmando la trasmissione di tracce preregistrate, controllando il volume audio e monitorando il funzionamento dei dispositivi 24 ore su 24 e 7 giorni su 7.
La soluzione non richiede una programmazione software particolare, perché tutti i dispositivi audio IP si connettono automaticamente a una rete LAN/WAN.

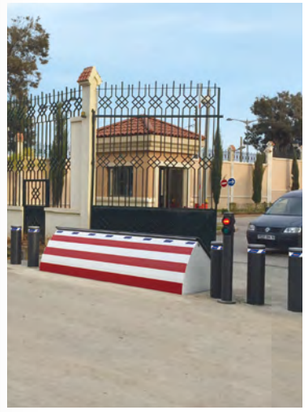
ERMES presenta: Citofoni per le Celle delle Stazioni Carabinieri

ERMES
(+39) 0438 308470
www.ermes-cctv.com

L'interfono da incasso **InterLAN-EC.1P** e l'interfono da tavolo **InterLAN-EO.12PM** risolvono in maniera semplice ed a costi contenuti il problema dell'installazione di citofoni all'interno delle celle di detenzione presenti nelle stazioni dei Carabinieri.
Ambedue gli apparati utilizzano tecniche di comunicazione IP e possono utilizzare per la loro interconnessione una rete dati già esistente o, nel caso questa non sia disponibile, un semplice switch POE che, su un unico cavo, fornisce sia l'alimentazione degli apparati sia la connessione dei dati.
InterLAN-EC.1P è in esecuzione da incasso e reca sul pannello frontale un pulsante di chiamata, un led di segnalazione, un microfono ed un altoparlante. Questi ultimi hanno un sistema di protezione che ne impedisce il danneggiamento.
La scatola da incasso è realizzata in acciaio con spessore 15/10 ed ha delle alette antistrappo che ne impediscono la rimozione; il pannello frontale è in acciaio inox con spessore di 30/10 ed è fissato con viti anti-manomissione monouso con testa sigillata.
Tra le funzioni implementate è presente la possibilità di attivare la comunicazione anche dal posto del piantone o di attivare l'ascolto ambientale silenzioso.
InterLAN-EO.12PM è in esecuzione da appoggio su tavolo e, avendo 12 pulsanti programmabili per la selezione dei periferici, può anche essere utilizzato per un numero maggiore di celle o per realizzare delle comunicazioni di servizio con altri locali della caserma.

Road blocker High Security Hörmann: la sicurezza raggiunge il vertice della performance

HÖRMANN ITALIA
(+39) 0461 244444
www.hormann.it



Il **Gruppo Hörmann** che ha fatto della sicurezza uno degli asset fondamentali per divenire leader mondiale nelle chiusure, entra oggi, per logica evoluzione, nel settore del controllo veicolare degli accessi.
Fiore all'occhiello della proposta dell'azienda per questo mercato, è la **High Security Line**, speciale linea di soluzioni per il controllo veicolare degli accessi ad aree di massima sicurezza e che presenta, accanto a dissuasori, barriere a movimento verticale e tyre killer, anche road blocker dalle prestazioni superiori.
I road blocker **Hörmann** sono progettati per aree sensibili quali edifici governativi, aeroporti, piazze o location in cui avranno luogo importanti manifestazioni, e sono indicati in prossimità di entrate e uscite ampie fino a 6 m.
Progettati nei centri ricerca e sviluppo Hörmann, questi road bocker sono prodotti in stabilimenti altamente specializzati e proposti nelle varianti 500 e 1000, in base all'altezza del brandeggio.
Dotate di una robustezza da primato, queste soluzioni possono essere utilizzate nei contesti più sensibili in quanto sono in grado di resistere ad energie d'urto estremamente elevate: fino a 80 km/h per un autocarro da 7,5 tonnellate di peso.
Come i dissuasori e le barriere a movimento verticale della High security Line, i road blocker Hörmann sono certificati mediante crash test eseguiti da istituti di verifica accreditati per il conferimento dell'omologazione ufficiale.

Redazionale Nexus 3G

INIM ELECTRONICS SRL
(+39) 0735 705007
www.inim.biz

Nexus/3GP

Inim lancia sul mercato il nuovo **Nexus/3G**, il comunicatore su reti 3G e 2G (HSPA/GSM), evoluzione tecnologica del Nexus. Il dispositivo è compatibile con le centrali Inim, **Prime e SmartLiving**, oltre che con tutte le reti 3G e 2G.
Nexus/3G viene proposto in due modelli: il **Nexus/3GP**, con contenitore plastico protetto, antenna integrata e 2 batterie stilo (AA) di backup che garantiscono la segnalazione di emergenza anche in caso di perdita di alimentazione e il **Nexus/3GU** con possibilità di alloggiamento in centrale e dotato di antenna remota.
Con Nexus/3G è possibile attivare via GPRS/3G una sessione di controllo remoto per leggere/scrivere la programmazione della centrale attraverso i servizi Inim Cloud.
Nexus/3G mette a disposizione delle centrali un comunicatore vocale digitale e IP verso le stazioni di vigilanza e consente, sia all'installatore che all'utente, di accedere ai servizi **Inim Cloud** o peer-to-peer.
Nexus/3G può essere utilizzato sia come periferica principale per la connessione al Cloud sia come periferica di backup, nel caso si perda la connessione attraverso il canale LAN cablato. Per connettersi alle reti 3G è necessaria una SIM card abilitata al servizio.
Nella centrale Prime è inoltre possibile la gestione simultanea di molteplici canali di comunicazione: connessione Cloud, chiamate vocali, chiamate di televigilanza, SMS.
Mail: info@inim.biz

Redazionali Tecnologie

TSec Coded Sensor Technology - CST-03

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

I **CST-03** sono sensori codificati completamente passivi basati sulla tecnologica **"Coded Sensor Technology"**, un brevetto **TSec** che consente di realizzare coppie di sensori e magneti codificate.
Grazie a questa tecnologia innovativa, il sensore passivo è in grado di riconoscere il proprio magnete.
Tentativi di utilizzare un magnete diverso da quello codificato causano l'apertura di un circuito di tamper 24h indipendente dal contatto primario. I sensori CST, nonostante la loro tecnologia avanzata, si presentano alle centrali come comuni contatti passivi, garantendo compatibilità completa con ogni marca di centrale.
I modelli **CST-03** aggiungono alla codifica una grande tolleranza, sono quindi adatti per portoni industriali, porte a libro e cancelli.
Questi sensori sono basati su tecnologia antimascheramento brevettata **Magnasphere**, hanno una scocca in alluminio anodizzato ad alta resistenza, vengono forniti con viti autofilettanti anti-rimozione inox e sono caratterizzati da una resinatura completa adatta sia ad un uso interno che esterno, essendo IP67.
Sono disponibili nella versione con cavetto da 3 mt, **CST-03** adatta ad installazioni in esterno oppure nella versione **CST-03-M** con terminali a morsetto.
Hanno la caratteristica di poter essere montati in linea o ad angolo retto senza necessità di staffe accessorie.
Come prassi consolidata, **tutti i sensori passivi di TSec sono garantiti 10 anni e sono prodotti interamente in Italia.**

essecome ONLINE

n. 05 luglio 2018
Anno XXXVIII
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Angelo Carpani, Nils Fredrik Fazzini, Filippo Gambino, Pietro Tonussi

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

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

REGISTRAZIONE
Tribunale di Milano n. 21
del 31 gennaio 2018

GRAFICA/IMPAGINAZIONE
contatto@lilastudio.it