TECNO

LE BUSSOLE DI TECNO

Security Manager,

verso quali prospettive tecnologiche e strategiche si stanno muovendo?

A cura di

LUMI 4 INNOVATION

In collaborazione con

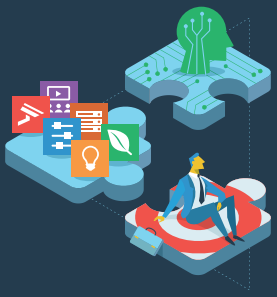
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

LABORATORIO PER LA SICUREZZA

TECNO

Nel complesso mercato dell'elettronica e delle sue applicazioni, siamo la bussola che guida chi realizza sistemi intelligenti e chi li integra.

Tracciamo percorsi per mettere in relazione la domanda e l'offerta



Siamo il partner che valorizza le aziende nell'ecosistema

RICERCHE DI MERCATO

LEAD GENERATION

COMUNICAZIONE

EVENTI

FORMAZIONE

Una linea di pubblicazioni scritte con un linguaggio concreto, focalizzate sulle prospettive tecnologiche e strategiche di funzioni chiave come quella di security, facility, energy manager

Un approfondito riferimento in Italia per manager e decisori che debbano comprendere in profondità le innovazioni digitali (HW e SW) che stanno trasformando il settore, rendendo fruibile la conoscenza sul tema e creando una comunità italiana attiva e aperta al confronto.

I dati contenuti nelle "Bussole di Tecno" sono riportati e aggregati come forniti dalle figure coinvolte.

L'Editore non risponde di eventuali omissioni o errori materiali, pur assicurando che nella compilazione è stata usata la massima diligenza.

©Tutti i diritti sono riservati.
La riproduzione parziale o totale del contenuto consentita previa autorizzazione

Per il produttore di sistemi di sicurezza fisica, il Security Manager rappresenta il cliente finale. È lui che sceglie gli strumenti con i quali mettere in sicurezza l'azienda per la quale lavora e che ne decide l'acquisto.
La ricerca condotta da LUMI4Innovation, in collaborazione con le Associazioni A.I.PRO.S. - Associazione Italiana Professionisti della Sicurezza e Laboratorio per la Sicurezza, ci restituisce il ritratto di una figura professionale, per alcuni aspetti, in bilico tra vecchio e nuovo, tra tecnologie ormai acquisite e nuovi trend, frenata, da un lato, dai limiti imposti dal GDPR all'applicazione di soluzioni di ultima generazione e, dall'altro, da dinamiche interne alle aziende in cui lavora, tra cui la mancanza di sinergia fra i reparti e fra saperi diversi.

SURVEY SICUREZZA

01

02

LE TECNOLOGIE UTILIZZATE

03

SCOUTING E CRITERI DI RICERCA

04

NUOVE SFIDE E ORIENTAMENTI

“La ricerca è stata realizzata mediante questionari a risposta multipla inviati a un campione di 50 Security Manager che si occupano di sicurezza fisica. Il valore di tale campione non è certo statistico, ma ci permette di delineare il “movimento”, gli orientamenti, le scelte tecnologiche di una figura professionale finora poco sondata eppure dal ruolo decisivo.”

Paola Cozzi
Direttore editoriale
LUMI4INNOVATION

PROFILO DEI SECURITY MANAGER CHE HANNO PARTECIPATO ALL'INDAGINE

Il campione della ricerca: 50 Security Manager

Dei 50 Security Manager che hanno risposto al nostro questionario a risposta multipla, una netta maggioranza (59,6%) è composta da professionisti che lavorano all'interno di aziende private dalle dimensioni importanti (oltre i 250 dipendenti).

Il 34% si dedica alla libera professione e solo il 6,4% lavora all'interno di un Ente pubblico. Sappiamo che le grandi imprese e le organizzazioni molto strutturate hanno tutte, al proprio interno, chi studia, progetta e mette a punto strategie e piani di sicurezza per prevenire e fare fronte a fenomeni di micro e macro criminalità ai danni di beni materiali, strutture fisiche e persone.
Nelle realtà di medie e piccole dimensioni, invece, il Security Manager dedito alla sicurezza fisica non è sempre presente o, comunque, non si tratta di una figura ben definita.
In questi contesti, infatti, è frequente che sia il titolare stesso, l'ufficio acquisti

o chi si occupa della manutenzione degli impianti, a ricoprire il ruolo di colui che mette in sicurezza l'azienda.
Gli intervistati lavorano in ambiti diversi.
A prevalere, sono i settori Commercio e Servizi (21,4% per entrambi), seguiti, in ordine, da Industria, Telecomunicazioni, Logistica e Trasporti ed Energia. Infine, una minoranza si occupa di Security in ambito Bancario, Alta Moda, Intelligence ed Enti fieristici.

ESERCITA LA SUA PROFESSIONE ALL'INTERNO DI UN'AZIENDA, IN UN ENTE PUBBLICO OPPURE È CONSULENTE ESTERNO?

SU QUALI APPLICAZIONI È MAGGIORMENTE FOCALIZZATO?

QUALI SONO GLI AMBITI IN CUI INCONTRA MAGGIORI CRITICITÀ?

Su quali applicazioni sono maggiormente focalizzati? L'85% del campione utilizza sistemi di videosorveglianza per proteggere l'azienda in cui lavora. Applicazione alla quale seguono controllo accessi (70% degli intervistati) e antintrusione (68%).

Troviamo, poi, in ordine, rilevazione presenze, antirapina, antincendio e antitaccheggio. Dunque, nonostante l'eterogeneità dei settori in cui operano e le specifiche esigenze di sicurezza di ognuno di questi, sono i sistemi di videosorveglianza gli "strumenti" chiave, sui quali maggiormente poggia la strategia dei Security Manager intervistati. A conferma dei dati elaborati da ANIE Sicurezza sull'andamento dei singoli comparti del settore, dai quali spicca - con un +12,5% di fatturato nel 2018, rispetto al 2017 - il dinamismo assoluto del segmento video.

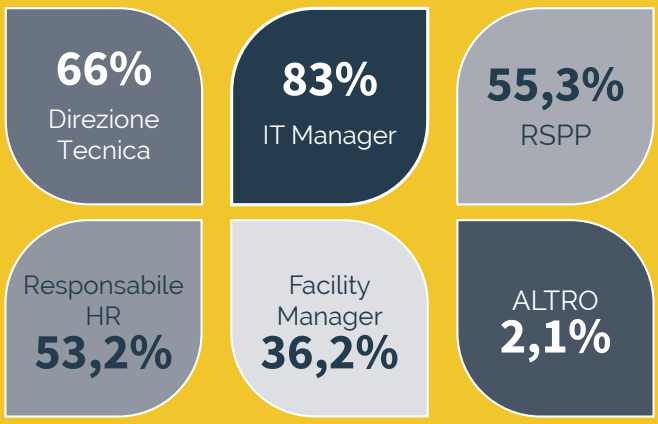
INTEGRAZIONE DEI SISTEMI E SINERGIE INTERNE GLI AMBITI PIÙ CRITICI

Quello del Responsabile della sicurezza fisica è un mestiere dai più volti. Al Security Manager professionista vengono richieste abilità diverse, che vanno dalla conoscenza delle policy e delle procedure di analisi e prevenzione dei rischi alla conoscenza delle tecnologie e del quadro normativo di riferimento, dalle capacità di organizzazione interna a quelle di gestione del budget dedicato all'acquisto di dispositivi e apparecchiature di sicurezza.
Ebbene, il 57,8% del campione afferma che l'aspetto del lavoro in cui incontra maggiori criticità è quello relativo all'integrazione dei sistemi. Perché?
Fare dialogare tra loro impianti diversi, farli convergere verso un unico sistema di supervisione, con l'obiettivo di ottimizzare la sicurezza di beni e persone, di controllare i consumi, l'illuminazione e altri apparti, presuppone, oltre agli aspetti

tecnologici di gestione, anche l'incrocio tra saperi diversi - propri di altre figure professionali - la collaborazione con altri reparti interni all'azienda, tra cui, ad esempio, chi si occupa di manutenzione, di facility management e di efficienza energetica.
E, analizzando le altre risposte - ricordiamo che sono multiple - emergono alcuni risvolti interessanti: se la scelta delle tecnologie (15,6%) e l'applicazione delle normative (22,2%) non sembrano destare preoccupazioni ai Security Manager intervistati, con, rispettivamente, il 55,6% e il 46,7% di risposte date, sono

la creazione di sinergie tra i reparti dell'azienda e l'organizzazione interna a rappresentare il secondo e il terzo ambito più critico, in correlazione, a nostro avviso, con le difficoltà nell'integrare sistemi diversi. Se, poi, prendiamo in considerazione la domanda sulle figure professionali con le quali i Security Manager intervistati si rapportano, scorgiamo, nelle risposte, una fotografia di quanto detto sopra: tra IT Manager, Direzione Tecnica, RSPP, Responsabili HR e Facility Manager, è con quest'ultima figura che il campione preso in esame si confronta di meno in azienda.

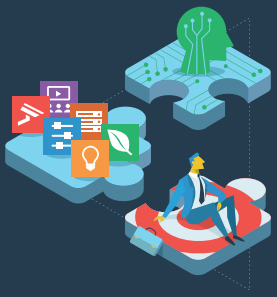
CON QUALI FIGURE PROFESSIONALI SI RAPPORTA ALL'INTERNO DELL'AZIENDA?



TECNO

Nel complesso mercato dell'elettronica e delle sue applicazioni, siamo la bussola che guida chi realizza sistemi intelligenti e chi li integra.

Tracciamo percorsi per mettere in relazione la domanda e l'offerta



Siamo il partner che valorizza le aziende nell'ecosistema

RICERCHE DI MERCATO

LEAD GENERATION

COMUNICAZIONE

EVENTI

FORMAZIONE

PRIVACY COMPLIANCE VISSUTA COME UN LIMITE DA PA E BANCHE

Risalgono al 2010 il Provvedimento del Garante della Privacy e al 2018 il Regolamento dell'Unione Europea noto con la sigla GDPR - General Data Protection Regulation. Oggi, nel 2019, insieme, costituiscono il complesso normativo

che richiama alla definizione di un corretto equilibrio tra riprese video/riconoscimento di dati biometrici e diritto alla riservatezza di ognuno.
Per la precisione, il GDPR si occupa di trattamento dei dati personali (compresi i dati biometrici) e di privacy. Non tratta specificatamente degli aspetti relativi alla privacy legati alla videosorveglianza. Entra nel merito con una sezione dedicata all'utilizzo delle telecamere con video-analisi a bordo e lo fa sempre in riferimento al trattamento dei dati rilevati.

Alla domanda su come affronta il tema della conformità alle norme in materia di privacy - prevalentemente legate all'utilizzo di sistemi di videosorveglianza e di sistemi di riconoscimento di tipo biometrico - il 57,4% del campione risponde positivamente: se viene fatta una corretta informativa, la normativa sulla privacy non è limitante.
E, ancora, fornendo una risposta multipla, la considera un segno distintivo per l'azienda (38,3%).
Un'altra parte del campione, al contrario, la vive come un limite: la normativa sulla privacy frena l'applicazione di alcune tecnologie dalle performance importanti (19%) e condiziona nella scelta delle tecnologie e delle soluzioni (14,9%).
Due atteggiamenti in antitesi, correlati a specifici settori di attività.
Più nel dettaglio, tra coloro che vivono la privacy compliance in modo negativo, figurano Security Manager che esercitano la libera professione,

Security Manager che lavorano nella Pubblica Amministrazione (sia locale che centrale) e, infine, chi lavora in ambito bancario.
Un possibile fil rouge che lega PA e Istituti bancari, è il loro essere uno "sportello" aperto al pubblico.
A differenza di comparti quali Servizi, Industria, Telecomunicazioni, Logistica, Trasporti ed Energia, ad esempio, si tratta di contesti caratterizzati da una dinamica impiegato/operatore-cliente di tipo consulenziale, in cui circolano dati particolarmente sensibili, documenti personali di tipo cartaceo contenenti informazioni riservate, che potrebbero essere ripresi - e, dunque, violati - da sistemi video non in linea con le prescrizioni del Garante della privacy. In tali ambienti, le prescrizioni del Provvedimento del Garante della Privacy e del GDPR in materia di videosorveglianza sono ancora più stringenti, a tutela dell'utente e del suo diritto alla riservatezza.
Da qui, il sentirsi "limitati" e "condizionati" da parte di un gruppo del nostro campione.

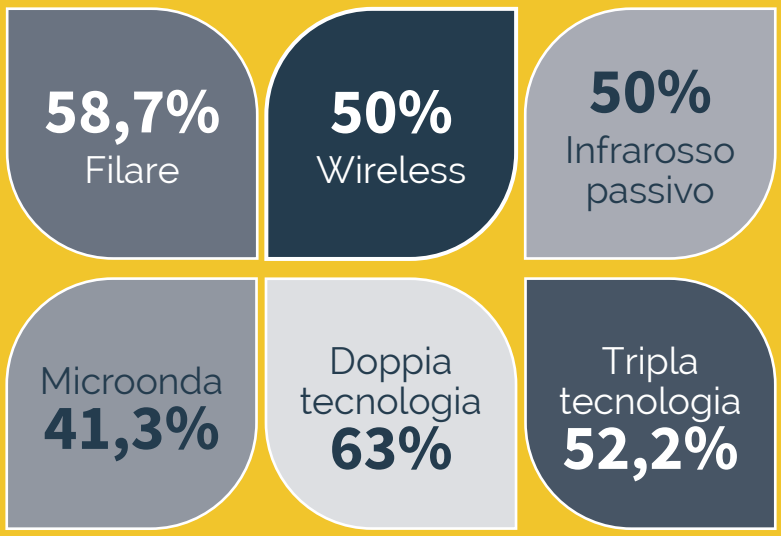
NELL'ANTINTRUSIONE IL FILARE VINCE SUL WIRELESS

Quali tecnologie utilizza, oggi, il Security Manager per ridurre i rischi e mettere in sicurezza l'azienda per la quale lavora? Per le applicazioni antintrusione, la maggioranza del campione (58,7%) si affida a rivelatori, centrali e sirene di allarme filari, vale a dire provvisti di cavi, contro il 50% che, invece, sceglie sistemi wireless (le risposte, lo ricordiamo, sono multiple).
Il maggiore utilizzo del "via filo" potrebbe essere giustificato da due motivi: il prezzo (l'antifurto filare è meno costoso del wireless, anche dal punto di vista della manutenzione)

e, non creando interferenze elettromagnetiche, è una tecnologia riconosciuta come particolarmente sicura.
I sistemi senza fili, al contrario, pur estremamente pratici (non necessitano di opere murarie per la stesura dei cavi) e flessibili (possono essere installati ovunque ed è possibile ampliarli, nel tempo, aggiungendo ulteriori rivelatori), sono più costosi e necessitano di una manutenzione più puntuale e frequente.
Inoltre, anche se, oggi, i senza fili più evoluti (con tecnologia a tripla frequenza, ad esempio) garantiscono prestazioni affidabili, esiste comunque il rischio che possano produrre - e subire essi stessi - interferenze elettromagnetiche e che possano essere facilmente manomessi rispetto ai filari.
Al di là di cavo o comunicazione radio, i Security Manager intervistati, tra rivelatori a doppia e a tripla tecnologia, prediligono i primi (63%, contro il 52,2%).
A differenza della doppia tecnologia - costituita da infrarosso e microonda - la "tripla"

LE TECNOLOGIE UTILIZZATE

ANTINTRUSIONE



ha, in aggiunta, un doppio infrarosso oppure una doppia microonda con una diversa taratura o, ancora, un'intelligenza artificiale data da algoritmi molto potenti.
Più performanti e affidabili dei sensori a doppia tecnologia, i rivelatori antintrusione a tripla tecnologia rappresentano la soluzione più innovativa,in grado di discernere in modo ancora più preciso i falsi allarmi dalle vere intrusioni.
A rappresentare la "seconda scelta" da parte degli intervistati, potrebbe esservi un fattore di prezzo.

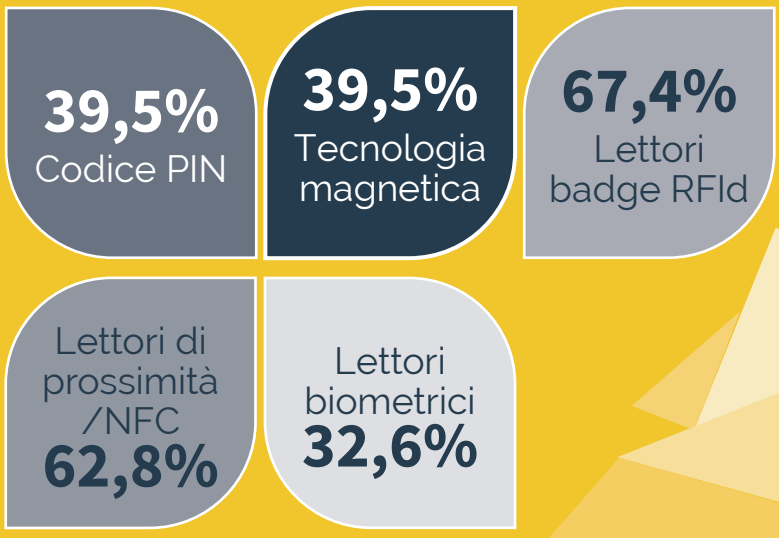
BIOMETRIA FANALINO DI CODA DEL CONTROLLO ACCESSI

Codice PIN, tecnologia magnetica, lettori di badge RFId, lettori di prossimità/NFC o lettori biometrici? Dalla tecnologia più datata a quella più evoluta, dal passato al futuro. Come si muovono i Security Manager tra questi due opposti?

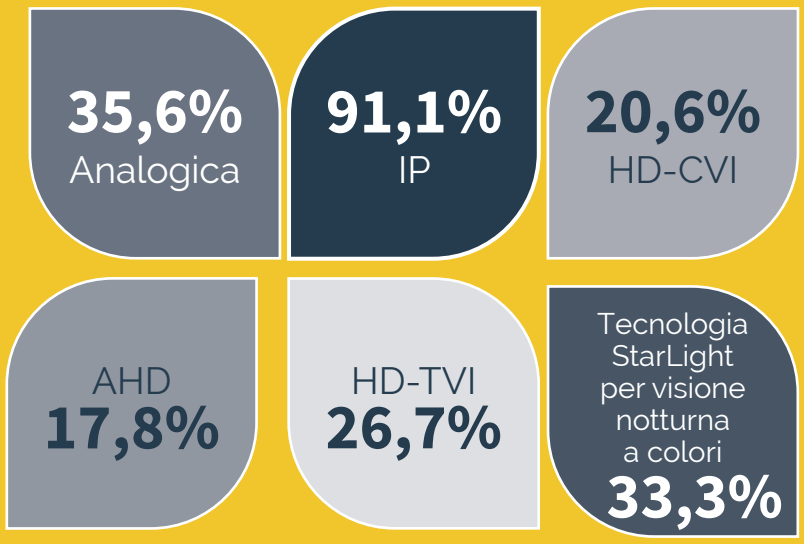
LE TECNOLOGIE UTILIZZATE

La maggior parte di coloro che hanno partecipato alla nostra indagine, per quanto concerne le soluzioni di controllo accessi, scelgono la tecnologia RFiD - Identificazione in Radio Frequenza (67.4%), seguita dai lettori di prossimità/NFC - Near Field Communication, ovvero "Comunicazione di prossimità" - (62,8%). Codice PIN e tecnologia magnetica occupano il terzo posto della classifica delle preferenze (entrambe al 39,5%), mentre la tecnologia basata sul riconoscimento biometrico è in ultima posizione, con il 32,6% delle risposte. Come spiegare tale dato? Innanzitutto, è doveroso dire che i sistemi di controllo accessi basati su riconoscimento biometrico non sono comuni. Non li troviamo ovunque. Quanto meno in Europa. Più sicuri rispetto a password,

CONTROLLO ACCESSI



VIDEOSORVEGLIANZA



PIN, badge e chiavi elettroniche, i dati biometrici - unici, appartenenti a ciascuno in modo assoluto e praticamente impossibili da duplicare e imitare - sono, però, questione complessa. Perché? Riguardando la sfera fisica e comportamentale delle persone, se trattati per fini diversi dal controllo accessi, possono arrecare danni sotto il profilo psicologico, andando a ledere la privacy più intima dell'individuo.

E qui entra in campo la Legge. L'art. 9, par. 1, del GDPR - General Data Protection Regulation vieta, in generale, il trattamento dei dati biometrici. Ammette solo alcune eccezioni: la prima, imprescindibile,

prevede che l'interessato abbia autorizzato il trattamento; un'altra consente l'utilizzo dei dati biometrici solo se necessario "in ambito lavorativo o nell'ambito della sicurezza sociale e collettiva".
Ve ne sono altre, ma interessano meno in questa sede. La seconda eccezione, in particolare, giustifica la presenza di sistemi basati su riconoscimento dei dati biometrici per l'accesso ad aree ritenute critiche.
Pensiamo, ad esempio, a quelle zone, all'interno di una grande industria, in cui sono presenti macchinari dall'utilizzo pericoloso per i non addetti ai lavori, ad alcuni laboratori all'interno degli ospedali, alle torri di controllo e alle aree speciali degli aeroporti, ai caveau delle banche, alle sale macchine delle navi.
Tutti contesti in cui, un controllo accessi di tipo biometrico è giustificato (e consentito) dal Garante della Privacy, a patto che l'interessato abbia autorizzato il trattamento e riceva la corretta informativa.

LE TECNOLOGIE UTILIZZATE

Dall'incrocio dei dati, emerge che la maggioranza dei Security Manager che adottano le tecnologie biometriche per applicazioni di controllo accessi lavorano nelle Telecomunicazioni.
A seguire, i Security Manager impiegati nella Sanità, nell'Industria e nel settore bancario, a conferma di quanto detto sopra ed espresso nell'art. 9 del GDPR a proposito di sistemi basati su riconoscimento dei dati biometrici per l'accesso ad aree critiche.
Infine, dall'indagine emerge che, tra coloro che scelgono il controllo accessi biometrico, vi è anche chi lavora in ambito Intelligence.

LE TECNOLOGIE UTILIZZATE

LA VIDEOSORVEGLIANZA È IP, MA L'ANALOGICO CONTINUA AD AVERE LA SUA FASCIA DI MERCATO

Le risposte alla domanda sulle tecnologie utilizzate in ambito video non lasciano spazio ad analisi interpretative: il 91% del campione sceglie telecamere che utilizzano il protocollo IP. E questo non meraviglia affatto, in quanto naturale epilogo di un lento processo di cambiamento iniziato nel 1996, quando sul mercato italiano fu introdotta la prima telecamera di rete, progettata con chip integrati per connetterla direttamente a qualsiasi rete dotata di indirizzo IP.
Da quel momento, per il comparto della videosorveglianza, con il passaggio dall'analogico all'IP, è iniziata la rivoluzione. Passaggio giunto, nell'ultimo decennio, nella sua fase matura,

tanto che oggi diremmo che si tratta di una transizione completata.
Ma le telecamere analogiche non sono scomparse dal mercato, come si profetizzava fino a quindici anni fa.
Come immaginabile, il loro prezzo è calato e - fattore economico a parte - settori come quello bancario, ad esempio, continuano a richiederle (spesso insieme alle telecamere IP, dando vita a impianti ibridi) perché la trasmissione su cavo coassiale è, ancora oggi, ritenuta più sicura.
Guardando ai dati emersi dal sondaggio, notiamo che il 35,6% dei Security Manager intervistati continua comunque a utilizzare telecamere analogiche, accanto a soluzioni, come la tecnologia HDTVI - High Definition Video Transport Interface (26,7% delle riposte), che coniugano cavo coassiale e High Definition, peculiarità, quest'ultima, tipica delle telecamere IP pure.
Più nel dettaglio, la tecnologia HDTVI è integrabile in sistemi preesistenti su cavo coassiale, con l'obiettivo di ottenere una trasmissione del segnale video in alta definizione (HD).
Il 20% del campione sceglie, poi, la tecnologia HD-CVI (brevettata da Dahua, va detto), grazie alla quale è possibile trasmettere il segnale video ad alta definizione su un normale cavo.
Infine, il 17,8% del campione opta per la tecnologia AHD - Analog High Definition, completamente compatibile con le telecamere analogiche e con qualsiasi videoregistratore, analogico o digitale.
In definitiva, secondo i risultati dell'indagine, sono i sistemi completamente IP, accanto a soluzioni mixed, ibride, a caratterizzare il trend della videosorveglianza italiana.

SUPPORTO COMPLETO E PRODOTTI CERTIFICATI GUIDANO NELLA SELEZIONE DEL BRAND

Analisi e valutazione dei rischi, elaborazione delle strategie e del piano di sicurezza, scelta delle tecnologie e degli strumenti con i quali intervenire: sono le attività che connotano la figura del Security Manager.
E, all'interno di queste attività, la scelta - e la conseguente decisione di acquisto – costituiscono il nocciolo della sua professione.
Ebbene, dai dati rilevati emerge che è il System Integrator (40,4% del campione) il "partner" per eccellenza del Security Manager nell'esplorare il mercato alla ricerca di nuovi prodotti e nuove tecnologie. Ed è sempre il System Integrator colui che lo supporta nella realizzazione dei progetti.
Anche il vendor e il progettista (indicati, entrambi, dal 34% dei partecipanti all'indagine) hanno un ruolo nella fase di scouting ma, dai dati, appare secondario rispetto a quello dell'integratore.
Certo, tutto dipende dal progetto e dalla tipologia di soluzione

SCOUTING E CRITERI DI RICERCA

A QUALE PARTNER SI AFFIDA PER LO SCOUTING TECNOLOGICO E LA REALIZZAZIONE DEI PROGETTI?

| CONSULENTE |
| 23,4% |

| VENDOR |
| 34% |

| PROGETTISTA |
| 34% |

| SYSTEM INTEGRATOR |
| 40,4% |

| INSTALLATORE |
| 34% |

| ALTRO |
| 2,1% |

COME SCEGLIE I PRODOTTI PIÙ ADATTI AL PIANO DI SICUREZZA ELABORATO?

| INCONTRO DI PERSONA I PRODUTTORI |
| 87,2% |

| SEGUO CONVEGNI/WORKSHOP/SEMINARI |
| 78,7% |

| PARTECIPO A FIERE DI SETTORE |
| 59,6% |

| D. PARTECIPO A TAVOLI DI LAVORO |
| 38,3% |

| ALTRO |
| 2,1% |

che il Security Manager sta cercando.
Dalla fase di ricerca a quella di scelta del prodotto.
E qui entra in gioco la figura del produttore. L'incontro diretto con quest'ultimo (87,2% delle risposte) è la "via" che conduce alla selezione dei prodotti con, in seconda posizione (78,7%), la partecipazione a convegni, workshop e seminari.
La partecipazione alle Fiere è, invece, al terzo posto nelle scelte degli intervistati, seguita dalla partecipazione a tavoli di lavoro.
Quali criteri vengono seguiti nella scelta del brand? Prezzo e ricchezza dell'offerta, dalle riposte fornite, non emergono quali parametri primari.
I Security Manager che compongono il nostro campione vanno oltre e indicano, al primo posto, con il 76,6% delle preferenze, il supporto completo - dal progetto alla pre e post-

QUALI CRITERI SEGUE NELLA SCELTA DEL BRAND?

| RICCHEZZA DELL'OFFERTA |
| 10,6% |

| PRODOTTI CERTIFICATI |
| 72,3% |

| SUPPORTO COMPLETO: DAL PROGETTO ALLA PRE E POST-INSTALLAZIONE |
| 76,6% |

| FORTE ETICA PROFESSIONALE |
| 57,4% |

| PREZZO |
| 34% |

| ALTRO |
| 2,1% |

installazione - e, al secondo posto (72,3%), i prodotti certificati quali tratti distintivi di un brand affidabile.
In particolare, il fatto di essere seguiti in tutte le fasi, a partire dal progetto, dallo studio della soluzione adatta alle specifiche esigenze di sicurezza fino all'installazione e al post installazione, si traduce in un rapporto di partnership destinato a durare nel tempo.

GLI INVESTIMENTI FUTURI? VIDEOSORVEGLIANZA CON VIDEO-ANALISI E TELECAMERE TERMICHE

Confrontarsi con un concetto più ampio di security, in cui sicurezza fisica e sicurezza dei dati e delle informazioni convergono: secondo l'83% dei Security Manager intervistati, questa è la nuova sfida alla quale sono chiamati.
Seguita da "fare i conti con le ricadute che l'Intelligenza

Artificiale avrà sempre di più sulla protezione di beni materiali, persone e dati" (44,7).
Due prove importanti, che li pongono a confronto con un sapere che, storicamente, non appartiene al mondo della sicurezza fisica, bensì a quello dell'informatica e del mondo digitale. Prove che chiedono loro di stare al passo, di compiere un salto culturale, iniziando a fare sempre più proprie conoscenze e abilità nuove.
Riguardo, invece, agli ambiti tecnologici in cui prevedono di fare investimenti futuri, il focus torna sulla videosorveglianza, che - lo ricordiamo - è l'ambito di applicazione sul quale il campione è più focalizzato (85% delle risposte), lo strumento sul quale maggiormente poggia la sua strategia di sicurezza. Infatti, il 78,7% dei nostri Securiy Manager conta di investire su telecamere con algoritmi di video-analisi a bordo (riposta che si riallaccia alla seconda sfida che è chiamato ad affrontare, ovvero al confronto con soluzioni dotate di AI) e il 53,2% sulla videosorveglianza con telecamere termiche.
Le prestazioni delle telecamere di videosorveglianza con intelligenza artificiale a bordo, oggi, sono molteplici e vanno dal riconoscimento facciale al conteggio di persone e veicoli, dal tracciamento degli spostamenti di soggetti,

NUOVE SFIDE E ORIENTAMENTI

SU QUALI ATTIVITÀ PREVEDE DI CONCENTRARSI NEI PROSSIMI 12-18 MESI?

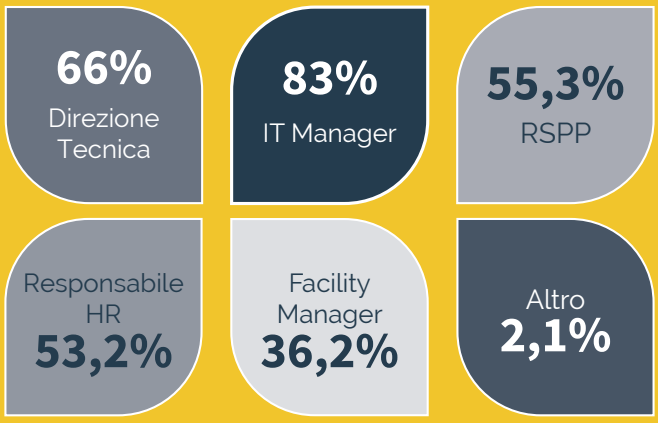
- TRACCIARE CASISTICHE LEGATE A NUOVI RISCHI — 51,1%
- AGGIORNARE LE PROCEDURE AZIENDALI LEGATE ALLA SICUREZZA — 61,7%
- DEFINIRE AUDIT SPECIFICI E FARE RIUNIONI MIRATE AL MONITORAGGIO DEI PUNTI CRITICI DELL'AZIENDA — 72,3%
- INTERAGIRE CON LA TERRITORIALITÀ, CREANDO RAPPORTI CON LE FORZE DELL'ORDINE — 40,4%
- ALTRO — 2,1%

IN QUALI AMBITI TECNOLOGICI PREVEDE DI FARE INVESTIMENTI FUTURI?

- PROTEZIONE VOLUMETRICA — 21,3%
- PROTEZIONE PERIMETRALE — 48,9%
- RICONOSCIMENTO BIOMETRICO — 31,9%
- VIDEOSORVEGLIANZA CON VIDEO-ANALISI — 78,7%
- VIDEOSORVEGLIANZA CON TELECAMERE TERMICHE — 53,2%
- VIDEOREGISTRAZIONE — 25,5%
- RIVELAZIONE DI FUMO — 6,4%
- RIVELAZIONE DI TEMPERATURA — 10,6%
- I. SISTEMI DI SPEGNIMENTO — 6,4%
- ALTRO — 2,1%

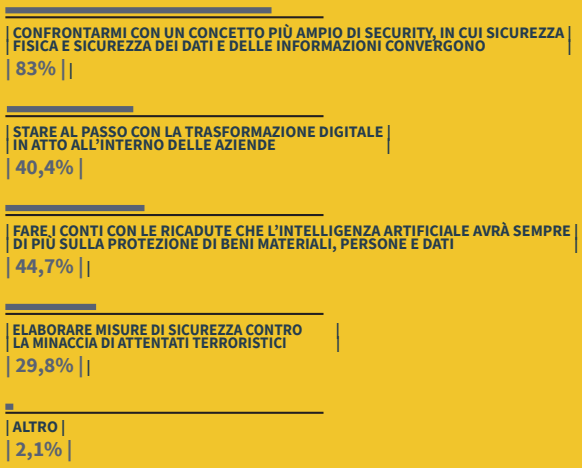
oggetti e mezzi di trasporto, fino all'analisi comportamentale delle persone, al rilevamento della velocità dei veicoli e al livello di densità del traffico.
Dunque, sono queste le tecnologie e i prodotti sui quali gli intervistati sono orientati, sempre facendo i conti con il GDPR e con quanto prevede per questo tipo di telecamere, primo fra tutti l'obbligo della valutazione di impatto sulla protezione dei dati (D.P.I.A. - Data Protection Impact Assessment), documento di valutazione preventiva dei rischi derivanti dal trattamento dei dati che si intende effettuare.
Rischi per la libertà e per il diritto alla privacy di tutti coloro che potrebbero essere ripresi da telecamere intelligenti, dotate di video/audio-analisi.

CON QUALI FIGURE PROFESSIONALI SI RAPPORTA ALL'INTERNO DELL'AZIENDA?



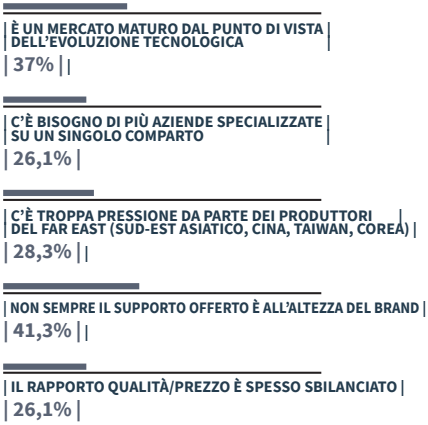
Un'altra area di investimento è rappresentata dalle telecamere termiche. Si tratta di una tipologia di telecamera che, riproducendo le immagini attraverso la rilevazione delle temperature di corpi e oggetti, non ha bisogno di luce per funzionare. La scelta di questo tipo di dispositivo video, quindi, è data dall'esigenza di fare fronte a problemi legati alle condizioni di luce - ombre, retroilluminazione, buio totale - nell'ambito di applicazioni che vedono al centro vasti perimetri e zone particolarmente a rischio per attività sospette.
I "bisogni", in termini di prodotti e tecnologie,

QUALI NUOVE SFIDE È CHIAMATO AD AFFRONTARE?



dei Security Manager che hanno preso parte alla nostra indagine, sembrano ruotare attorno a due categorie di apparati video, lontane tra loro sotto il profilo tecnico e delle prestazioni, ma molto vicine in quanto a obiettivi, che sono quelli di un video-controllo sempre più analitico e puntuale in tutte le condizioni, per un'azione anticrimine più decisa e più profonda.

QUAL È IL SUO PARERE SUL MERCATO ITALIANO DELLA SICUREZZA?

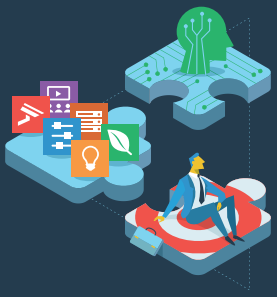


“Grazie a tutti i Security Manager
che hanno dedicato il loro
tempo alla nostra indagine”

TECNO

Nel complesso mercato dell'elettronica e delle sue applicazioni, siamo la bussola che guida chi realizza sistemi intelligenti e chi li integra.

Tracciamo percorsi per mettere in relazione la domanda e l'offerta



Siamo il partner che valorizza le aziende nell'ecosistema

RICERCHE DI MERCATO

LEAD GENERATION

COMUNICAZIONE

EVENTI

FORMAZIONE

seguici su:

www.lumi4innovation.it

TECNO

LUMI
4 INNOVATION

Il portale che racconta il nuovo mercato dell'integrazione
per i professionisti dell'ambiente costruito
(progettisti, system integrator, installatori, facility manager,
energy manager, security manager, CTO)