N. 75 - 2024 - WWW.SNEWSONLINE.COM

S News

Exprivia e il futuro dell'ICT: AI, ESG, CyberSecurity

I PRINCIPALI EVENTI *del settore*

STORIE E TESTIMONIANZE *degli Stakeholders della Sicurezza*

NIS2 E STRATEGIA UE *nella Cybersicurezza e Resilienza*

ELAN®
CAVI & BATTERIE

CRESCE LA FAMIGLIA DEI CAVI CERTIFICATI

Abbiamo aggiunto tre nuovi cavi certificati alla nostra linea ELANFIRE EN50200 PH120

Cavi segnale twistati e schermati resistenti al fuoco.
Certificati con una classe di reazione al fuoco Cca – s1a, d0, a1

info@elan.an.it - elan.an.it
+39 071 7304258

SCARICA I CATALOGHI

paso
Since 1973

Soluzioni innovative per la progettazione della sicurezza antincendio

ROUTE EN 54

Scopri il nuovo format di eventi formativi dedicati a Progettisti, Professionisti della Sicurezza Antincendio, Installatori e Distributori.

Aggiornamenti tecnico-normativi e case studies sul mondo della progettazione antincendio.

www.route-en54.it

safetyexpo 2024 Fiera di Bergamo | 18/19 Settembre 2024 | Pad. B - Stand 9/4

AM1000CL – AM2000CL – AM6000CL

Centrali indirizzate di Rivelazione Incendi con Protocollo clip

Notifier Italia presenta la nuova gamma di centrali di rivelazione incendi AM-CL, adatte per ampio range di configurazioni impiantistiche. Il sistema offre soluzioni di rivelazione incendio integrate per moltissime applicazioni, tra cui alberghi, uffici commerciali e scuole.

Le centrali dispongono di loop di comunicazione basati sull'affidabilità e retrocompatibilità con tutti i nostri dispositivi di campo. La programmazione della centrale avviene tramite tool di configurazione da PC (PK-AMCL). Inoltre le centrali sono predisposte per la gestione dell'impianto mediante postazione in rete locale, tramite i sistemi di supervisione Notifier, oppure con Honeywell CLSS - Connected Live Safety Services, piattaforma cloud che monitora il sistema sotto tutti gli aspetti; dalla manutenzione al controllo dello stato di ogni singolo componente del sistema.

La centrali AM1000CL, AM2000CL e AM6000CL sono certificate in conformità alle normative di riferimento UNI EN 54-2, UNI EN 54-4 e UNI EN 54-13.

www.notifier.it

Notifier Italia S.r.l.
Via Achille Grandi 22
20097 San Donato Milanese (MI)
Tel.: +39 02 51 89 71
Fax: +39 02 51 89730
notifier@notifier.it

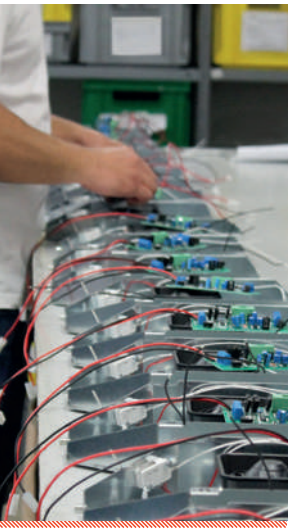
NOTIFIER® by Honeywell

La collaborazione dei saperi nella sicurezza

a cura di Monica Bertolo e di Alessandro Cherubin

Tutti sottolineiamo a gran voce che il momento attuale è complesso, perché l'iperveloce evoluzione tecnologica in atto ci obbliga a riconsiderare i nostri approcci al lavoro, alla sfera socio-politica, alla vita. Esempio lampante di questa necessità viene dato da Domenico Raguseo, Head of CyberSecurity di Exprivia, nel suo intervento all'evento sull'AI e la NIS2 recentemente tenutosi a Milano. "Le innovazioni dirompenti sono spesso divisive, tra chi le considera la soluzione ai mali dell'umanità e chi invece la fine dell'umanità stessa. [...] La realtà è che l'AI è oggi, e l'innovazione non può rallentare: si deve fare il possibile per regolarla".
Di fronte a tali sfide, i concetti di interdisciplinarità e progettualità – temi principali di questo numero Speciale – si stagliano: il successo di una nostra risposta non può prescindere dall'attingere da una vasta area di competenze nel piano dello scibile, che si estende sia in orizzontale (attraverso discipline) sia in verticale (attraverso fasi diverse di un progetto). Ma il mondo di oggi è molto diverso da quello del Rinascimento, la griglia che separa le aree di competenza di ognuno ha la trama così fitta che coprire tali superfici implica la collaborazione tra figure specializzate.
Ecco che tutto ciò che contribuisce a facilitare la messa a fattor comune di eccellenze specifiche è più che mai rilevante; rientrano in questa categoria la consapevolezza stessa dei benefici delle collaborazioni e la conoscenza di potenziali partners con cui stabilirle. Per queste ultime, noi di S News da sempre crediamo di poter dare un apporto. Lo facciamo ancora una volta, trasmettendo le testimonianze degli stakeholders del settore, variegate nei profili e negli approcci.

Exprivia e il futuro dell'ICT: AI, ESG, CyberSecurity



AMC: potenziale storico e rinnovamento odierno per la crescita in Italia e all'Estero

HIKVISION

POLYMER CAMERA

C5-M

NEMA 4X

SCOPRI
LA TELECAMERA
POLYMER 8"

PERFORMANCE & RESISTENZA A 360°

La nuova Speed Dome 8" in poliammide rinforzata è un concentrato di tecnologia racchiuso in un innovativo housing anticorrosivo che coniuga leggerezza e resistenza in un nuovo paradigma prezzo-prestazioni. Certificata NEMA 4X e C5-M, questa telecamera dalle dimensioni compatte è ideale per la protezione degli ambienti altamente corrosivi, come l'industria chimica e le zone soggette a salsedine. La sua immunità alle correnti galvaniche, contrariamente ad ogni altro materiale, la rende inoltre la soluzione definitiva per i porti e i cantieri nautici. Dotata delle migliori tecnologie di ripresa, come DarkFighter e AcuSense, di una risoluzione 4 MP e di un potente zoom ottico e digitale, garantisce immagini nitide e dettagliate anche in assenza di illuminazione per una protezione senza compromessi anche nelle situazioni più critiche.

Hikvision Italy
Vittorio Veneto | Roma | Milano | Bologna | Napoli | Bari | Palermo
info.it@hikvision.com
www.hikvision.com/it

SOLUTION
Exclusive Selection

EL.MO. e l'Atelier D-Factory: insieme per un business più sicuro

SOS Arctic WindSled Expedition: Esplorando l'Artico con le batterie FIAMM

tp-link | VIGI

Security Never Shuts Down

VIGI

Sistemi di videosorveglianza con gestione centralizzata da remoto

VIGI è la gamma professionale di TP-Link dedicata alle attività di videosorveglianza in scenari enterprise. Funzionalità avanzate di Smart-AI, unite alla semplicità di installazione e alla qualità dei prodotti a marchio TP-Link, operano insieme per garantire la sicurezza di spazi indoor e outdoor con attività di monitoraggio personalizzabili in base alle esigenze del business.

- Riprese ad alta definizione
- Smart AI e personalizzazioni
- Connettività Ethernet o Wi-Fi
- Installazione Plug & Play
- Numerose opzioni di storage
- Supporto ONVIF
- Microfono e speaker integrato
- Allarme integrato

Exprivia e il futuro dell'ICT: AI, ESG, CyberSecurity

Incontriamo Domenico Favuzzi, Presidente e AD Exprivia, Domenico Raguseo, Head of CyberSecurity e Rosita Galiandro, Responsabile Osservatorio CyberSecurity.

a cura di Monica Bertolo

Dottor Favuzzi, chi è Exprivia oggi, quali i suoi punti di forza, a chi si rivolge, quali la valenza e l'apporto operativo che può offrire ai propri clienti?

Il **Gruppo Exprivia** è tra i **principali player italiani della trasformazione digitale**. L'anno scorso – lo dico con orgoglio – abbiamo per la prima volta **superato i 200M€ di ricavi**. Un risultato straordinario, anche superiore alle attese. Contestualmente abbiamo anche superato i **27M€ di EBITDA**. In poche parole, un'**azienda sana** e **in crescita costante** negli anni. In un mercato ICT in cui sempre più soggetti sono acquisiti in toto o in parte da capitali stranieri, rivendichiamo fra l'altro di essere **un player davvero italiano, nel senso che tutti i nostri shareholder sono italiani**. Exprivia conta oggi **2.500 professionisti** in diversi ambiti della tecnologia e digitalizzazione: dall'Intelligenza Artificiale alla Cybersecurity, dai Big Data al Cloud, dall'IoT al BPO, dal Networking alla Collaboration, dal CRM all'ERP, con particolare riferimento al presidio dell'offerta SAP.

Abbiamo importanti clienti in **tutti i principali settori di mercato**: Banking, Aerospazio, Energy & Utilities, Sanità, Pubblica Amministrazione, Manufacturing, Telco, etc. Exprivia è inoltre presente anche in **6 Paesi esteri** tra **America, Asia e Europa** con un focus particolare su **Spagna, Brasile** e **Cina**. Recentemente abbiamo anche annunciato l'apertura di una **subsidiary in India**.

Per quanto riguarda l'Italia abbiamo sedi a **Milano, Roma, Trento, Vicenza, Matera, Lecce, Palermo** e a **Molfetta**, vicino a Bari, dove è basato l'**Headquarter** e dove è cominciata questa storia di successo. La storia di una **società pugliese dell'ICT**, che si è nel tempo allargata fino a coprire tutto il territorio nazionale e a sviluppare una **strategia di espansione anche all'estero**.

Entusiasmante quanto ci ha appena narrato! Ora, guardando in prospettiva, come a suo avviso si svilupperà il settore? Quali saranno le prossime sfide e quali le risposte di Exprivia alle future necessità?

La digitalizzazione – che è sotto gli occhi di tutti – è un fenomeno che sta davvero **trasformando il mondo in cui viviamo** e operiamo quotidianamente. L'impatto delle

Domenico Favuzzi

tecnologie digitali è oggi davvero **dirompente: solo con importanti investimenti ICT le imprese italiane possono recuperare il gap di produttività**, che si è purtroppo venuto a creare dagli anni '90 del secolo scorso in avanti. Bisogna riconoscere che i vari governi che si sono succeduti hanno perfettamente compreso la tematica e hanno correttamente **indirizzato verso il digitale** molti degli investimenti previsti nel **PNRR**, con uno sguardo particolarmente attento alla **Pubblica Amministrazione**, che deve appunto diventare protagonista della trasformazione digitale, così da migliorare la vita quotidiana dei cittadini. Pensiamo, a puro titolo di esempio, alla riduzione delle code nella sanità o alla facilità nel gestire le richieste di documenti verso la PA.

Ora, **nel futuro di Exprivia**, vedo **tre grandi direttrici evolutive** che si possono declinare con azioni di **ricerca e sviluppo**, con **azioni verso il mercato** e con **azioni di adoption interna**.

• Innanzitutto, l'**Intelligenza Artificiale**, che sta diventando sempre più pervasiva. In tempi non sospetti, sostenevo che l'AI sarebbe coincisa con un **fenomeno davvero rivoluzionario** e i recenti accadimenti lo stanno confermando. L'AI nei prossimi anni avrà un **impatto dirompente sul mercato ICT**, integrando strumenti e tools esistenti. Molti processi verranno radicalmente semplificati e velocizzati, liberando risorse preziose. Lo sviluppo stesso del Software verrà rivoluzionato. **Exprivia** sta investendo da tempo in questa direzione e vuole anzi


Domenico Raguseo

configurarsi come un **punto di riferimento per le tecnologie AI in Italia**.

• Parlo poi di tematiche **ESG**; i nostri clienti ci chiedono sempre più spesso un supporto per aiutarli ad indirizzare con la tecnologia i loro processi di **supporto all'ambiente, all'inclusione, alla sostenibilità a 360°**. Noi stessi, al nostro interno, stiamo sempre più investendo in processi e prassi che ci consentano di essere quanto mai aderenti agli obiettivi ESG.

• Infine, la **CyberSecurity**, che è poi il vostro tema d'elezione. Naturalmente tutto il processo d'inevitabile ed auspicabile digitalizzazione porta, come effetto collaterale indesiderato, un **aumento** delle superfici di esposizione e quindi dei **rischi informatici**. Ormai gli attaccanti malevoli possono rivolgere le loro attenzioni a **qualunque settore del vivere quotidiano**: dalla sanità alle grandi infrastrutture critiche. **Proteggersi adeguatamente** è un **diritto** e un **dovere** e Exprivia in questi anni ha sviluppato un'offerta distintiva in ambito Cybersecurity.

Ecco, entriamo ora, dottor Raguseo, più nel dettaglio della vostra factory dedicata alla CyberSecurity. Quali sono i suoi aspetti distintivi?

Il mercato della Cybersecurity è estremamente **frammentato e in continua evoluzione**, spinto da **questioni geopolitiche, innovazioni tecnologiche e motivazioni criminali** che tendono a sfruttare l'irreversibilità del processo di digitalizzazione da cui dipende, come detto prima, la vita delle aziende e delle persone. Per indirizzare le necessità di un mercato così articolato, Exprivia propone un **approccio olistico ai servizi di Cybersecurity**, utilizzando un modello di **delivery estremamente flessibile**. Pertanto, dall'identificazione del rischio fino alla gestione dell'incidente, passando per attività di monitoraggio della sicurezza sia in ambito IT che OT, Vulnerability Assessment e Penetration Test, Security by Design, Zero Trust, Exprivia ha una **capacità di proposta** che copre qualunque necessità con i **migliori partner** vendor selezionati e con **personale certificato**, sia sui processi che sulle tecnologie stesse, lasciando al cliente la possibilità di avere il servizio erogato a casa propria, oppure tramite il **Security Operation Centre (SOC)** localizzato nell'headquarter di Bari.

Exprivia si rende anche conto delle necessità del mercato di **ottimizzare gli investimenti senza disperdere energie** utili in attività e processi, o in contesti e territori diversi dal proprio. Per questo abbiamo deciso di dotarci di un **servizio di Threat Intelligence**

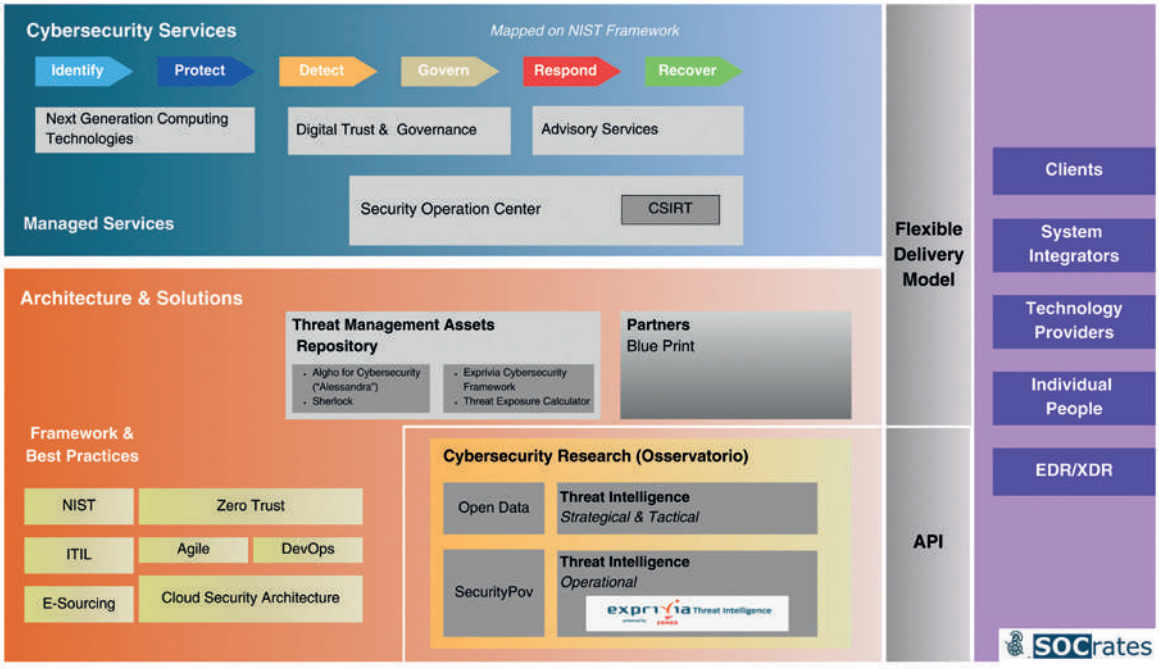
di carattere strategico, tattico e operativo.

In che senso, nello specifico? E qui mi rivolgo alla dottoressa Galiandro.

Dotandosi di un **Osservatorio Cybersecurity**, che si occupa di raccogliere e registrare eventi di sicurezza informatica. Parliamo di attacchi informatici, incidenti di sicurezza e violazioni della privacy, censiti attraverso un'analisi di fonti **OSINT**. Tali record, successivamente analizzati, processati e classificati adoperando strumenti tra cui il framework **MITRE ATT&CK®** , sono utilizzati per **produrre un Threat Intelligence Report periodico** (con cadenza trimestrale e personalizzato secondo eventuali specifiche richieste del cliente), che fornisce una **valutazione strategica ed operativa**, completa di evoluzioni e approfondimenti in termini di Tecniche, Tattiche e Procedure (**TTP**) adoperate dagli attaccanti, nonché sull'andamento del cybercrime e delle minacce informatiche. Questo supporto consente ai clienti di **prendere decisioni** strategiche informate e di implementare efficaci misure di mitigazione e protezione.

Oltre al contributo strategico e operativo, Exprivia offre anche un **supporto tattico**. I suoi **analisti** conducono una ricerca continua di vulnerabilità e Indicatori di Compromissione (**IoC**) relativi a minacce emergenti, utilizzando anche strumenti di Intelligence delle minacce di terze parti, per garantire un servizio completo ed efficiente. I dati raccolti vengono condivisi con il cliente, tramite canali di comunicazione concordati in una fase preliminare.


Rosita Galiandro



ABBIAMO AUMENTATO LO SPAZIO PER FAR CRESCERE LE NOSTRE NUOVE IDEE

EEA
ELECTRONIC
EQUIPMENTS
ANTINTRUSION

DETECTION

MADE IN ITALY

www.eea-security.com

Nasce Route EN 54:
l'evento PASO sulla progettazione antincendio. Prima tappa a Como

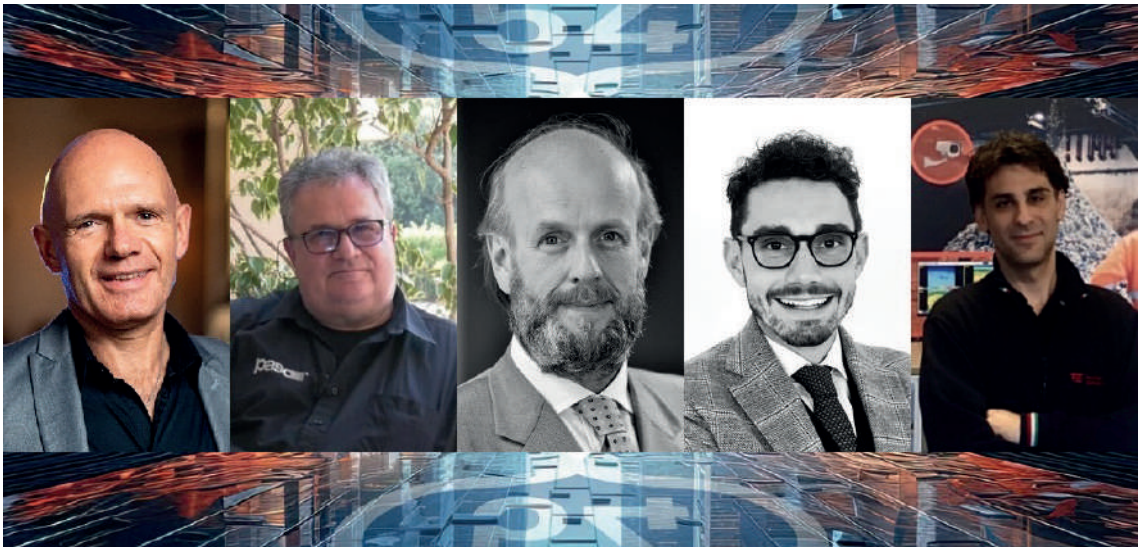
a cura di Monica Bertolo

Grande ed entusiastico riscontro alla **prima tappa** di **Route EN 54**, l'evento sull'**alta formazione** di **PASO**, in collaborazione con **Thermostick**, sulle **Soluzioni innovative per la progettazione della Sicurezza Antincendio**.
La tappa d'apertura del nuovo format, dal nome decisamente evocativo, si è tenuta nella suggestiva cornice del **Lago di Como** all'Hilton Lake Como mercoledì 12 giugno.

Per scoprire di che cosa si tratta S News ha incontrato **Antonio Faccioni**, Amministratore Delegato **PASO S.p.A.** con **Roberto Megazzini**, Direttore Tecnico Commerciale e **Agostino Dello Monaco**, Amministratore Delegato **Thermostick Elettronica Srl** con **Davide Barillà** Direttore Commerciale e **Daniel Frazzica**, Direttore Tecnico.

Perché nasce Route EN 54?

(A.F.) Da sempre PASO collabora strettamente



Antonio Faccioni e Roberto Megazzini di Paso, Agostino Dello Monaco, Davide Barillà e Daniel Frazzica di Thermostick Elettrotecnica

allo **sviluppo dei progetti**, sia con i progettisti che, tramite le nostre agenzie, con gli end users, fornendo anche supporto sul fronte delle normative oltre che sugli aspetti prettamente tecnici e tecnologici. Ci siamo così resi conto che c'è sempre più una **forte convergenza tra questi fattori**, determinanti per chi progetta.
Considerato poi che oggi PASO spazia su tutta la gamma antincendio, dall'EVAC sino ai **sistemi di aspirazione**, abbiamo ritenuto vincente strutturare un format d'evento che possa presentare **soluzioni innovative per la progettazione della sicurezza antincendio**.
Nasce così **Route EN 54** che mette assieme le **normative** di settore, le **tecnologie** e le **best practices** che abbiamo sviluppato in **anni di esperienza sul campo**.

Chiarissimo. E questo nome così evocativo e al contempo curioso, da dove deriva?

(R.M.) Volevamo un nome breve ed esaustivo, facile da ricordare e anche simpatico, ma che non sminuisse il **vero obiettivo** di questi nuovi seminari: **la formazione e la prevenzione nella progettazione della sicurezza antincendio**. Viaggeremo, dopo la prima tappa di Como, lungo la nostra bellissima Italia per incontrare Progettisti, Professionisti della Sicurezza Antincendio, Installatori e Distributori. Come fatto a Como, desideriamo creare **un'atmosfera colloquiale**, cercando di **coinvolgere il più possibile i partecipanti** per rendere ogni incontro decisamente **interessante e costruttivo per tutti**. Sarà un viaggio straordinario e stimolante con collaboratori e partners eccezionali, tutti animati da grande passione. Forse tutto questo **viaggiare** con un fine così ambizioso è un poco utopistico… quasi un sogno! Ed ecco la scintilla che accende il fuoco (tanto per restare in tema): la parola 'sogno'. Per me, oramai 'falso giovane', il viaggio da sogno resta sempre quello lungo la **Route 66** (il mitico coast-to-coast). A questo punto l'immagine della nostra locandina inizia a delinearsi: un logo con lo **scudo di protezione dal fuoco**, il numero **54** e, per non lasciar dubbi, il suffisso EN delle norme. Abbiamo così trovato un modo semplice per richiamare l'idea di un itinerario di tappe formative sulla protezione e la sicurezza antincendio, con anche il riferimento alle norme EN 54. Ma non soddisfatto e incuriosito mi sono chiesto: ma dove inizia la vera Route 54? Immediatamente consulto internet e trovo che la **U.S. Route 54 inizia da 'El Paso'**. Beh, 'Nomen omen': così è nata ROUTE EN 54!

Genesi avvincente! Tornando a lei ingegner Faccioni, molto strutturato il programma e già definito il calendario per il 2024, ci risulta.

(A.F.) Certo. Route EN 54 nasce come **progetto strutturato**, con una **visione a lungo termine**, che per quest'anno vede **3 tappe**: la prima tenutasi a **Como** per poi proseguire su **Parma** in ottobre e su **Firenze** a novembre. Da sempre siamo promotori e forti sostenitori della **formazione di alto livello** nei confronti dei progettisti e degli operatori del settore antincendio. Le normative evolvono continuamente e l'aggiornamento è indispensabile. Ancora più veloce è l'innovazione tecnologica e di processo. Se a questo aggiungiamo i molti **case studies** che

Un momento del Seminario con il Comandante Provinciale VV.F. di Como. Ing. Claudio Giacalone e parte dei partecipanti in sala.

possiamo testimoniare in **varie verticalità di mercato**, ne esce un **format completo**, che permette a chi ha il compito di sviluppare un progetto di potersi **aggiornare e confrontare** su casi reali, con professionisti ed **esperti che operano sul campo tutti i giorni**, specializzati in questo settore, con esperienza a livello nazionale ed internazionale. Alto lo standing dei relatori, che vedono sempre un **Comandante dei Vigili del Fuoco** tenere il primo intervento, l'**ing. Dario Nolli**, esperto che tutti conoscono e stimano, il nostro **ing. Roberto Megazzini**, che oltre alla grande preparazione ha anche una spiccata abilità (da tutti riconosciuta) nel saper trasmettere nozioni, sia teoriche che pratiche, senza annoiare i discenti, e l'esperto in sistemi di rivelazione di fumo **Daniel Frazzica** di **Thermostick**, azienda che con noi promuove e diffonde con Route EN 54 l'alta formazione per la progettazione della sicurezza antincendio. Per la parte logistico/organizzativa collaboriamo con l'Associazione **Prevenzioneincenditalia**, nostra partner anche in altre iniziative da anni, e non poteva certo mancare la media partnership di **S News**, che da sempre ci segue con professionalità sul fronte della comunicazione di settore.

Benissimo e grazie ingegner Faccioni. Rivolgendomi a lei ingegner Dello Monaco ed a lei ingegner Barillà, quale l'apporto di Thermostick Elettronica a Route EN 54?

(A.D.M.) e (D.B.) Quando PASO ci ha proposto di collaborare su questa iniziativa, abbiamo accettato subito e con entusiasmo. Per un'azienda come la nostra **specializzata in rivelazione incendi** è importante **comunicare il nostro approccio alle differenti soluzioni oggi richieste sul mercato**. Thermostick, grazie alla sua lunga esperienza iniziata nel 1964, oggi riesce a proporre valide soluzioni per **numerosi campi di applicazione, con l'ausilio di performanti ed innovative tecnologie**. Focalizzando il nostro obiettivo sulla passione per le nuove tecnologie applicate alla rivelazione incendi e guardando oltre quanto era già presente sul mercato, siamo orgogliosamente riusciti a **proporre e rendere consueti prodotti innovativi** che hanno **migliorato la metodologia di rivelazione** in alcuni campi di applicazione. Sono proprio la **nostra esperienza**, con le abilità maturate in tanti anni sul campo, **l'apporto tecnico e formativo** che possiamo dare **a Route EN 54**.

Addentrandoci quindi nelle tematiche, quali i contenuti e le dinamiche del format, ingegner Megazzini?

(R.M.) L'attenzione viene focalizzata sulle **normative**, sullo **stato dell'arte**, sulle **tecnologie**, e sulle **best practices** che convergeranno per **individuare le soluzioni più innovative** nel campo della **progettazione** della **sicurezza antincendio**, il tutto in **un'atmosfera costruttiva** e **sinergica**.
Ad aprire i lavori sarà sempre il Comandante dei Vigili del Fuoco, nel caso di Como l'**Ing. Claudio Giacalone**, che approfondisce la **rivelazione incendi attraverso le regole tecniche di prevenzione incendi**.
L'intervento dell'**Ing. Dario Nolli**, uno dei massimi esperti in materia di rivelazione automatica d'incendi e riferimento del settore in termini di consulenza tecnica, ci porta nel mondo dei **sistemi IRAI**, con una **panoramica di tutte le nuove normative pubblicate**.
Ovviamente io richiamo l'attenzione sull'**evoluzione tecnico-normativa dei sistemi di evacuazione vocale** con tutti i necessari riferimenti al **Nuovo Codice di prevenzione incendi** e presento un **case history**, evidenziando le soluzioni adottate nel rispetto delle normative e sulla base delle varie richieste tecnico funzionali di progetto. Non tralascio di parlare anche di **Fire Safety Engineering**, un **approccio ingegneristico innovativo e altamente efficace** per garantire la sicurezza antincendio.
A tutti gli interessati consiglio di visitare il nostro sito web, **www.route-en54.it**, dove è possibile seguire tutte le tappe, consultare i programmi e, ovviamente, **registrarsi ai seminari**.

Molto bene. Mi rivolgo ora a lei Frazzica. Quale il suo contributo all'interno del format?

(D.F.) L'innovazione tecnologica ha un ruolo fondamentale nel settore della prevenzione incendi. Il seminario tecnico-formativo è focalizzato principalmente su due tecnologie e relative normative: **sistemi di aspirazione fumi ad aspirazione a campionamento e rivelatori ottici lineari di fumo**. Tali tecnologie sono oggi molto utilizzate nei sistemi per la rivelazione precoce del fumo e andiamo quindi a descrivere in dettaglio la **procedura per la progettazione, installazione e manutenzione degli stessi**. Discutiamo e affrontiamo gli argomenti evidenziando **quali siano i vantaggi tecnici e applicativi** dei sistemi presi in considerazione e **condividiamo con i presenti le nostre esperienze**.

www.saltosystems.com/

Accesso intelligente senza chiavi e tramite smartphone:

Il modo più efficiente, sicuro e conveniente per proteggere il tuo edificio e le tue risorse.

Senza cablaggi
Stand-alone, virtualmente in rete
serrature intelligenti senza cablaggi

Digital key - BLE /NFC & RFID

SVN
SVN-Flex
BLUEnet Wireless
JustIN Mobile

Costruita per coprire qualsiasi punto di accesso

Gestisci facilmente la sicurezza del tuo sito 24 ore su 24, 7 giorni su 7 con una tecnologia di chiusura elettronica avanzata e affidabile che soddisfa tutti i requisiti di sicurezza. Garantisci la sicurezza e l'accessibilità della struttura per gestire in modo efficiente il tuo edificio fornendo una migliore esperienza senza chiavi e tramite smartphone al tuo utente.

Facile retrofitting: Queste soluzioni rendono possibile l'accesso intelligente su qualsiasi porta.

Tecnologia di accessi Smart: Piattaforma di gestione del controllo accessi ad alte prestazioni per semplificare l'esecuzione di attività critiche e di routine.

Accesso senza chiavi: Soluzioni tecnologiche per il controllo accessi on-premise e basato su Cloud compatibili con dispositivi mobili.

Sicurezza all'avanguardia: Gestisci chiavi digitali, monitora tutte le attività della porta e assegna diversi livelli di accesso agli utenti.

Cilindro Elettronico: SALTO Neo

Serratura Elettronica: SALTO XS4 One

Lucchetto Elettronico: SALTO Neoxx

SALTO Systems srl
Tel.: +39 051 72 77 98 | **Email:** info.it@saltosystems.com | **www.saltosystems.com**

SALTO inspiredaccess

TKH Security:
il Meeting Landmarks Italia 2024!

a cura di Monica Bertolo

Nella splendida cornice di Verona, il 28 e 29 Maggio **TKH Security Italia** ha riunito **l'intero gruppo di lavoro Nazionale "LandMarks Italia"**.
È stata un'**Edizione Speciale**, durante la quale si è celebrato il **decennio del progetto "LandMark... il Piacere di Condividere Successi"!**
I LandMarks Italia sono un gruppo di **Distributori Professionisti** con i quali TKH Security Italia, nel corso del decennio, ha **condiviso il proprio business**.
Per saperne di più, incontriamo l'ingegner **Denis Nadal**, AD di TKH Security.

Ingegner Nadal, questo evento ha registrato numeri da record a livello di presenze. A cosa attribuisce un tale successo?

Sì, proprio così, e siamo davvero fieri del risultato. A questo Meeting, edizione per noi tutti Speciale, ha partecipato **quasi l'intero gruppo di lavoro Nazionale LandMarks Italia**.
Ben **35 aziende** con **oltre 50 professionisti** in **2 giornate di lavori**. A tale proposito ringrazio la **MT Distribuzione** per averci concesso la loro **splendida nuova sede** per la prima giornata di Meeting.
È un risultato importante che premia la **nostra tenacia** nel credere in un **progetto ambizioso**, in controtendenza con le politiche di tutti i players presenti sul mercato. Abbiamo sempre creduto che fosse **strategico non inseguire sempre la ricerca del prezzo più basso**, ma proporre soluzioni di **qualità** ed una **politica commerciale seria, trasparente e riservatissima**.
Ritengo che un progetto riscontri successo se

L'ing. Denis Nadal durante l'evento

sostenuto da **professionisti che credono nelle proprie scelte**, senza lasciarsi distrarre da quanto accade sul mercato. Sono **particolarmente orgoglioso della squadra LandMarks**: un gruppo di Distributori Partners presenti sul territorio Nazionale, che per noi rappresentano il **braccio commerciale**.

Non posso dire di meno dei **colleghi interni**, che quotidianamente con **estrema professionalità** svolgono appieno le proprie mansioni con **passione**.

Il Pay-off del nostro progetto, "Il Piacere di Condividere Successi", in questi due giorni di lavoro traspariva sui volti di noi tutti.

Quali i temi trattati nel corso dei lavori?

Guardi, come ad ogni appuntamento di lavoro, tutti si aspettano novità legate a nuovi prodotti.

Abbiamo soddisfatto questa aspettativa presentando ufficialmente l'innovativo **sistema di controllo accessi ATLAS** ed alcuni **nuovi prodotti della linea TKH Skilleye**, che integreremo nel catalogo del prossimo settembre.

ATLAS è un sistema di controllo accessi estremamente innovativo, che non necessita di **alcun cablaggio**, gestito integralmente da **cloud e da smartphone**. Utilizza tecnologie **NFC e Bluetooth crittografate**, permettendo la piena operatività **anche in assenza di connettività dello smartphone**.

È una soluzione smart, semplice da gestire ma soprattutto **molto apprezzata dagli installatori**, perché riduce moltissimo i tempi di installazione.

La parte sicuramente più interessante però del meeting è stata quella che abbiamo dedicato a **sviluppare un nuovo progetto**, che mi auguro ci vedrà protagonisti nei prossimi anni.

Un nuovo progetto? Di che cosa si tratta?

È un progetto che **valorizza le soluzioni esclusive del Gruppo TKH Security** ed investimenti su **percorsi formativi certificati**. Mette insieme la **forza di un grande gruppo internazionale**, TKH Security, ed una squadra di **LandMarks commercialmente e tecnicamente ben strutturati**.

Con le **molteplici tecnologie e soluzioni integrate**, sviluppate dal gruppo TKH Security, la **squadra dei nostri fedelissimi Landmarks** e la **collaborazione di diversi consulenti**, abbiamo come obiettivo quello di **far crescere la presenza del gruppo in Italia**.

A tal fine abbiamo lavorato molto nell'ultimo anno per creare tutta una serie di **tools e una documentazione** specifica per gli **studi di progettazione** e, non ultimo, abbiamo **completamente rinnovato il nostro sito tkhsecurity.com/it**.

Molto interessante. Ritornando alle due giornate di Meeting, ci risulta che non si è trattato di solo lavoro, corretto?

Sì, verissimo. È un gruppo di lavoro composto innanzi tutto da **amici**, con molti dei quali lavoriamo da 10 anni insieme. Abbiamo dedicato la giusta importanza anche ai **momenti conviviali** nella **splendida cornice di Verona, nel cuore della città**. Questi momenti rendono piacevole il lavoro, tant'è che si sono già tutti prenotati per il meeting del prossimo anno!

Perchè prendere un cane da guardia quando puoi avere QHUBO?

Moduli 4G + Wi-Fi integrati

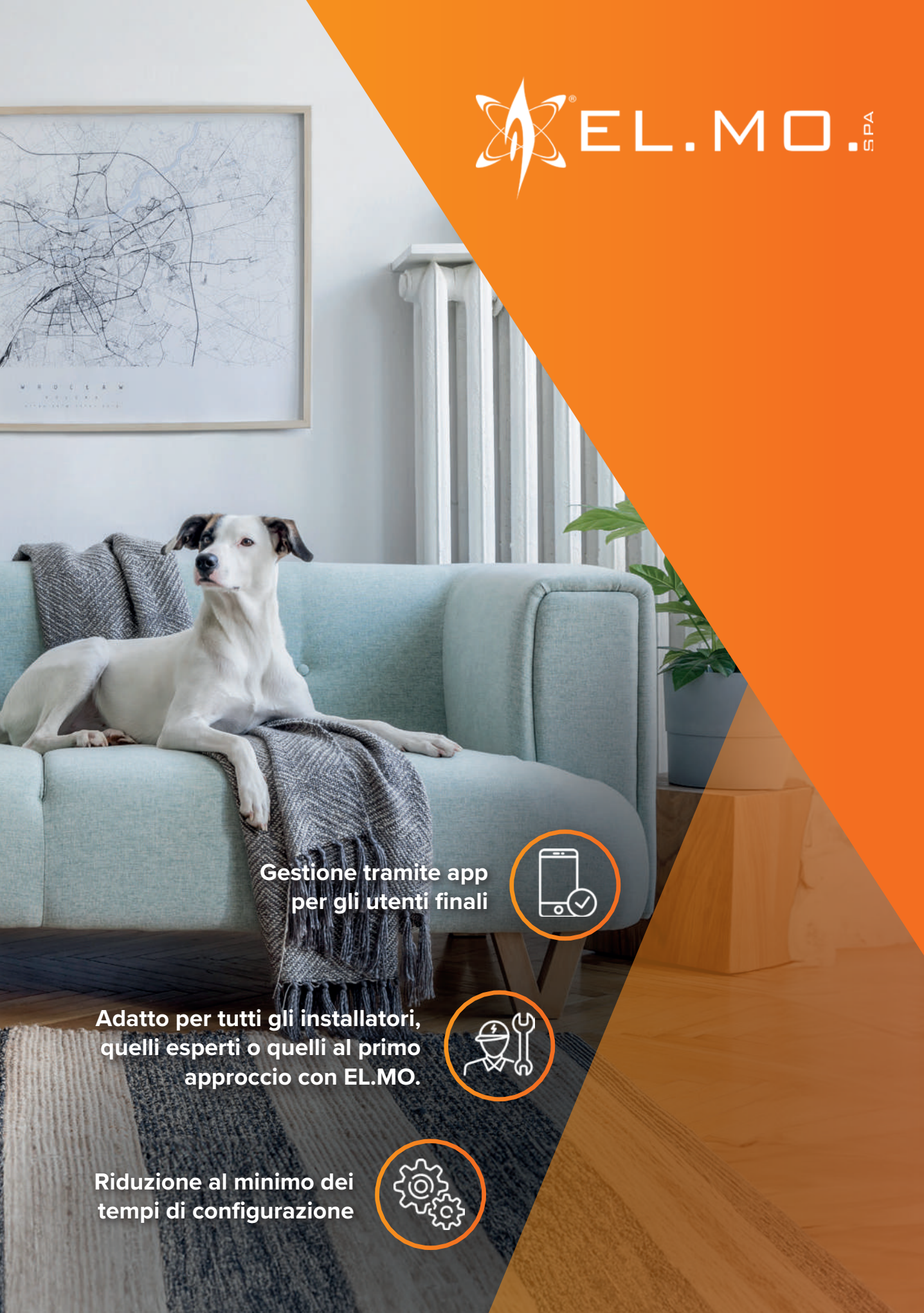
Ideale per contesti residenziali, negozi e uffici, QHUBO è l'HUB antintrusione che **unisce efficacia, semplicità d'uso, innovazione e design**.

32

Dispositivi wireless di input gestiti

8

Utenti con profili differenziati



EL.MO. SPA

Gestione tramite app
per gli utenti finali

Adatto per tutti gli installatori,
quelli esperti o quelli al primo
approccio con EL.MO.

Riduzione al minimo dei
tempi di configurazione

Evoluzione della Normativa sulla Sicurezza Antincendio nei Luoghi di Lavoro

a cura di Linda R. Spiller

Si è tenuto **venerdì 21 giugno a Mantova il Seminario Tecnico di Alta Formazione Antincendio** a cura di Eraya, Inim e Paso dal titolo **"Evoluzione della normativa sulla sicurezza antincendio nei luoghi di lavoro: dal d.m. 10 marzo 1998 ai d.d.mm. 1, 2 e 3 settembre 2021"**.
L'evento formativo, valido ai fini dell'**aggiornamento di cui all'art. 7 del D.M. 5 agosto 2011 – ex legge 818/84**, vede

il supporto operativo di Assosicurezza e la media partnership di S News.
L'incontro, che ha riscosso **attento interesse** da parte dei professionisti dell'antincendio della signorile città dei Gonzaga e dintorni, si terrà in autunno anche a Perugia.

Il Seminario: finalità e CFP

La finalità del seminario è fornire i criteri da seguire nella **progettazione, nell'esecuzione, nella verifica e nella manutenzione degli impianti secondo la regola dell'arte, ottemperando a tutte le normative vigenti**.

Tenuto da docenti certificati, il seminario è rivolto a **Progettisti, Security Managers, Distributori, Installatori** e a tutti coloro che lavorano o investono nel settore della sicurezza.

La partecipazione all'evento, della durata di 4 ore, ha consentito l'acquisizione di **n. 4 CFP, da parte dell'Ordine dei periti industriali e dei periti industriali laureati della provincia di Mantova**, ai sensi dell'art.7, comma 3 del DPR 137/2012 e del Regolamento per la Formazione Continua dei Periti Industriali e Periti Industriali Laureati.

ICMQ bu CERSA, riconosce crediti formativi ai fini del mantenimento e rinnovo della certificazione delle figure professionali **Professionista della Security** – UNI 10459:2017 (4 CFP), Perito Liquidatore Assicurativo – UNI 11628:2016 (4 CFP) e **Esperto in Impiantistica Elettronica di Sicurezza Anticrimine**.

Il Programma del Seminario Formativo di Eraya, Inim e Paso "Evoluzione della normativa sulla sicurezza antincendio nei luoghi di lavoro"

14:30 Dr. Franco Dischi – Assosicurezza – Presentazione del Seminario

- **Ing. Piergiacomo Cancelliere – Comandante Provinciale VVF di Rimini**
Evoluzione della normativa sulla sicurezza antincendio nei luoghi di lavoro: Dal d.m. 10 marzo 1998 ai d.d.mm. 1, 2 e 3 settembre 2021.

- **Ing. Roberto Megazzini – Paso Spa**
Aggiornamenti sulla normativa dei sistemi di evacuazione vocale (UNI-ISO 7240-19, UNI/CEN TS 54 - 32, EN 54-16, EN 54-24 e EN 54-4).

- **Stefano Morelli – Inim Electronics Srl**
Progettazione ed installazione dei sistemi di rivelazione incendio; evoluzione normativa delle norme attuali (UNI 9795, UNI 11224, UNI 11744).

- **Ing. Cristiano Montesi – Eraya Srl**
Obblighi dei progettisti al rispetto dei parametri relativi alle connessioni nei sistemi di rivelazione automatica d'incendio al fine di evitare malfunzionamenti, in particolare nei sistemi analogici indirizzati.

18:30 Conclusione dei lavori e aperitivo di networking tra partecipanti e relatori

Help desk gratuito

Parte del format è anche l'Help Desk Gratuito, un **numero WA sempre attivo** che viene comunicato nel corso dell'evento a cui si potranno inviare domande, richieste di chiarimenti e di informazioni nei giorni o nei mesi successivi al seminario. Sarà sufficiente fare riferimento alla data del seminario a cui si è partecipato.

eraya The Italian Power Solution

inim® Evolving Protection

paso Since 1973

Rivoluzione digitale: NIS2 e AI per una Nuova Era della CyberSecurity

a cura di Linda R. Spiller

Exprivia, in collaborazione con **Akamai, Pointsharp e Sophos**, nella spettacolare cornice del **Rooftop di Copernico Isola S32** nel cuore pulsante del fintech district milanese, ha tenuto giovedì 27 giugno l'evento **"Rivoluzione digitale: NIS2 e AI per una Nuova Era della CyberSecurity"**, che ha visto S News media partner.

L'evento si è aperto con l'intervento di **Domenico Raguseo**, Head of CyberSecurity Unit di Exprivia, con un focus dal titolo estremamente attuale: "AI between deepfake, hallucinations and adversarial AI".

A lui è seguita la presentazione dei dati del **Threat Intelligence Report** dell'Osservatorio di CyberSecurity di Exprivia, a cura di **Valeria Vetrano**, Cyber Threat Intelligence Specialist di **Exprivia**.

Un momento della tavola rotonda con, da sinistra, Marco Finocchi, Alessandro Rivara, Daniele Urbano, Luca Guarino, Monica Bertolo

La tavola rotonda

Dopo la presentazione dei dati e quindi della fotografia dello scenario della cybersecurity in Italia, ha preso il via la **tavola rotonda** che ha visto partecipare:

- **Marco Finocchi**, Senior Channel Account Executive, **Sophos**,
- **Alessandro Rivara**, Regional Sales Manager, **Akamai**,
- **Daniele Urbano**, Head of Sales CyberSecurity, **Exprivia**,
- **Luca Guarino**, Business Development Manager International, **Pointsharp**,

moderati da **Monica Bertolo**, Direttore di S News.

Indubbiamente l'**AI** e oggi sempre più la **NIS2** sono tra le protagoniste per gli addetti ai lavori della **nuova Era della Cybersecurity**. **Molti i contenuti**, su tali temi, che sono **scaturiti** dalla tavola rotonda, contenuti e approcci che hanno coinvolto i professionisti presenti, in un **clima di confronto e di condivisione**. Eccone alcuni.

"L'AI – ha sottolineato **Urbano** di **Exprivia** – **può supportare le aziende nel raggiungimento della conformità alla direttiva NIS 2**, con l'obiettivo di **ridurre i costi** e **ottimizzare le risorse** dedicate al percorso di adeguamento normativo. Inoltre può essere utilizzata nella gestione di diversi requisiti chiave della NIS 2 a partire dalla **gestione automatizzata del rischio, delle minacce e delle vulnerabilità**, fino ad arrivare alla realizzazione di programmi di formazione mirati attraverso simulazioni **realistiche di attacchi informatici**".

"A tal proposito – ha specificato **Finocchi** – **Sophos** utilizza da tempo l'intelligenza artificiale, il machine learning e la threat intelligence per realizzare servizi avanzati e, grazie alla piattaforma **cloud Sophos Central**, consente una **gestione integrata e centralizzata, sfruttando un data lake e delle OPEN API per integrare una moltitudine di soluzioni di sicurezza di terze parti**".

Rivara, a sua volta, ha evidenziato: "**Akamai**, l'azienda di servizi cloud che abilita e protegge la vita online, gestisce il **30% del traffico web mondiale**. Questa posizione consente di monitorare le tendenze dei cyber attacchi e di proteggere i clienti tramite il big data generato dalla propria infrastruttura e gli algoritmi predittivi.
Nel **primo trimestre del 2024, Akamai ha bloccato oltre 70 miliardi di attacchi web**, inclusi attacchi applicativi, sicurezza delle API, ransomware e DDoS. La piattaforma utilizza AI e Machine Learning per riconoscere utenti attendibili, rilevare bot sofisticati e migliorare le analisi di marketing. Inoltre, con la **chatbot generativa Guardicore AI e il modello Zero Trust**, Akamai supporta la **conformità alla direttiva NIS2**, che impone rigorosi controlli di sicurezza per ridurre i rischi e prevenire danni ai sistemi e ai dati. La piattaforma garantisce visibilità e protezione avanzata, elementi essenziali per la continuità operativa. Nonostante la complessità e i costi, le soluzioni di Akamai sono essenziali per proteggere gli assets aziendali e ridurre i rischi, mantenendo la **continuità operativa**. Akamai supporta decine di **Infrastrutture Critiche nazionali e Operatori di Servizi Essenziali** per migliorare la loro postura di sicurezza e garantirne la business continuity".

"**Pointsharp** – ha precisato **Guarino** – **azienda europea** specializzata nella **protezione dello scambio di dati e nella gestione sicura delle identità e degli accessi**, fornisce alle imprese e alle organizzazioni grazie alle soluzioni **IAM**, **User Authentication** ed **Information Security** strumenti per un approccio facile e sicuro, sia per gli utenti che il reparto IT".

Valeria Vetrano durante la presentazione dei dati del Threat Intelligence Report

HIKVISION: evolve la BU Solution in Project per i progetti di fascia alta

Incontriamo Massimiliano Troilo, General Manager HIKVISION Italy

a cura di Monica Bertolo

Da tempo HIKVISION ha scelto di suddividere il mercato di riferimento in Business Units focalizzate, al fine di soddisfare le esigenze specifiche di ciascun segmento. Il compito di rispondere alle sfide degli ambiti verticali più importanti e critici a livello di sicurezza è affidato ad una BU in particolare. Quali le novità a riguardo?

È di fatto iniziata una **nuova era per questa Business Unit**, a partire dal cambio di nome. Prima con il termine "Solution" si identificava sia la Business Unit, tra l'altro unica in Italia per focalizzazione e numero di persone, sia la selezione esclusiva di soluzioni altamente innovative e top di gamma non solo nell'ambito della Videosorveglianza, ma anche nel Controllo Perimetrale, Controllo e Gestione degli Accessi e della Comunicazione. Ora la Business Unit, con a capo **Francesco Panarelli**, si chiamerà **Project**. Una distinzione che distingue in maniera inequivocabile catalogo e BU operativa, per **sottolineare la nuova direzione intrapresa da HIKVISION nei confronti del mercato**.

Quale l'obiettivo della BU Project?

Attraverso **soluzioni end to end ad alte performances**, la BU si propone di fornire un **supporto specifico e continuo a System Integrator, System Installer e Security Managers**, garantendo il ritorno dell'investimento e la futuribilità delle tecnologie utilizzate. Di fronte alla crescente complessità degli scenari di mercato, la BU Project fornisce una risposta tecnologica completa, scalabile e specifica, che va oltre il semplice prodotto, con una pluralità di offerta che riflette la natura di ***Total Solution Provider*** di HIKVISION e permette di tutelare e proteggere persone, beni, infrastrutture e ambiente a 360°.

Rispetto agli anni passati, si sta consolidando sempre più la posizione di HIKVISION anche nel mercato di fascia alta. A cosa si deve questo interesse crescente da parte dei players del settore e dei loro interlocutori?

All'inizio, la BU Solution aveva un approccio più trasversale, abbracciava cioè vari mercati con una gamma diversificata di soluzioni. Oggi si può parlare di vera e propria focalizzazione e


Massimiliano Troilo

di una maggiore verticalizzazione che ha reso la BU sempre più indipendente. Questo nuovo approccio, di fatto, si traduce in un'attenzione più marcata verso le **attività di Business Development e i Progetti di fascia alta**, con lo scopo di migliorare l'efficienza operativa, la business continuity, la gestione dei flussi, l'analisi dati e il controllo dei processi nei settori particolari come **Energy, Transportation, Retail, Government, Banks e Logistic**. Un'attenzione che ha determinato anche il cambio di nome.

Quali i fattori che hanno reso possibile questa evoluzione?

Innanzitutto non dobbiamo dimenticare l'impegno in **R&D**, con investimenti che ammontano a **oltre il 12% del fatturato globale** di HIKVISION e che hanno reso possibile l'**estensione di garanzia di molti prodotti a 5 anni**. Ma ci sono altri aspetti, come l'attenzione **alla sicurezza cyber e dei dati informatici**, con l'adozione dei **più importanti standards e certificazioni internazionali** per minimizzare i rischi di vulnerabilità. Anche il software **Hik Central** e gli altri strumenti di integrazione tecnologica rappresentano un ulteriore valore aggiunto, in quanto permettono di soddisfare gli scenari unici della committenza, grazie ad una **filosofia progettuale** che garantisce apertura e estendibilità futura.

Dal punto di vista tecnologico, come si articola l'offerta Solution della BU Project?

Il Catalogo Solution è disponibile in due connotazioni diverse e complementari, che rispecchiano le esigenze dei diversi destinatari di riferimento. Il Catalogo **Dealer**, dedicato ai **Partners che intendono distinguersi nel mercato**, offre un'ampia selezione che comprende, solo per citare alcuni dei trends più importanti, telecamere con a bordo ripresa panoramica, visione notturna, Deep Learning, tecnologia termica e anticorrosione, nonché prodotti ingegnerizzati per la lettura targhe, NVR DeepInMind, sensori intelligenti, dispositivi di Public Alarm e terminali di controllo accessi.
La versione **Project**, invece, è più focalizzata sui progetti e sulle sfide tecnologiche avanzate che **vanno oltre la Security** e include, tra l'altro, Sistemi di Intelligent Trafic e di Intelligenza Artificiale in ambito di **controllo del territorio** e **Tecnologia Termica** per i progetti di salvaguardia dell'ambiente ed applicazioni industriali di controllo di processo.

Dal punto di vista dei servizi, invece, cosa offre la BU Project?

I Partners possono contare su una **squadra di professionisti** che si distingue per competenze, focalizzazione e visione strategica, composta da responsabili commerciali, team territoriali e team di supporto tecnico che, a loro volta, possono contare sugli oltre 100 dipendenti di HIKVISION Italy.

Il punto di forza è l'**approccio consulenziale** e **operativo**: non ci si limita alla proposizione di prodotti e apparati, ma offriamo servizi tecnico-commerciali di alto profilo, fornendo supporto sia ai progetti, durante la fase di definizione dei dispositivi e dimensionamento dei siti, sia nella fase post-vendita, per risolvere eventuali criticità. Inoltre, il servizio di **Help Desk e il supporto tecnico di 2° livello** sono sempre a disposizione dei partners per garantire un'assistenza completa. A tutto questo si aggiunge un **Partner Program** dedicato che offre vantaggi commerciali e tecnici specifici.

Guardando in prospettiva, quali i vostri prossimi obiettivi?

Miriamo a soddisfare le **più importanti necessità di sicurezza e gestione di spazi e persone**, tanto in ambito **pubblico** quanto in ambito **enterprise**. Il nostro obiettivo è continuare a trasferire al mercato l'attenzione alla focalizzazione che ci contraddistingue e, attraverso l'attività continua di proposizione tecnico-commerciale, essere riconosciuti come **partner tecnologico innovativo ed affidabile dai professionisti del settore e** come **risorsa fondamentale dagli utenti finali**.

OPTEX: 45 anni d'innovazione nel rilevamento e un futuro sempre all'insegna dell'eccellenza

OPTEX Sensing Innovation

Incontriamo Marco Censi, Regional Sales Manager Italia di OPTEX

a cura di Monica Bertolo

Marco Censi

Quest'anno OPTEX celebra un traguardo importante: 45 anni di storia e di costante innovazione nel rilevamento. Com'è riuscita OPTEX a diventare leader riconosciuta sul mercato?

È un onore celebrare il 45° anniversario di OPTEX, un traguardo che riflette la nostra **lunga e vincente storia**. Fin dall'inizio, siamo stati guidati da **valori** chiave come **l'innovazione costante, la qualità impeccabile e l'affidabilità**. Questi aspetti ci hanno permesso di sviluppare soluzioni di **sicurezza all'avanguardia**, che rispondono alle esigenze sempre più sofisticate del mercato. La nostra capacità di adattarci e perfezionare continuamente le tecnologie del settore, unita a una rigorosa attenzione alla qualità dei prodotti e alla soddisfazione dei clienti, ci ha permesso di costruire una **solida reputazione**. Questi elementi, insieme alla nostra rete globale di partners e alla formazione continua del nostro team, ci hanno permesso di consolidare la nostra leadership nel mercato.

Quali le peculiarità delle tecnologie di OPTEX, tali da posizionarla all'avanguardia nell'innovazione?

La nostra storia con le tecnologie per la sicurezza è un viaggio di continua innovazione. Dai primi sensori a infrarossi passivi, abbiamo inserito nel nostro portfolio tecnologie più avanzate, come i sensori con tecnologia **LiDAR** e

Toru Kobayashi, fondatore di OPTEX, con colleghi della direzione nei primi anni di attività dell'azienda

fibra ottica, passando attraverso l'implementazione della **doppia tecnologia** con la **microonda** e lo sviluppo della logica di riconoscimento del segnale potenziata digitalmente (**SMDA**) per migliorare significativamente la precisione e l'affidabilità dei sensori **per interno e per esterno**. Tutti i **nostri sensori offrono vantaggi ineguagliabili**: operano efficacemente in condizioni ambientali difficili, sono versatili e adattabili a diversi bisogni e contesti, e offrono una riduzione quasi totale dei falsi allarmi. I **feedbacks** dei clienti, dei partners, degli installatori e le **valutazioni interne** sono sempre stati e continuano ad essere spunti preziosi per perfezionare i prodotti esistenti e svilupparne di nuovi.

La sicurezza fisica richiede un'attenzione particolare, specialmente per i settori verticali come la sicurezza di infrastrutture critiche, aeroporti, data centres. Quali strategie sta adottando OPTEX per affrontare le sfide crescenti in questi settori?

OPTEX affronta le sfide quotidiane in tali settori con estremo entusiasmo e fiducia. Siamo consapevoli delle difficoltà e particolarità che dobbiamo affrontare ma, oltre alle varie **tecnologie e prodotti adatti alle varie applicazioni**, abbiamo alle nostre spalle un team estremamente preparato. Tra questi, vorrei dare il benvenuto e ringraziare personalmente **Andrea Tiberti** che, forte di **un'ultra ventennale esperienza** nel settore della sicurezza, da qualche mese fa parte del team OPTEX nel ruolo di **tecnico/pre-sales per il Mercato Italiano**. Sarà lui ad affiancare i nostri clienti nella scelta e nella formazione del prodotto o della tecnologia adatta. Tutto questo avviene in un periodo molto particolare nel quale, oltre alla **chiusura di grossi accordi con multinazionali operanti nei settori energetico, data centres e logistico**, stiamo riscontrando una sempre maggior crescita di richieste specifiche nei vari **progetti/settori**. Pertanto possiamo rassicurare tutti i nostri clienti che siamo pronti ad accettare e vincere ogni sfida che il mercato ci porrà davanti.

Guardando al futuro, quali sono le prospettive di sviluppo per OPTEX e come intende l'azienda continuare a innovare nel settore della sicurezza?

Guardiamo con entusiasmo e determinazione al futuro del settore. Le esigenze del merca-

to continueranno a evolversi, richiedendo **soluzioni sempre più sofisticate e integrate**. Le future sfide per la tecnologia del rilevamento includono la necessità di affrontare minacce sempre più complesse e di garantire un alto livello di sicurezza in diversi contesti. Il team di ricerca e sviluppo continua a studiare **nuove tecnologie**, compatibilità con protocolli sicuri e **nuovi standards di integrazione**, come il protocollo **LoRa**, per migliorare la connettività e la comunicazione nel rilevamento delle intrusioni. OPTEX è pronta a **perseverare nell'eccellenza** che da sempre la contraddistingue, offrendo soluzioni innovative e affidabili. Inoltre, ci stiamo impegnando attivamente nella preservazione dell'ambiente, attraverso l'implementazione di pratiche di **produzione sostenibile** e tramite lo sviluppo di **prodotti eco-compatibili**.

L'attenzione all'ambiente, insieme alla continua soddisfazione dei nostri clienti, è parte integrante della nostra missione, **mantenendo sempre alto il nostro standard di qualità e servizio**.

D-Pulse Advanced di EL.MO.: visione avanzata della Sicurezza

Incontriamo Salvatore Pastorello, Project Manager EL.MO.

a cura di Monica Bertolo

Non è sempre facile integrare in maniera intelligente, rapida e intuitiva diversi sistemi di sicurezza tra loro… È così, ingegner Pastorello?

Sì, è decisamente così. Molto spesso la nostra azienda si imbatte in installatori che devono operare su **impianti complessi**, dove i clienti richiedono l'**implementazione di soluzioni articolate con più opzioni**. Ad esempio, un sistema **antintrusione** autonomo potrebbe necessitare dell'aggiunta di un sistema **TVCC** per il controllo visivo degli ambienti, aumentando le specificità degli allarmi e la sicurezza complessiva. In queste situazioni, l'installatore deve valutare attentamente quali dispositivi installare, garantendo che comunichino efficacemente tra loro e che permettano al cliente di **gestire tutto da un'unica piattaforma**. Questa fase è spesso complicata e il successo dipende dalla **predisposizione dei sistemi prescelti a integrarsi in maniera efficace**.

Chiarissimo. Quale soluzione avete quindi sviluppato per far fronte a questa criticità?

Dopo aver appreso di **questa particolare esigenza da parte degli installatori**, ci siamo concentrati sullo **sviluppo di una soluzione tecnologica capace** di rilevare eventi di allarme come intrusioni, attraversamenti di linea o oggetti abbandonati tramite telecamere.
Da questo obiettivo è nata la **tecnologia D-Pulse Advanced**, che enfatizza l'integrazione tra i sistemi di videosorveglianza **e-Vision** basati su intelligenza artificiale e le nostre centrali antintrusione **PROXIMA** e **SUPERIA**: lo scopo di questa evoluzione è stato dotare l'intero sistema di nuove funzionalità mirate a renderlo più intelligente e versatile, garantendo una sicurezza avanzata.
La nuova tecnologia Advanced permette di **isolare la rete** per la gestione dell'impianto antintrusione, tenendola separata dalla rete di gestione TVCC: in questo modo diventa possibile gestire gli eventi TVCC attraverso l'**NVR**, che funge da **collettore delle informazioni dell'intero sistema**.
In sostanza, grazie a D-Pulse Advanced è possibile quindi rilevare eventi di allarme come intrusioni, attraversamenti di linea o oggetti abbandonati semplicemente attraverso l'uso di **telecamere basate su Intelligenza Artificiale**. Queste migliorano le prestazioni, la flessibilità e l'affidabilità dell'intero sistema aumentando ulteriormente l'efficienza della rilevazione.

Andando nello specifico, in che modo il sistema di sicurezza diventa più efficiente, grazie alla nuova tecnologia D-Pulse Advanced?

Ci sono **vari vantaggi** associati all'utilizzo di questa tecnologia di ultima generazione.
Innanzitutto la scelta di basare la tecnologia


Salvatore Pastorello

sull'utilizzo di telecamere basate sull'**Intelligenza Artificiale** ha un significato importante. Questo accorgimento oltre a migliorare le prestazioni, la flessibilità e l'affidabilità dell'intero sistema ne aumenta sensibilmente l'**efficienza**, superando l'accuratezza della rilevazione propria dei tradizionali rilevatori antintrusione.

Rispetto alla precedente tecnologia, la versione Advanced aggiunge degli ulteriori vantaggi: una novità fondamentale è rappresentata dalla funzione di **"split degli allarmi"**, che consente di **suddividere le segnalazioni d'allarme per ciascun analitico presente sulla telecamera**. Questo livello di dettaglio nella gestione delle situazioni di allarme rappresenta un notevole miglioramento, fornendo una panoramica più chiara e dettagliata degli eventi.

La capacità di gestire molteplici analitici, con particolare enfasi su quelli di tipo **GALAXY** sulle telecamere e-Vision AI, aggiunge un **importante miglioramento**. Questa caratteristica amplia le possibilità di utilizzo delle telecamere, offrendo un controllo più raffinato sulle funzioni di analisi e riconoscimento.

Un'altra innovazione significativa è rappresentata dagli **ingressi separati in centrale**. Ogni analitico è trattato come un ingresso fisico autonomo, permettendo una **personalizzazione estremamente flessibile durante la programmazione** delle logiche di gestione degli allarmi. Questo fornisce una soluzione su misura, adattabile alle esigenze specifiche di sicurezza di ogni ambiente.

Anche l'introduzione della possibilità di **connettere direttamente gli NVR alla centrale** è un pas-

so in avanti considerevole, poiché questa **novità** consente di gestire gli eventi AI delle telecamere senza necessariamente collegare la centrale alla "sottorete telecamere". Ciò offre una maggiore flessibilità nell'organizzazione del sistema, migliorando l'efficienza della gestione degli eventi.
Oltre a tutto questo viene aggiunto un **ulteriore strumento di controllo**, dato dalla possibilità di monitorare lo stato in vita di un NVR e lo stato degli HDD a bordo, in quanto consente di intervenire prontamente in caso di anomalie, contribuendo a **mantenere il sistema in condizioni ottimali**.

Passando ai campi applicativi, quali i contesti nei quali tale funzionalità può essere sfruttata appieno?

D-Pulse Advanced offre una soluzione avanzata e flessibile che garantisce una gestione efficiente e personalizzata degli allarmi e consente una maggiore integrazione tra i diversi dispositivi del sistema di sicurezza a tutti i livelli.
Questo passo avanti nella tecnologia rappresenta una scelta ideale per soddisfare le esigenze di **sorveglianza avanzata e controllo delle intrusioni**. La possibilità di personalizzare la gestione degli allarmi consente agli utenti di adattare il sistema alle proprie **specifiche esigenze**, migliorando la reattività e l'efficacia delle risposte agli eventi di allarme.
Inoltre, l'integrazione senza soluzione di continuità tra vari dispositivi assicura una comunicazione fluida e coordinata, **riducendo i tempi di risposta e aumentando l'efficienza complessiva del sistema**. D-Pulse Advanced non solo innalza gli standards di sicurezza, ma semplifica anche l'esperienza utente, permettendo una configurazione intuitiva e un monitoraggio costante. La flessibilità del sistema è un punto di forza che lo rende adattabile a diverse situazioni, dal controllo di **grandi impianti industriali** alla protezione di **residenze private**.

Quale dunque, ingegner Pastorello, il messaggio che EL.MO. intende trasmettere al mercato con la sua nuova tecnologia D-Pulse Advanced?

L'uso di tecnologie all'avanguardia come D-Pulse Advanced garantisce un alto livello di **affidabilità** e una riduzione dei falsi allarmi, **migliorando la fiducia degli utenti nel sistema**. In un mondo in cui la sicurezza è sempre più cruciale, noi di EL.MO. partiamo da un'**accurata analisi dell'esigenza dell'utilizzatore**, per poter sviluppare un sistema che garantisca un **elevato grado di soddisfazione**. D-Pulse Advanced rappresenta proprio una soluzione perfettamente in linea con questa logica, una **tecnologia completa e avanzata** pronta a rispondere alle sfide del presente e del futuro.

Nessun traguardo è impossibile se t'impegni a superarlo

DIGITRONICA.IT

Soluzioni software per ogni idea di sicurezza aziendale con un approccio che mette il codice a servizio del risultato finale

www.digitronica.it

Digitronica.IT
Your Security Our Software

La nuova era di EEA!

Incontriamo Alessandro Brancaleoni, Amministratore Delegato di EEA

a cura di Monica Bertolo

Ultimamente c'è davvero grande fermento in EEA considerato che ora vi siete trasferiti nel nuovissimo stabilimento, che è tre volte le dimensioni del precedente. Cosa rappresentano questa nuova dimensione, questo cambiamento?

Abbiamo ultimato il trasloco di **tutte le linee di produzione a fine marzo** e dal **1° aprile siamo operativi** in questo nuovo stabilimento che ha il grande pregio di essere più grande e quindi poterci ospitare in modo **più confortevole**, aprendo anche **spazi nuovi per attività** che avevamo dovuto mettere in stand-by, proprio per motivi legati alla dimensione dell'opificio precedente. Ma l'elemento cardine è che **questo trasloco rappresenta un vero e proprio punto di partenza**, non un punto di arrivo: un punto di partenza **per il progetto di medio/lungo periodo che caratterizzerà l'EEA per i prossimi anni**.

Tale progetto si concretizza anche grazie alle **nuove figure professionali** che abbiamo deciso di inserire **all'interno della nostra struttura**, a partire dalla **nuova figura** che è un **trait d'union tra la produzione e la progettazione**, che ci sta già supportando a velocizzare e ad ottimizzare i vari processi e l'innovazione stessa dei prodotti. Abbiamo introdotto anche un'altra figura, dedicata all'**Export Management**

ed una **figura Commerciale lato Italia**, che seguirà i clienti, anche quelli di dimensioni più contenute, che hanno delle potenzialità ma al contempo necessitano di un certo tipo di supporto. **Ulteriori due figure** entreranno nel nostro team: un **Back Office Commerciale con visione strategica** di mercato, che dovrà supportare la Direzione Commerciale, e un **Progettista lato Comunicazione**.

Complimenti per la vostra crescita, di questi tempi di buonissimo auspicio! Passando al fronte delle soluzioni, a Fiera Sicurezza avevate presentato importanti novità, sia sotto il profilo ingegneristico che del design. Quale la risposta del mercato?

A Sicurezza avevamo portato sostanzialmente due macro tematiche: un **sensore della linea Velvet**, che è un **bidirezionale e quindi crea due tende virtuali destra e sinistra a copertura di una parete** che può essere anche di 24 metri. La seconda tematica riguarda un **sensore** del quale ci saranno **declinazioni in diverse versioni** e, come tutte le linee dei rilevatori EEA, vedrà la **gamma filare**, quindi con il collegamento diretto con dei fili alla centrale, ma anche **quella a basso assorbimento per i sistemi via radio**. Il tutto permetterà di integrare i nostri sensori con diversi sistemi, uno tra questi è il sistema di collegamento su **BUS**.

Per quanto riguarda il **Velvet**, che come avevo anticipato uscirà dopo l'estate/verso fine anno, è stato molto bene accolto ed abbiamo avuto **ottimi feedbacks**, sia in fiera che soprattutto successivamente. I nostri vari **distributori**, così come i **produttori** per i quali sviluppiamo **prodotti customizzati**, stanno molto **premendo per avere questa nuova soluzione**, sia per gli **aspetti estetici** ed il **design** che già abbiamo presentato che, soprattutto, per le **molte funzionalità**. Per quanto riguarda le due aree di questo sistema di connessione, tale aspetto è ancora in fase di ulteriore sviluppo, e sono certo che **ci darà l'opportunità di creare un grande mercato a supporto dei produttori**.

Chiarissimo! La vostra visione strategica, come lei aveva avuto modo di sottolineare in una precedente intervista con S News, sta nello spostare tutta la comunicazione tra sensori e sistema su BUS, desiderando EEA incrementare integrazioni e sinergie con produttori di centrali o sistemi. Come sta procedendo tale progetto?

In qualche modo mi ricollego a quanto detto precedentemente. La nostra strategia sta **procedendo in modo significativo** e anche **spedito**,

ma ha bisogno ovviamente di **tempistiche che non sono immediate**. Questo perché richiede di trovare un **accordo con un produttore o con "n" produttori**. Al momento abbiamo diversi accordi in via di sviluppo, soprattutto con quei **partners che sentiamo particolarmente a noi affini**. La tempistica però non può essere immediata perché il lavoro non è solo lato EEA, ma su **entrambi i fronti**, e si deve lavorare **sia in termini di hardware** che di **gestione software**. Siamo molto impegnati su questo fronte e sono fiducioso che **già all'inizio dell'anno prossimo usciranno i primi frutti di queste collaborazioni**.

Guardando quindi in prospettiva, come evolverà il settore della rilevazione, quali le future esigenze alle quali dare risposte, secondo lei?

Volendo suddividere il mercato della rilevazione **antintrusione** in **due macro categorie di rilevatori, da interno e rilevatori da esterno**, dove per esterno abbiamo anche l'esterno protetto, diciamo che per quanto riguarda **l'interno la rilevazione sta andando sempre più verso il supporto**, oltre che all'antintrusione, alla **domotica**, e quindi il rilevatore di presenza di un possibile intruso diventa ora un **concentratore di altri rilevatori**. Questo permette l'**ottimizzazione sia in termini economici**, che **installativi e di integrazione**, perché a quel punto il sistema si integrerebbe facilmente con un sistema domotico, che è la direzione in cui stanno andando diversi produttori. Guardando invece **all'esterno**, lì l'integrazione della rilevazione va **verso il video**, e quindi una sorta di **doppia rilevazione**, che ha come ultimo obiettivo quello di **avere la certezza di ciò che sta succedendo**, oltre alle modalità con cui questo succede.

Da un punto di vista strategico, in termini di processo, l'attenzione è sempre più focalizzata sulle tematiche del **Green**, anche per quanto riguarda le nostre produzioni. Il prodotto sensore non è di suo energivoro, come non lo è il sistema antintrusione. A livello di **processo produttivo** però si può fare molto e anche noi in EEA, come altri produttori, ci stiamo muovendo in tale direzione. Pensiamo, ad esempio, a quanto detto prima in relazione alla **domotica**. Ed è proprio su tale fronte che ci stiamo concentrando.

Guardando oltre confine, prima aveva accennato che state implementando anche la parte Export. Ci sono quindi prospettive interessanti anche su questo fronte?

Sì. Storicamente abbiamo importanti attività in **Belgio, Grecia, Tunisia, Israele, Algeria**, dove abbiamo una presenza costante. Ma ci sono anche altri Paesi che sono interessati alla nostra proposta, come il **Regno Unito**, il **Nord Europa** e degli spunti ci sono arrivati dal **Sud America**. Per questo abbiamo deciso di **concentrare una risorsa e degli investimenti** anche in quella direzione perché, al di là del fatturato, il **potersi confrontare con realtà diverse ci consente di aprirci mentalmente sempre più**.

AMC: potenziale storico e rinnovamento odierno per la crescita in Italia e all'Estero

Incontriamo Luigi Nevano, Direttore Commerciale AMC Elettronica

a cura di Monica Bertolo


Luigi Nevano

AMC Elettronica vanta una lunga storia, essendo stata fondata nel lontano 1974. Chi è AMC oggi?

Oggi Amc Elettronica è un'azienda che, sia pure nell'ottica della continuità con il suo **glorioso passato**, prova a **rinnovarsi profondamente** nell'ambito di un mercato in continua evoluzione che genera sempre nuove sfide e grandi opportunità.

In questa veste rinnovata, l'azienda si è posta ben 2 **macro obiettivi**.

In primis, il **consolidamento del brand**, la cui percezione da parte del mercato andava rinnovata e, se possibile, migliorata. Di qui un sostanzioso restyling della politica commerciale, della rete distributiva, delle regole di ingaggio, delle modalità di assistenza pre e post vendita, fino a una vera e propria rivoluzione della partnership con il cuore pulsante del mercato: gli **installatori**. Di grande impatto il processo di **certificazione** degli ***Installatori Pro Amc***, che in tutta Italia assurgono a veri e propri **C.A.T.** virtuali al servizio di rivenditori, installatori e utenti finali.

D'altro canto, e su precisa richiesta di molte aziende anche multinazionali, l'Azienda ha accolto con passione e determinazione la sfida attraverso cui poter ergersi a **fabbricante di riferimento di importanti marchi nazionali ed esteri**.

Oggi Amc Elettronica si pregia produrre oltre che per sé stessa, anche per **Marchi di altissimo profilo** e che rappresentano il Gotha dello scenario internazionale della sicurezza.

In sintesi Amc Elettronica oggi è non solo **Brand** e tutto ciò che concerne il consolidamento e la crescita dello stesso, ma è anche **produzione**

nella migliore accezione del **Made in Italy.**

Molti gli eventi che vi hanno visti protagonisti recentemente, a conferma, anche, della dinamicità della nuova Direzione Commerciale a lei affidata. Quali i più significativi?

Abbiamo **esordito col botto** grazie a un **imprenditore ingegnoso e visionario come Paolo Domè**, che per l'uopo ha messo a disposizione la bellissima e rinnovata sede della sua **Dado Tecna a Palermo** e il **favoloso casale di famiglia a Marsala**.

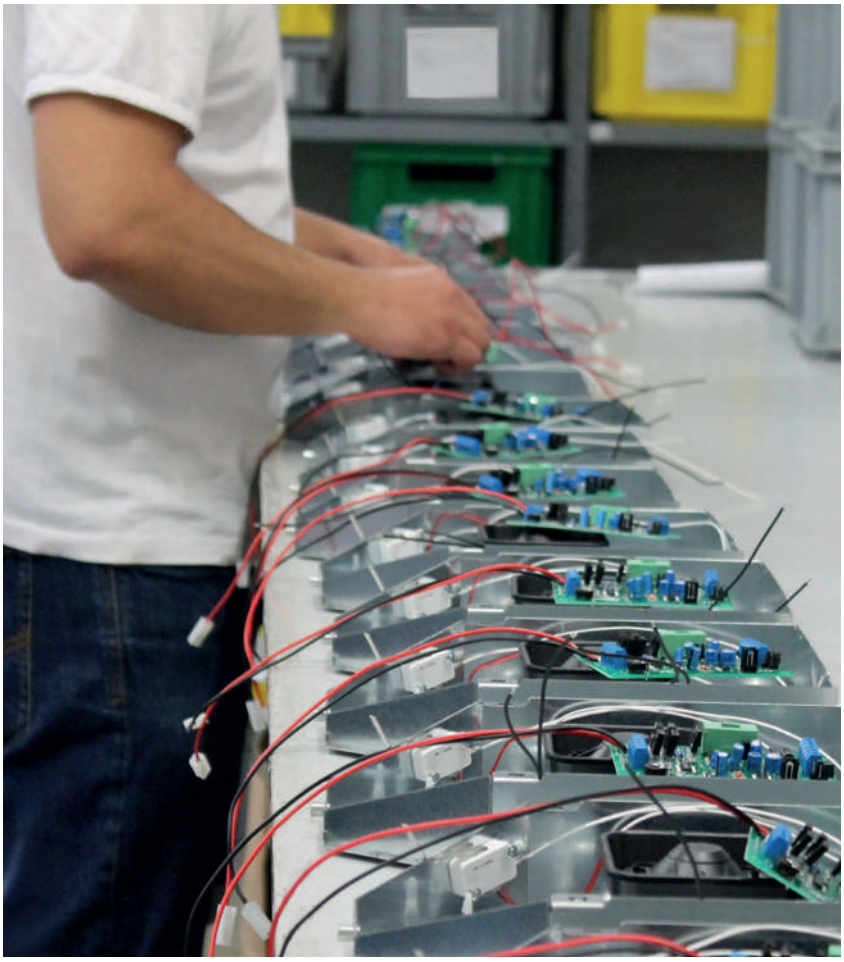
Come in molti hanno sottolineato, non è stato un caso che sia stato Paolo Domè a tenere a battesimo la **"prima"** di un **progetto itinerante e ambizioso** che vedrà Amc Elettronica protagonista di un tour nazionale. Paolo Domè ha rappresentato per anni il punto di riferimento di Amc per il mercato siciliano, e dovendo tracciare un solco importante che tenesse conto del passato ma si accingesse a vivere il futuro, quale migliore scelta se non affidarsi a lui che in tempi record e con la genialità di pochi ha tirato fuori il coniglio dal cilindro: gli **Orange Day**. Tra Marsala e Palermo abbiamo **presentato la nuova veste di Amc a oltre 80 aziende**, che sono intervenute per approfondire le novità commerciali, tecniche e di servizio indicate all'ordine del giorno.

La risposta in termini di consenso e apprezzamento è stata **cosi fragorosa che a distanza di soli 15 giorni e sulla scia di quanto ideato da Paolo, abbiamo replicato a Catania** dove, grazie al nostro **partner territoriale Pino Agosta** di **Global Security**, abbiamo potuto presentare il nuovo progetto a oltre **60 tra rivenditori e installatori**, provenienti da tutte le province della **Sicilia Orientale**. Questo l'inizio di un tour che ci vedrà impegnati **in tutte le principali regioni italiane fino a novembre 2024**.

A Luglio sono previste 2 tappe campane, poi da Settembre abbiamo in calendario Puglia, Veneto e Lombardia. Seguiranno Lazio, Marche e le altre regioni del centro ai primi di Ottobre.

Programma intenso e molto motivante! Passando quindi alle soluzioni, con ViTA inizia una nuova era per AMC. Corretto?

Si! **ViTA** rappresenta fedelmente il concetto di **rinnovamento** che poggia sulle solide radici di



una storia di tanti anni, ma guarda con rinnovata visione al futuro.
La nuova piattaforma fonda le sue basi su una struttura consolidata e molto cara al mercato, la **serie X**. Ovviamente dovendo proiettarsi alle nuove esigenze e opportunità di un mercato sempre più esigente, si apre a concetti nuovi come **video verifica**, **video analisi, integrazione e convergenza**.
Pur mantenendo i suoi plus di assoluto valore come, affidabilità, semplicità di configurazione e gestione, e grazie alla compatibilità con accessori e periferiche delle linee precedenti, **ViTA si apre alla tecnologia di parti terze** e con esse accoglie il meglio di quanto disponibile oggi in termini di tecnologia e funzioni. **L'obiettivo era offrire ai propri clienti e ai clienti dei propri clienti strumenti semplici di gestione di impianti di sicurezza complessi e iper performanti**.

Guardando in prospettiva a breve/medio periodo, quale l'evoluzione del mercato a suo avviso e quali le nuove dinamiche che lo governeranno?

Non vorrei sembrare ripetitivo rispetto a coloro che da tempo sostengono che il mercato è cambiato. Fino a 10 anni fa assistevamo a episodi, eventi che si ripetevano con una certa ciclicità, che i più bravi definivano corsi e ricorsi storici.
Bene o male, i periodi di successo o le grandi crisi si riproponevano ciclicamente.
Oggi viviamo una tempesta continua, con **variazioni costanti ma anche inattese**, in funzione delle quali è difficile fare previsioni.
L'intrusione vola spedita verso il concetto di facile utilizzo e proposizione diretta, in mercati sempre più verticali che tendenzialmente **stritolano la filiera** a cui eravamo abituati.
Amc Elettronica rimane fedele al concetto di tutela e supporto dell'intera filiera distributiva (produttore, distributore, rivenditore, installatore e solo in ultimo utente finale), ma si pone **al servizio di tutti i canali operativi** che desiderano avvalersi di un **Know How in costante crescita**. Per intenderci, come dicevo all'inizio, Amc Elettronica oggi dispone di mezzi (uomini, competenze, esperienze, macchinari all'avanguardia) che la pongono ai vertici della compagine dei produttori intrusione in Italia e all'estero.
Questo **enorme potenziale è a disposizione del brand e quindi della sua rete distributiva e di tutta la filiera**, ma è anche oggetto del desiderio e della **fruizione di importanti Players di livello mondiale, grazie ai quali la proposta complessiva si arricchisce e si qualifica costantemente**.
Tutto ciò ci consente di guardare al futuro con una certa **serenità e grandi aspettative**, disponendo di tutto il necessario per soddisfare i diversi bisogni di mercati, segmenti e canali diversi.

Urmet, il Sales Force 5.0 e la forte innovazione tecnologica

Incontriamo Giulio Smarrazzo, Sales Manager Italia

a cura di Linda R. Spiller

Di recente lei è stato nominato nuovo Sales Manager Italia e in Urmet si parla di Sales Force 5.0. Di che cosa si tratta?

Sales Force 5.0 è un **piano strategico** che ci accompagnerà nei prossimi anni con una **visione a medio e lungo termine**, una sfida per conseguire un **fatturato importante**, segnata da una strategia che mette insieme parole chiave appunto di una cultura 5.0: digitalizzazione, sostenibilità, marketing e comunicazione e non da ultimo il team compatto, coeso, orientato verso il successo e con obiettivi chiari in testa, appoggiato ad una **cultura valoriale quasi centenaria**.
Urmet, infatti, è una grande azienda che merita di avere una "sales force" all'altezza, **premiando il singolo** come elemento di un team di lavoro che si sente partecipe di un progetto che gli stiamo comunicando in più modi: inizialmente ai primi livelli, poi attraverso un **"road show"** e, a fine anno, con una **convention**. Credo fermamente che le persone vadano coinvolte nel disegno progettuale di tutto ciò e che se ne sentano **coautori**.

Chiaro il messaggio che trasmette quindi Urmet con questo nuovo organigramma Sales Management Italia, ovvero quello di un'azienda che fa crescere i propri collaboratori, le proprie persone, sia dal punto di vista professionale che motivazionale. Corretto?

Assolutamente sì. L'azienda ha scelto di **puntare sul proprio organico "in house"**, offrendo un'opportunità di crescita

ai professionisti che già erano parte dell'organizzazione commerciale, ognuno nel proprio ambito territoriale, ottenendo risultati rilevanti negli ultimi anni. Quindi, abbiamo deciso di **premiare le competenze e l'esperienza** di chi già conosce il mercato e il mondo Urmet in profondità, sia a livello umano sia a riguardo degli aspetti tecnici e commerciali: il **fattore umano** è senz'altro un valore importante a cui teniamo, strettamente correlato alle **skills professionali**.

E passando agli obiettivi che con l'intero Sales Management Italia si prefigge a breve-medio termine di raggiungere, quali sono i prioritari?

L'obiettivo è di continuare il nostro lavoro incrementando, nel medio termine, il trend positivo degli ultimi anni e puntare ad una crescita significativa nelle area a bassa quota, grazie alle capacità di visione strategica e profonda conoscenza del mercato del nostro team. Da subito stiamo lavorando per rafforzare la presenza e lo sviluppo di Urmet sul mercato nazionale, anche grazie all'esperienza di **Mirco Megna** e **Gianni Bonanni**, nominati rispettivamente **sales manager centro-nord Italia e centro-sud Italia per affiancarmi**. In questi ruoli, ciascuno per la propria area, presidieranno e coordineranno gli obiettivi di vendita sia di **"sell-in"** (vendite dal produttore al venditore) che di **"sell-out"** (vendite dal produttore al consumatore) grazie alle skills acquisite dopo anni di lavoro sul campo.

Spostando ora l'attenzione sul mercato, in continua e veloce evoluzione, quali le maggiori sfide che impegneranno il settore a suo avviso?

In generale, il mercato edile è in difficoltà, perché il contesto nel quale viviamo è complesso. Lo stesso comparto della sicurezza sta attraversando una fase di cambiamento. Per fortuna possiamo però segnalare un dato positivo, che ci incoraggia: l'attenzione si sta focalizzando sulle **novità**. Di conseguenza, chi in questo momento è in grado di puntare sull'**innovazione tecnologica** riesce sicuramente a distinguersi. Le sfide per Urmet si concentreranno quindi in un ulteriore salto in avanti nel campo della **digitalizzazione**, dei **sistemi integrati**, ma anche nello sviluppo di nuove **competenze** e **professionalità**.

Le nostre soluzioni vanno sempre più verso **un'integrazione di funzioni e di utilizzo**, al servizio delle nuove esigenze sia dei clienti installatori sia ai clienti utilizzatori. **Una convergenza di funzioni** d'impianto che consente di poter disporre di sistemi aperti alle diverse **integrazioni di cui un edificio necessita: videosorveglianza, antintrusione, antincendio, controllo accessi, climatizzazione, videocitofonia, automazioni e domotica**. Con la possibilità di configurare **il tutto da remoto**, **attraverso dispositivi diversi con tool di programmazione e configurazione pensati per ogni tipo di dispositivo, come desktop, mobile o tablet, da utilizzare in qualsiasi momento e luogo.**

EY Global Integrity Report 2024:
etica e integrità priorità di business

a cura di Linda R. Spiller

Le **aziende italiane** considerano una **priorità di business l'etica e l'integrità aziendali**, secondo i principali risultati emersi dall'**EY Global Integrity Report 2024**, l'indagine che ha sondato le opinioni di **oltre 5000 membri di consigli di amministrazione, managers e professionisti** in oltre 50 Paesi, Italia inclusa.

I dati dell'EY Global Integrity Report 2024 e l'analisi

Le aziende italiane considerano quindi l'etica e l'integrità aziendali cruciali, ma **si può fare di più: il 70%** dei managers nel Paese dichiara che la propria azienda prevede delle attività volte alla promozione di comportamenti etici, ma solo il **39%** ha percepito un miglioramento degli standards di integrità negli ultimi due anni.
Questo dato riflette un tema importante: se da un lato le aziende italiane pongono l'integrità aziendale al centro delle proprie priorità, esistono delle **sfide oggettive che ne rendono complessa l'attuazione**, anche in virtù dell'attuale contesto geopolitico instabile. Lo conferma **1 manager su 2** che ritiene che sia **sempre più complesso mantenere alti gli standards di integrità** in un'epoca di rapide e grandi trasformazioni nonché di incertezze economiche.
"La business integrity, in Italia – sottolinea **Fabrizio Santaloja**, EMEIA Leader di EY Forensics & Integrity Services – è per adesso una scommessa vinta a metà. Se, da un lato, i recenti indirizzi normativi, le regolamentazioni di settore, i codici di comportamento delle aziende e le scelte di investimento considerano l'etica negli affari questione prioritaria, c'è **da valutare quanto realmente, poi, i comportamenti riflettano nella realtà questi principi virtuosi**. E **i dati confermano che c'è ancora strada da fare**".
Il **21%** delle aziende italiane coinvolte nell'indagine EY ha riscontrato casi di comportamenti non etici nel corso degli ultimi due anni. Nello specifico, per il **24%** si era trattato di casi di corruzione, per il **19%** di frodi e furti e per il **10% di violazioni della sicurezza dei dati (contro il 21% a livello mondiale)**. Di tutti questi casi, **l'81% ha riguardato terze parti (con un'incidenza del 20% superiore alla media mondiale), nonostante il 75% degli intervistati in realtà sia convinto che i partners della propria organizzazione si comportino eticamente e seguano i codici di condotta**.

Il Whistleblowing

In questo contesto, il panorama italiano sulle tematiche di **whistleblowing** presenta ancora margini di miglioramento sia in termini di sicurezza sia di facilità di utilizzo dei sistemi di segnalazione di condotte illecite. A questo proposito, solo il **29%** dei rispondenti testimonia che ci siano stati progressi in questo ambito. **L'implementazione di un sistema di whistleblowing efficace è indicativa dell'impegno delle aziende nei confronti della promozione dell'integrità e dell'etica**. Tuttavia, il **45%** dei rispondenti ha

Fabrizio Santaloja, durante un convegno EY

dichiarato di aver percepito una certa pressione nell'effettuare una segnalazione. Un dato comunque inferiore al **54%** registrato a livello mondiale. Dati che provano una difficoltà nella cultura aziendale, come conferma il **35%** degli intervistati, secondo cui la propria azienda non fornisce programmi di training sul tema dell'etica e integrità per la formazione del personale.

L'AI e i dati dell'EY Global Integrity Report 2024

Sempre in riferimento alla gestione della business integrity, sotto i profili più tecnologici e digitali l'introduzione dell'**intelligenza artificiale (IA)** nel business sta trasformando il modo in cui le realtà aziendali operano, migliorandone l'efficienza e l'accuratezza. Infatti, **l'88%** dei rispondenti ha dichiarato che la propria azienda abbia già adottato o si stia preparando a adottare determinati strumenti legati all'AI nei propri processi. Nonostante le potenziali opportunità di questa tecnologia, è richiesta anche una gestione attenta per affrontare le **eventuali sfide etiche e di governance**. Infatti, il **90%** delle aziende italiane sta già **affrontando proattivamente i rischi di frode e privacy legati all'AI**, dimostrando un impegno concreto verso un utilizzo etico e responsabile delle nuove tecnologie.

Trasparenza e comunicazione

Anche nell'ambito della trasparenza e della comunicazione relativa a temi prioritari per le aziende del Paese, esistono ancora degli ostacoli significativi e su cui occorre consolidare le pratiche in materia. Le questioni legate agli **ESG** (Environmental, Social, Governance), ad esempio, sono ormai di prioritaria importanza per le aziende, ma solo il **54%** ritiene che le proprie organizzazioni comunichino chiaramente e in modo appropriato le iniziative su temi ambientali, sociali e di governance. Sebbene oltre il **60%** confermi un allineamento tra le dichiarazioni e le azioni ESG sempre in ambito business, il **51%** riconosce che la leadership dovrebbe rafforzare ulteriormente l'integrità in questo ambito e più del **30%** auspica una maggiore trasparenza nella comunicazione con obiettivi ESG definiti e misurabili.

Ancora nessun equilibrio sulle gare d'appalto per la sicurezza

a cura di Maria Cristina Urbano

Ricordate quando il contratto della **sicurezza privata**, per quanto riguardava la parte afferente ai **servizi fiduciari**, era considerato un **contratto "povero"** e sentenze della **Corte di Cassazione intimavano di rivederlo** perché in contrasto con quanto stabilito dall'art. 36 della Costituzione, quello sulla retribuzione proporzionata alla quantità e qualità del suo lavoro? E ricordate quanto accaduto negli ultimi mesi, con una **contrattazione estremamente faticosa tra parti datoriali e parti sindacali** che lo scorso febbraio sono tuttavia riuscite a sottoscrivere un **addendum al CCNL**, a sua volta già rinnovato a maggio 2023 con **significativi miglioramenti dal punto di vista retributivo**, innalzando ulteriormente e in maniera consistente la remunerazione, così da allinearlo a larga parte degli altri CCNL vigenti in Italia?

Ebbene, secondo il **mercato agroalimentare di Padova** tutto ciò non è mai avvenuto! In un **recente capitolato di gara** per l'affidamento del servizio di portineria e custodia, infatti, all'art. 19 veniva specificato che "in ragione della necessità di evitare che il committente sia esposto a richieste di pagamento del giusto salario ai sensi dell'art. 36 della Costituzione, anche in ragione di quanto stabilito dalla Cass. 27711 del 2 ottobre 2023, viene espressamente **esclusa l'applicabilità del contratto collettivo per la vigilanza privata e dei servizi fiduciari"**. È evidente come la stazione appaltante ignorasse l'iter del rinnovo di detto contratto, con un'affermazione peraltro gravemente lesiva del lavoro e dell'impegno delle rappresentanze delle parti sociali tutte. Quanto determinatosi ha costretto **ASSIV** a inviare lo scorso 10 giugno istanza in **autotutela**. La stazione appaltante ci ha prontamente risposto di aver **già revocato la gara**, e noi speriamo vivamente che sia perché avvedutisi dell'errore.

La posizione e l'operato di ASSIV sulle gare d'appalto per la sicurezza

Per anni la vigilanza privata ha denunciato, e per la verità continua a denunciare, **gare d'appalto indette con valori del costo orario dei lavoratori ben al di sotto delle tabelle pubblicate dal Ministero del Lavoro** (ormai obsolete), indicando proprio in questa prassi assurda la vera ragione della povertà delle retribuzioni dei propri lavoratori. Ora che, dopo anni faticosi di confronto e scelte coraggiose (forse ardite!) da parte delle aziende, si è arrivati a riconoscere con il **nuovo CCNL livelli salariali adeguati agli operatori dei servizi fiduciari**, venire additati come paria da quelle stesse stazioni appaltanti che hanno creato il problema e che poco fanno per risolverlo mi pare **ironico e tragico al contempo**!

FIRE 4G

La soluzione per servizi certificati EN54-21

100% a norma • **100%** made in **Urmet ATE**

Vantaggi

- Soluzione 100% a norma
- Integrato
- Made in Italy
- Multivettore
- Compatibile con tutti i centri di gestione allarmi
- Di semplice installazione

Per Istituti di Vigilanza

Urmet Ate ha realizzato una soluzione per il monitoraggio dei sistemi antiincendio adatta a tutte le esigenze. È composta da un **nuovo e performante comunicatore multivettore Fire 4G** ed un ricevitore Software dedicato alla gestione bidirezionale dei prodotti installati in campo. Questa soluzione permette di mettere a norma sia l'impianto antiincendio del cliente, con un comunicatore dedicato e **certificato EN54-21**, sia il servizio erogato dall'Istituto di vigilanza utilizzando il ricevitore software EN54-21 collegato ad un **sistema di centralizzazione allarmi EN 50518.**

urmet ATE

urmet-ate.it

Il punto di vista ASSIV sui PDL Iezzi e Spelgatti e il concetto moderno di sicurezza

a cura di Maria Cristina Urbano

Con questo articolo vogliamo riprendere il filo del discorso iniziato con l'approfondimento uscito sulle colonne di S News **"ASSIV e le nuove PDL di diretto interesse della Sicurezza Privata"** in febbraio *(ndr. S News n.73, pagg.58–62)*, quando abbiamo illustrato **alcune delle proposte di legge** riguardanti il comparto della sicurezza presentate in **questa prima parte di legislatura**.
Restarono, allora, fuori da quella disamina le proposte di **Igor Iezzi** della **Lega** e di **Alberto Balboni** di **Fratelli d'Italia**. Oggi l'intenzione è di colmare parzialmente la lacuna, dedicando la nostra riflessione alla **PDL Iezzi** e altri, presentata il 5 settembre 2023.

L'analisi di ASSIV sulla PDL Iezzi e il nuovo concetto di sicurezza "partecipata"

Si tratta di una proposta legislativa **molto ambiziosa**, perché si pone come obiettivo la **disciplina delle attività di sicurezza sussidiaria svolte da soggetti privati**. La premessa è incoraggiante, infatti gli estensori prendono in considerazione il **nuovo concetto di sicurezza che diviene "partecipata"**, e si pongono l'obiettivo di raccogliere in **un unico strumento legislativo ciò che ora si trova nel TULPS, nel Regolamento di attuazione, nel DM 269/2010 e nelle leggi speciali che costituiscono la fonte normativa dei servizi di sicurezza "sussidiari"** (porti, aeroporti, stazioni), ossia **in affiancamento o in sostituzione (ma sotto il coordinamento) delle Forze dell'Ordine**.

Il concetto moderno di sicurezza: stretta collaborazione tra operatori pubblici e privati

Si tratta di un'impostazione **ampiamente condivisa da tutti gli operatori**, in linea con un **concetto moderno di sicurezza** che vede la **stretta collaborazione tra operatori pubblici e privati**, i secondi sotto la direzione dei primi, coerente con il quadro di sistema sicurezza Paese individuato in linea di principio (ma mai applicato del tutto) dalla vigente normativa. **Tuttavia, a nostro avviso come ASSIV, nei 26 articoli che compongono il disegno di legge si nascondono molte insidie**.

Le molte insidie nella PDL Iezzi secondo ASSIV

Il DM 269/2010, che norma nel dettaglio la disciplina degli **IVP** (Istituti di Vigilanza Privata), dei **requisiti dei servizi di sicurezza** e delle **GPG**, viene per così dire **"scomposto"** e riassemblato all'interno della proposta di legge, disarticolando ciò che adesso, a distanza di 14 anni dalla sua entrata in vigore, ha trovato applicazione, con prassi amministrative certamente migliorabili ma consolidate.

Leggendo con attenzione, si rinviene **la tendenza a riportare nella discrezionalità delle Prefetture alcuni importanti aspetti della vita aziendale degli IVP** che **adesso sono regolati in maniera oggettiva**, per esempio l'ammontare della cauzione, (punto 9 art.2). Vale la pena di ricordare che **uno degli aspetti a suo tempo censurati dall'UE**, perché contrari ai principi normativi eurocomunitari e che portarono all'abrogazione del previgente quadro legislativo nazionale, era rappresentato proprio dai margini di discrezionalità cui veniva sottoposta l'attività imprenditoriale da parte della PA. Di più: all'**art. 5** si elencano i motivi per cui la **licenza può essere negata, sospesa o revocata**, e si leggono, fra questi, "il fondato pericolo che l'istituto la società o l'impresa interessata acquisisca una posizione predominante nel territorio o nel settore di attività" (punto d) o "la presenza nel territorio di un numero non proporzionato di istituti o imprese di servizi di guardie giurate o di altri operatori abilitati" (punto e), con facoltà dell'autorità di provvedere alla nomina di commissari straordinari per garantire la continuità operativa di quegli istituti oggetto di sospensione o revoca. **Ancora più anacronistica è la reintroduzione dell'ambito territoriale**, che prevede eccezioni e deroghe concesse dal Prefetto, ma che tornerebbe ad essere la regola. Insomma, la proposta di legge in esame **reintrodurrebbe nel nostro sistema proprio alcuni dei più significativi vulnus** che caratterizzarono la precedente normativa e che ne hanno determinato il destino. Oggi che gli stessi principi in base ai quali venne imposta l'abrogazione della norma nazionale costituiscono in maniera inderogabile una delle trame del tessuto normativo UE, **l'eventuale approvazione da parte del nostro Parlamento di una siffatta norma significherebbe certamente un nuovo intervento delle autorità europee e l'inaugurazione di un nuovo periodo di incertezza normativa, a tutto danno di un sistema di imprese che nel corso degli ultimi dieci anni ha dovuto adeguarsi, con grande dispendio di risorse umane ed economiche, al nuovo ecosistema legislativo**. Fatto, questo, che certamente è alla base delle buone prestazioni del comparto anche in momenti di grande difficoltà per il Paese, quali la pandemia da Covid-19 e la crisi da questa generata. Ciò perché **la vigente normativa**, pur con tutti i ritardi e le difficoltà applicative riscontrate, **ha spinto verso una sempre maggiore qualificazione delle aziende e degli operatori**, operando una selezione che ha consentito la sopravvivenza alle aziende finanziariamente e organizzativamente solide. Infine, anche per i **servizi di sicurezza disarmati**, disciplinati nel dettaglio dalla PDL Iezzi e altri, si prevedono per gli operatori specifici requisiti riguardanti la condotta (previsione comprensibile e condivisa da chi scrive, ma già ampiamente attuata dalle aziende) e il **loro collocamento sotto il controllo delle Prefetture**, che ne terrebbero appositi registri. **Ci nasconderemmo dietro un dito se non dicessimo chiaramente che una simile previsione significherebbe la paralisi del settore, perché le Prefetture non hanno le risorse per svolgere questa ulteriore incombenza**. Inutile constatare come un intervento normativo che vorrebbe sistematizzare e quindi semplificare, in tal modo otterrebbe l'effetto opposto.

Insomma, il **progetto di legge pare un ritorno all'antico**, immemore dei principi contenuti nella sentenza Corte di Giustizia Europea del dicembre 2007, che **condannò l'Italia per un quadro legislativo largamente difforme dai principi del Trattato europeo** e diede inizio al processo di riforma che **ancora non ha trovato compiuta applicazione**, e sul quale il Ministero dell'Interno, di concerto con le sue terminazioni territoriali, dovrebbe mostrare maggiore impegno, anche nel coinvolgimento di tutti gli stakeholders di settore, per il miglioramento ed aggiornamento delle prassi applicative.

La posizione e le richieste di ASSIV

Prendiamo atto del fatto che l'iniziativa di legge è a cura di partiti della maggioranza, anzi sembra essere una proposta di riforma organica identitaria per la Lega. Sembra confermarlo quanto avvenuto a **febbraio al Senato**, con la presentazione da parte della **senatrice Spelgatti e di tutto il gruppo della Lega del DDL "Disciplina delle attività di sicurezza sussidiaria svolte da soggetti privati"**. Esatto carbon copy della PDL Iezzi e altri. Chiediamo dunque ai parlamentari firmatari delle proposte di legge in oggetto di **voler aprire un confronto sui loro contenuti, nella certezza che l'obiettivo loro e nostro sia identico: garantire all'Italia un sistema sicurezza moderno, efficace ed efficiente, che benefici della grande dedizione delle nostre Forze dell'Ordine ma che sappia mettere a fattor comune le enormi risorse organizzative, tecnologiche e professionali del comparto della vigilanza privata.** Noi restiamo, come sempre, disponibili a fornire un contributo costruttivo.

Securducale:
la forza di un grande Gruppo, la volontà di mettere a sistema l'innovazione

Incontriamo Claudio Borgonovo, Amministratore Delegato e Titolare di Licenza di Securducale Vigilanza Srl

a cura di Monica Bertolo

Quale la valenza della nuova UNI 11926 per un'azienda come Securducale?

La certificazione **UNI 11926** assume un'**importanza fondamentale** in un **settore che punta oggi all'innovazione, sia tecnologica che di processo**.

Securducale Vigilanza fa parte del **gruppo Dussmann, società multinazionale tedesca** presente in numerosi Paesi del mondo e che in Italia, con **oltre 25.000 dipendenti**, si occupa di **Facility Management, Sanificazione e Ristorazione**.

Securducale entra a far parte di questa grande famiglia nel 2010 ed opera in forza di una Licenza prefettizia per i servizi di vigilanza e sicurezza sui territori di PR-RE-MO-BO, mentre è attiva **sull'intero territorio nazionale per l'offerta di servizi ausiliari di sicurezza**.

Claudio Borgonovo

Oggi occupa **oltre 200 dipendenti, di cui 60 Guardie Giurate**, mentre i restanti sono dislocati su tutto il territorio nazionale.

Oltre alle certificazioni **ISO 9001:2015, UNI 45001:2018, UNI 10891:2000**, Securducale ha ottenuto le certificazioni **SA8000** relativa alla Responsabilità Sociale, **UNI PdR 125:2022** in relazione alla parità di genere in azienda, **UNI 11926** relativamente ai Servizi ausiliari alla sicurezza, ed è in fase di ottenimento la certificazione **ISO 14001:2015** relativa al Sistema di gestione ambientale.

Per i servizi ausiliari di sicurezza non era prevista, fino ad oggi, una regolamentazione specifica, essendo questi servizi assolutamente differenti da quelli riservati per legge allo Stato oppure a soggetti economici provvisti di autorizzazione specifica come gli Istituti di vigilanza.

La nuova norma **11926** indica come i servizi ausiliari devono essere realizzati, attraverso quali attività di tipo tecnico, gestionale ed organizzativo, **marcando una sensibile differenza tra l'efficienza e l'efficacia del servizio reso da aziende come la nostra, che ha ottenuto la certificazione, ed altre che non l'hanno**.

È stata di recente presentata alla Camera dei Deputati la proposta di legge, a prima firma dell'on. Gianluca Caramanna, in merito alle "Disposizioni in materia di prestazione di servizi ausiliari alla sicurezza". Quali gli auspici da imprenditore e da associato ASSIV?

È importante che si sia finalmente intrapreso un percorso che miri alla certificazione dell'affidabilità delle imprese e della qualità dei servizi resi.

L'obiettivo è quello di promuovere la **fornitura dei servizi di sicurezza ausiliaria**, fino ad oggi considerati scarsamente efficaci anche a motivo della varietà di offerte e di contratti di lavoro applicati in modo non sempre trasparente.
Noi auspichiamo che questa certificazione possa **costituire il discrimine commerciale per l'offerta dei servizi ausiliari di sicurezza sul mercato**, perché da una parte ci qualifica come operatori seriamente impegnati nell'offerta di **servizi sempre più specializzati**, mentre dall'altra ci rende maggiormente attrattivi nei confronti dei nostri collaboratori, per i quali si apre finalmente la prospettiva di **percorsi professionalizzanti**.
ASSIV ha svolto e svolge tuttora un ruolo fondamentale nel definire il perimetro ed i contenuti in discussione per la **modernizzazione del nostro settore, in ottica di stretta collaborazione tra gli associati e le istituzioni**.
In un quadro che si fa maggiormente complesso è utile poter condividere esperienze e mettere in comune interessi tra aziende che operano, affrontando gli stessi problemi in realtà differenti.

ASSIV da tempo si prodiga con grande e professionale impegno su questo ed ulteriori fronti per la tutela e la crescita del comparto. Quali a suo avviso le esigenze maggiormente sentite dalle imprese di sicurezza oggi, sul piano normativo e sul riconoscimento del vostro ruolo?
Il settore della vigilanza privata impegna un gran numero di aziende e consistenti risorse economiche, organizzative e professionali sul nostro territorio.
Quel che abbiamo visto succedere negli ultimi mesi, le aziende commissariate, le gare pubbliche bandite in violazione del Codice, gli affidamenti al massimo ribasso, hanno messo e tuttora mettono a grave rischio la sopravvivenza delle aziende e, quindi, il lavoro degli addetti.
La sensazione è quella di trovarci oggi in una **fase di cambiamento che potrebbe dispiegare i suoi effetti nel corso dei prossimi anni**. È però fondamentale **mettere a sistema una serie iniziative non necessariamente legislative** (le norme esistono, spesso semplicemente non vengono applicate), **perché l'impegno delle aziende possa tradursi in un riconoscimento del valore dei nostri servizi sia in termini qualitativi che economici**.
Al trattamento economico equo della forza lavoro, risultante dall'applicazione di CCNL stipulati dalle associazioni sindacali maggiormente rappresentative sul piano nazionale, deve essere **associata la responsabilità del committente, ancor più se si tratti di committente pubblico, all'applicazione di tariffe congrue rispetto al costo del lavoro**.
Il lavoro potrà così dispiegare il massimo cambiamento in termini di **qualità**, di **professionalità degli addetti**, di **competizione** tra operatori del settore **non più basata esclusivamente sul prezzo di vendita**.

Guardando in prospettiva, quale la sua visione sul futuro a breve/medio termine per il settore?
Dal punto di vista delle risorse umane, la richiesta di incremento di professionalità e competenze non proviene più solo dai committenti, ma anche dagli **addetti**, che non considerano più la loro professione come residuale e complementare rispetto ad altre agenzie di sicurezza, ma reclamano giustamente un **ruolo di maggior protagonismo** rispetto alle dinamiche sicuritarie che quotidianamente si trovano a dover gestire.
La **tecnologia**, poi, assumerà un'importanza sempre maggiore nel panorama del settore, a maggior ragione con gli interessanti sviluppi consentiti dall'**intelligenza artificiale**.

L'**interazione tra questi due fattori**, se ben guidata, può sicuramente **sviluppare grandi vantaggi non solo tra gli operatori, ma per intere comunità e territori**.

Strategia dell'UE in materia di cybersicurezza e resilienza

Elementi chiave e necessità di regolamentare le strutture di sicurezza delle entità critiche nazionali

a cura di Corrado Miralli
Security Manager, CISO e Cultore della materia della Security Aziendale

L'analisi si apre partendo dalle varie **Direttive europee**, riguardanti i settori di riferimento. Le **minacce informatiche** al settore **energia, trasporti, bancario**, fino a ricomprendere il settore delle **utilities**, sono per loro natura **transnazionali**, ed in **continuo aumento**, complice anche l'uso di sistemi di offesa basati su **intelligenza artificiale** (AI).
Le **infrastrutture critiche** per loro natura sono particolarmente esposte al rischio di **DDOS e Ransomware**; in questi casi la risposta di sicurezza richiede uno sforzo congiunto **pubblico-privato**. Per i settori infrastrutturali critici di importanza nazionale le **agenzie governative dovrebbero collaborare con l'industria** e sviluppare **modelli di security** idonei a gestire concordate strategie per la protezione.
Gli attacchi cyber si posizionano tra i primi 5 scenari di rischio con più alta probabilità di accadimento.
Per far fronte a questo trend, dal 2023 il patrimonio normativo dell'Unione Europea si è arricchito con nuove direttive: la direttiva **NIS 2** (direttiva UE 2022/2555), pubblicata a dicembre 2022 insieme alla direttiva **CER** (Critical Entity Resilience) (direttiva UE 2022/2557), ed al **"Digital Operational Resilience Act"** o regolamento **DORA** (Regolamento 2022/25541/UE) sulla sicurezza ICT delle entità del settore finanziario e bancario, che mirano a **meglio definire la strategia cyber comunitaria**, chiedendo a tutti gli Stati membri di adottare **misure coordinate per garantire la continuità operativa** di infrastrutture che sono critiche per l'economia, la salute, la sicurezza pubblica e privata.

La direttiva NIS 2 è entrata in vigore su tutto il territorio dell'Unione Europea il 17 gennaio 2023 e gli Stati membri avranno l'obbligo di adottare e pubblicare gli atti normativi necessari a recepirla **entro e non oltre il 17 ottobre 2024**.
Essa estende il perimetro per l'applicazione delle norme europee in materia di sicurezza cyber già indicato dalla direttiva 2016/1148/UE recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. "direttiva NIS"), primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza informatica (valutazione della minaccia, obblighi di mitigazione del rischio,

obblighi di comunicazione di eventi significativi, certificazione della sicurezza per prodotti e servizi TIC, obblighi di vigilanza), che era stata recepita in Italia con D.Lgs 18 maggio 2018, n. 65.
La NIS 2 si applicherà agli operatori dei settori e dei sotto settori ritenuti ESSENZIALI (grandi imprese e soggetti già individuati dalla NIS) o IMPORTANTI (medie imprese), denominati entità critiche.

In particolare la NIS 2

- Identifica nuovi settori, 9 altamente critici e 7 critici, ai quali si affiancano soggetti identificati come critici dalla direttiva
- Distingue i soggetti destinatari in entità essenziali e importanti, identificati sulla base di specifici criteri oggettivi (dalle medie imprese in su, salvo eccezioni), lasciando al Governo la facoltà di identificare ulteriori soggetti
- Adotta un approccio multi-rischio, sia fisico che cyber, (coordinamento con direttiva CER) con un maggior dettaglio nella definizione di misure di sicurezza che devono avere il carattere della proporzionalità
- Comprende misure per la continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi
- Introduce nel modello di resilienza la sicurezza della catena di approvvigionamento. Le interruzioni delle supply chains sperimentate in epoca pandemica hanno costretto l'industria a rivedere le proprie strategie di approvvigionamento. Inflazione, incertezza geopolitica, crisi energetica, cambiamento climatico, situazioni di guerra ai confini dell'Europa e nel Middle East, aumentato rischio offshore nel Mar Rosso, hanno ulteriormente intensificato la situazione di incertezza e le conseguenze sull'economia mondiale
- Adotta un processo di notifica più comprensivo, con poteri ispettivi e sanzionatori rafforzati (allineamento al modello sanzionatorio del GDPR – Regolamento 2016/679 UE)

Il **17 gennaio 2025** è il termine indicato per la definizione dei soggetti – entità critiche – destinatari della norma.

La Direttiva CER

La Direttiva CER (Critical Entity Resilience), che si occupa della **resilienza delle entità critiche e altamente critiche**, ovvero reti e beni infrastrutturali che, se danneggiati o distrutti, causerebbero ripercussioni alle funzioni cruciali della società, esponendo i cittadini a gravi danni per la mancanza di infrastrutture e di servizi primari, mira a **garantire la fornitura di servizi essenziali ed a migliorare la cooperazione transfrontaliera tra le autorità competenti**, ferma restando la responsabilità dei singoli stati dell'UE per la tutela della sicurezza nazionale (la direttiva CER non si applica agli enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto alle attività criminali).
La direttiva CER, nata sulla spinta dei fatti che hanno visto coinvolto il gasdotto North Stream, evidenziando la fragilità e le dipendenze dei settori critici nazionali, sostituisce la direttiva 2008/114/CE del Consiglio, dell' 8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, fungendo da **norma di raccordo tra quanto previsto dalla NIS 2 a livello europeo e la legge nazionale n. 133/19 e DPCM successivi** "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", che già aveva introdotto stringenti protocolli di sicurezza e di notifica degli incidenti per i soggetti inizialmente qualificati come Infrastrutture Critiche/Operatori di Servizio Essenziale (OSE).

Il termine di recepimento della direttiva CER, come per la NIS 2, è fissato per il **18 ottobre 2024**, mentre entro il **17 luglio 2026** ogni stato dovrà individuare i soggetti critici destinatari della normativa.

Tipologie di soggetti introdotti dalla NIS2, confronto con CER e PSNC

Il Digital Operational Resilience Act, o **regolamento DORA** dell'UE, stabilisce un **framework vincolante per la gestione del rischio** delle tecnologie di informazione e comunicazione (ICT) per le entità finanziarie e i loro fornitori critici di servizi tecnologici di terze parti, che dovrà essere recepito dai singoli stati membri entro il **17 gennaio 2025**.
La NIS 2 e la direttiva CER riconciliano il concetto di sicurezza fisica con quello della sicurezza logica (o cyber), a partire dalla valutazione del rischio che dovrà tenere conto – come nel caso delle entità destinatarie della seconda – non solo di minacce cyber, ma anche di minacce cinetiche sia naturali che antropiche, volontarie o involontarie, ivi compresa la minaccia terroristica.

Settori	PSNC	NIS2	Altre normative	Collegamento
PA centrale	Governativo, Interno, Previdenza	PA Centrale	CAD Regolamento Cloud	CER
PA locale	Interno	PA Locale		CER
Difesa	Difesa			
Spazio e aerospazio	Spazio e aerospazio	Spazio		CER
Energia	Energia	Elettrico, Teleriscaldamento, Petrolio, Gas, Idrogeno	NCCS	CER
Telco	Telecomunicazioni	Servizi e reti di comunicazione elettronica pubblici	EECC	CER
Infrastrutture e servizi digitali	Infrastrutture e servizi digitali	Infrastrutture e servizi digitali, MS(S)P	Regolamento Cloud	eIDAS
Economia e Finanza	Economia e finanza	Bancario, Infrastrutture dei mercati finanziari		DORA
Trasporti	Trasporti	Trasporto aereo, ferroviario, per vie d'acqua, su strada, TPL	Regolamento 2015/1998	CER
Tecnologie e ricerca	Tecnologie critiche	Ricerca		CER
Salute		Assistenza, Laboratori di analisi, Farmaceutico		CER
Ambiente		Acqua potabile, Acque reflue, Gestione rifiuti		CER
Servizi postali		Servizi postali e di corriere		
Fabbricazione		Fabbricazione (dispositivi medici, computer e elettronica, apparecchiature elettriche, macchinari, mezzi di trasporto), nonché Fabbricazione, produzione e distribuzione di sostanze chimiche		
Alimentare		Produzione, trasformazione e distribuzione di alimenti		CER

Analisi: focus sull'elemento organizzativo

Il punto di attenzione per l'UE è proprio questo: la **convergenza tra sicurezza fisica e cyber security in materia di protezione dei settori critici**, elemento che non potrà non avere ripercussioni sull'organizzazione aziendale degli operatori privati destinatari della normativa europea.

L'approccio tradizionale di isolare le infrastrutture critiche dal mondo esterno non è più praticabile e mentre si sta sviluppando una sempre maggiore connessione dei sistemi industriali tramite reti IT, si sta ampliando il divario tra la capacità di offesa e quella di difesa.

I criteri di adozione della CER a livello nazionale, i requisiti di sicurezza per i vari settori, l'indicazione dell'entità che dovrà garantirne l'attuazione ed il monitoraggio, sono ancora in fase di definizione. **Non è ancora chiaro l'indirizzo politico che si vorrà seguire in Italia**, se lasciare la competenza in ambito **militare**, coinvolgere **ACN** con un ampiamento delle sue competenze o creare un'**agenzia**, omologa della ACN, ma con competenze sulla sicurezza cinetica, come è stato per il Department of Homeland Security – DHS statunitense, in ottica di convergenza della sicurezza fisica e logica in materia di protezione dei settori critici.

La direttiva CER *(Critical Entity Resilience)* (direttiva UE 2022/2557), così stabilisce:

*"(29) I soggetti critici dovrebbero adottare **misure tecniche**, di **sicurezza** e **organizzative adeguate** e proporzionate ai rischi cui sono esposti, allo scopo di prevenire gli incidenti, di proteggersi da essi, di darvi risposta, di resistervi, di mitigarli, assorbirli, di adattarvisi e di ripristinare le proprie capacità operative. …//… Per promuovere un approccio coerente a livello di Unione, la Commissione dovrebbe, previa consultazione del gruppo per la resilienza dei soggetti critici, adottare linee guida non vincolanti per specificare ulteriormente tali misure tecniche, di sicurezza e organizzative. Gli Stati membri dovrebbero provvedere affinché ciascun soggetto critico designi **un funzionario di collegamento o equivalente come punto di contatto con le autorità competenti**".*

*"(30) A fini di efficacia e di responsabilizzazione, i soggetti critici dovrebbero descrivere le misure da essi adottate con un livello di dettaglio che consegua sufficientemente gli obiettivi di efficacia e di responsabilizzazione stabiliti, tenuto conto dei rischi individuati, in un piano di resilienza o in uno o più documenti equivalenti a un piano di resilienza, e dovrebbero mettere in pratica tale piano. Qualora un soggetto critico abbia già adottato misure tecniche, di sicurezza e organizzative e redatto documenti conformemente ad altri atti giuridici pertinenti per le misure di rafforzamento della resilienza ai sensi della presente direttiva, esso dovrebbe poter utilizzare tali misure e documenti per soddisfare i requisiti riguardo alle misure di resilienza di cui alla presente direttiva. Al fine di evitare duplicazioni, **un'autorità competente** dovrebbe poter dichiarare conformi ai requisiti della presente direttiva, in tutto o in parte, misure di resilienza esistenti adottate da un soggetto critico che rispondono ai suoi obblighi di adottare misure tecniche, di sicurezza e organizzative ai sensi della presente direttiva"*

In questo quadro in continua evoluzione volevo condividere delle riflessioni sulle direttive co-

munitarie citate che, sebbene rappresentino un passo importante nella direzione di sviluppare una strategia di resilienza comunitaria, **non definiscono in maniera chiara e cogente requisiti di tipo organizzativo per l'operatore privato nazionale**, chiamato a fare investimenti ed a garantire il rispetto dei requisiti di sicurezza richiesti.
L'elemento organizzativo può influenzare molto la capacità di una azienda/entità critica di migliorare la postura di cyber security come richiesto dalla NIS 2 e di garantire i livelli di resilienza richiesti dalla direttiva CER, ed avere un impatto in termini di **responsabilità che potrebbe risalire fino al vertice aziendale**.
Si pensi, ad esempio, alla responsabilità della gestione ICT per le entità finanziarie che il Regolamento DORA fa risalire fino ai membri del **Consiglio di Amministrazione, ai dirigenti e senior managers** i quali dovranno definire adeguate strategie di gestione del rischio, a partire dalla valutazione di impatto sui processi critici e dalla definizione di piani di continuità operativa e disaster recovery.
Un tiepido riferimento organizzativo lo troviamo in Italia nel **DPCM 14 aprile 2021, n. 81** "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", dove la misura ID.AM-6 inclusa nell'Allegato B indica :
*"È nominato, nell'ambito dell'articolazione di cui al punto 2, **un incaricato, e un eventuale sostituto**, con il compito di gestire l'attuazione delle disposizioni del decreto-legge previste per i soggetti inclusi nel perimetro, in possesso di **specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto incluso nel perimetro** ed assicura, almeno:*
• l'efficace implementazione delle misure di sicurezza di cui al DPCM 2;
• la corretta esecuzione degli adempimenti relativi alla notifica degli incidenti aventi impatto su un bene ICT ai sensi dell'articolo 1, comma 3, lettera a), del decreto-legge;
• la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS), e con i soggetti incaricati dello svolgimento delle attività di verifica e ispezione di cui all'articolo 1, comma 6, lettera c), del decreto-legge."
Accade che in aziende, anche di grandi dimensioni e che potremo considerare come entità critiche, la **funzione che gestisce le attività riconducibili al processo di security trovi collocazione organizzativa nei modi più diversi da settore a settore, spesso non a riporto della funzione datoriale e del vertice aziendale** che detiene il potere decisionale. A volte la funzione di cyber security è separata dalla organizzazione che si occupa di sicurezza fisica, oppure "integrata" all'interno della funzione ICT, che ha come scopo dover garantire l'erogazione dei servizi IT, con un focus relativo sugli aspetti di security.
Una funzione security che non riporti direttamente al vertice ed al board aziendale avrà una montagna da scalare, prima di ottenere gli strumenti anche economici per adeguare l'organizzazione ai nuovi ed elevati livelli di sicurezza richiesti dalla normativa europea, dovrà fare uno **sforzo immane per ottenere il *change management* necessario**, nonostante l'obbligatorietà della trasformazione.
In considerazione del nuovo quadro normativo europeo, gli **organi di controllo interno di una entità critica**, destinataria delle citate direttive europee in materia di sicurezza, **dovranno dotarsi delle competenze necessarie per svolgere le azioni di loro pertinenza**.
Lo stesso varrà per i **membri del Consiglio di Amministrazione**, che dovranno mettersi in condizione di poter **valutare adeguatamente il rischio cyber dell'azienda che fosse individuata come infrastruttura critica e quindi soggetta alle restrizioni dell'UE**.
È fondamentale quindi definire ruoli e responsabilità ed una robusta governance che possa aiutare a mitigare i rischi informatici e garantire la disponibilità di adeguate risorse umane e tecnologiche.

Ipotesi di lavoro

Alla luce di queste considerazioni sarebbe opportuno **lavorare sul tavolo del legislatore nazionale, per inserire in fase di recepimento della normativa europea anche dei modelli organizzativi *"standard"* in materia di sicurezza fisica e cyber almeno per gli operatori destinatari della NIS 2, direttiva CER, regolamento DORA.**
Lavorare sulle nuove norme europee potrebbe essere un'**ottima opportunità**, per colmare le lacune del D.L 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro e nel D.Lgs 231/2001 Responsabilità amministrativa

delle società e degli enti – "colpevoli" – se così si può dire, di non aver espressamente previsto il ruolo di security manager a supporto del Datore di Lavoro, sebbene abbiano contribuito in maniera determinante ad affermare la necessità, da parte del Datore di Lavoro, di dotarsi di un'efficiente organizzazione per valutare e gestire tutti i rischi, inclusi quelli specifici di security.

Il **CISO** – Chief Information Security Officer, è un profilo professionale oggi sempre più diffuso nelle moderne e grandi aziende che, grazie a competenze, conoscenze e ad una profonda consapevolezza dei processi interni, è in grado di assumere il ruolo di Responsabile della sicurezza informatica definendo la giusta strategia di protezione degli assets aziendali dalla minaccia cyber.

Un'unica funzione aziendale per la sicurezza logica e la sicurezza fisica, inclusiva del ruolo di CISO – Chief Information Security Officer, potrebbe **assicurare il coordinamento necessario nella gestione della sicurezza fisica e cyber di un'organizzazione critica**.

In tal senso si era espressa anche la **ISO/IEC 27014** – "Governance of Information Security", per la quale la governance della sicurezza delle informazioni dovrebbe garantire che gli obiettivi di sicurezza delle informazioni siano **completi e integrati** e che le attività riguardanti la **sicurezza fisica e logica siano strettamente coordinate**.

Un sistema così centralizzato e coordinato, necessariamente a riporto del vertice aziendale, **potrebbe assicurare**:

- coinvolgimento della funzione security di riferimento e delle figure specialistiche di security in tutte le attività gestionali e operative, sin dalla fase strategica delle attività di business;
- conformità all'ampiezza e alla complessità (a livello nazionale e internazionale) del quadro normativo, tecnico e regolamentare di riferimento;
- garanzia che la funzione security a tutti i livelli abbia la capacità di gestire emergenze e crisi, in un ambiente operativo volatile in tutto il mondo, dove gli accadimenti non sempre sono riconducibili solo ad un evento fisico o solo ad un evento cyber, ma spesso hanno cause concorrenti (si pensi ad esempio ad un attacco cyber ad un mezzo in navigazione, oppure ad una piattaforma petrolifera in perforazione, oppure ai danni di un aeroplano in volo, ovvero ai danni di una condotta sottomarina);
- ottimizzazione, vale a dire utilizzo più efficiente delle risorse;
- offerta di soluzioni di security ottimizzate per le operazioni del business;
- analisi di impatto sui processi critici, piani di continuità operativa;
- collegamento con ICT, funzione commerciale, Affari Legali e Compliance, entreprise risk management;
- certificazione di beni o servizi considerati critici;
- qualifica della catena di approvvigionamento per beni o servizi valutati come critici.

Una volta definito uno o più **modelli tipo di organizzazione di security aziendale**, che siano di riferimento per i Paesi membri UE, sarà più semplice sviluppare misure coordinate per garantire la **continuità operativa** di infrastrutture che sono critiche per l'economia, la salute, la sicurezza pubblica e privata.

Un supporto verrà anche da **ENISA** "Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione" istituita nel 2004 che, con l'aggiornamento del **"Cybersecurity Act"** ha assunto un ruolo molto più operativo nella gestione di un cyberattacco, ed in materia di certificazione.

Il *"Framework Nazionale per la Cybersecurity e la Data Protection"*, versione italiana del più noto **"Cybersecurity Framework"** ideato dal **NIST** – *"National Institute of Standard and Technology"*, rappresenta poi uno strumento possibile in Italia per l'organizzazione della strategia di difesa rispetto alle minacce cibernetiche, un percorso che le organizzazioni – qualunque esse siano – potrebbero seguire per **misurare la propria postura di cybersecurity in relazione al contesto di riferimento**.

Ultima considerazione – ma non di minor valore – è quella relativa al fatto che **l'adeguamento alle nuove norme europee in materia di sicurezza (fisica e logica) e resilienza comporterà anche un notevole impegno economico** da parte degli operatori privati/entità critiche impattati, che dovrà essere considerato e regolato in fase di recepimento nazionale, per non compromettere la competitività degli stessi sul mercato.

Conclusioni

Riferimenti normativi comuni, linguaggio comune, un elevato livello di preparazione di chi è chiamato a ricoprire ruoli manageriali, ma soprattutto una **funzione security integrata come unico interlocutore con le competenti entità nazionali governative**, sono garanzie per l'ottenimento degli obiettivi comunitari di resilienza fissati dall'UE con le nuove direttive.

"La buona notizia c'è, ed è quella che ormai non si può più tornare indietro".

Va, pensiero.

Dall'indifferenza al panico, il pensiero tormentato della sicurezza

a cura di Cristhian Re

Introduzione

L'articolo di Corrado Miralli *(ndr. pagg. 56, 57, 58)* si abbatte come un macigno sul lastricato di indifferenza ai temi della sicurezza che nelle aziende è diventato pavimento di rappresentanza. Quello di Miralli non è un avvertimento, ma un **grido d'allarme**, rispetto a quell'**indifferenza incongrua davanti alla produzione legislativa che si scarica a valanga**, stimolata da urgenze che tutti si erano illusi di aver lasciato nel millennio trascorso. Il mondo è cambiato, sostiene un luogo comune dettato dal senso pure comune; il mondo è sempre quello, ribattono coloro che del mondo qualcosa capiscono. Alle facili illusioni bisogna opporre la concretezza di un **realismo consapevole**, che istinti e pulsioni sono rimasti praticamente immutati dal tempo non molto lontano delle caverne. **L'allarme di Miralli** non ci ha colti di sorpresa e, in passato, in più occasioni siamo intervenuti su molti degli aspetti chiamati in causa e, soprattutto, sulle dinamiche di quella cultura della sicurezza che per troppo tempo si è limitata a discettare di organizzazione dei turni di vigilanza ai cancelli. Neppure nel Medioevo il concetto aveva assunto un profilo così meschino.

Ci chiediamo se il **Legislatore, artefice di questa valanga**, forse a sua insaputa, non sia **in preda a un attacco di panico**. Solo così si giustifica questa fibrillazione legislativa che dissemina di **straordinari e inaffrontabili incombenti** quel sentiero della sicurezza che per i più era ingentilito dalle fioriture primaverili che nascondevano le asperità di un puntuto acciottolato.

Insomma, a una sola figura professionale vengono richieste, di colpo, competenze la cui sola definizione comporterebbe l'impiego di un professionista.

Un guazzabuglio. Ecco l'allarme.

Alla ricerca di un metodo. Tavole di normativa comparativa

I **regolamenti** dell'Unione Europea hanno portata generale e, in quanto atti giuridici vincolanti, sono direttamente applicabili in ciascuno Stato membro. Le norme contenute in un regolamento entrano in vigore e cominciano a produrre effetti giuridici, senza bisogno di misure di recepimento da parte dei singoli Stati.

Le **direttive**, invece, hanno portata individuale e sono obbligatorie solo nel fine che intendono perseguire. Sarà il Legislatore nazionale che, nel recepirle, sceglierà i mezzi per ottenerlo. L'elemento principale che contraddistingue le direttive dai regolamenti è la libertà di iniziativa normativa.

Le recenti **NIS 2** (Network and Information Systems) e **CER** (Critical Entity Resilience) sono direttive UE come lo erano le rispettive ascendenti **NIS** e **2008/114/EC**, la seconda delle quali, ad esempio, nonostante il recepimento del **D. Lgs. n. 61/2011**, è rimasta **lettera morta**. Perché si trasformasse in lettera viva mancava il decreto attuativo, ma soprattutto il formale atto di designazione delle infrastrutture ritenute appunto critiche. In compenso, però, al torpore dell'Italia ha fatto da contrappunto la solerzia di Paesi vivaci e ricettivi come la Romania che

ne ha designate da subito parecchie decine. Tre anni per recepire una direttiva e sedici per non attuarla. Nel frattempo, l'Unione Europea ha deciso di legiferare ancora: ha abrogato la vecchia sostituendola con una nuova, per molti aspetti quasi analoga. In entrambe, pochi lo sottolineano, si prevede espressamente la figura del **funzionario di collegamento**, ovvero il punto di contatto all'interno delle Organizzazioni (Pubblica Amministrazione e aziende) con le autorità competenti. **Non si tratta di un mero obbligo amministrativo. Si traduce in cambiamenti organizzativi di rilievo** e, come sempre, **risorse da impiegare e capitali da investire**. Tutto questo mentre in azienda i budgets si contraggono. Chi ha legiferato ha forse pensato ai profili (e relative competenze) da ricercare e ingaggiare? Ha pensato ai riflessi organizzativi interni che gli interventi richiesti provocheranno? Ha pensato ai denari che le aziende dovranno spendere per la realizzazione di quelle determinate attività e misure da adottare?

Altra norma di ambito. Per i soggetti inclusi nel **Perimetro di Sicurezza Nazionale Cibernetica (PSNC)**, tra le innumerevoli cose, si segnala anche la necessità di nominare un incaricato (e un eventuale sostituto), in possesso di specifiche professionalità e competenze in materia di sicurezza cibernetica, con il compito di gestire l'attuazione del Decreto-Legge Perimetro e di riferire direttamente al vertice gerarchico, nonché un apposito **referente tecnico** (e almeno un suo sostituto), in possesso di competenze specialistiche in materia, per lo svolgimento delle funzioni di interlocuzione con il **Computer Security Incident Response Team (CSIRT)** ai fini della gestione degli incidenti. Anche qui potremmo anaforicamente ripetere le stesse domande di cui sopra.

In ambito Tutela del Segreto di Stato, invece, il **D.P.C.M. 5/2015** prevede la nomina di un **funzionario alla sicurezza**, oltretutto di elevato livello gerarchico e munito di adeguata abilitazione di sicurezza (**NOS**), che svolga compiti di direzione, coordinamento, controllo, nonché attività ispettiva e di inchiesta in materia di protezione e tutela delle informazioni classificate. Idem come sopra.

Potremmo proseguire, ma preferiamo fermarci qui. L'**elenco** delle norme (cogenti e volontarie), in particolare negli ultimi anni, **si è esteso così notevolmente da sembrare una esplosione, e si è rivolto a singoli settori di business** (o a più settori tra loro omogenei) al punto che per comprenderne davvero la complessità si deve essere abili nel convertire i contenuti delle norme in check lists (o questionari di rilevazione, come si definivano fino a qualche anno fa) e poi accostarle tra loro, esattamente come con le tavole di linguistica comparativa. Si viene colti da un senso di vertigine, per superare il quale si è costretti a **far ricorso a database capaci di interrelare e correlare documenti, dati, informazioni**, ecc. trasferendo la relazione dal piano bidimensionale (lunghezza) a quello tridimensionale (profondità).

Spirito critico come argine alla superfetazione normativa

Tornando alla nostra casistica, prendiamo in esame una azienda che opera nel settore spaziale, fornendo soluzioni ad alta tecnologia (civile e militare) per telecomunicazioni, navigazione, osservazione della Terra, gestione ambientale, ricerca scientifica e infrastrutture orbitali. Essa risulta destinataria delle quattro norme sopracitate (D.P.C.M. 5/2015, PSNC, NIS 2, CER). Supponendo che l'azienda disponga già di un Security Manager, egli sommerà anche gli incarichi di funzionario alla sicurezza, incaricato e funzionario di collegamento? Sarà in grado di reggere i quattro differenti incarichi? Riunirà i requisiti (anche giuridici) richiesti e le competenze necessarie? Saprà tracciare i confini, ammesso che ci siano, tra l'una, l'altra e le restanti norme? E se l'azienda decidesse, per ragioni legate a equilibri interni o di carattere interpretativo, di assegnare i ruoli a quattro soggetti diversi, chi sarebbe l'interlocutore per la sicurezza? Perché, ricordiamocelo, la **Sicurezza** è **sempre e solo una**. E, infine, se oltre al Security Manager ci fossero anche un Chief Information Officer (CIO) e/o un Chief Information Security Officer (CISO), cosa andrebbe al primo, cosa ai secondi?

Fin qui il tema legato a ruoli e responsabilità. Passiamo al **lavoro**, aspetto ben più rilevante del precedente. Le quattro normative impongono adempimenti amministrativi, interventi tecnico-organizzativi e specifiche contromisure solo in parte congruenti e con finalità diverse, perché distinti sono gli interlocutori della Pubblica Amministrazione e differenti i livelli di robustezza, i modelli di maturità, la postura di sicurezza! Solo chi quotidianamente compulsa e pratica quelle norme può comprendere a pieno le difficoltà e la fatica che la loro applicazione richiede.

Come mi ripeteva **Giulio Carducci**, "solo dopo aver aggiunto i calli alle mani a quelli al cervello sarai in grado di comprendere gli effettivi contorni del lavoro che ti attende e le concrete ricadute

sull'organizzazione. È **Lavoro**, non dimenticarlo". Limitarsi a intuire cosa richiede la norma e delegare l'attuazione a docili collaboratori o corrivi consulenti non sviluppa lo spirito critico del manager, anche se diventa il suo argomento in convegni, seminari e interviste.
Per paradossale che sia, quanto sopra descritto è ciò che accade in un **mondo "ideale"**, cioè dove magicamente dall'alto piovono disposizioni conformi al disposto normativo che producono cambiamenti in un ambiente già pronto (organizzativamente e finanziariamente) a riceverle e attuarle. Sforzatevi ora di immaginare cosa accade nel **mondo "reale"**, quello in cui, muovendo affannosamente dal basso, si deve spiegare al Decisore (il Top Management) le novità introdotte da una o più norme, le ridondanze, le bizzarrie e le contraddizioni intrinseche, le ripercussioni sull'organizzazione e le finanze, i nuovi perimetri di responsabilità, gli scenari caratterizzati da resistenze interne, le sanzioni che ne derivano, ecc. È **un'impresa improba**, poiché si è **chiamati a razionalizzare iniziative legislative carenti di un'unitaria visione d'insieme**. "Un fenomeno – affermava **Paul Watzlawick** – resta inspiegabile finché il campo di osservazione non è abbastanza ampio da includere il contesto". Probabilmente bisognerà attendere quel momento. Arriverà, abbiate fede. Oggi, però, siamo ancora lontani da una trattazione chiara, ordinata e sistematica della materia, come invece è avvenuto per la Safety (**TU 81/08**), la sicurezza privata (**DM 269/2010**), gli appalti (**D.Lgs. 36/2023**), la Privacy (**Regolamento 2016/679**) e altre discipline.

Il maestro e Margherita

Siamo abbastanza maturi per ricordare la **BS 7799**, lo standard britannico **"Code of Practice for Information Security Management"**, pubblicato nel 1995 dal British Standards Institution (BSI), la progenitrice della più nota ISO 27001. Certificazione (la BS 7799) ambitissima, elitaria ed estremamente selettiva. In Italia, in quel periodo e in ambito Security, l'unico a parlarne fu il maestro **Carducci, Giulio** non Giosuè. Con ragguardevole intuito egli notò questa Margherita emergere nel vasto campo, neppure dissodato, della sicurezza. Un autentico coup de foudre. Ne seguì un poderoso manuale divenuto un caposaldo per gli analisti del settore: **"La tutela dei dati nelle aziende e nelle istituzioni"** (Ed. Franco Angeli – 1999). Un antesignano. Erano anni in cui l'IT pensava a ben altro che **all'Information Security**. Noi si andava in giro parlando di Knowledge Base Building (KBB), engine, metriche, indici, terna RID, triadi, sistemi, classificazione dei macrodati, istanziazioni dei componenti, modellazione dei perimetri di intervento, classi di vicarianza, rischi ontologici, criticità specifica, funzionale, ereditata e tanto altro ancora. Marziani. Dal 2016, data della pubblicazione della NIS, la **Cyber Security** si è gradualmente e progressivamente insinuata nel tessuto pubblico e in quello privato sino al punto di soppiantare tutto, nonostante le ristrettezze di ambito e di applicazione. Oggi, forse per una questione di fascinazione semantica, è il **tema di maggiore interesse** di cui si dibatte, quello intorno al quale maggiormente si iperlegifera e in forza del quale si costituiscono enti governativi (**DPCM 223/2021**) capaci di prevenire e fronteggiare attacchi fantascientifici. È bene ricordare, infatti, che esiste una netta differenza tra l'Information Security e la Cyber Security, benché vi sia l'erronea e diffusa tendenza a utilizzarle in modo intercambiabile, quasi fossero sinonimi. L'Information Security si riferisce alla protezione dei dati fisici e digitali da uso, accesso e modifica non autorizzati. La Cyber Security, invece, alla protezione dei soli dati digitali da uso, accesso e modifica non autorizzati. È un di cui. Se chiediamo a uno del mestiere di quale titolo preferirebbe fregiarsi, direbbe senza indugio il primo, perché contiene il secondo. Al di sopra di entrambe, l'infinito **Cyber Space**.

Non occorre essere un guru in Information Security per avvertite un moto di tenerezza al suono del prefisso cyber (timone), basta un po' di curiosità linguistica. È proprio il suo etimo, infatti, a svelarci la relazione metonimica che regge le due sfere della Security: l'Information sta alla Cyber, come il veliero sta al timone. E il Cyber Space? L'oceano intergalattico quadridimensionale in cui naviga il nostro veliero servendosi anche (e non solo) del tanto magnificato timone. Magari andrebbe deferentemente sussurrato all'orecchio del solerte Legislatore.

Conclusione

Caro Legislatore, il nostro, per quanto ponderoso, è appena un sussurro perché il tema nella sua complessità è tale da atterrire e rendere afona ogni voce. Perché correre il rischio che d'improvviso sia un coro a levare la protesta? Sia un coro a intonare l'allarme? Sia un coro a svegliare le coscienze? **A quando un Testo Unico?** Noi intanto riflettiamo.

La strada del successo lavorativo:
coltivare le emozioni

a cura di Giulia Cavalli
psicologa psicoterapeuta, psicoanalista

Ormai (si spera!) sembra superata l'immagine del lavoratore "freddo", che svolge al meglio i suoi compiti se si comporta come un robot senza emozioni. Tuttavia non è così semplice, nella concretezza del lavoro quotidiano, capire come e quali emozioni siano davvero utili. È esperienza comune che alcune emozioni ostacolino i processi cognitivi (comprendere le situazioni, prendere decisioni, agire razionalmente,…), ma non è sempre così. Gli studi sul cervello umano, svolti negli ultimi decenni dai neuroscienziati interessati a capire come si apprende con successo qualcosa e come si riesca ad applicare ciò si è appreso in diversi contesti, possono aiutarci a far luce sulla questione.

In sintesi, emergono due aspetti fondamentali, a mio parere, non solo in contesti di puro apprendimento (come la scuola), ma anche in ambito lavorativo:

- **cognizione ed emozione non possono essere separati**, perché **le emozioni** (non tutte, ma poi specificheremo quali) **guidano con successo** verso le strade più giuste nel risolvere un problema, nel decidere, nell'analizzare e così via;
- coloro che svolgono ruoli dirigenziali sono fondamentali, perché si creino **ambienti sociali di lavoro in cui emozioni e cognizioni possano davvero andare a braccetto**.

L'Iowa Gambling Task

Per comprendere quali emozioni siano utili per guidare al successo lavorativo, può essere utile analizzare ciò che avviene solitamente in un contesto sperimentale, a lungo studiato nelle ricerche, denominato ***Iowa Gambling Task*** (ideato da Bechara e collaboratori nel 2005). Di fatto è un gioco d'azzardo, in cui il giocatore deve pescare delle carte da quattro mazzi. Ogni carta pescata può far vincere o perdere somme più o meno consistenti di denaro. Il giocatore non è a conoscenza del fatto che alcuni mazzi hanno probabilità di generare grosse vincite rispetto ad altri e che questi stessi mazzi possono portare a consistenti perdite occasionali, per cui a lungo termine non conviene continuare a pescare da questi.

Come fa il giocatore a soppesare i risultati dei vari mazzi e a compiere quindi, in breve tempo ed efficacemente, le scelte vincenti? Non si tratta di calcolare le probabilità (cosa che potrebbe richiedere molto tempo), anzi, la razionalità non c'entra nulla.

La risposta che i ricercatori hanno trovato è che tutto questo (che sembra un processo puramente razionale e cognitivo) avviene attraverso le emozioni, in particolare quelle che vengono definite **"intuizioni emotive"**, che inizialmente non sono coscienti.

In pratica il giocatore pescando dai vari mazzi, prima ancora di capire le regole sottostanti, **mostra delle risposte emotive anticipatorie**: per esempio, se sta per prendere una carta da un mazzo ad alto rischio di perdita, inizia ad avere le mani sudate in maniera microscopica (non ne è consapevole). Come a dire, che la **parte subcosciente** sta accumulando informazioni sui mazzi più "sicuri" e quelli più rischiosi, grazie alle risposte emotive, che progressivamente vengono accumulate come **risorsa preziosa, ma ancora inconsapevole, per orientare il comportamento**. Dopo aver giocato per un po', il giocatore riesce facilmente a dire a parole, quindi coscientemente, quali sono le regole dei mazzi.

Il ruolo delle emozioni

Le emozioni hanno, perciò, funzionato come un **navigatore** e consentono di **richiamare le conoscenze rilevanti per guidare nel tempo i comportamenti**. Imparare a cogliere in sé le intuizioni emotive legate a un certo processo lavorativo, consente di arrivare più rapidamente al successo, perché insegnano come muoversi e lo fanno attraverso **reazioni emotive di disappunto, eccitazione, preoccupazione e così via**. Quando diciamo che "a naso" o "di pancia" prendere una strada piuttosto che un'altra non ci convince o ci sembra una buona idea, probabilmente l'intuizione emotiva ci sta guidando.

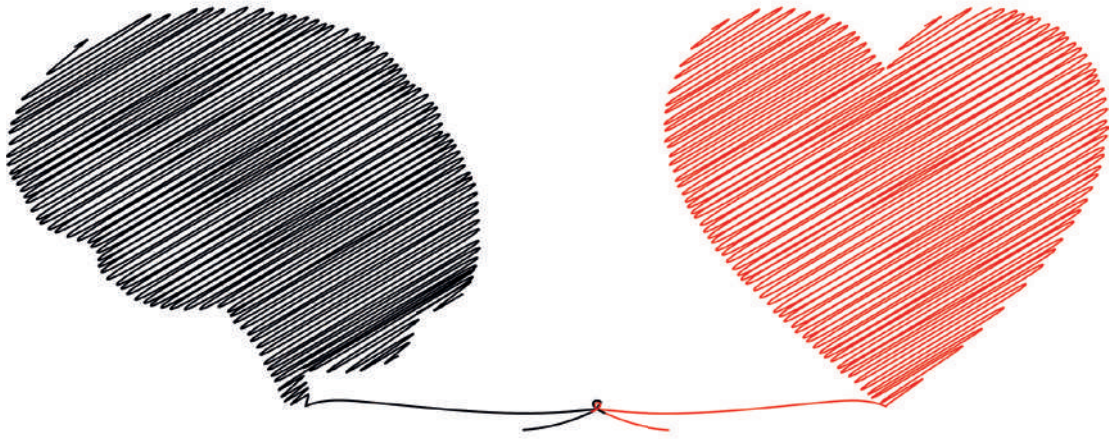
Ma non sempre queste intuizioni sono corrette, a volte perché metaforicamente non c'è stato il tempo di pescare dai vari mazzi e, quindi, di esplorare la situazione, ma il più delle volte perché le emozioni provate non sono completamente riferite a ciò che stiamo vivendo in quel contesto.

Perché i "capi" al lavoro sono così importanti?

Perché i **loro feedbacks**, che andranno necessariamente a coinvolgere l'emotivo dei loro collaboratori, imprimono una direzione alle intuizioni emotive. Banalmente ricevere un complimento o un incoraggiamento, piuttosto che uno sguardo di biasimo o una lavata di capo fine a sé stessa (cioè, non con l'obiettivo di far crescere chi si ha di fronte, ma per sfogarsi di qualcosa andato storto) da parte di un capo, è come pescare da un mazzo con buone probabilità di vincita (soddisfazione) o di perdita (paura). **Le emozioni si connettono implicitamente e immediatamente alla conoscenza cognitiva di quell'ambito e nel futuro tutte le mosse fatte in quell'ambito saranno guidate da questo tipo di sottofondo emotivo, con le relative conseguenze.**

Vivere, per esempio, la paura, anche se in modo inconsapevole, nello svolgere un determinato compito, non lascia spazio alle altre emozioni, che potrebbero essere utili per sviluppare delle buone intuizioni emotive. Se, nel caso del gioco di carte, il giocatore vive con ansia il pescare le carte, magari a causa delle ansie di un proprio superiore, come può sentire i sottili cambiamenti emotivi che gli rivelano quali sono i mazzi migliori? Ma anche se il giocatore è troppo preso da emozioni estremamente positive non relative a ciò che sta svolgendo (magari perché la sua testa è già alla gioiosa serata con gli amici), difficilmente potrà imparare qualcosa sulle regole dei mazzi. Ovvero **quando le emozioni non sono suscitate da ciò che si sta facendo, ma sono indipendenti da esso, allora le emozioni sì che diventano elementi di distrazione e fanno fallire l'intuizione emotiva!**

In effetti le ricerche mostrano che in questi casi, in cui le emozioni non sono generate direttamente dal gioco, il giocatore non riesce a capire le regole sottostanti dei vari mazzi. Non è efficace rimuovere le emozioni del tutto (come mostrano bene i pazienti con danni neurologici, che non avendo emozioni, non riescono a prendere buone decisioni o a trovare le strade migliori per il successo), così come non lo è vivere emozioni irrilevanti rispetto a ciò che si sta svolgendo. Si tratta allora di **coltivare contesti lavorativi dove le emozioni siano rilevanti rispetto al lavoro**. Ed è importante dar spazio a queste emozioni, per consentire **l'integrazione efficace di emozioni e cognizioni**.



Fai un salto con la sicurezza di PASO

a cura di Roberto Megazzini,
Direttore Tecnico Commerciale PASO

Le norme di riferimento per le attività di pubblico spettacolo

Le manifestazioni di pubblico spettacolo che si svolgono in luoghi e spazi all'aperto accessibili a chiunque, sono anch'esse presenti nell'elenco attività soggette ai controlli di prevenzione incendi (**attività n. 65 del DPR 151/2011 - Regolamento della prevenzione incendi**).
La nuova Regola Tecnica Verticale (RTV), emanata con il **DM del 22/11/2022**, per le attività di intrattenimento e di spettacolo introduce nel Codice di Prevenzione Incendi il **capitolo V.15** "Attività di intrattenimento e di spettacolo a carattere pubblico".
Anche in questo caso la nuova RTV è l'alternativa a quella di cui al **DM del 19/08/1996**, confermando la caratteristica principale che contraddistingue il Codice di Prevenzione Incendi: quella di non abrogare norme precedenti e poter essere applicato facoltativamente in alternativa. Fa eccezione il **DM 15/05/2020**, in vigore dal 19/11/2020, che, oltre ad approvare la RTV per le attività di autorimessa (**capitolo V.6**), ha abrogato il **DM 01/02/1986**.

Il sistema di allarme vocale per l'evacuazione di emergenza (EVAC) e le attività di pubblico spettacolo

Nelle attività di intrattenimento e pubblico spettacolo, sia a carattere fisso che temporaneo, il sistema **EVAC** consente di informare tempestivamente le persone di un'eventuale situazione di pericolo in atto, cosa che con i tradizionali sistemi ottici acustici non sempre è di immediata comprensione.
Lo scopo di questo tipo di impianti è quello di fornire, in condizioni di emergenza, **comunicazioni chiare volte ad informare e guidare tutte le persone presenti** nelle aree a rischio, in modo che possano agire nel modo più appropriato.
Gli impianti EVAC sono in grado di trasmettere mes-

saggi dai **contenuti specifici**, che possono andare dal semplice avvertimento fino all'avviso in caso di evacuazione vera e propria; possono inoltre trasmettere **messaggi con qualunque contenuto e in qualunque lingua**, aspetto importante per quelle attività a carattere internazionale, rendendoli quindi uno strumento utile ed efficace anche per le comunicazioni ad un vasto pubblico. In questo articolo vogliamo evidenziare come l'impianto di evacuazione vocale possa essere definito ***"dual purpose"***, ossia essere utilizzato anche in condizioni ordinarie per diffondere musica o annunci. Questa è la funzione che rende l'impianto EVAC particolarmente flessibile nell'uso ma soprattutto è **la caratteristica che permette di coniugare in un'unica soluzione sicurezza e servizi per l'attività**.

A tal proposito, una delle applicazioni più interessanti che PASO ha realizzato è stato **l'impianto di evacuazione vocale** di un **grande centro equestre**, dove vengono organizzati concorsi di salto ostacoli fino ai massimi livelli, con la partecipazione dei grandi nomi dell'equitazione italiana ed internazionale.

PASO S.p.A. con i suoi sistemi di **diffusione sonora per l'evacuazione vocale** è stata in grado di rispondere alle specifiche richieste dalle norme vigenti e di offrire **contemporaneamente una soluzione completa per la realizzazione di un impianto audio di diffusione sonora** al servizio della struttura, durante il normale svolgimento degli innumerevoli eventi e gare di livello internazionale che ospita.

Il centro dispone di strutture di altissimo livello che comprendono più campi gara (**sia indoor, che outdoor**): l'impianto è stato quindi realizzato con un'architettura decentralizzata utilizzando i compatti **ALL-IN-ONE** della serie **PAW4500-VES** (sistemi d'evacuazione vocale integrati per impianti di emergenza, dotati di unità di controllo certificata a norma **EN 54-16** ed **EN 54-4**). L'impiego di diffusori sonori (tipo C1100-EN, certificati EN 54-24), idonei per installazioni in esterno

e caratterizzati da un'eccellente riproduzione sia della musica che del parlato, hanno completato l'impianto, rendendo gradevole la **qualità audio della musica** di sottofondo e trasmettendo gli annunci, le informazioni delle gare e i vari **messaggi di servizio chiari e perfettamente intelleggibili**.

Il Regolamento Prodotti da Costruzione (CPR)

a cura di Cristina Andreoni, CEO ELAN

La normativa CPR è, da tempo, argomento di discussione sia per gli installatori che per i progettisti della Sicurezza.
Il **Regolamento Prodotti da Costruzione (CPR)** è la normativa europea che definisce i **requisiti base e le caratteristiche essenziali armonizzate** che tutti i prodotti progettati per essere installati in maniera permanente in opere di costruzione devono soddisfare nell'ambito di applicazione dell'**UE**.


Cristina Andreoni

Tutti i cavi installati in **edifici** e **opere di ingegneria civile** soggetti a **requisiti prestazionali di reazione al fuoco**, siano essi di energia o di comunicazione o fibra ottica, devono essere **classificati**.
L'obiettivo del Regolamento CPR è, di fatto, quello di uniformare una volta per tutte le diverse normative presenti. Le norme sui cavi presenti a livello europeo differiscono, infatti, da quelle nazionali originando quindi livelli di sicurezza differenti. La CPR introduce nuovi criteri di classificazione e classi comuni, le cosiddette **Euroclassi** per l'intero territorio europeo.

La norma coinvolge tutti gli operatori economici della filiera:
- **fabbricante**, qualsiasi persona fisica o giuridica che fabbrichi un prodotto da costruzione o che faccia progettare o fabbricare tale prodotto e lo commercializza con il suo nome o con il suo marchio (Art.11)
- **mandatario**, qualsiasi persona fisica o giuridica stabilita nell'Unione Europea che abbia ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti (Art.12)
- **distributore**, qualsiasi persona fisica o giuridica nella catena di fornitura, diversa dal fabbricante o all'importatore, che metta un prodotto da costruzione a disposizione sul mercato (Art.13)
- **importatore**, qualsiasi persona fisica o giuridica, stabilita nell'Unione Europea, che immetta sul mercato dell'Unione Europea un prodotto da costruzione proveniente da un Paese terzo (Art.14).

I soggetti coinvolti sono tenuti a mostrare:
- **la marcatura CE**
- **la Dichiarazione di Prestazione** (DoP)
- **il Sistema di valutazione e verifica della costanza delle prestazioni** (AVCP) – a seconda della classificazione l'appartenenza ad una determinata classe e la costanza delle presta-

zioni dovranno essere controllate e certificate da Organismi Notificati (i cosiddetti Notified Bodies) indipendenti (es. IMQ).

La CPR, ELAN ed ELANFIRE

Sin dall'inizio, **ELAN ha costantemente lavorato per rendere conformi i propri cavi sicurezza LSZH e i cavi antincendio alla normativa CPR**.
Da oltre trent'anni ELAN è un'azienda produttrice di cavi bassa tensione e batterie ricaricabili per il comparto Sicurezza. All'interno della gamma di prodotti, è presente la **linea Elanfire, il cavo antincendio che si conferma come uno dei prodotti di punta dell'azienda Made in Italy**. In ELAN l'aggiornamento è continuo, proprio per adeguarsi alla sempre maggiore sensibilità del mercato ai cavi certificati. **L'ultima novità del 2024 è l'ampliamento della gamma cavi certificati Cca-s1a, d0, a1 secondo i requisiti della CPR EN 50575**.
Tre sono le tecnologie utilizzate finora per la produzione dei cavi resistenti al fuoco.
Nella prima tipologia, il conduttore in rame è ricoperto da un nastro di mica. I conduttori isolati con PPE non rispondono alla CEI 20/22 poiché molto infiammabili. L'affidabilità del cavo è dunque proporzionale alla qualità della mica.
La seconda generazione di cavi impiega il silicone. Tuttavia, anche in questo caso, la qualità molto economica dello stesso lascia dubbi sull'affidabilità in caso di incendio.

Tecnologia mica con mescola reticolata di tipo E29

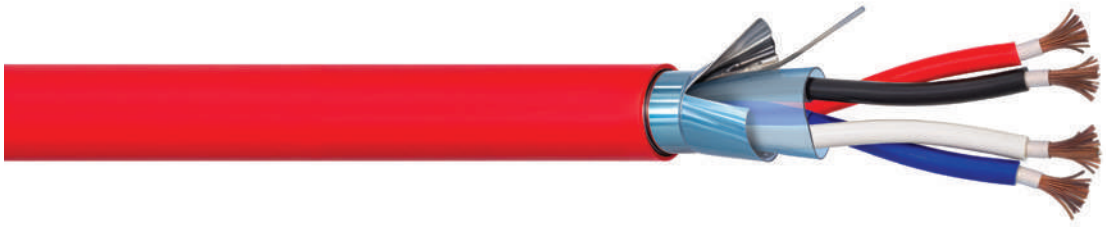
ELAN ha sviluppato una terza tecnologia denominata **ELANFIRE (PH120)**, il cavo resistente al fuoco che utilizza la tecnologia mica con impiego di mescola reticolata di tipo E29 **come da CEI 20-105V2**.
Nello specifico, **i cavi resistenti al fuoco ELANFIRE rientrano nella classe Cca – s1a, d0, a1**.
Questi cavi sono conformi alla EN 50200 PH120 (resistente al fuoco a 850°C per 2 ore), alla CEI 20-105, UNI 97-95 e CEI 36762.

Un ulteriore aspetto da tenere in considerazione per la scelta di un cavo fire sono le caratteristiche elettriche.
Con la CEI 20-105V2 si differenziano i cavi resistenti al fuoco in base alla tipologia di isolamento utilizzato dal produttore: nel caso di cavi isolati con silicone ceramizzante, il cavo dovrà essere marcato FTS29M16 se non schermato e FG29OHM16 se schermato. Se il cavo è isolato con mescola reticolata di tipo E29 e nastro di vetro micato, dovrà essere marcato FTS29OM16 se non schermato e FTE29OHM16 se schermato. Questo perché, anche se le 2 tipologie di cavo hanno la stessa resistenza al fuoco e stessa classificazione di reazione al fuoco, la tipologia di isolamento ne cambia le caratteristiche elettriche e quindi il cavo deve essere marcato con una delle sigle sopracitate.

La UNI 9795:2021 è molto più specifica e prescrive proprio che: "Si rende indispensabile la verifica dei parametri trasmissivi dei cavi (induttanza, capacità, impedenza, ecc…) con i requisiti minimi richiesti dai singoli costruttori di apparati al fine di evitare malfunzionamenti del sistema stesso".

Visitando il sito aziendale è possibile scaricare liberamente tutte le Dichiarazioni di Performance, le conformità e le schede tecniche dei cavi in oggetto. ELAN garantisce inoltre un'assistenza tecnica e commerciale quotidiana a tutti coloro che necessitino di informazioni specifiche su cavi e batterie. **Ulteriori informazioni sul sito www.elan.an.it**

Vi aspettiamo inoltre al Safety Expo 2024 a Bergamo, dal 18 al 19 Settembre 2024 al nostro stand 76 al Padiglione B.



Telecamere Polymer HIKVISION:

anticorrosione per ambienti critici

HIKVISION presenta le **telecamere Polymer**, progettate con un **materiale rivoluzionario** che assicura la quasi totale immunità agli agenti corrosivi e che offre **robustezza eccezionale**, anche nelle condizioni più estreme.

CARATTERISTICHE E VANTAGGI DELLE TELECAMERE POLYMER HIKVISION

La **corrosione è un nemico silenzioso** che minaccia la durata e l'efficacia dei sistemi di sicurezza, specialmente in ambienti soggetti a condizioni estreme. L'accumulo di umidità, la presenza di sostanze corrosive e l'esposizione prolungata agli agenti atmosferici possono **compromettere rapidamente l'integrità delle telecamere di sorveglianza**. Le **telecamere Polymer di HIKVISION** sono progettate con un **innovativo concetto di housing** che unisce leggerezza, robustezza e **design in dimensioni compatte**, offrendo una protezione superiore agli agenti corrosivi senza sacrificare l'estetica e le prestazioni. Il tutto ad un costo accessibile, per **un'efficace alternativa alle telecamere in acciaio inox**.

CHI?
HIKVISION

CHE COSA?
TELECAMERE POLYMER

CHE COS'È?
TELECAMERE PROGETTATE CON UN RIVOLUZIONARIO POLIMERO CHE ASSICURA LA QUASI TOTALE IMMUNITÀ AGLI AGENTI CORROSIVI

UN MATERIALE RIVOLUZIONARIO

"Le telecamere Polymer – spiegano dagli headquarters di **HIKVISION Italy** – sono **progettate con un rivoluzionario polimero che assicura la quasi totale immunità agli agenti corrosivi, senza trattamenti o rivestimenti speciali**. Grazie ai forti legami chimici delle poliammidi e al rinforzo aggiuntivo fornito dai materiali miscelati, questo polimero assicura maggiore stabilità e durata riducendo al minimo le reazioni con altre sostanze, inclusi gli ossidanti aggressivi. Secondo la **British Plastics Federation**, le poliammidi offrono una buona resistenza a una vasta gamma di sostanze chimiche. **Test rigorosi condotti sugli acidi, sugli alcali e sulla nebbia salina, hanno dimostrato che le poliammidi rinforzate mantengono un'eccezionale integrità del materiale, rendendole ideali per gli housing** delle telecamere. Questa peculiarità rende le telecamere Polymer **immuni anche alla corrosione galvanica**, che invece è **problematica per quelle in acciaio inox,** rendendo le Polimer ideali anche in porti turistici e commerciali".

QUALITÀ CERTIFICATA: IP68, C5-M, NEMA 4X

Le telecamere Polymer possiedono le **certificazioni più importanti** per l'**applicabilità in ambienti marini e altamente corrosivi**,

come **IP68** (protezione totale contro le polveri e immersione permanente, assicurando il perfetto funzionamento dei dispositivi anche sott'acqua); **C5-M** (resistenza alla corrosione estrema); **NEMA 4X** (elevata protezione contro polvere, acqua e corrosione in condizioni ambientali difficili). La lettera **"X" indica inoltre una resistenza superiore alla corrosione**, rendendo queste telecamere idonee all'applicazione in ambienti altamente corrosivi o all'esposizione ad agenti caustici.

RESISTENZA E ROBUSTEZZA

Ma le telecamere Polymer non si limitano alla protezione dalla corrosione. Con una resistenza alla trazione 3 volte superiore (200 MPa), resistenza all'impatto di 1,2 volte superiore (12 kJ/m2) e distorsione al calore 2 volte superiore (180°), le Polymer offrono una **robustezza eccezionale anche nelle condizioni più estreme**, vantando inoltre una resistenza all'invecchiamento superiore del 30%.

LE APPLICAZIONI

Ampie le applicazioni che queste telecamere offrono. Da quelle per l'**industria chimica** sino ai **comuni marittimi** esposti a salsedine e sbalzi termici, porti commerciali e turistici esposti alle correnti galvaniche, e ancora **lidi e strutture alberghiere** esposte a vento, sabbia e sale, ma anche **case al mare**.

Le **dimensioni compatte**, la **leggerezza** e il **costo simile** a quello delle telecamere **standard**, rendono infatti le telecamere Polymer **ideali anche per la videosorveglianza domestica nelle seconde case al mare**.

Elmax: CONTACT VIDEO PRO, integrazione a portata di utente

Il miglior modo per esprimere l'**integrazione** delle varie tecnologie agli occhi dell'utente è la **nuova tastiera** grafica touch screen: **Contact Video Pro**.
La Contact Video Pro è l'ultima evoluzione della linea di tastiere grafiche di Elmax.

CHI?
ELMAX

CHE COSA?
CONTACT VIDEO PRO

CHE COS'È?
LA NUOVA TASTIERA GRAFICA TOUCH SCREEN DI ELMAX

CARATTERISTICHE E VANTAGGI DELLA CONTACT VIDEO PRO DI ELMAX

Progettata per offrire funzionalità avanzate e un'esperienza utente eccezionale, grazie all'ampio schermo touch capacitivo da 10 pollici, la tastiera consente un controllo intuitivo e immediato delle **applicazioni domotiche e di sicurezza** con un **design accattivante e raffinato**.

SCHERMO TOUCH CAPACITIVO DA 10 POLLICI E TECNOLOGIA IPS

Un display da **10"** consente una grande visibilità e un controllo superiore. Grazie alle generose dimensioni, la tastiera si presta soprattutto per **applicazioni domotiche** (mappe grafiche, widget), per applicazioni **videocitofoniche (SIP)** e come monitor per sistemi di **videosorveglianza**.

MULTI CONNESSIONE

La tastiera dispone di due tipi di connessione dati, Ethernet **LAN PoE e/o Wi-Fi**, per dare il massimo della versatilità più una connessione al **Bus proprietario Elmax** su standard **RS485**. La connessione Bus RS485 consente un collegamento privilegiato con la centrale antintru-

sione ai fini di un elevato livello di sicurezza.
La connessione IP permette di poter fruire di vari servizi quali la visualizzazione di telecamere, videocitofoni IP e servizi meteo. In aggiunta la connettività **Wi-Fi** permette maggiore flessibilità di installazione.
La presenza della multi connessione filare permette di alimentare la tastiera indifferentemente tramite **Bus e/o PoE**.

ICONE PERSONALIZZABILI (WIDGET) E NUOVO SET DI ICONE

La Contact Video Pro dispone di un **nuovo set di icone** per la costruzione di una Home Page confacente ai gusti e alle necessità dell'utente. Infatti la tastiera, alla prima accensione, visualizza una Home predefinita dove l'installatore, nella massima libertà, può arricchire in base alla necessità dell'utente. Possono essere introdotte **più pagine Home** che l'utente può visualizzare con un semplice swipe a sinistra e a destra, come peraltro avviene sui dispositivi mobili che quotidianamente vengono utilizzati.

MONITOR TELECAMERE IP

La Contact Video Pro può essere utilizzata per visualizzare flussi video provenienti da telecamere di videosorveglianza o da registratori in rete (DVR/NVR). Nella visualizzazione in live è possibile **sovrapporre widget di comando** per azionare, ad esempio, l'apertura di un cancello mentre viene mostrato il flusso video relativo.

VIDEOCITOFONIA IP

La Contact Video Pro **funge anche da telefono IP su protocollo SIP/2.0** per finalità telefoniche o videocitofoniche. Può essere utilizzato come posto interno e sono possibili anche le chiamate tra tastiere della serie Contact Video o telefoni IP di terze parti (interfono). Se presente un centralino SIP può essere utilizzata come postazione telefonica IP per inoltrare e ricevere telefonate.

MAPPE GRAFICHE

Come ogni tastiera grafica anche la Contact Video Pro permette la configurazione di una o più mappe grafiche. Su queste mappe, immagini 2D o 3D, è possibile sovrapporre widget di vario tipo quali **sensori, telecamere, comandi domotici, per personalizzare al massimo** e rendere il sistema molto intuitivo per l'utente. Ovviamente, come per la sezione Home, se sono presenti più mappe, l'utente può scorrere attraverso le stesse con comode gesture (swipe a sinistra/destra).

MAPPA GRAFICA WEB

Anche la Contact Video Pro dispone dell'originale funzionalità denominata Mappa Grafica Web. Infatti se si dispone, ad esempio, un **sistema domotico di terze parti gestito da un Web Server** (locale o remoto), è possibile visualizzare le proprie pagine nella tastiera e gestirle direttamente da essa, **insieme alla sezione antintrusione. Funzione unica nel suo genere**.

PROGRAMMAZIONE SMART

La programmazione della tastiera può avvenire localmente in tastiera o tramite piattaforme di programmazione **Elmax Studio** e **Elmax Studio Web**. Pertanto **l'installatore dispone di strumenti di programmazione molto evoluti** per costruire Home e Mappe Grafiche personalizzate.

Lettori in vetro Salto Glass XS: la ridefinizione del controllo accessi intelligente

Salto presenta la **nuova serie di lettori in vetro Glass XS**, che rappresentano la ridefinizione del controllo accessi intelligente.

CARATTERISTICHE E VANTAGGI DEI LETTORI IN VETRO SALTO GLASS XS

La nuova serie di lettori murali in vetro **Salto Glass XS Reader** è una linea di prodotti innovativi che stabilisce un **nuovo standard nella tecnologia di controllo accessi per i**

CHI?
SALTO

CHE COSA?
SALTO GLASS XS

CHE COS'È?
NUOVA SERIE DI LETTORI MURALI IN VETRO CHE STABILISCE UN NUOVO STANDARD NELLA TECNOLOGIA DI CONTROLLO ACCESSI

lettori murali. Questa gamma di lettori murali offre esperienze di accesso intelligenti senza precedenti, con un design elegante e dettagli ultrafini. La serie Glass XS Reader eleva il controllo accessi a livelli ineguagliabili, fondendo **eleganza, design, semplicità** e garantendo al contempo una **sicurezza di altissimo livello**.

Il nuovo lettore in vetro Glass XS Reader, che fa parte del portafoglio di prodotti dei lettori murali Salto XS, trasforma gli spazi in ambienti sofisticati e arricchiti. Grazie al suo design

unico e alla tecnologia all'avanguardia, offre agli utenti e agli operatori di sistema un'esperienza di controllo accessi ottimale. Il lettore murale in vetro Glass XS offre una soluzione di sicurezza completa per le situazioni in cui il **controllo deve essere online e in tempo reale, come barriere, ascensori, porte scorrevoli o cancelli elettronici**.

"Siamo entusiasti di presentare la serie Glass XS Reader – evidenzia **Fabrizio Nerone**, Managing Director di **Salto Italia** – un prodotto che rappresenta il **futuro della tecnologia di controllo degli accessi**. Grazie al suo design straordinario e alle sue funzioni avanzate, il lettore Glass XS offre agli utenti un **livello superiore di controllo e sicurezza"**.

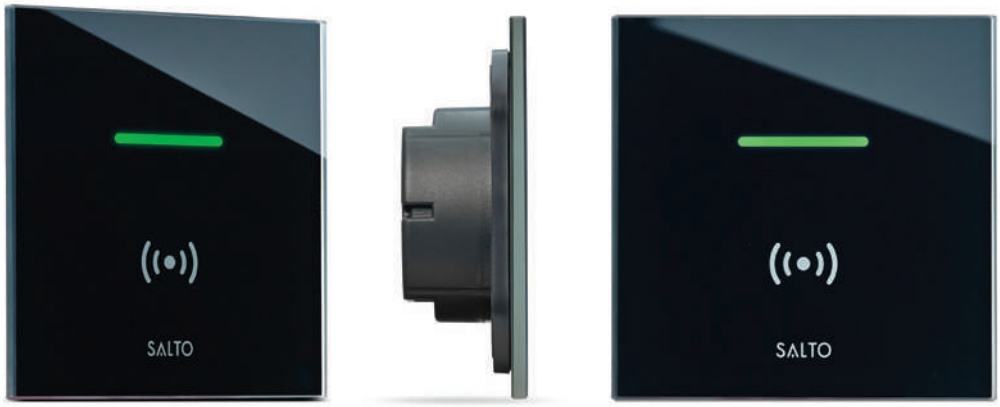
RESISTENTI E RAPIDI DA INSTALLARE

Realizzato con materiali di alta qualità, il lettore Glass XS è dotato di un pannello frontale in **vetro temperato altamente resistente e antigraffio**, che garantisce una lunga durata con una **manutenzione minima** e una **rapida installazione**. Il suo design elegante e moderno è personalizzabile grazie alla scelta di frontali in vetro **bianco o nero**, che lo rendono ideale per il montaggio a **incasso in ambienti interni e in scatole di derivazione universali**.

LE PRINCIPALI CARATTERISTICHE TECNICHE

- Design elegante: Design minimalista extra piatto, solo 4 mm di spessore
- Materiale Pannello: Vetro temprato
- Collegamento al controllore della porta: 4 fili
- Tecnologia NFC e Bluetooth LE per l'uso dello smartphone come della tessera
- Compatibilità MIFARE® DESFire® - iCLASS®
- Display di stato del lettore con indicatori luminosi e sonori
- Montaggio ad incasso a parete con scatola di meccanismo universale
- Compatibile con le piattaforme Salto KS, Space, e Homelok

Con il lettore Salto XS Glass, l'accesso **tramite cellulare o credenziali è semplice, veloce e intuitivo**. Tenendo lo smartphone vicino al lettore, la porta si apre automaticamente, **garantendo solo l'ingresso autorizzato**.



Digitronica.IT: applicativo web-based per rendere smart la gestione visitatori

Quando si parla della **crescita di un'azienda**, il pensiero si concentra sempre sugli stessi punti: l'aumento del fatturato e degli utili, il consolidamento dei rapporti con clienti e fornitori e l'importanza della comunicazione. Sebbene questi aspetti siano fondamentali, spesso si dimentica che l'azienda possiede anche **asset, informazioni e beni cruciali per la crescita stessa e proteggerli deve essere una priorità** per continuare a innovare e svilupparsi.

La **sicurezza** va perseguita sotto ogni punto di vista, ne è **un esempio il processo di gestione dei visitatori in azienda**. Il flusso di persone in entrata e in uscita solleva questioni delicate, soprattutto quando diventa intenso e diversificato. Sapere esattamente chi è presente e per quanto tempo offre vantaggi considerevoli, ma per garantire una **verifica ottimale** non si possono creare code e attese infinte. Per rispondere a questa esigenza, **Digitronica.IT** ha sviluppato una **soluzione estremamente smart e adattabile alle necessità delle singole aziende**: l'applicazione modulare **PhotoGuest**, software che consente una **gestione intuitiva dei visitatori, eliminando i rallentamenti nelle procedure**.

CHI?
DIGITRONICA.IT

PER CHI?
PER TUTTE LE AZIENDE CHE NECESSITANO DI AMPLIARE LA GESTIONE VISITATORI E DEGLI INGRESSI/USCITE TRASPORTI

CHE COSA?
PHOTOGUEST PIATTAFORMA WEB BASED PER INFORMATIZZAZIONE CENTRALIZZATA, AUTOMAZIONE E SNELLIMENTO FLUSSI DEI VISITATORI

DIGITRONICA.IT: IL PROCESSO DI GESTIONE VIRTUALE DEI VISITATORI

Una **piattaforma web based, flessibile e user friendly**, realizzata per l'**informatizzazione centralizzata**, l'automazione e lo snellimento dei flussi dei visitatori nelle sedi aziendali: questo è **PhotoGuest**, che, attraverso i suoi tre moduli di

- **accreditamento visitatori,**

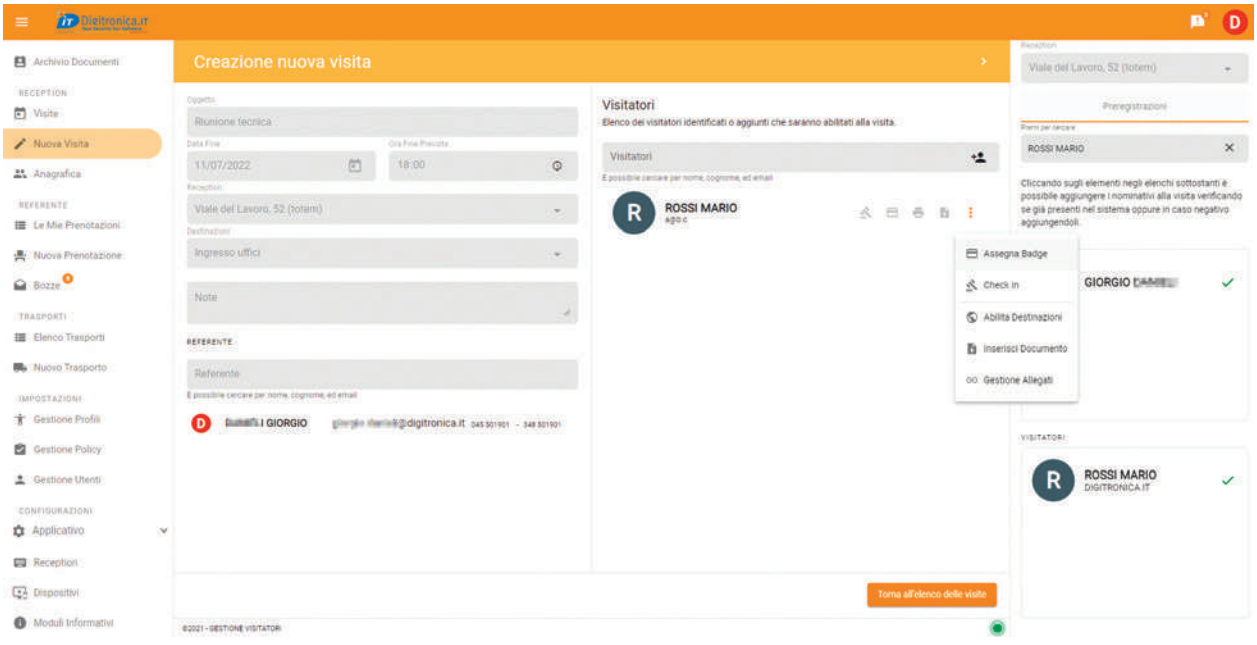
• **prenotazione visite** e
• **virtual reception,**
permette di gestire in **tempo reale** tutte le fasi dell'esperienza di un ospite in azienda, dall'invito fino al congedo.

LA REALIZZAZIONE E I BENEFICI DELLA SOLUZIONE DIGITRONICA.IT PER LA GESTIONE DEI VISITATORI

Nella pratica, l'applicativo concepito da **Digitronica.IT** permette al personale abilitato di **creare e gestire le prenotazioni delle visite programmate direttamente nel sistema**, mentre i visitatori possono registrarsi autonomamente una volta arrivati in azienda. Utilizzando **tablet o totem posti alla reception, l'ospite può inserire i propri dati personali e il codice invito ricevuto via mail dal referente** che ha creato la visita. Inoltre, il visitatore può visionare **eventuali contenuti multimediali**, questionari, moduli informativi proposti come ad esempio privacy, safety e confidenzialità. Una volta completato il check-in, l'ospite può incontrare il suo referente e, al termine dell'incontro, viene registrato nel sistema come **"congedato"**.
Un esempio di **funzionamento semplice, immediato e automatizzato**, che permette di tenere traccia costante della visita e che **ogni azienda può adattare alle proprie esigenze**. Ma, a prescindere da come si decida di declinarlo nello specifico, i **benefici di questo sistema sono comunque evidenti e valorizzano l'immagine aziendale**.

I BENEFICI ASSICURATI DAL SOFTWARE DI DIGITRONICA.IT

Ecco i vantaggi garantiti dall'applicativo PhotoGuest:
• **Sicurezza a un livello superiore**. Conoscere, in ogni istante, gli spostamenti dei visitatori e le tempistiche dell'incontro aumenta la sicurezza e agevola la gestione delle emergenze: identità e posizione dei presenti in azienda sono visibili in real time attraverso il software;
• **Ottimizzazione dei tempi**. Programmazione calendarizzata delle visite, eliminazione delle code e possibilità di agire anche sulle sedi non presidiate fisicamente: accedere nell'azienda non è solo più sicuro, ma anche più rapido;
• **Risparmio**. Grazie alla modalità in self check-in e l'automatizzazione dei processi si ottiene un abbattimento dei costi;
• **Gestione oculata delle informative**. Il software, conservandole nel suo database, gestisce scadenze, rinnovi e aggiornamenti delle varie informative, tutelando l'azienda nel rapporto con i suoi visitatori;
• **Versatilità**. L'applicativo è personalizzabile secondo le proprie esigenze, anche per tutte le aziende che necessitano di ampliare il concetto di gestione visitatori a un controllo smart degli ingressi e delle uscite dei trasporti.



EL.MO. e l'Atelier D-Factory: insieme per un business più sicuro

D-Factory rappresenta un'**eccellenza** nel mondo delle **autofficine specializzate** nell'applicazione di pellicole protettive per **auto di lusso**. Questo spazio, dedicato agli appassionati delle quattro ruote, si distingue non solo per la qualità dei servizi offerti, ma anche per l'ambiente unico in cui sorge. Situata in un'area spaziosa e **priva di cancelli e recinzioni**, D-Factory offre un ambiente che rispecchia la libertà e la passione per le auto, ma che al contempo **richiede soluzioni di sicurezza avanzate per proteggere i suoi preziosi veicoli**.

Non si tratta di una semplice autofficina, ma un vero e proprio **atelier** dove le auto di lusso vengono trattate con la massima cura e attenzione. Qui, i proprietari di auto possono trasformare i loro veicoli con pellicole che non solo proteggono, ma esaltano l'estetica e la personalità delle loro vetture. Ogni auto che entra in D-Factory riceve un trattamento su misura, con pellicole che variano dai semplici toni oscuranti ai rivestimenti più complessi e artistici. Questo livello di dettaglio e personalizzazione rende **D-Factory un punto di riferimento nel settore**, attirando una **clientela esigente e appassionata**.

CHI?
EL.MO.

PER CHI?
D-FACTORY

CHE COSA?
SISTEMA INTEGRATO CHE COMBINA TECNOLOGIA AVANZATA E INTELLIGENZA ARTIFICIALE

LA REALIZZAZIONE DELLA SOLUZIONE EL.MO. PER D-FACTORY

Nonostante l'ambiente accogliente e aperto, D-Factory aveva un'**esigenza cruciale**: garantire la sicurezza del proprio patrimonio automobilistico, specialmente durante le ore di chiusura. L'assenza di barriere fisiche come cancelli rendeva il capannone vulnerabile a curiosi e potenziali intrusi. Per questo motivo, la necessità di un sistema di sicurezza avanzato e affidabile era fondamentale. La **protezione richiesta doveva essere totale**, coprendo ogni possibile punto di accesso e garantendo una **vigilanza continua**.

Per rispondere a queste esigenze, D-Factory si è affidata a EL.MO., un leader nel settore della sicurezza. La soluzione proposta da EL.MO. è stata un **sistema integrato** che combina **tecnologia avanzata e intelligenza artificiale**. Sono state installate **telecamere perimetrali** collegate a dispositivi **AIUNIT per la videoanalisi**, capaci di rilevare qualsiasi movimento sospetto. Questo sistema di

videoanalisi è configurato per riconoscere il superamento di una linea virtuale, attivando un avviso vocale preventivo che scoraggia eventuali intrusi. In caso di persistente tentativo di intrusione, il sistema scatena un allarme completo.

Oltre alle telecamere e ai dispositivi di videoanalisi, la protezione di D Factory è stata ulteriormente rafforzata con **contatti su finestre e portoni**, insieme a **radar interni di backup**.

I BENEFICI DELLA SOLUZIONE EL.MO.

Questa combinazione di tecnologie garantisce una protezione a 360 gradi, **coprendo ogni possibile vulnerabilità e assicurando che l'intera struttura sia monitorata in ogni momento**. La presenza di queste misure di sicurezza ha trasformato D-Factory in una **fortezza**, pur mantenendo l'accessibilità e l'apertura che la caratterizzano durante le ore di operatività.

Grazie alla soluzione di sicurezza implementata, D-Factory può ora operare con una tranquillità senza precedenti. La protezione **24/7** assicura che **ogni veicolo** all'interno dell'officina sia **costantemente monitorato**, eliminando ogni preoccupazione legata a possibili furti o vandalismi. Le telecamere e i sistemi di videoanalisi intelligente non solo rilevano intrusioni, ma sono anche in grado di fornire **prove concrete** in caso di incidenti, aumentando ulteriormente il livello di sicurezza.

L'investimento in un sistema di sicurezza avanzato non solo protegge il presente di D Factory, ma ne garantisce anche il **futuro**. La sicurezza senza compromessi permette all'officina di continuare a offrire i suoi servizi di **alta qualità**, attrarre **nuovi clienti** e mantenere la **fiducia** di quelli esistenti. In un settore dove la cura e la protezione delle auto di lusso sono fondamentali, D Factory può ora affermare con **orgoglio di essere un luogo sicuro e affidabile**, dove ogni auto è trattata come un'opera d'arte. D-Factory ha dimostrato come l'innovazione e la tecnologia possano essere integrate efficacemente per risolvere problemi pratici. Grazie alla collaborazione con EL.MO l'autofficina ha raggiunto un livello di sicurezza che le permette di operare serenamente e con fiducia. Questo **esempio di eccellenza nella sicurezza** rappresenta un modello per altre realtà del settore, mostrando come **la protezione e la passione per le auto possano convivere armoniosamente**.

SOS Arctic WindSled Expedition:

Esplorando l'Artico con le batterie FIAMM

FIAMM
Your World, Our Energy

L'**Artico**, una regione remota e affascinante, sta affrontando sfide senza precedenti a causa dei **cambiamenti climatici**. Per comprendere meglio questi cambiamenti e il loro impatto sugli ecosistemi artici, è fondamentale condurre **ricerche scientifiche approfondite**. La SOS Arctic WindSled Expedition, un progetto innovativo che unisce la **scienza**, la **tecnologia** e la **tradizione Inuit**, rappresenta un passo importante in questa direzione.

LA REALIZZAZIONE DELLA SOLUZIONE FIAMM E I BENEFICI

Al centro di questa spedizione c'è la **WindSled**, una slitta speciale, trainata da un **kite**, disegnata dall'esploratore spagnolo **Ramon Larramendi**. La slitta, dotata di un sistema di alimentazione ad **energia solare** e da **batterie FIAMM**, monta strumentazione scientifica dell'Istituto di Scienze Polari del **CNR**. Grazie a questa slitta, gli scienziati del CNR riescono infatti a condurre ricerche in aree altrimenti inaccessibili. Le batterie FIAMM, **le stesse che vengono utilizzate** in svariate applicazioni come la **videosorveglianza** e le **luci di emergenza**, si sono dimostrate **ideali per questo ambiente estremo**, grazie alla loro **resistenza alle basse temperature e alla loro elevata affidabilità**.

CHI?
FIAMM

PER CHI?
SOS ARCTIC WINDSLED EXPEDITION

CHE COSA?
BATTERIE FIAMM

UN'IMPRESA SCIENTIFICA CON UN FOCUS SU TECNOLOGIE OPEN-SOURCE E SOSTENIBILITÀ

Tra gli obiettivi della spedizione SOS Arctic WindSled Expedition c'è **raccogliere dati scientifici** su diversi aspetti dell'ambiente artico, tra cui la qualità dell'aria, la contaminazione ambientale e l'adattamento di specie di micro-organismi. Questi dati saranno utilizzati per comprendere meglio i cambiamenti climatici e il loro impatto sugli ecosistemi artici.

Tra i ricercatori del CNR impegnati nell'attività, il **Dr. Federico Dallo** guida il team che ha progettato lo **strumento di monitoraggio** che, a bordo della Windsled, raccoglie dati relativamente ai gas e alle polveri presenti nell'atmosfera artica, e che è **alimentato da batteria FIAMM**.

Il ricercatore sottolinea uno dei fini del progetto: "Questa spedizione vuole provare come **tecnologie low-cost e open-source** permettano di monitorare importanti valori dell'atmosfera anche in zone remote come quella artica".

Un altro aspetto fondamentale della spedizione è l'impegno per la **sostenibilità**. Il WindSled,

alimentato da energia solare, permette di ridurre al minimo l'impatto ambientale della spedizione. Inoltre, i ricercatori collaborano con gli Inuit per imparare dalle loro conoscenze tradizionali e per sviluppare soluzioni sostenibili per la salvaguardia dell'ecosistema artico.

LE BATTERIE FIAMM: UN ELEMENTO CHIAVE PER IL SUCCESSO DELLA SPEDIZIONE

Le batterie FIAMM svolgono un ruolo fondamentale nel successo della SOS Arctic WindSled Expedition. Queste batterie, che vengono utilizzate in svariate applicazioni industriali e commerciali, si dimostrano ideali per questo ambiente estremo grazie alle loro caratteristiche, che qui di seguito vengono evidenziate.

- **Resistenza alle basse temperature**: le batterie FIAMM sono in grado di funzionare correttamente anche a temperature molto basse, fino a -30/-35°, tipiche dell'Artico.
- **Elevata affidabilità e bassa manutenzione:** le batterie FIAMM garantiscono un'alimentazione affidabile e costante al WindSled, permettendo ai ricercatori di condurre le loro ricerche in modo sicuro ed efficiente, senza necessità di frequenti manutenzioni.
- **Durata prolungata:** le batterie FIAMM hanno una lunga durata, il che significa che devono essere sostituite meno frequentemente, riducendo l'impatto ambientale della spedizione.

OLTRE LA RICERCA SCIENTIFICA: UN MESSAGGIO DI SPERANZA PER L'ARTICO

La SOS Arctic WindSled Expedition rappresenta un'impresa scientifica di **grande valore**, ma è anche un **messaggio di speranza per l'Artico**. La spedizione dimostra che è possibile esplorare e studiare questo ambiente fragile in modo sostenibile, utilizzando tecnologie innovative e collaborando con le popolazioni locali. I risultati della spedizione saranno preziosi per comprendere meglio i cambiamenti climatici e per sviluppare **soluzioni per proteggere l'Artico per le generazioni future**.

AMC: ViTA, allarme e TVCC in un'unica soluzione

AMC ELETTRONICA
www.amcelettronica.com
Tel. 031 - 632780

ViTA è la piattaforma di centrali antintrusione, ultima nata in casa AMC Elettronica.
Si articola su 3 modelli di centrali d'allarme 24, 64 e 128 zone, che conservano i plus e le caratteristiche della piattaforma della serie X, ma sono state sviluppate con il preciso intento di integrare i flussi delle telecamere di videosorveglianza, nella duplice modulazione di sistema di Video verifica e Video analisi.

Le centrali ViTA dispongono di scheda di rete integrata e sono compatibili con tutte le periferiche e accessori, cablati e via radio, della gamma AMC.
Per renderla fruibile al maggior numero possibile di utenti utilizzatori, la piattaforma ViTA integra tutti i principali produttori di video sorveglianza all'interno di un ampio parterre di telecamere e sistemi video compatibili.

A seconda delle esigenze del cliente, la piattaforma si presta così alle integrazioni video di cui sopra, conservando la medesima struttura di software e l'estrema semplicità di configurazione e gestione delle apparecchiature di campo.

Cavo SPITFIRE® FTP NETWORK di Eraya

ERAYA
www.eraya.it/it
Tel. 071 8760563

Eraya, realtà imprenditoriale italiana all'avanguardia e al passo con le nuove tecnologie, specializzata nella produzione di cavi per sistemi d'allarme, reti dati, TVCC, sistemi antincendio e, su richiesta, di cavi personalizzati, ha progettato e realizzato un nuovo cavo che va incontro alle esigenze degli impianti di rivelazione incendi di ultimissima generazione: è il cavo SPITFIRE® .

Il cavo SPITFIRE® FTP NETWORK è il cavo corretto che risponde alla norma EN 50289-4-16.
Come recita la UNI 9795, al fine di garantire l'identificabilità di queste linee all'interno del sistema stesso, è preferibile che il cavo LAN, per il collegamento delle basi microfoniche del sistema EVAC, abbia la guaina esterna di colore viola e il cavo BUS (RS232 e RS485), per il collegamento tra centrali e ripetitori, abbia il rivestimento di colore rosso.
Tutti i cavi SPITFIRE® resistenti al fuoco hanno superato i tests di prova EN 50200 e EN 50289-4-16 con un risultato di 120 minuti (PH120).

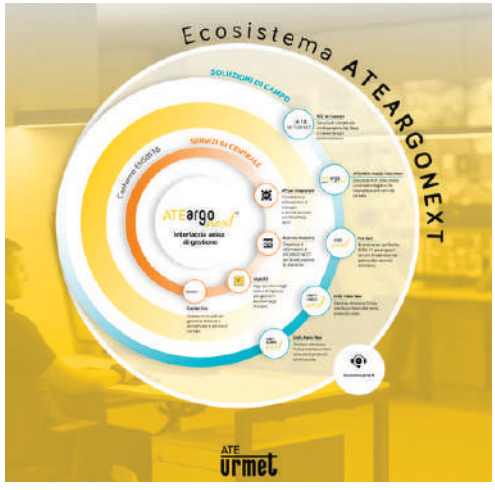
Notifier: nuova Serie di Centrali AM Cloud Ready

Notifier Italia presenta la nuova linea di centrali con protocollo CLIP serie AM Cloud Ready.
Il design richiama al "Family Feeling" Notifier, un mix tra classico e moderno, che rinnova la serie AM, introducendo dettagli presenti sino ad oggi solo nella linea Advanced Protocol quali l'ampio display a colori touch screen da 7".
Sono disponibili le versioni AM1000CL a 1 loop, AM2000CL a 2 loop e AM6000CL modulare ed ampliabile con schede di espansione da 2 loop ciascuna. Queste centrali hanno uscita seriale per i pannelli remoti in cui è possibile visualizzare tutti i punti/zone dell'impianto o solo una parte, come pure poter indicare le sole segnalazioni di allarme, il tutto liberamente configurabile.
Le centrali oltre alla certificazione CPR in conformità alle UNI EN 54-2 e 4 sono certificate anche UNI EN 54-13, garantendo ai progettisti e agli installatori la massima sicurezza dell'impianto testato in ogni sua parte. Una chiave hardware abilita la comunicazione verso i sistemi di monitoraggio e supervisione, in modo da poter gestire l'impianto grazie al CLSS.

NOTIFIER ITALIA
www.notifier.it
Tel. 02 518971

L'Ecosistema Ateargo Next di Urmet ATE

Dalla ventennale esperienza di Urmet ATE nasce l'Ecosistema Ateargo Next, un gestionale eventi certificato EN50518 per le centrali operative degli Istituti di Vigilanza. Il sistema, modulare e integrabile con altri software, centralizza il controllo di migliaia di dispositivi e decine di operatori, semplificando il lavoro quotidiano grazie a un'interfaccia intuitiva.
Il modulo Business Analytics facilita l'analisi dei dati, mentre l'app VigilATE consente agli utenti di gestire autonomamente gli impianti. Il modulo Contact Evo ottimizza i processi telefonici e le API garantiscono integrazioni fluide con software terzi. Le soluzioni Unify Video Next e Unify Alarm Next gestiscono impianti di videosorveglianza e antintrusione multiprotocollo, riducendo i tempi di gestione degli eventi.
Il sistema include anche ATEARGO Analisi Video Next e il ricevitore Fire Next, conforme alla normativa EN54-21. L'assistenza h24 e il supporto sistemistico assicurano risposte tempestive a ogni problematica. Ateargo Next è la soluzione espandibile, aperta e longeva,



ideale per migliorare efficienza, sicurezza e sostenibilità operativa negli Istituti di Vigilanza.

URMET ATE
www.urmet-ate.it
Tel. 0444 268211

IN QUESTO NUMERO

SEGUICI SU

www.snewsonline.com
www.twitter.com/SNewsOnline
www.linkedin.com/company/s-news
www.facebook.com/SNewsOnline

Servizio abbonamenti: per informazioni telefonare allo **0424.383049** o inviare un'e-mail all'indirizzo **abbonamenti@snewsonline.com** Il servizio è in funzione dal lunedì al venerdì dalle 9:00 alle 13:00. L'importo dell'abbonamento annuale **(5 numeri)** è pari ad **Euro 40,00** (solo Italia) comprese le spese di spedizione. Verrà inviato all'indirizzo e-mail fornito dal richiedente, il modulo di richiesta abbonamento, da compilare e restituire con i dati anagrafici completi dell'intestatario. L'abbonamento potrà avere inizio in qualsiasi momento dell'anno. Il pagamento andrà eseguito tramite bonifico bancario intestato a S News S.r.l. Via Trieste, 6 - 36061 Bassano del Grappa (VI), come specificato nel modulo di richiesta abbonamento. Spedizione postale con **Postatarget Creative.** L'Editore garantisce la massima riservatezza dei dati forniti dall'abbonato, e la possibilità di richiederne gratuitamente la rettifica o la cancellazione ai sensi degli artt. 15 e ss. del GDPR 2016/679. Le richieste vanno rivolte a: privacy@snewsonline.com

ISSN 2281-1222 S News
ANNO XIII - N. 75 Speciale 2024

DIRETTORE RESPONSABILE
Monica Bertolo

COMITATO SCIENTIFICO
Giulia Cavalli, Claudio Pantaleo, Cristhian Re, Fabio Spotti, Giancarlo Valente, Domenico Vozza

REDAZIONE
Monica Bertolo, Nadia Biasion, Giulia Cavalli, Alessandro Cherubin, Cristhian Re
redazione@snewsonline.com

PIANIFICAZIONE
Andrea Cherubin
pianificazione@snewsonline.com

GRAPHIC DESIGN
Nadia Biasion (impaginazione)

SEGRETERIA DI REDAZIONE
segreteria@snewsonline.com

UFFICIO ESTERO
international@snewsonline.com

PUBBLICITA'
marketing@snewsonline.com

ABBONAMENTI
abbonamenti@snewsonline.com

AMMINISTRAZIONE
amministrazione@snewsonline.com

SEDE
S News Srl - Via Trieste, 6
36061 Bassano del Grappa (VI)
Tel./Fax +39 0424 383049
info@snewsonline.com
www.snewsonline.com

REGISTRAZIONE
Registrazione al Tribunale di Bassano del Grappa n. 3/2012 ora di Vicenza

ISCRIZIONE AL ROC
S News S.r.l. è iscritta al ROC (Registro Operatori di Comunicazione) al n. 22328 del 24/04/2012

STAMPA
Grafiche Antiga SpA

PRIVACY

Il trattamento dei dati dei destinatari del presente Periodico ha la finalità di assicurare informazioni tecniche e specializzate a soggetti che per la loro attività sono interessati ai temi trattati. I dati sono trattati nel rispetto del Regolamento EU 2016/679 e D. Lgs. 196/2003.
Il Titolare del trattamento dei dati raccolti in banche dati ad uso redazionale è **S News S.r.l.**, con sede in **Via Trieste, 6 - 36061 Bassano del Grappa (VI)**. Gli interessati possono far valere i propri diritti contattando il Titolare all'indirizzo privacy@snewsonline.com

isiwi

redi+

Protezione immediata **dove e quando vuoi**

Attraverso l'utilizzo di una **batteria 9.600 mAh** e una connessione con rete **4G LTE**, Redi + è sempre pronto a proteggerti!

SIM CARD INCLUSA

CONNETTIVITÁ 4G LTE

MOVIMENTO PT

TECNOLOGIA DUALIGHT

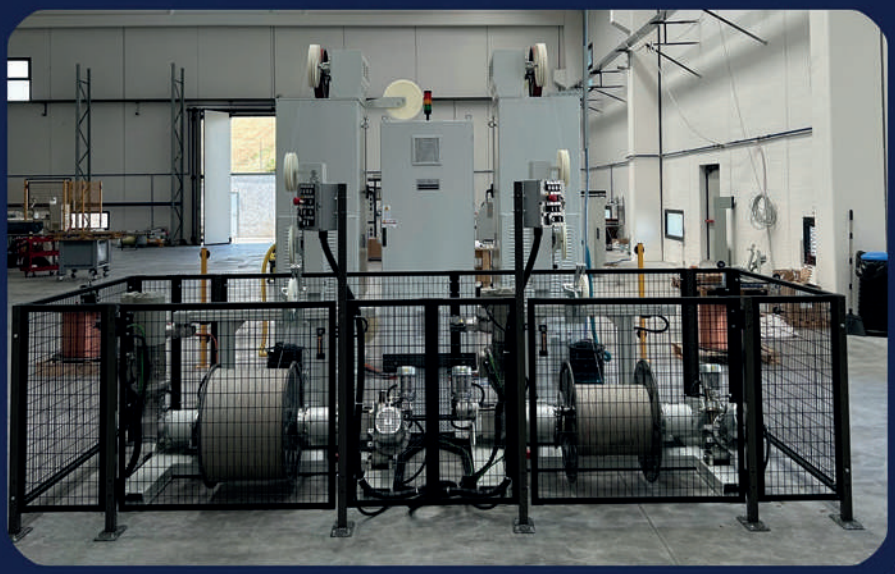
Una protezione in + con il pannello **Solar 3**

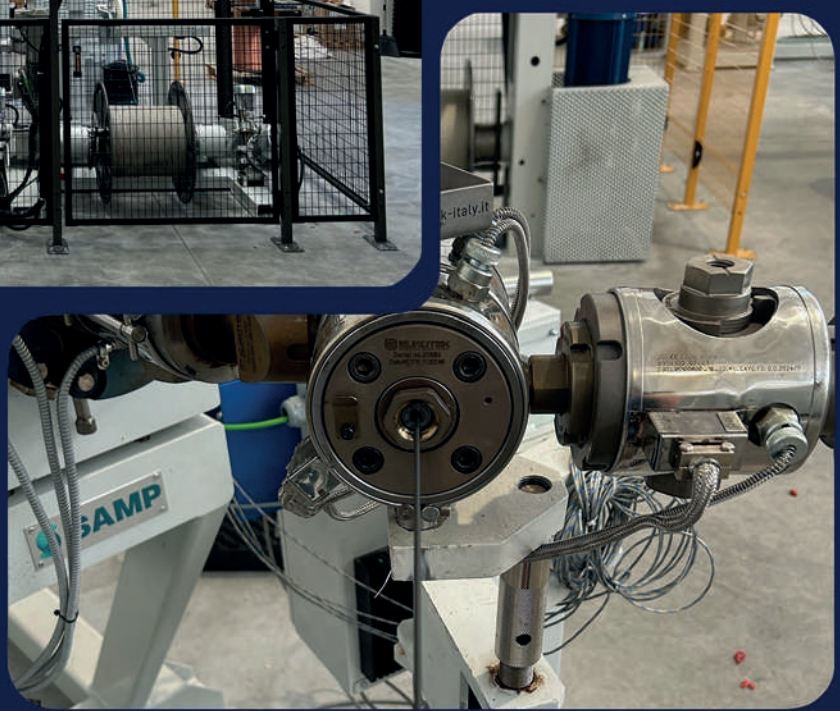
Con l'utilizzo combinato di Redi + ed il pannello **Solar 3**, la tua protezione diventa costante.

Che aspetti? scopri i dettagli su
www.isiwi.it

Il lato ***isi*** della videosorveglianza

We link our experience and your project





I nostri prodotti

- Cavi sicurezza
- Cavi dati
- Cavi antincendio
- Cavi coax
- Cavi speciali

IQNet GLOBAL CERTIFICATION
UKAS MANAGEMENT SYSTEMS 0007
Assessed to ISO 9001:2015
Cert/Ref No.1771

eraya
The Italian Power Solution

www.eraya.it | info@eraya.it