



Cyber security

Come cambia il crimine online e l'attività di contrasto. Intervengono il generale Antonio Mancazzo, Massimo Chirivi e Paolo Spagnoletti



Ambiente Lavoro

Nuove tecnologie, simulazioni di rischio ed esperienze virtuose di wellbeing corporate in vetrina dal 26 al 30 maggio

SICUREZZA

REPORT

Speciale Cyber Security

UNA VISIONE INTEGRATA

di CG



Wanda Ferro, sottosegretario di Stato al Ministero dell'Interno

Il tema della sicurezza è uno dei pilastri fondamentali dell'azione del Governo Meloni, perché rappresenta il presupposto della libertà, della coesione sociale e della fiducia dei cittadini nelle istituzioni. «Per troppo tempo alcuni fenomeni sono stati sottovalutati o affrontati con un approccio ideologico che ha finito per lasciare soli i territori e per indebolire la presenza dello Stato. Abbiamo dunque scelto - mette in evidenza il sottosegretario al Ministero dell'Interno Wanda Ferro - una linea diversa: concreta e pragmatica, fondata su investimenti, prevenzione e capacità di intervento». I numeri dimostrano che la direzione è quella giusta.

>>> segue a pagina 8

ALL'INTERNO



Le sfide della Farnesina

Al centro della nuova architettura, voluta dal ministro Tajani, è Alessandro De Pedys

Rischio digitale

L'analisi di Luca Savoldi e Fabrizio Fiorini sull'evoluzione della cybersicurezza



MARINA CALDERONE

RAFFORZARE LA CRESCITA

In un mercato del lavoro che continua a registrare segnali positivi sul fronte dell'occupazione, il Governo punta ora a consolidare la crescita trasformandola in lavoro stabile, qualificato e meglio retribuito. Dal salario giusto agli incentivi per l'occupazione, passando per il rinnovo dei contratti e l'impatto dell'intelligenza artificiale sul mercato del lavoro: il DI Lavoro rappresenta uno dei pilastri della strategia economica del Governo. Al centro del confronto anche il tema della sicurezza e della prevenzione, considerati elementi fondamentali per tutelare lavoratori e imprese. Ne parliamo con il ministro del Lavoro Marina Calderone, per capire quali siano le priorità dell'esecutivo e come cambierà il mondo del lavoro nei prossimi anni.

Ministro qual è oggi la priorità economica che guida l'impianto del DI Lavoro e in che modo il Governo intende conciliare crescita, occupazione e tutela del potere d'acquisto?

«La priorità risiede nella volontà di ren-

dere la crescita più solida, trasformandola in occupazione stabile e lavoro di qualità. Il DI 1° maggio nasce nell'ambito di una fase oggettivamente positiva per l'occupazione italiana, che al momento non sembra rallentare. Sarebbe però un errore fermarsi ai numeri. Resta ancora il gap rispetto ad alcuni problemi strutturali che conosciamo bene: il potere d'acquisto dei salari, gli squilibri territoriali e una partecipazione al lavoro storicamente troppo bassa per giovani e donne. L'ulteriore intervento sul mondo del lavoro di questo provvedimento guarda in particolare all'inclusione lavorativa dei disoccupati di lunga durata, alle giuste retribuzioni e a un patto di responsabilità con le parti sociali per la qualificazione dell'occupazione in Italia. Abbiamo ribadito il nostro pensiero: la crescita non si difende comprimendo tutele e trasparenza. Un'economia competitiva ha bisogno di imprese forti, ma anche di lavoratori motivati, qualificati e ben retribuiti. In questa direzione vanno il sostegno del

Governo alla contrattazione collettiva, gli incentivi per l'occupazione stabile e strumenti come la piattaforma SIISL, che mette finalmente in connessione competenze, imprese e opportunità».

Il Governo ha più volte ribadito la centralità del "salario giusto" e della contrattazione collettiva: come pensa che queste misure possano migliorare concretamente stipendi e qualità del lavoro senza penalizzare produttività e competitività delle imprese?

«Partiamo da un principio semplice: il lavoro non può essere valutato soltanto in relazione a una retribuzione oraria. Dall'integrale applicazione di un CCNL discendono diritti, tutele, welfare, sicurezza, formazione, progetti di vita. Per questo il decreto 1° maggio valorizza il TEC, il Trattamento Economico Complessivo previsto dai contratti sottoscritti dalle organizzazioni comparativamente più rappresentative.

>>> segue a pagina 4

INFINIDAT

AI-Ready, Cyber-Centric **Enterprise Storage**



Reduce AI hallucinations
with RAG workflows



Easily create cyber-resilient
storage environments



Reduce threat windows with
Automated Cyber Protection



Identify compromised data
using AI-based cyber detection



Recover known good
copies of data quickly



Backed by InfiniSafe
cyber storage guarantees

WWW.INFINIDAT.COM



Colophon

Direttore onorario
Raffaele Costa



Direttore responsabile
Marco Zanzi
direzione@golfarellieditore.it

Vice Direttore
Renata Gualtieri
renata@golfarellieditore.it

Redazione
Tiziana Achino, Lucrezia Antinori,
Tiziana Bongiovanni, Silvia Brundu,
Eugenia Campo di Costa, Cinzia Calogero,
Anna Di Leo, Cristiana Golfarelli, Simona
Langone, Leonardo Lo Gozzo,
Michelangelo Marazzita,
Guia Montefamelio, Marcello Moratti,
Michelangelo Podestà, Alessandro Gallo,
Desna Ruscica, Debora Stampone,
Giuseppe Tatarell

Relazioni internazionali
Magdi Jebreal

Hanno collaborato
Ginevra Cavalieri, Gaetano Gemitì,
Bianca Raimondi, Guido Anselmi,
Angelo Maria Ratti, Fiorella Calò,
Francesca Druidi, Francesco Scopelliti,
Lorenzo Fumagalli, Gaia Santi,
Maria Pia Telese, Gloria Martini,
Linda Zorza

Sede
Tel. 051 228807 - Piazza Cavour 2
40124 - Bologna - www.golfarellieditore.it

Relazioni pubbliche
Via del Pozzetto, 1/5 - Roma

Tiratura complessiva: 60.000 copie



La priorità è rafforzare la crescita

Dal DI Lavoro agli incentivi per giovani e donne, fino all'impatto dell'intelligenza artificiale e alla sicurezza nei cantieri: il ministro Marina Calderone traccia la linea del Governo tra occupazione stabile, contrattazione collettiva e innovazione

In un mercato del lavoro che continua a registrare segnali positivi sul fronte dell'occupazione, il Governo punta ora a consolidare la crescita trasformandola in lavoro stabile, qualificato e meglio retribuito. Dal salario giusto agli incentivi per l'occupazione, passando per il rinnovo dei contratti e l'impatto dell'intelligenza artificiale sul mercato del lavoro: il DI Lavoro rappresenta uno dei pilastri della strategia economica del Governo. Al centro del confronto anche il tema della sicurezza e della prevenzione, considerati elementi fondamentali per tutelare lavoratori e imprese. Ne parliamo con il ministro del Lavoro Marina Calderone, per capire quali siano le priorità dell'esecutivo e come cambierà il mondo del lavoro nei prossimi anni.

Ministro qual è oggi la priorità economica che guida l'impianto del DI Lavoro e in che modo il Governo intende conciliare crescita, occupazione e tutela del potere d'acquisto?

«La priorità risiede nella volontà di rendere la crescita più solida, trasformandola in occupazione stabile e lavoro di qualità. Il DI 1° maggio nasce nell'ambito di una fase oggettivamente positiva per l'occupazione italiana, che al momento non sembra rallentare. Sarebbe però un errore fermarsi ai numeri. Resta ancora il gap rispetto ad alcuni problemi strutturali che conosciamo bene: il potere d'acquisto dei salari, gli squilibri territoriali e una partecipazione al lavoro storicamente troppo bassa per giovani e donne. L'ulteriore intervento sul mondo del lavoro di questo provvedimento guarda in particolare all'inclusione lavorativa dei disoccupati di lunga durata, alle giuste retribuzioni e a un patto di responsabilità con le parti sociali per la qualificazione dell'occupazione in Italia. Abbiamo ribadito il nostro pensiero: la crescita non si difende comprimendo tutele e trasparenza. Un'economia competitiva ha bisogno di imprese forti, ma anche di lavoratori motivati, qualificati e ben retribuiti. In questa direzione vanno il sostegno del Governo alla contrattazione collettiva, gli incentivi per l'occupazione stabile e strumenti come la piattaforma SIISL, che mette finalmente in connessione competenze, imprese e opportunità».

Il Governo ha più volte ribadito la centralità del "salario giusto" e della contrattazione collettiva: come pensa che queste misure possano migliorare concretamente stipendi e qualità del lavoro



TUTTI GLI INDICATORI MOSTRANO CHE LADDOVE CRESCE L'OCCUPAZIONE FEMMINILE AUMENTANO COMPETITIVITÀ, PRODUTTIVITÀ E CAPACITÀ DI INNOVARE. NON È SOLTANTO UNA QUESTIONE DI EQUITÀ SOCIALE, MA DI CRESCITA ECONOMICA

senza penalizzare produttività e competitività delle imprese?

«Partiamo da un principio semplice: il lavoro non può essere valutato soltanto in re-

lazione a una retribuzione oraria. Dall'integrale applicazione di un CCNL discendono diritti, tutele, welfare, sicurezza, formazione, progetti di vita. Per questo il decreto 1°



maggio valorizza il TEC, il Trattamento Economico Complessivo previsto dai contratti sottoscritti dalle organizzazioni comparativamente più rappresentative. Una scelta che valorizza la qualità della contrattazione collettiva italiana e che rifiuta l'idea che la competitività passi dalla compressione del costo del lavoro. Le economie più forti sono quelle che investono sulle competenze, sull'innovazione e sul capitale umano. Il compito del Governo è creare condizioni favorevoli a garantire questo equilibrio, sostenendo imprese e lavoratori facilitando il dialogo tra le parti sociali. Quando il lavoro cresce in qualità, cresce pure la forza dell'intero sistema produttivo».

Sul fronte dell'occupazione, quali incentivi ritiene più efficaci per favorire assunzioni stabili, soprattutto per giovani e donne, e quale ruolo avranno i rinnovi contrattuali nel rafforzare il mercato del lavoro?

«Gli incentivi funzionano davvero quando

aiutano a costruire lavoro stabile, correttamente retribuito, e sono capaci di intercettare le giuste platee di beneficiari. Proprio per questo, la revisione delle agevolazioni per le assunzioni nel Decreto 1° maggio avviene sulla base dei dati che i nostri sistemi informativi ci restituiscono. Sono oltre 165mila le assunzioni agevolate dai bonus del decreto Coesione, 84mila donne. Oggi, con un tasso di disoccupazione attorno al 5 per cento e la crescita dell'occupazione trainata dai contratti a tempo indeterminato, il focus deve spostarsi su chi non partecipa al mondo del lavoro. Il DI 62/2026 sostiene l'assunzione di chi è disoccupato di lunga durata, superando il precedente vincolo del "mai assunto a tempo indeterminato", e vincola il bonus al riconoscimento del salario giusto. Gli esoneri contributivi per under 35 e per donne disoccupate di lungo periodo, che nelle aree Zes arrivano fino a 800 euro mensili, servono proprio a creare ulteriore occupazione stabile. Sostenere il lavoro femminile non è soltanto una questione di equità sociale, ma di crescita economica. Tutti gli indicatori mostrano che laddove cresce l'occupazione femminile aumentano competitività, produttività e capacità di innovare. Insieme agli incentivi, i rinnovi contrattuali restano decisivi per rafforzare il potere d'acquisto delle retribuzioni e accompagnare le trasformazioni del mercato del lavoro».

L'intelligenza artificiale sta trasformando rapidamente professioni e competenze: quali sono, secondo lei, i principali rischi e le opportunità dell'la nel mondo del lavoro e come il Ministero sta preparando lavoratori e imprese a questa transizione?

«L'intelligenza artificiale non è più una prospettiva lontana: è già dentro le fabbriche, gli uffici, i servizi, le piattaforme digitali. Cambia il lavoro, cambia la richiesta di competenze, cambia il modo stesso di organizzare la produzione. I rischi esistono e riguardano soprattutto l'obsolescenza delle competenze e l'uso distorto degli algoritmi nei rapporti di lavoro. Ma le opportunità sono enormi: maggiore produttività, più sicurezza, riduzione delle attività ripetitive e nuovi lavori ad alto valore aggiunto. La sfida vera è non subire la trasformazione. Per questo abbiamo scelto un approccio antropocentrico: la tecnologia deve restare uno strumento al servizio delle persone. Stiamo investendo sulla formazione digitale, sulla piattaforma SIISL, sui programmi di aggiornamento professionale e sull'Osservatorio sull'adozione dell'la nel lavoro, che ci permette di monitorare gli impatti concreti sul mercato occupazionale e costituisce una vera e propria cabina di regia. La tecnologia diventa pericolosa soltanto quando l'uomo rinuncia a governarla».

Facendo riferimento ai dati sugli incidenti sul lavoro, quanto è centrale oggi il



LA SICUREZZA NON DEVE ESSERE PERCEPITA COME UN VINCOLO BUROCRATICO, UN MERO ADEMPIMENTO, UN COSTO: È, INVECE, IL MODO PIÙ EFFICACE CON CUI UNA SOCIETÀ DIMOSTRA RISPETTO PER LE PERSONE E PER LA DIGNITÀ DEL LAVORO

tema della prevenzione?

«La prevenzione è un pilastro della qualità del lavoro e della competitività del nostro sistema produttivo. Un'impresa che investe in sicurezza è un'impresa più forte, più effi-

ciente e capace di crescere. Il tema della sicurezza non può essere affrontato solo dopo una tragedia: deve essere un impegno quotidiano, che considero parte integrante della mia responsabilità istituzionale

e della mia storia professionale. Tra i molti interventi messi in campo, voglio ricordare l'istituzione della patente a crediti, introdotta sedici anni dopo la previsione di legge: uno strumento di qualificazione graduale delle imprese, adottato per l'edilizia, da estendere in altri settori e destinato a mostrare pienamente il suo valore nel tempo. Stiamo inoltre dando attuazione alla previsione del decreto Sicurezza sul badge di cantiere, ancora una volta partendo da una sperimentazione e utilizzando l'area del Cratere Sisma 2016, il più grande cantiere d'Europa. Entrambe le misure hanno come obiettivo la promozione della legalità nel mondo del lavoro e la tutela della salute e della sicurezza. La prevenzione deve diventare parte della cultura d'impresa, dell'organizzazione del lavoro e della formazione quotidiana».

Ci sono interventi che ritiene prioritari per rafforzare la cultura della sicurezza nelle aziende italiane?

«In questi anni abbiamo potenziato l'attività ispettiva e concentrato i controlli nei settori più esposti al rischio, ma sappiamo che le ispezioni da sole non bastano. Abbiamo avviato l'assunzione di centinaia di ispettori dopo anni di blocco del turn over. Abbiamo promosso l'uso della tecnologia per migliorare vigilanza e prevenzione. E sia pure gradualmente, abbiamo riscontrato una generale diminuzione dei casi mortali: una preziosa inversione di tendenza. Nei prossimi mesi continueremo a intervenire in materia di sicurezza. Bisogna insistere lungo questa strada: investire nelle ispezioni, nella formazione continua, nell'innovazione organizzativa e nelle tecnologie che migliorano in concreto la sicurezza degli ambienti di lavoro. Bisogna investire in cultura diffusa della vita sicura. La sicurezza non deve essere percepita come un vincolo burocratico, un mero adempimento, un costo: è, invece, il modo più efficace con cui una società dimostra rispetto per le persone e per la dignità del lavoro». • CG

Marina Calderone, ministro del Lavoro



L'ITALIA SI FA STRADA



 **anas**
GRUPPO FS ITALIANE

Con una rete di 32mila chilometri di strade e autostrade uniamo il Paese, da più di 90 anni.

Siamo l'azienda del Gruppo Ferrovie dello Stato Italiane che gestisce le strade di interesse nazionale. Oggi siamo il **primo gestore della rete stradale in Europa** e forniamo un servizio fondamentale: sulle nostre strade circolano ogni giorno oltre 8 milioni di veicoli passeggeri e oltre 400mila veicoli merci. Lavoriamo per garantire una **mobilità più sostenibile, tecnologica e integrata**.

Siamo presenti sul mercato estero con servizi di ingegneria.



32.000 km
di strade e autostrade



38 sedi
sul territorio



1.300 km
di autostrade



2.157
gallerie



18.720
viadotti



8.000
persone

www.stradeanas.it

Una visione integrata

Dal Decreto Sicurezza al valore del riutilizzo dei beni confiscati come leva di legalità, sviluppo e presenza dello Stato nei territori più fragili. Il sottosegretario Wanda Ferro illustra le azioni messe in campo dal Governo

Il tema della sicurezza è uno dei pilastri fondamentali dell'azione del Governo Meloni, perché rappresenta il presupposto della libertà, della coesione sociale e della fiducia dei cittadini nelle istituzioni. «Per troppo tempo alcuni fenomeni sono stati sottovalutati o affrontati con un approccio ideologico che ha finito per lasciare soli i territori e per indebolire la presenza dello Stato. Abbiamo dunque scelto - mette in evidenza il sottosegretario al Ministero dell'Interno Wanda Ferro - una linea diversa: concreta e pragmatica, fondata su investimenti, prevenzione e capacità di intervento». I numeri dimostrano che la direzione è quella giusta. «Nel 2025 i delitti complessivi sono diminuiti del 2 per cento rispetto all'anno precedente. Abbiamo garantito il turnover al 100 per cento nelle Forze dell'Ordine, assunto oltre 42 mila unità e programmato ulteriori 27 mila ingressi entro la fine della legislatura. Sono stati stanziati oltre 1 miliardo e mezzo di euro per i rinnovi contrattuali, insieme al potenziamento di mezzi, tecnologie e sistemi di videosorveglianza».

Oggi la sicurezza richiede soprattutto una visione integrata.

«Esattamente. Non esiste più una distinzione netta tra sicurezza urbana, infrastrutturale, economica o digitale. Pensiamo alle minacce cyber contro infrastrutture strategiche, ai fenomeni di degrado urbano che alimentano criminalità e violenza giovanile, oppure ai rischi legati alla sicurezza del trasporto pubblico e ferroviario. Per questo il Governo sta lavorando su una strategia complessiva che tiene insieme controllo del territorio, rigenerazione urbana, legalità e prevenzione sociale. In questo quadro si inseriscono anche operazioni come "Strade Sicure" e "Stazioni Sicure" e il modello Caivano, che considero uno degli esempi più efficaci di ritorno dello Stato nei territori più difficili: non soltanto repressione, ma recupero urbano, scuola,

sport, servizi e restituzione degli spazi ai cittadini perbene».

Quali sono i pilastri principali del nuovo Decreto Sicurezza e quali obiettivi si pone nel

breve e medio periodo? dono direttamente sulla vita quotidiana delle persone. Parliamo di occupazioni abusive, borseggi, truffe agli anziani, spaccio diffuso, violenze contro le Forze dell'Ordine, blocchi

gali delle strade o le aggressioni alle Forze dell'Ordine significa tutelare i diritti della grande maggioranza dei cittadini che rispettano le regole. Purtroppo ogni volta che si tratta di raffor-



IL DECRETO SICUREZZA CONTIENE NORME DI ASSOLUTO BUON SENSO. CONTRASTARE LO SPACCIO, LE OCCUPAZIONI ABUSIVE, I BLOCCHI ILLEGALI DELLE STRADE O LE AGGRESSIONI ALLE FORZE DELL'ORDINE SIGNIFICA TUTELARE I DIRITTI DELLA GRANDE MAGGIORANZA DEI CITTADINI CHE RISPETTANO LE REGOLE

breve e medio periodo?

«Il Decreto Sicurezza nasce per dare risposte concrete a problemi concreti, quelli che inci-

stradali e ferroviari, fenomeni di degrado e criminalità urbana. Abbiamo introdotto strumenti più efficaci per prevenire e contrastare questi fenomeni, rafforzando allo stesso tempo le tutele per chi ogni giorno indossa una divisa e rappresenta lo Stato. Penso, ad esempio, alle norme contro le aggressioni agli operatori delle Forze dell'Ordine, al contrasto delle manifestazioni violente e dei blocchi illegali delle infrastrutture strategiche, oppure al rafforzamento dei controlli nelle aree più esposte al degrado».

Alcune forze di opposizione parlano di un rischio di compressione delle libertà individuali. Come risponde a queste critiche?

«Rispondo che difendere la legalità e garantire sicurezza ai cittadini non significa comprimere le libertà, ma renderle effettive. La vera limitazione della libertà è quando una persona ha paura di prendere un treno la sera, di uscire nel proprio quartiere o di mandare i figli a scuola serenamente. Il Decreto Sicurezza contiene norme di assoluto buon senso. Contrastare lo spaccio, le occupazioni abusive, i blocchi ille-

zare la sicurezza, spesso ci troviamo davanti ad un'opposizione pregiudiziale. Si invoca più sicurezza a parole, ma poi si contestano tutte le misure concrete che servono a garantirla. Noi invece abbiamo scelto di stare dalla parte dei cittadini onesti, di chi chiede più presenza dello Stato, più legalità e più tutela. Poi il nostro approccio non è solo repressivo. Lo dimostra il modello Caivano e lo dimostrano gli investimenti sulla rigenerazione urbana, sulla scuola, sul recupero sociale e sui beni confiscati. La sicurezza si costruisce con il controllo del territorio, ma anche combattendo marginalità, degrado ed esclusione sociale».

Un capitolo particolarmente importante riguarda la violenza giovanile.

«Abbiamo introdotto norme più severe sul porto di coltelli e il divieto di vendita ai minori di strumenti che troppo spesso diventano armi nelle mani dei ragazzi. È una scelta di buon senso, necessaria davanti all'aumento di episodi di aggressione e baby gang. Fondamentale è anche il rafforzamento dei sistemi di



videosorveglianza, che svolgono una funzione non solo repressiva ma soprattutto deterrente. Una telecamera spesso evita che un reato venga commesso e aiuta a restituire sicurezza ai cittadini. Vogliamo aumentare la presenza dello Stato nei territori, rafforzare la percezione di sicurezza, prevenire il degrado e dare alle Forze dell'Ordine strumenti più adeguati per intervenire in modo tempestivo ed efficace».

Al Viminale è stata firmata un'intesa importante su riuso, legalità e rigenerazione urbana: che valore ha questo accordo per i territori coinvolti?

«Ha un valore strategico molto importante, perché dimostra che il contrasto alle mafie non si esaurisce nelle attività repressive, ma passa anche dalla capacità dello Stato di restituire ai cittadini ciò che la criminalità aveva sottratto. Mi riferisco innanzitutto al rinnovo dell'accordo tra l'Agenzia Nazionale per i beni confiscati e la Regione Calabria, un protocollo che consolida un modello di collaborazione istituzionale estremamente efficace. In Calabria gli immobili confiscati già destinati sono 3.869, di cui oltre 3.100 trasferiti ai Comuni. Parliamo di beni che diventano centri sociali, presidi di legalità, strutture contro le dipendenze, luoghi di inclusione e anche sedi delle Forze di Polizia. Questo modello ha già prodotto risultati concreti. Penso, ad esempio, alla demolizione dell'ecomostro "Palazzo Mangeruca" a Melissa, nel Crotonese, per realizzare un'area camper: un simbolo di rigenerazione urbana e restituzione del territorio alla collettività. L'esperienza è stata così positiva che accordi analoghi sono stati stipulati anche con Sicilia, Lombardia e Campania, mentre presto verrà coinvolto anche il Piemonte».

E per quanto riguarda la rigenerazione urbana?

«Dal Viminale sono stati destinati oltre 600 milioni di euro ai Comuni per progetti di riqualificazione urbana, messa in sicurezza degli edifici e recupero delle aree degradate. Una città è più sicura quando i cittadini sentono che lo Stato è presente e che i luoghi vengono curati, recuperati e protetti. Al contrario, il degrado urbano e l'abbandono degli spazi pubblici favoriscono insicurezza e illegalità. La cosiddetta teoria delle 'finestre rotte' mostra che dove lo Stato arretra, dove prevalgono incuria, vandalismo e marginalità, cresce più facilmente la criminalità diffusa. Per questo rigenerare un quartiere, recuperare un immobile confiscato, riqualificare una piazza o rafforzare un presidio di legalità non significa soltanto migliorare il decoro urbano e la vivibilità dei luoghi, ma prevenire fenomeni criminali e ricostruire fiducia tra cittadini e istituzioni».

Oltre 3.800 immobili sottratti alla criminalità organizzata verranno restituiti alla collettività: quale impatto concreto potrà avere questa operazione sul tessuto sociale ed economico?

«L'impatto può essere molto significativo, perché ogni bene confiscato restituito alla collettività rappresenta insieme una vittoria dello Stato e un'opportunità concreta di sviluppo e riscatto sociale. Parliamo di immobili che possono diventare scuole, centri di aggregazione, strutture



UNA CITTÀ È PIÙ SICURA QUANDO I CITTADINI SENTONO CHE LO STATO È PRESENTE E CHE I LUOGHI VENGONO CURATI, RECUPERATI E PROTETTI. AL CONTRARIO, IL DEGRADO URBANO E L'ABBANDONO DEGLI SPAZI PUBBLICI FAVORISCONO INSICUREZZA E ILLEGALITÀ

sociali, sedi istituzionali o presidi delle Forze dell'Ordine, trasformando luoghi che erano simboli del potere mafioso in spazi di legalità, partecipazione e crescita civile. L'esempio più recente e significativo è stata la demolizione di Palazzo Fienga a Torre Annunziata, il cosiddetto "Fortapàsc" della camorra, storico simbolo del clan Gionta, da cui partì l'ordine di uccidere il giornalista Giancarlo Siani. In questi anni oltre 18 mila beni confiscati sono tornati nella disponibilità dei cittadini. Abbiamo rafforzato l'Agenzia nazionale, accelerato le procedure di destinazione e costruito una rete stabile con prefetture, procure, enti locali e privato sociale per trasformare questi patrimoni in strumenti di crescita e coesione. C'è poi un aspetto fondamentale: accompagnare le aziende confiscate che possono superare il cosiddetto "shock di legalità", restare sul mercato e continuare a produrre occupazione sana. Questo significa tra-

sformare patrimoni criminali in occasioni di sviluppo e crescita per i territori».

Il riutilizzo dei beni confiscati può diventare anche uno strumento di prevenzione oltre che di contrasto alla criminalità: in che modo il Governo intende rafforzare questo approccio?

«Oggi il riutilizzo sociale dei beni confiscati è uno dei più efficaci strumenti di prevenzione antimafia, perché colpisce le organizzazioni criminali nel loro vero centro di potere: la capacità economica e il controllo del territorio. Le mafie moderne agiscono sempre più come sistemi economici e finanziari, infiltrandosi nell'economia legale e creando consenso sociale. Sequestrare e confiscare patrimoni mafiosi significa prevenire nuove infiltrazioni e indebolire le reti criminali prima ancora della repressione penale. Il modello italiano delle misure di prevenzione patrimoniale è oggi guar-

dato con grande interesse anche dai nostri partner europei e internazionali. Non è un caso che la nuova direttiva europea sul recupero e la confisca dei beni si ispiri proprio all'esperienza italiana. Il Governo Meloni intende rafforzare ulteriormente questo approccio accelerando le procedure di destinazione, sostenendo gli enti locali e potenziando il coordinamento tra istituzioni, perché ogni bene restituito ai cittadini diventa un presidio concreto di legalità, inclusione e presenza dello Stato». •CG

Wanda Ferro, sottosegretario di Stato al Ministero dell'Interno



Con te,
in Prima
linea.

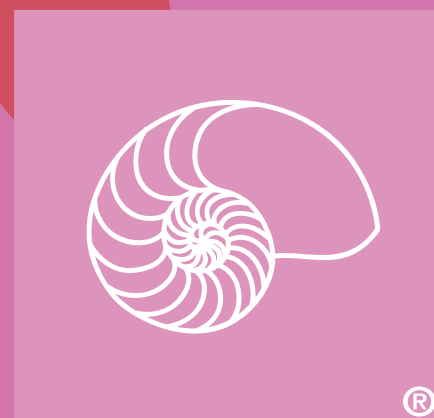
CENTRALINO NAZIONALE
ATTIVO H24
7 GIORNI SU 7



06 37 51 82 82

Dal 1988 sosteniamo le donne e i minori vittime di violenza, offrendo gratuitamente accoglienza, protezione, alloggi sicuri, consulenze legali, psicologiche e nutrizionali, percorsi mirati di fuoriuscita dalla violenza e appropriazione della propria autonomia.

TELEFONO
ROSA



Più forti insieme.

telefonorosa.it



Una risposta forte alla crescente complessità che ci circonda

In un quadro di instabilità pervasiva globale, le attenzioni della Difesa sono concentrate su ogni latitudine geografica. Il sottosegretario di Stato Isabella Rauti descrive l'impegno dell'Italia su scala globale

La sicurezza nazionale e la libertà collettiva sono priorità del Governo e della Difesa. Dopo decenni di pace, percepita come garantita e data per scontata, il paradigma si è spezzato. «Da quattro anni, dopo l'aggressione russa all'Ucraina- spiega Isabella Rauti, sottosegretario di Stato alla Difesa- la guerra scuote il cuore dell'Europa. Nuovi conflitti nel Golfo Persico e in Medio Oriente generano instabilità alle porte del Mediterraneo- "un continente liquido", per citare le parole dello storico Fernand Braudel- condizionando gli equilibri globali. Siamo di fronte a nuove forme di guerra, combattute non soltanto "bootson the ground" ma ibride e non convenzionali, che si sviluppano in tutti i domini: nel dominio digitale e cibernetico, in quello spaziale, nell'ambito cognitivo e nella dimensione dell'underwater».

Quali sono le principali priorità della Difesa, in un contesto internazionale così sfidante?

«In questo quadro di instabilità pervasiva globale, le attenzioni della Difesa sono concentrate su ogni latitudine geografica; sul "Fianco Est" e sul "Fronte Sud" ma anche nel "Grande Nord". La Regione artica oggi rappresenta uno spazio strategico per la sicurezza euro-atlantica e per gli equilibri mondiali anche in relazione alla protezione delle infrastrutture critiche e delle linee energetiche che collegano scenari lontani ma interconnessi. Penso anche alle nuove tensioni geopolitiche che la guerra in Iran ha generato (Paesi arabi, Mar Rosso, Stretto di Hormuz) che ci ricordano quanto fragile sia l'equilibrio energetico globale e quanto siano interdipendenti ecosistemi distanti e diversi».

In che modo l'Italia sta bilanciando gli impegni nel quadro della cooperazione con la Nato e con altri partner internazionali, soprattutto nelle missioni all'estero?

«L'Italia è un alleato leale della Nato e un membro dell'Ue, di cui stiamo rafforzando le capacità di difesa come pilastro complementare della Nato; ovvero aumentando e investendo su un'industria con standard comuni by design. Oggi la guerra si combatte nel dominio cyber, nello spazio, nella dimensione subacquea e nell'ambito cognitivo. La risposta- come indicato nel "non paper" del ministro Crosetto- deve essere proattiva



Come le politiche di Difesa possono contribuire alla promozione e tutela dei valori nazionali e al rafforzamento del ruolo dell'Italia nel mondo?

«La cultura della Difesa è un sistema di valori, "un patrimonio materiale e immateriale", come dichiarato anche di recente dal ministro Crosetto. Difesa significa tutela delle istituzioni della Repubblica, salvaguardia delle infrastrutture strategiche e delle reti essenziali per il funzionamento del Paese, insieme alla protezione del sistema industriale e tecnologico, del patrimonio storico e dell'identità nazionale. Non si tratta di una forma di militarizzazione ma della responsabilità di preservare le libertà individuali e collettive e di rafforzare la capacità di risposta nella crescente complessità che ci circonda. La partecipazione dell'Italia alle missioni internazionali è uno strumento di diplomazia strategica che rafforza il dialogo con i partner e consolida le relazioni bilaterali in aree di interesse geopolitico».

Quali opportunità vede per il made in Italy nei filoni di cooperazione industriale e tecnologica legati alla difesa

OCCORRE MUOVERSI IN UN'OTTICA DI RESPONSABILITÀ NAZIONALE FAVORENDO LE RELAZIONI INDUSTRIALI, ABBATTENDO LA LENTEZZA PROCEDURALE CUI CI VINCOLA LA BUROCRAZIA, INVESTENDO IN CYBERDIFESA, IN TECNOLOGIE DUAL-USE, NELLA NEW SPACE ECONOMY E NELLA BLUE ECONOMY

e integrata, puntando sulla deterrenza difensiva, sulla prevenzione, sulla resilienza e sulla cooperazione tra Stati. Da decenni siamo impegnati nelle missioni internazionali di pace e stabilità, nelle coalizioni multinazionali e con i nostri contingenti schierati siamo tra i maggiori contributori su scala globale. La presenza italiana nei teatri operativi è orientata non solo a garantire condizioni di sicurezza e di deterrenza delle minacce ma anche al supporto alla popolazione civile e alla cooperazione con le istituzioni locali. L'Italia è tra i Paesi più attivi nell'applicazione delle Risoluzioni delle Nazioni Unite su "Donne, pace e sicurezza" e sulle pari opportunità, nonché sull'impegno e nella ricostruzione post-conflict».

e alla sicurezza internazionale?

«Il Governo lavora alla valorizzazione del tessuto produttivo nazionale, favorendo un circolo economico virtuoso; anche le spese per la difesa sono un investimento che produce lavoro e indotto occupazionale. In questa prospettiva, la cooperazione industriale e tecnologica rappresenta una leva strategica per rafforzare il posizionamento del made in Italy nei principali programmi internazionali; penso al Global Combat Air Programme (GCAP), un'iniziativa congiunta di Regno Unito, Italia e Giappone per sviluppare una nuova generazione di caccia multi ruolo avanzato di sesta generazione entro la metà degli anni 2030. E al programma Eurodrone, che segna un passaggio fondamentale nella costru-

zione di una capacità europea autonoma nel dominio dei sistemi a pilotaggio remoto, rafforzando al contempo il ruolo dell'industria nazionale nelle tecnologie avanzate per la sorveglianza, l'intelligence e la sicurezza».

Per garantire sovranità, vantaggio competitivo e strategico cosa bisogna fare?

«Per garantire sovranità, vantaggio competitivo e strategico dobbiamo continuare a sviluppare le nuove tecnologie; governare l'intelligenza artificiale, utilizzare il quantum computing e la sensoristica avanzata, secondo un modello di difesa integrato e completo che coinvolga le industrie, le università, la società civile e il sistema Italia. In questo quadro, l'integrazione tra pubblico e privato e tra dimensione nazionale ed europea diventa determinante per sostenere l'innovazione e accrescere la resilienza industriale. La Difesa perciò deve continuare a muoversi in un'ottica di responsabilità nazionale: favorendo le relazioni industriali; abbattendo la lentezza procedurale cui ci vincola la burocrazia; investendo in cyberdifesa; in tecnologie dual-use; nella new space economy- decisiva per la sicurezza delle infrastrutture critiche e la resilienza delle reti- al pari della blue economy, sempre più centrale per la sicurezza delle rotte, la protezione delle infrastrutture sottomarine e la continuità energetica. Si tratta di due ambiti complementari che contribuiscono in modo crescente alla proiezione strategica e industriale dell'Italia». •LZ



Isabella Rauti, sottosegretario di Stato alla Difesa

Ognuno è un ingranaggio consapevole

È la fiducia incondizionata, radicata nella conoscenza reciproca, nel rispetto e nella condivisione degli stessi valori, che nei momenti decisivi può fare la differenza. A guidare l'equipaggio nella riuscita delle loro missioni è il comandante Sara Vinci

Ogni comandante porta con sé un patrimonio unico fatto di esperienze, valori e tratti personali, ed è proprio l'unicità della persona, più che il genere, a riflettersi in modo determinante nel proprio stile di leadership. «Questa dimensione individuale, che si sovrappone a quella propria di ogni ufficiale di Marina- precisa Sara Vinci, comandante della Nave Alpino della Marina Militare- rappresenta una risorsa preziosa: la varietà dei vissuti e dei punti di vista arricchisce il modo in cui si affrontano le sfide quotidiane e si costruiscono le relazioni a bordo».

In che modo la leadership femminile può arricchire e influenzare la dinamica a bordo e la gestione dell'equipaggio?

«Nella mia esperienza, cerco di coltivare ogni giorno il senso di appartenenza dell'equipaggio e di mantenere alto il morale per garantire la massima efficacia operativa. Un equipaggio che si sente parte di un obiettivo comune, motivato e valorizzato nelle proprie individualità, è un equipaggio più coeso, reattivo e affidabile. In questo contesto, "remare all'unisono" non è soltanto un principio guida, ma una condizione imprescindibile per il successo di ogni missione. Significa costruire, giorno dopo giorno, una fiducia solida e autentica che nasce nel rapporto tra equipaggio e comandante, ma che si sviluppa anche in modo trasversale tra tutti i membri dell'equipaggio stesso».

Quali sono le principali responsabilità e sfide nel comando di una nave della Marina Militare come la Alpino?

«Il comandante ha come responsabilità primaria quella di garantire, in modo parimenti imprescindibile, la piena efficienza del mezzo e la prontezza operativa del personale, affinché l'unità sia sempre in grado di assolvere la missione assegnata. La nave rappresenta uno strumento tecnologicamente avanzato e complesso, ma è l'equipaggio, adeguatamente formato e addestrato, a renderlo realmente efficace e capace di esprimere tutte le sue potenzialità. Per questo motivo, accanto alla cura costante dell'efficienza della piattaforma e dei sistemi, che richiede attenzione continua, manutenzione accurata e gestione rigorosa delle risorse, riveste un ruolo centrale l'addestramento del personale per consolidarne prontezza, flessibilità e resilienza anche in contesti complessi e multi-dominio. La sfida principale consiste



IL COMANDANTE HA COME RESPONSABILITÀ PRIMARIA QUELLA DI GARANTIRE, IN MODO PARIMENTI IMPRESCINDIBILE, LA PIENA EFFICIENZA DEL MEZZO E LA PRONTEZZA OPERATIVA DEL PERSONALE, AFFINCHÉ L'UNITÀ SIA SEMPRE IN GRADO DI ASSOLVERE LA MISSIONE ASSEGNATA

sicuramente nel garantire questo equilibrio in un contesto caratterizzato da una rapida e costante evoluzione. Le tecnologie si sviluppano con grande velocità e gli scenari operativi diventano sempre più dinamici e interconnessi, includendo nuove realtà come il dominio cibernetico e la dimensione cognitiva. Questo richiede non solo capacità di adattamento ma anche un aggiornamento continuo per integrare innovazione tecnologica e fattore umano in modo efficace».

Quali strumenti e percorsi formativi ritiene fondamentali per preparare ufficiali e marinai alle complesse operazioni militari e alle missioni internazionali?

«La Marina dispone di percorsi formativi ben delineati e strutturati, studiati per preparare al meglio il personale dei diversi ruoli ad affrontare la complessità delle operazioni militari e delle missioni internazionali. La formazione si costruisce su un sistema organico che integra preparazione di base, specializzazione e aggiornamento professionale, con contenuti sempre al passo con l'evoluzione degli scenari operativi e delle tecnologie. La formazione ci accompagna per tutta la carriera secondo un modello dinamico e circolare che favorisce il continuo sviluppo delle compe-

tenze indispensabili nei contesti complessi e multi-dominio. Particolare rilevanza assume l'addestramento secondo il principio del "train as you fight" preparando quotidianamente il personale ad operare in condizioni il più possibile aderenti agli attuali scenari internazionali».

Quanto conta la resilienza, la disciplina e la capacità di adattamento nella vita quotidiana a bordo e nelle missioni più complesse?

«La disciplina è la base di partenza, il punto fermo. Non è solo rispetto delle regole, ma è ciò che crea fiducia tra le persone, che rende ogni azione prevedibile, coordinata, affidabile. La resilienza, invece, è un fattore chiave per chi svolge il nostro lavoro. Significa non fermarsi alla difficoltà, ma attraversarla, mantenendo lucidità, equilibrio e capacità decisionale anche sotto pressione. Infine, la capacità di adattamento è ciò che permette di armonizzare la dimensione personale con quella collettiva: ognuno diventa un ingranaggio consapevole, capace di lavorare in sintonia con gli altri, contribuendo a un'unica azione coordinata ed efficace. Bisogna inoltre sapersi adattare al contesto che cambia continuamente perché cambia la missione o l'area geografica di gravitazione della nave».

Quali prospettive e opportunità vede per le donne nelle Forze Armate, e quale messaggio vorrebbe trasmettere alle giovani che aspirano a intraprendere una carriera militare?

«Sono entrata in Marina agli albori del reclutamento femminile e ho avuto il privilegio di vivere in prima persona un percorso di trasformazione profondo. Ho visto evolvere la Difesa italiana fino a diventare oggi una delle realtà più avanzate in termini di piena integrazione, fondata sul merito, sulle competenze e sul riconoscimento delle capacità individuali, indipendentemente dal genere. È vero, per una questione temporale il percorso non è ancora completamente maturo dal punto di vista numerico, ma la direzione è chiara. Proprio per questo guardo al futuro con fiducia e con l'aspettativa di vedere quanto questa integrazione continuerà a generare valore. Un'organizzazione più diversificata è, infatti, anche più solida, più pronta ad affrontare le sfide e, in definitiva, più resiliente. Alle giovani che oggi desiderano intraprendere questa strada direi che si tratta di una scelta certamente impegnativa, sia sul piano professionale che personale, ma anche straordinariamente arricchente. È un percorso che permette di acquisire competenze autentiche, vivere esperienze uniche e assumere responsabilità importanti fin da giovani. In Marina non si impara soltanto una professione, si cresce come persone in un contesto che si fonda su valori profondi e immutabili. Ed è proprio questo che dà un significato pieno e concreto alla nostra scelta di vita».

•Ginevra Cavalieri



Sara Vinci, comandante Nave Alpino Marina Militare

Dalla piazza fisica al terreno virtuale

In un'economia non solo globalizzata ma anche digitalizzata le organizzazioni criminali rinnovano strategie e tecniche per insinuarsi negli spazi anonimi della rete, così da compiere le stesse attività illecite perpetrate nel mondo reale. Il generale Antonio Mancazzo ci spiega come è cambiato il crimine online e l'attività di contrasto della Guardia di Finanza

La trasformazione digitale dell'economia ha aperto scenari senza precedenti per cittadini, imprese e mercati, ma allo stesso tempo ha ampliato il terreno d'azione della criminalità informatica. Oggi le frodi online non colpiscono più soltanto singoli utenti o sistemi isolati: coinvolgono infrastrutture strategiche, flussi finanziari globali e intere filiere produttive attraverso attacchi sempre più sofisticati e transnazionali. Dal furto d'identità digitale ai ransomware, fino all'utilizzo dell'intelligenza artificiale per costruire truffe credibili e difficili da individuare, il cybercrime rappresenta una delle principali sfide contemporanee per la sicurezza economico-finanziaria. In questo contesto il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza, guidato dal generale Antonio Mancazzo, svolge un ruolo centrale nel presidio investigativo della rete, operando anche negli spazi più opachi del deep e dark web.

Negli ultimi anni le frodi online sono diventate sempre più sofisticate: quali sono oggi le minacce economico-finanziarie più diffuse che colpiscono cittadini e imprese sulla rete?

«Mi sia consentita una doverosa premessa: oggi siamo di fronte a un'economia non solo globalizzata ma, grazie alle tecnologie, anche digitalizzata. A fronte degli indubbi vantaggi che tutto ciò comporta sia per i cittadini che per le imprese, non si può sottovalutare come, in tale scena-



I RANSOMWARE ATTACK, SE ATTIVATI, PRECLUDONO L'ACCESSO AI DATI UTILIZZANDO DELLE SOFISTICATE TECNICHE CRITTOGRAFICHE E ALIMENTANO COSÌ UN VERO E PROPRIO MERCATO CRIMINALE PARALLELO BASATO SUL PAGAMENTO DEI RISCATTI, SPESSO EFFETTUATI TRAMITE CRIPTOVALUTE PARTICOLARMENTE AMBITE DAI CYBERCRIMINALI PER LA LORO NATURA PSEUDO ANONIMA

rio, anche le organizzazioni criminali, a diversi livelli, avvertono l'esigenza di rinnovare le proprie strategie e tecniche

attraverso le quali potersi insinuare negli spazi anonimi della rete così da compiere le stesse attività illecite perpetrate nel mondo reale. Infatti, le attività investigative dimostrano proprio come negli ultimi tempi si stia assistendo ad uno spostamento dell'illecito dalla piazza fisica al terreno virtuale. L'utilizzo illecito delle nuove tecnologie ha portato, quindi, la Guardia di Finanza a rafforzare il dispositivo di contrasto che oggi è anche orientato al controllo economico del web attraverso il monitoraggio della rete telematica, soprattutto quella nascosta. Il riferimento è in particolare al deep e dark web dove si annidano le attività più perniciose portate avanti da soggetti dediti a delinquere e che hanno solide radici nel mondo reale. In tale ambito, il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche rappresenta, ad oggi, il Reparto del Corpo specializzato nel contrasto al cybercrime in ogni sua forma garantendo il co-

stante presidio di polizia economico-finanziaria in rete».

Tornando alla mia domanda?

«Cercando di rispondere alla sua domanda, devo effettivamente sottolineare come purtroppo stiamo assistendo a un forte aumento delle frodi a monte delle quali, è bene sottolinearlo, c'è quasi sempre un furto d'identità digitale. Ecco perché bisogna prestare massima attenzione a non far circolare sul web, laddove non estremamente necessario, dati riferibili alla propria persona e/o che possano far risalire a posizioni di titolarità (come ad esempio quelle bancarie). In generale, si parla di minacce evolute attuate, ad esempio, attraverso i ransomware o attacchi alle infrastrutture critiche, spesso transnazionali, che sfruttano competenze e strumenti digitali avanzati, tecniche di ingegneria sociale, piattaforme online e persino sistemi basati sull'intelligenza artificiale per rendere le truffe più credibili



e difficili da individuare. I ransomware attack, se attivati, precludono l'accesso ai dati utilizzando delle sofisticate tecniche crittografiche e alimentano così un vero e proprio mercato criminale parallelo basato sul pagamento dei riscatti, spesso effettuati tramite criptovalute particolarmente ambite dai cybercriminali per la loro natura pseudo anonima».

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche opera in un contesto in continua evoluzione: quanto conta oggi la collaborazione internazionale nel contrasto ai crimini digitali?

«Il contrasto ai crimini digitali è oggi, per definizione, una sfida globale: le infrastrutture informatiche, i servizi cloud, le piattaforme di pagamento e le reti criminali operano senza confini spazio temporali. Questo significa che le attività illecite possono essere pianificate in un Paese, essere eseguite attraverso server collocati in un altro e potenzialmente produrre effetti in più Stati contemporaneamente. In questo scenario, diventa fondamentale la collaborazione tra Forze di Polizia, autorità giudiziarie, organismi europei e internazionali per condividere informazioni, tracciare flussi finanziari, acquisire dati digitali e coordinare operazioni complesse in tempi che necessariamente devono essere compatibili con la rapidità dell'ambiente cyber».

Le criptovalute e i sistemi di pagamento digitali stanno cambiando il panorama finanziario: quali sono le principali difficoltà investigative nel tracciare flussi economici illeciti online?

«Sebbene la blockchain sia per natura pubblica, la vera sfida è identificare l'effettivo titolare di un wallet o di un'operazione registrata nella citata "catena di blocchi". E, qui, entrano in gioco le abilità dei nostri investigatori digitali che, attraverso il ricorso a tecniche specifiche di blockchain analysis e intelligence, cercano di anonimizzare i possessori di criptovalute. Attività che diventa ulteriormente complessa allorché i cyber criminali ricorrono a exchange collocati in giurisdizioni poco collaborative, mixer e privacy coin. Un ulteriore aspetto



IL CONTRASTO AI CRIMINI DIGITALI È OGGI, PER DEFINIZIONE, UNA SFIDA GLOBALE: LE INFRASTRUTTURE INFORMATICHE, I SERVIZI CLOUD, LE PIATTAFORME DI PAGAMENTO E LE RETI CRIMINALI OPERANO SENZA CONFINI SPAZIO TEMPORALI

riguarda la velocità con cui i proventi illeciti possono essere frammentati e trasferiti tra diversi strumenti finanziari digitali, rendendo più complessa la ricostruzione

del percorso del denaro. Per questo motivo, le indagini economico-finanziarie in ambito cyber richiedono oggi un approccio multidisciplinare che integri competenze investigative, informatiche e di analisi finanziaria avanzata».

Sul fronte della prevenzione, quali comportamenti e strumenti ritiene fondamentali per aiutare cittadini e aziende a difendersi dalle frodi tecnologiche?

«La prevenzione rappresenta oggi la prima e più efficace linea di difesa contro le frodi tecnologiche, non a caso si parla di educazione finanziaria. Per i cittadini, questo deve tradursi nell'adozione di comportamenti semplici ma essenziali: utilizzo di password robuste e differenti, attivazione di sistemi di autenticazione a più fattori, aggiornamento costante dei

dispositivi e software, verifica dell'identità di chi richiede dati sensibili o trasferimenti di denaro, attenzione a comunicazioni allarmistiche o troppo vantaggiose. Noi ribadiamo sempre un adagio del passato, oggi più che mai attuale: "Se vi viene proposto qualcosa di troppo bello per essere vero, allora non è vero!!" È, altrettanto, importante segnalare tempestivamente tentativi di truffa alle autorità competenti, perché ogni segnalazione contribuisce a rafforzare la capacità di prevenzione collettiva. Per le imprese, soprattutto per le piccole e medie aziende che spesso dispongono di minori risorse dedicate alla sicurezza informatica, la prevenzione deve tradursi in investimenti concreti in cybersecurity, formazione del personale e protezione delle infrastrutture digitali. La sicurezza, pertanto non può essere percepita come un costo aggiuntivo, ma come un investimento strategico per la competitività e la continuità operativa».

L'intelligenza artificiale è sempre più presente anche nel mondo cyber: l'AI può essere utilizzata per commettere illeciti, ma allo stesso tempo rappresenta una risorsa investigativa. Come sta cambiando il vostro lavoro e quali sono oggi le principali opportunità e incognite legate a questa tecnologia?

«Da un lato, l'intelligenza artificiale potrebbe rappresentare uno strumento sfruttato anche in modo illecito: pensiamo alla creazione di campagne di phishing sempre più credibili, ai deepfake, all'automazione delle frodi online o alla produzione massiva di contenuti ingannevoli. Dall'altro lato, la stessa tecnologia costituisce una risorsa strategica per le attività investigative che possono analizzare grandi quantità di dati, individuare anomalie, correlare eventi, supportare il monitoraggio delle minacce e accelerare le attività di analisi forense digitale. La sfida principale, tuttavia, consiste nel mantenere un equilibrio tra innovazione, sicurezza e garanzie democratiche, nel rispetto dei principi di legalità, proporzionalità, tutela dei diritti fondamentali e protezione dei dati personali».

• **Lucrezia Antinori**

Il generale Antonio Mancazzo, comandante Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza





Dal 1815 aiutiamo a spedire merci verso ogni destinazione

Quando il successo dipende dal commercio globale, sappiamo quanto è importante che le merci arrivino puntuali a destino. Ecco perchè DHL Global Forwarding promette di offrire sempre consegne affidabili, flessibili ed efficienti da e verso ogni Paese del mondo, in totale conformità con le normative locali.

infodgf.it@dhl.com

Excellence. Simply delivered.
dhl.com



La Farnesina è in prima linea

Su indicazione del ministro Antonio Tajani la struttura è stata incaricata di assicurare uno stretto raccordo tra la cybersicurezza del Ministero e delle sedi all'estero, da un lato, e l'azione di politica estera dell'Italia nei settori delle minacce ibride, della sicurezza cibernetica e delle tecnologie emergenti dall'altro. A guidarla è Alessandro De Pedys

La trasformazione digitale e l'accelerazione tecnologica stanno ridefinendo equilibri geopolitici, modelli economici e sistemi di difesa. Oggi il cyberspazio è diventato un terreno strategico nel quale si intrecciano sicurezza nazionale, tutela delle infrastrutture critiche, diplomazia e competizione internazionale. In questo scenario, l'Italia punta a rafforzare il proprio ruolo attraverso una strategia fondata su cooperazione multilaterale, resilienza tecnologica e governance condivisa. Ne parla Alessandro De Pedys, direttore generale per le questioni cibernetiche della Farnesina, al centro della nuova architettura voluta dal ministro Antonio Tajani per affrontare le sfide del dominio digitale e delle minacce ibride.

Com'è cambiata la missione della Direzione Generale dopo la riforma cyber e digitale promossa dal ministro Antonio Tajani e quali sono oggi le priorità strategiche dell'Italia nel cyberspazio?

«Il panorama internazionale è caratterizzato da una forte accelerazione del processo di innovazione tecnologica e, al tempo stesso, dalla progressiva digitalizzazione delle società avanzate. Le nostre società sono ormai rette da infrastrutture digitali tanto essenziali quanto vulnerabili e, in questo contesto, le dipendenze tecnologiche e le attività cibernetiche malevole sono alcune delle sfide che l'Italia è chiamata ad affrontare. Per questo la Farnesina si è dotata, su indicazione del ministro Tajani, di una struttura incaricata di assicurare uno stretto raccordo tra la cybersicurezza del Ministero e delle sedi all'estero, da un lato, e l'azione di politica estera dell'Italia nei settori delle minacce ibride, della sicurezza cibernetica e delle tecnologie emergenti dall'altro. D'altronde, quello digitale è un dominio nel quale l'interconnessione fra Paesi e aree del mondo è particolarmente evidente. Per questo motivo occorre adoperarsi attraverso molteplici iniziative di cooperazione internazionale per porre in essere misure volte a garantire la stabilità, la pace e la sicurezza, anche a tutela dei nostri interessi nazionali. In questo senso, la Farnesina collabora strettamente con tutte le Amministrazioni competenti per accrescere la propria postura di sicurezza cibernetica, definire una governance globale del cyberspazio, imperniata sulla cornice ONU di comportamento responsabile degli Stati, e contribuire alla costruzione di capacità informatiche nei



LA FARNESINA COLLABORA CON TUTTE LE AMMINISTRAZIONI COMPETENTI PER ACCRESCERE LA PROPRIA POSTURA DI SICUREZZA CIBERNETICA, DEFINIRE UNA GOVERNANCE GLOBALE DEL CYBERSPAZIO, IMPERNIATA SULLA CORNICE ONU DI COMPORTAMENTO RESPONSABILE DEGLI STATI, E CONTRIBUIRE ALLA COSTRUZIONE DI CAPACITÀ INFORMATICHE NEI PAESI IN VIA DI SVILUPPO

Paesi in via di sviluppo».

Quali strumenti diplomatici e operativi ritiene oggi più efficaci per affrontare minacce sempre più ibride e

globali, come attacchi alle infrastrutture critiche, interferenze nei processi democratici, campagne di disinformazione?



«Nell'attuale scenario globale, dove si afferma sempre di più un approccio competitivo- quando non di aperto confronto- tra Paesi o gruppi di Paesi portatori di interessi e valori diversi, è essenziale che alle strategie di deterrenza e difesa si sommino attività di preparazione e risposta sviluppate in maniera integrata, soprattutto a fronte del moltiplicarsi delle minacce di natura ibrida. Questo significa innanzitutto coinvolgere tutte le istituzioni a vario titolo interessate, sviluppando un approccio coordinato che permetta di fronteggiare sul serio tali sfide, in tutte le loro molteplici dimensioni».

Cos' altro occorre?

«È essenziale il coinvolgimento- oltre che delle istituzioni- del settore privato e industriale e, più in generale, della società civile, con l'obiettivo di garantire la stabilità della società e il suo sistema democratico, la continuità dei servizi essenziali per i cittadini, gli approvvigionamenti industriali,

il funzionamento delle infrastrutture critiche. Inoltre, le minacce ibride, per loro natura, sono caratterizzate da una dimensione transnazionale, che rende fondamentale il coordinamento internazionale e la cooperazione fra Paesi partner e alleati. L'Unione Europea, il G7, la NATO, le Nazioni Unite rimangono i principali punti di riferimento nell'ambito dei quali sviluppare strumenti adeguati. In primis, puntando ad alzare il "costo politico" di chi- attore statale o non statale- porta avanti campagne ibride. E farlo sempre insieme con i nostri partner, perché nella battaglia contro le minacce ibride la cooperazione internazionale ci offre strumenti dei quali da soli, altrimenti, non potremmo mai disporre. Su questo, la Farnesina è in prima linea».

Quanto è importante arrivare a regole internazionali condivise nel cyberspazio e quali sono i principali ostacoli alla costruzione di una governance digitale realmente globale?

«Delineare regole internazionali condivise nel cyberspazio è fondamentale per garantire la sicurezza nazionale e la tutela dei diritti umani, ma anche la stabilità economica, in un mondo in cui non c'è ambito dell'esperienza umana che sia rimasto estraneo alla digitalizzazione. Emerge, dunque, la necessità di trovare valori e standard condivisi per lo sviluppo di tecnologie umano-centriche. Sebbene si registrino importanti passi avanti multilaterali, la strada verso una governance realmente globale si scontra con ostacoli geopolitici, tecnici e ideologici».

Quali sono i più critici?

«Se sul fronte europeo e con i Paesi like-minded esiste un accordo di massima rispetto a tali principi di governance, occorre riconoscere che non tutti condividono la nostra visione. Agire senza essere vincolati da regole può consentire di guadagnare un vantaggio tecnologico, commerciale e strategico. Questo vale per tutte le nuove tecnologie dirompenti, dal cyber all'intelligenza artificiale al quantum. In breve, l'ostacolo principale alla costituzione di una governance globale è proprio la potenzialità di queste tecnologie, sono gli evidenti vantaggi comparati di cui godrà chi le dominerà per primo. Ciò detto, non bisogna essere troppo pessimisti: come si è riusciti a definire regole per l'uso dell'energia nucleare, creso sia possibile fare altrettanto anche per questi nuovi strumenti».

In uno scenario internazionale segnato da tensioni geopolitiche e competizione tecnologica, quale ruolo può giocare l'Italia nel promuovere un modello di cybersicurezza fondato su cooperazione, innovazione e tutela dei valori democratici?

«L'Italia è impegnata per promuovere uno spazio cibernetico aperto, libero, sicuro, accessibile. Convinti della forza del multi-



LE MINACCE IBRIDE, PER LORO NATURA, SONO CARATTERIZZATE DA UNA DIMENSIONE TRANSNAZIONALE, CHE RENDE FONDAMENTALE IL COORDINAMENTO INTERNAZIONALE E LA COOPERAZIONE FRA PAESI PARTNER E ALLEATI

lateralismo e del primato del diritto internazionale- anche in una fase in cui il rispetto del diritto sembra essere un dettaglio trascurabile- partecipiamo attivamente a molteplici iniziative di politica estera cibernetica, guardando non solo alle questioni di principio ma anche agli aspetti più concreti della collaborazione internazionale. Queste iniziative sono concepite per rispondere non solo alle sfide che minacciano la nostra sicurezza, ma anche all'esigenza di collaborazione fra Paesi dal comune sentire: penso, ad esempio, ai lavori in seno alla NATO, all'ONU, all'Unione Europea, all'OSCE, al G7 e ad altre coalizioni informali».

Tra queste iniziative qual è la più importante?

«Una di esse, che mi piace ricordare, è il Meccanismo di Tallinn: si tratta di una piat-

taforma internazionale per il coordinamento dei progetti di assistenza cyber civile all'Ucraina. L'Italia ne deterrà la presidenza da luglio a dicembre di quest'anno. Vista l'esperienza maturata in questo settore dagli Ucraini in questi anni, si tratta evidentemente di attività che consentono un arricchimento reciproco. Con lo stesso spirito sosteniamo, inoltre, progetti di costruzione delle capacità informatiche nei Paesi in via di sviluppo, in linea con l'approccio cooperativo promosso dal Piano Mattei. Quale che sia il fronte di impegno, è per noi prioritario stimolare il partenariato pubblico-privato, quale strumento vincente per lo scambio di informazioni, l'elaborazione di politiche settoriali e la realizzazione di progetti. Solo attraverso un gioco di squadra possiamo, infatti, posizionare in maniera

efficace l'Italia quale attore di primo piano nel campo della cybersicurezza». • **Lucrezia Antinori**

Alessandro De Pedys, a capo della Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica del Ministero degli Affari Esteri e della Cooperazione Internazionale



Nell'era della cyber resilience

Fabrizio Fiorini, ceo di 4Shiva, e Luca Savoldi, ceo di Abissi, analizzano l'evoluzione del rischio digitale tra la generativa, normative europee, resilienza industriale e continuità operativa nelle filiere produttive

Nel panorama economico e industriale contemporaneo, la cybersecurity non rappresenta più soltanto una questione tecnica legata alla protezione delle reti informatiche, ma un elemento strutturale della continuità operativa e della competitività aziendale. L'evoluzione dell'intelligenza artificiale, la diffusione dei sistemi connessi e l'integrazione tra infrastrutture digitali e processi fisici stanno ridefinendo il concetto stesso di rischio. In questo quadro si colloca l'esperienza di Abissi e 4Shiva, realtà specializzate nella cyber resilience, nella governance della sicurezza digitale e nei percorsi di adeguamento normativo per aziende e infrastrutture critiche.

Perché oggi non è più corretto parlare soltanto di cybersecurity ma di cyber resilience?

Fabrizio Fiorini: «Perché il concetto tradizionale di protezione non è più sufficiente. Per anni abbiamo immaginato la sicurezza informatica come una barriera perimetrale: firewall, antivirus e sistemi di difesa pensati per impedire l'accesso agli attaccanti. Oggi però il mondo digitale è completamente integrato con quello fisico. I software controllano automobili, impianti industriali, infrastrutture energetiche e dispositivi medicali. In questo contesto non possiamo più ragionare solo in termini di difesa, ma di capacità di continuare a operare anche mentre un attacco è in corso. Questa è la vera differenza tra cybersecurity e cyber resilience».

Uno dei temi più critici è quello dello "zero day clock". Perché rappresenta un cambio di paradigma così importante?

Luca Savoldi: «Perché il fattore tempo si sta azzerando. In passato passavano mesi tra la scoperta di una vulnerabilità e il suo sfruttamento su larga scala. Oggi possono bastare poche ore. Questo significa che le aziende non hanno più margine per processi decisionali lenti o per approcci burocratici. Quando emerge una vulnerabilità zero-day, il sistema deve reagire quasi automaticamente, isolando la minaccia e proteggendo le funzioni essenziali del business».

Quanto incide l'intelligenza artificiale in questa evoluzione?

F.F.: «Incide in modo enorme e con una doppia valenza. Da una parte l'intelligenza artificiale è diventata uno strumento potentissimo nelle mani degli attaccanti: automatizza la ricerca di vulnerabilità, genera malware sempre più sofisticati e rende gli attacchi di social engineering estremamente realistici. Dall'altra parte però è anche l'unico strumento realmente efficace per difendersi in



NEL SETTORE INDUSTRIALE LA CYBER RESILIENCE COINCIDE SEMPRE DI PIÙ CON LA SAFETY, CIOÈ CON LA PROTEZIONE CONCRETA DEI LAVORATORI, DEGLI IMPIANTI E DEI PROCESSI PRODUTTIVI

un ecosistema dove il volume e la velocità degli attacchi hanno superato le capacità umane di analisi. Oggi la sfida non è più tra hacker e sistemisti, ma tra algoritmi offensivi e algoritmi difensivi».

L'Europa sta rispondendo con normative molto stringenti come Cra e Nis2. Che impatto avranno sulle aziende?

L.S.: «Avranno un impatto enorme perché cambiano completamente il concetto di re-

sponsabilità. Il cyber resilience act introduce per la prima volta l'obbligo di progettare prodotti digitali sicuri by design e by default. Questo significa che i produttori saranno responsabili della gestione delle vulnerabilità per tutto il ciclo di vita del prodotto. Parallelamente, la Nis2 amplia il numero di aziende coinvolte negli obblighi di governance e gestione del rischio. La conformità normativa non sarà più soltanto un requisito ammini-

strativo, ma il passaporto necessario per operare nelle filiere internazionali».

Quindi la conformità diventa una leva competitiva?

F.F.: «Assolutamente sì. Oggi le grandi aziende e le infrastrutture critiche chiedono ai propri fornitori livelli di maturità cyber sempre più elevati. Essere resilienti significa essere affidabili. Non esserlo significa rappresentare un rischio per tutta la supply chain. Per questo la cybersecurity sta diventando un fattore competitivo, economico e reputazionale».

Quali sono oggi i settori più esposti?

L.S.: «Sicuramente automotive e industria manifatturiera avanzata. Un'automobile moderna contiene oltre cento milioni di righe di codice ed è di fatto un computer in movi-

LE ATTIVITÀ DI ABISSI E 4SHIVA

Affrontare i rischi cyber nel 2026 richiede un approccio multidisciplinare che vada ben oltre la sola competenza tecnica, integrando cybersecurity avanzata, automazione e AI-Aware Security, attività di threat intelligence e incident response, protezione degli ambienti Ot e IoT, metodologie DevSecOps, governance aziendale, gestione del rischio, conoscenza delle normative cogenti e volontarie, oltre a competenze organizzative e fattori umani. In uno scenario in cui le minacce evolvono con estrema rapidità, diventano fondamentali la formazione continua, l'aggiornamento costante e l'adozione di modelli "Zero Trust" orientati alla verifica permanente di utenti, dispositivi e processi. In questo contesto, realtà specializzate come Abissi e 4Shiva operano come partner strategici nei percorsi di resilienza e anti-fragilità digitale, supportando le imprese nell'analisi delle vulnerabilità, nella validazione di prodotti connessi e nei processi di adeguamento alle normative e agli standard internazionali. Le attività comprendono cybersecurity assessment, supporto al conseguimento delle certificazioni, implementazione e miglioramento continuo dei sistemi di gestione, oltre al monitoraggio dell'evoluzione delle minacce e dei requisiti normativi.

mento. Lo stesso vale per le fabbriche Industry 4.0, dove It e Ot sono ormai completamente integrati. Una vulnerabilità in un sensore o in un dispositivo connesso può provocare il fermo di una linea produttiva o addirittura compromettere la sicurezza fisica delle persone».

Quindi il rischio cyber non è più soltanto digitale?

F.F.: «Esatto. Oggi un attacco informatico può avere conseguenze fisiche dirette. Nel settore industriale la cyber resilience coincide sempre di più con la safety, cioè con la protezione concreta dei lavoratori, degli impianti e dei processi produttivi».

Sostenete che molte aziende abbiano ancora un problema di governance più che di tecnologia. Perché?

L.S.: «Perché oltre il 60 per cento degli attacchi sfrutta vulnerabilità già note e mai corrette. Questo significa che spesso le tecnologie esistono già, ma manca una gestione efficace dei processi, delle responsabilità e del monitoraggio continuo. La cybersecurity non può essere delegata solo all'ufficio It: deve diventare parte integrante della governance aziendale».

Quanto stanno diventando centrali oggi certificazioni e normative europee nella gestione del rischio digitale?

F.F.: «Oggi certificazioni e framework normativi non rappresentano più semplici strumenti formali, ma veri indicatori della maturità tecnologica e organizzativa di un'azienda. Standard internazionali come la Iso /Iec 27001:2022 attestano la presenza di un sistema strutturato per la gestione della protezione delle informazioni, garantendo controllo del rischio, continuità operativa e tutela dei dati. Parallelamente, normative come la Nis2 hanno introdotto obblighi molto più stringenti per settori critici e infrastrutture strategiche, attribuendo responsabilità dirette anche al management aziendale. Accanto a questi strumenti stanno emergendo nuovi riferimenti specifici per i diversi ambiti tecnologici e industriali. La Uni/PdR 174:2025, sviluppata con il supporto dell'Agenzia per la Cybersicurezza Nazio-

nale, facilita i percorsi di adeguamento alla Nis2, mentre il regolamento Dora impone al settore finanziario standard rigorosi di resilienza operativa digitale. Sul fronte dell'intelligenza artificiale, la Iso/Iec 42001:2023 rappresenta il primo standard internazionale dedicato alla governance responsabile dei sistemi Ia, introducendo principi di trasparenza, controllo ed etica applicata alle tecnologie intelligenti».

Anche il comparto automotive sta vivendo una trasformazione profonda?

L.S.: «Esattamente, con la Iso/Sae 21434, che definisce requisiti di protezione informatica lungo tutto il ciclo di vita del veicolo connesso. A questo si aggiunge il nuovo schema europeo Eucc, ormai diventato un riferimento strategico per la certificazione dei prodotti Ict all'interno del mercato europeo. Oggi, quindi, aderire a questi standard significa molto più che dimostrare conformità normativa: significa offrire garanzie concrete a clienti, partner e filiere internazionali sulla capacità dell'azienda di governare il rischio digitale in modo strutturato, continuo e credibile».

Che ruolo avranno gli standard internazionali nei prossimi anni?

F.F.: «Avranno un ruolo sempre più centrale. Le certificazioni non saranno più viste come un semplice bollino, ma come prova concreta della capacità di gestire il rischio cyber in modo strutturato».

Nel vostro approccio parlate anche di antifragilità. Cosa significa concretamente?

L.S.: «Significa superare l'idea impossibile dell'invulnerabilità. Nessun sistema potrà mai essere completamente immune agli attacchi. L'obiettivo reale è costruire organizzazioni capaci di imparare dagli stress e diventare più forti dopo ogni evento critico. Un sistema antifragile non si limita a resistere, ma evolve continuamente grazie alle informazioni raccolte dagli incidenti e dalle minacce».

In questo contesto, quanto sono importanti i partner strategici?

F.F.: «Sono fondamentali, perché oggi nes-



QUANDO EMERGE UNA VULNERABILITÀ ZERO-DAY, IL SISTEMA DEVE REAGIRE QUASI AUTOMATICAMENTE, ISOLANDO LA MINACCIA E PROTEGGERE LE FUNZIONI ESSENZIALI DEL BUSINESS

suna azienda può affrontare da sola un ecosistema di minacce così complesso. Servono competenze multidisciplinari che integrino cybersecurity, normativa, gestione del rischio, intelligenza artificiale e cultura organizzativa. Realtà come Abissi e 4Shiva lavorano proprio in questa direzione: non come semplici fornitori tecnici, ma come partner strategici nel percorso verso la resilienza e l'antifragilità».

Qual è l'errore più grande che oggi le aziende continuano a commettere?

L.S.: «Pensare che la sicurezza sia un obiettivo statico da raggiungere una volta sola. In realtà la cybersecurity è un processo continuo, in costante evoluzione. Le minacce cambiano ogni giorno, così come cambiano

le tecnologie e le normative. Senza un approccio dinamico, integrato e continuativo, qualsiasi sistema è destinato prima o poi a diventare vulnerabile».

In conclusione, quale sarà la vera sfida dei prossimi anni?

F.F.: «La vera sfida sarà costruire organizzazioni capaci di convivere con l'incertezza tecnologica. Il tempo tra vulnerabilità e attacco continuerà a ridursi, l'intelligenza artificiale renderà il contesto sempre più complesso e la convergenza tra mondo digitale e fisico aumenterà ulteriormente i rischi. Per questo la cyber resilience non sarà più una scelta tecnica, ma una condizione essenziale per la sopravvivenza e la competitività delle imprese». • **Cristiana Golfarelli**

Luca Savoldi, ceo di Abissi, e Fabrizio Fiorini, ceo di 4Shiva



CONFORMITÀ COME CRESCITA

L'obiettivo di Abissi e 4Shiva è trasformare la conformità normativa — dal Cra alla Nis2, fino agli standard Iso e Uni/PdR — in uno strumento concreto di innovazione, capace non solo di rafforzare i sistemi di prevenzione e protezione, ma anche di offrire evidenza tangibile dell'affidabilità organizzativa verso clienti, stakeholder e filiere produttive. Parallelamente, assume un ruolo centrale anche la diffusione di una cultura aziendale della resilienza, nella quale ogni persona sia consapevole del proprio ruolo nella protezione delle infrastrutture digitali e nella gestione del rischio informatico. Collaborare con partner come Abissi e 4Shiva significa affrontare la cyber resilience come un processo continuo di evoluzione e governance, consapevoli che la protezione digitale non è un traguardo definitivo ma un'attività costante che richiede competenze, aggiornamento e alleanze strategiche solide.

Nessuno si salva da solo

Il centro di competenza Cyber 4.0 svolge un ruolo decisivo: accompagnare le imprese nella comprensione dei propri bisogni, del proprio livello di maturità e dei rischi associati ai processi di trasformazione digitale. Interviene il presidente Paolo Spagnoletti

La sicurezza informatica non riguarda più soltanto la protezione dei dati, ma il funzionamento stesso di sistemi industriali, infrastrutture e tecnologie intelligenti sempre più interconnesse. L'avanzata di intelligenza artificiale, cloud e automazione sta infatti ampliando il perimetro dei rischi digitali, rendendo centrale la capacità di progettare ecosistemi tecnologici sicuri, affidabili e resilienti. «Oggi il problema - precisa il presidente di Cyber 4.0 Paolo Spagnoletti - non riguarda più soltanto la protezione del dato o delle infrastrutture It tradizionali. La trasformazione digitale sta portando intelligenza e connettività dentro oggetti fisici, processi industriali e catene di fornitura sempre più distribuite. Questo significa che ai rischi di security si aggiungono sempre più rischi di safety: una vulnerabilità non compromette solo informazioni, ma può influenzare il comportamento di sistemi autonomi, droni, robot o dispositivi intelligenti interconnessi. In questo scenario diventa essenziale governare l'intero ciclo di vita di prodotti e servizi digitali, perché la sicurezza non riguarda più soltanto la protezione dei sistemi, ma la capacità di garantire comportamenti affidabili e controllabili di tecnologie sempre più autonome e interconnesse».

In un contesto sempre più complesso e interconnesso, come si può costruire una digitalizzazione realmente sicura?

«Credo che il tema della security by design sia fondamentale, ma vada anche affrontato con grande concretezza. Abbiamo molto da imparare da settori come quello spaziale, dove progettare sistemi sicuri by design non è una scelta teorica ma una necessità: quando un satellite viene lanciato, intervenire successivamente è estremamente difficile. Per molti anni il digitale ha vissuto nell'idea implicita che fosse sempre possibile cor-



UNA DIGITALIZZAZIONE REALMENTE SICURA RICHIEDE CAPACITÀ PROGETTUALI, SIMULAZIONE, TESTING E UNA FORTE INTEGRAZIONE TRA COMPETENZE TECNOLOGICHE, CONOSCENZA DEI PROCESSI OPERATIVI E CAPACITÀ DI PROGETTARE SISTEMI AFFIDABILI IN CONTESTI CRITICI

reggere dopo. Oggi non è più così, soprattutto quando il software controlla infrastrutture, mobilità, energia o sistemi autonomi. Una digitalizzazione realmente sicura richiede quindi capacità progettuali, simulazione, testing e una forte integrazione tra competenze tecnologiche, conoscenza dei processi operativi e capacità di progettare sistemi affidabili in contesti critici».

Qual è il ruolo di Cyber 4.0 nel supportare le aziende italiane, in particolare le Pmi, nell'adozione di tecnologie sicure e nella crescita della resilienza digitale?

«Più che parlare di "adozione di tecnologie sicure", credo sia importante parlare della capacità di rendere sicure le tecnologie nei loro specifici contesti d'uso. È proprio qui che un centro di competenza come Cyber 4.0 può svolgere un ruolo decisivo: accompagnare le imprese nella comprensione dei propri bisogni, del proprio livello di maturità e dei rischi associati ai processi di trasformazione digitale. Questo significa trasferire conoscenza, facilitare l'accesso a competenze avanzate e creare connessioni tra università, imprese e territori. Per le Pmi, in particolare, è fondamentale poter contare su un ecosistema che le aiuti non solo a investire in innovazione, ma a farlo in modo sostenibile e

sicuro».

Formazione e competenze rappresentano una delle grandi sfide del settore cyber. Come si può colmare il gap di professionalità specializzate e preparare le nuove generazioni ai lavori della sicurezza digitale?

«Oggi la sicurezza digitale non è più un tema riservato agli informatici. Le tecnologie intelligenti stanno trasformando il lavoro, le imprese e le istituzioni, e questo richiede competenze capaci di unire tecnologia, management, diritto e più in generale scienze sociali. Con la crescente automazione, il ruolo dell'uomo sarà sempre più legato alla supervisione, al controllo e alla gestione dei rischi associati ai sistemi digitali. Allo stesso tempo, le normative europee stanno introducendo responsabilità sempre più rilevanti per organizzazioni e professionisti. Per questo è fondamentale formare figure in grado non solo di usare le tecnologie, ma anche di comprenderne gli impatti economici, organizzativi e sociali e di governarle in modo responsabile».

Intelligenza artificiale, cloud e automazione stanno cambiando profondamente il panorama tecnologico: ritiene che queste innovazioni aumenteranno soprattutto le

opportunità di difesa oppure i rischi legati agli attacchi informatici?

«Come spesso accade nelle grandi trasformazioni tecnologiche, aumenteranno entrambe le dimensioni. Le stesse tecnologie che possono rendere più sofisticati gli attacchi permettono anche di sviluppare capacità di prevenzione, rilevamento e risposta molto più avanzate. La vera sfida sarà la velocità con cui riusciremo a trasferire conoscenze e competenze tra settori diversi: tra ambito militare e civile, tra grandi imprese e Pmi, tra pubblico e privato. Oggi la sicurezza digitale dipende sempre più dalla capacità di mettere in relazione esperienze e competenze diverse, perché nessun attore può affrontare da solo la complessità dei nuovi scenari tecnologici». • **Linda Zorza**



Paolo Spagnoletti, docente alla Luiss e presidente Cyber 4.0

L'Internet of Things sta vivendo una nuova fase di trasformazione: non basta più innovare, oggi i dispositivi connessi devono garantire affidabilità, resilienza digitale e conformità normativa. In Europa, il Cyber Resilience Act, i nuovi requisiti cybersecurity introdotti dalla RED e gli standard En 18031 stanno ridefinendo gli standard del settore, imponendo alle aziende di integrare cybersecurity e requisiti normativi già nelle prime fasi di progettazione dei prodotti IoT.

È in questo contesto che si inserisce System Technology Innovations, realtà specializzata nello sviluppo, nella validazione e nell'analisi di sistemi embedded e dispositivi connessi. L'azienda nasce con una missione precisa: supportare le imprese nella transizione verso una nuova generazione di prodotti IoT progettati secondo criteri di sicurezza, sostenibilità tecnologica e conformità normativa.

L'approccio adottato da System Technology Innovations ruota attorno al concetto di "security by design", oggi considerato uno dei pilastri fondamentali dell'ingegneria dei sistemi connessi. La filosofia è semplice quanto strategica: integrare gli aspetti di cybersecurity sin dalle prime fasi di progettazione del prodotto, anziché intervenire successivamente per correggere vulnerabilità o criticità emerse durante la certificazione. Un modello che consente non solo di ridurre i rischi di sicurezza, ma anche di abbattere i costi di rilavorazione, accelerare i tempi di sviluppo e affrontare con maggiore efficienza i processi di certificazione richiesti dal mercato europeo. L'azienda opera su diversi ambiti tecnologici altamente specializzati: sistemi embedded Linux e RTOS, piattaforme cloud per monitoraggio, diagnostica remota e gestione dei dispositivi. Competenze che trovano applicazione soprattutto nei settori in cui affidabilità e continuità operativa rappresentano requisiti essenziali, come trasporti, industria e mobilità intelligente. Proprio la capacità di integrare competenze tecniche e aspetti normativi rappresenta uno degli elementi distintivi di System Technology Innovations.

Fabrizio Crudo, ceo di System Technology Innovations



Cybersecurity e normative IoT europee

System Technology Innovations sviluppa un nuovo modello per i dispositivi connessi integrando cybersecurity, validazione normativa, automazione e tecnologie intelligenti per industria, trasporti e mobilità del futuro



La cybersecurity non rappresenta più soltanto un requisito tecnico, ma un elemento strategico che coinvolge progettazione, governance aziendale, gestione del rischio e ciclo di vita del prodotto. Le nuove normative europee stanno imponendo alle aziende obblighi sempre più stringenti in termini di gestione del rischio, aggiornamenti di sicurezza, tracciabilità e documentazione tecnica. L'azienda supporta inoltre le imprese nella preparazione della documentazione tecnica, nella validazione dei requisiti cybersecurity e nell'automazione delle attività di test e raccolta evidenze. Particolare rilevanza assume la collaborazione con Elmec Elettronica, storica realtà specializzata nei sistemi tecnologici per il trasporto pubblico e la mobilità intelligente. La partnership è orientata allo sviluppo, alla sperimentazione e alla validazione di nuove soluzioni IoT dedicate al settore dei trasporti, con un focus specifico su router industriali, sistemi embedded di bordo, infrastrutture di monitoraggio remoto e piattafor-

me cloud per la gestione della mobilità intelligente. L'obiettivo della collaborazione non è soltanto quello di sviluppare nuovi prodotti, ma costruire un ecosistema tecnologico evoluto capace di integrare cybersecurity, monitoraggio remoto, diagnostica avanzata e gestione intelligente dei dati. La collaborazione con Elmec Elettronica rappresenta inoltre un importante laboratorio tecnologico per la sperimentazione di metodologie innovative legate alla validazione continua, all'automazione dei test e alla verifica della robustezza dei sistemi embedded e connessi.

me cloud per la gestione della mobilità intelligente. L'obiettivo della collaborazione non è soltanto quello di sviluppare nuovi prodotti, ma costruire un ecosistema tecnologico evoluto capace di integrare cybersecurity, monitoraggio remoto, diagnostica avanzata e gestione intelligente dei dati. La collaborazione con Elmec Elettronica rappresenta inoltre un importante laboratorio tecnologico per la sperimentazione di metodologie innovative legate alla validazione continua, all'automazione dei test e alla verifica della robustezza dei sistemi embedded e connessi.

La sinergia tra le due realtà ha portato allo sviluppo di un modello che consente alle aziende di affrontare la conformità normativa non più come una fase finale e separata del progetto, ma

L'APPROCCIO ADOTTATO DA SYSTEM TECHNOLOGY INNOVATIONS RUOTA ATTORNO AL CONCETTO DI "SECURITY BY DESIGN", OGGI CONSIDERATO UNO DEI PILASTRI FONDAMENTALI DELL'INGEGNERIA DEI SISTEMI CONNESSI

me cloud per la gestione della mobilità intelligente. L'obiettivo della collaborazione non è soltanto quello di sviluppare nuovi prodotti, ma costruire un ecosistema tecnologico evoluto capace di integrare cybersecurity, monitoraggio remoto, diagnostica avanzata e gestione intelligente dei dati. La collaborazione con Elmec Elettronica rappresenta inoltre un importante laboratorio tecnologico per la sperimentazione di metodologie innovative legate alla validazione continua, all'automazione dei test e alla verifica della robustezza dei sistemi embedded e connessi.

Accanto all'aspetto tecnologico emerge il tema

come parte integrante dell'intero ciclo di sviluppo del prodotto. L'obiettivo è ridurre criticità, anticipare eventuali problemi di certificazione e accelerare il time-to-market.

Parallelamente, System Technology Innovations sta investendo nello sviluppo di strumenti di supporto all'analisi documentale, alla verifica dei requisiti normativi e all'automazione delle attività di validazione cybersecurity. Le nuove piattaforme in fase di sviluppo puntano a supportare attività di validazione documentale, analisi dei requisiti e verifica preliminare della robustezza dei sistemi connessi.

• Gaia Santi

PROGETTI IN CORSO

System Technology Innovations guarda con crescente interesse allo sviluppo di dispositivi proprietari innovativi nei settori della mobilità intelligente, della nautica e delle infrastrutture energeticamente autonome. Tra i progetti attualmente in fase di sviluppo figurano soluzioni basate su pannelli solari, sistemi intelligenti di alimentazione e piattaforme di ricarica progettate per applicazioni outdoor, ambienti smart e infrastrutture ad alta efficienza energetica.

Si tratta di un'evoluzione che riflette una tendenza sempre più evidente nel mercato tecnologico europeo: l'integrazione tra sostenibilità energetica, connettività intelligente e cybersecurity.

Uscire dal cerchio ristretto degli specialisti

La cybersecurity sta diventando sempre più una professione di frontiera, dove tecnologia, diritto, economia e fattore umano si incontrano. Proprio per questo è, secondo Massimo Chirivì, una delle professioni più affascinanti e più necessarie per il futuro del nostro Paese

«La sicurezza informatica è una sfida centrale per il nostro tempo e il nostro impegno sarà quello di sostenere i professionisti del settore e promuovere una cultura della sicurezza digitale in tutta Italia». Ad assicurarlo è Massimo Chirivì, presidente AIPSI, Associazione Italiana Professionisti Sicurezza Informatica.

Quali sono oggi le priorità nella diffusione della cultura della sicurezza digitale nel Paese?

«La prima cosa da fare è cambiare proprio il modo in cui guardiamo alla sicurezza digitale. Per troppo tempo è stata considerata una faccenda tecnica, roba da informatici. Oggi non è più così: riguarda tutti, dal cittadino che usa lo smartphone al dirigente pubblico, dall'imprenditore al ragazzo delle scuole superiori. Le priorità concrete, dal mio punto di vista, sono tre. Anzitutto serve una formazione di base che arrivi davvero alle persone. La maggior parte degli attacchi che vanno a segno non sfruttano tecnologie sofisticate, ma la disattenzione di chi clicca su un link sbagliato o usa la stessa password ovunque. Phishing, credenziali deboli, leggerezza nella gestione dei dati personali: sono ancora questi i veri problemi».

E poi?

«Bisogna inserire la sicurezza digitale nei programmi scolastici e universitari in modo serio e strutturato, partendo già dalle medie e dalle superiori. C'è un equivoco da sfatare: il fatto che i ragazzi siano nati con uno smartphone in mano non significa affatto che sappiano usarlo in sicurezza. Anzi, spesso è vero il contrario. Su questo, come AIPSI, ab-

Massimo Chirivì presidente AIPSI, Associazione Italiana Professionisti Sicurezza Informatica



BISOGNA INSERIRE LA SICUREZZA DIGITALE NEI PROGRAMMI SCOLASTICI E UNIVERSITARI IN MODO SERIO E STRUTTURATO, PARTENDO GIÀ DALLE MEDIE E DALLE SUPERIORI

biamo voluto fare la nostra parte con un'iniziativa concreta: si chiama AIPSI School ed è un piano che mettiamo a disposizione di tutte le scuole italiane. In pratica, i nostri soci- che sono professionisti del settore- intervengono gratuitamente negli istituti per portare a studenti e insegnanti momenti di sensibilizzazione e formazione sulla sicurezza digitale. È il nostro modo di restituire al Paese una parte delle competenze che abbiamo, partendo da dove tutto comincia, cioè dai ragazzi. Infine, va rafforzata la collaborazione tra pubblico e privato. Quando ciascuno si difende da solo, perde. Servono scambio di informazioni sulle minacce, una regia nazionale chiara, e la consapevolezza che stiamo combattendo tutti la stessa battaglia».

Quali sono gli obiettivi principali di AIPSI?

«AIPSI è nata per dare voce e rappresentanza ai professionisti della sicurezza dell'informazione qui in Italia. La missione sta in poche parole: competenza, etica del mestiere, cultura della sicurezza. Siamo il capi-

tolo italiano di ISSA, e questo è un punto importante, perché ci consente di attingere a un patrimonio di esperienze che arriva da tutto il mondo e di calarlo nella nostra realtà, che ha caratteristiche sue, fatte di tante Pmi, di una pubblica amministrazione articolata, di un tessuto produttivo molto diversificato».

In che modo l'associazione intende supportare aziende, pubbliche amministrazioni e professionisti nel prossimo futuro?

«Per i prossimi anni stiamo lavorando su tre fronti. Il primo riguarda i professionisti del settore: vogliamo offrire loro spazi di aggiornamento, webinar, momenti di networking, occasioni in cui ci si possa parlare tra colleghi senza filtri commerciali. Sembra poco, ma in un mondo in cui ogni evento sembra finalizzato a vendere qualcosa, avere un luogo dove ci si confronta da pari a pari fa la differenza. Il secondo è il dialogo con le aziende e con la pubblica amministrazione. Abbiamo avviato diversi gruppi di lavoro tematici, dove i nostri soci mettono in comune competenze ed esperienze per produrre cose utili davvero; penso ad esempio a linee

guida operative pensate per chi deve affrontare la sicurezza nella pratica di tutti i giorni. L'attenzione, in particolare, è verso quelle organizzazioni che non hanno al loro interno strutture di sicurezza articolate, e che spesso si trovano sole davanti a problemi complessi. Il terzo fronte è la divulgazione. Convegni, webinar, tavoli di lavoro: tutto ciò che serve a far uscire la sicurezza dal cerchio ristretto degli specialisti. La nostra ambizione è essere un riferimento credibile, indipendente e- questo lo sottolineo- non commerciale. Vogliamo poter parlare con la stessa serietà al ciso di una grande azienda e al piccolo imprenditore che gestisce una manciata di dipendenti. Sono mondi diversi, ma le domande di fondo, in fin dei conti, si somigliano molto».

In un contesto caratterizzato da attacchi cyber sempre più sofisticati, quanto è importante investire nella formazione continua dei professionisti della sicurezza informatica?

«È una cosa da cui non si può prescindere. La sicurezza informatica ha questa particolarità, che credo non abbia uguali in altri settori: ciò che si è imparato due anni fa, oggi rischia già di essere superato, almeno in parte. Le tecniche di attacco corrono a una velocità che faticiamo a immaginare. Basta guardare cosa sta succedendo da quando

l'intelligenza artificiale generativa è diventata uno strumento alla portata di chiunque: campagne di phishing scritte in italiano perfetto, deepfake audio e video che ingannano anche persone preparate, malware che si auto-modificano per evitare i controlli. Cose che fino a poco tempo fa sembravano roba da film. In questo scenario, un professionista che smette di aggiornarsi non è semplicemente meno bravo: diventa, suo malgrado, un fattore di rischio per l'organizzazione in cui lavora. Per questo l'aggiornamento va vissuto come parte naturale del mestiere, non come qualcosa da ritagliare nei momenti liberi. Ed è qui che le associazioni come la nostra possono dare un contributo importante. Non tanto sostituendosi a chi fa formazione di mestiere, quanto creando comunità di pratica: ambienti dove i professionisti si parlano tra loro, raccontano cosa è successo davvero nelle proprie aziende, discutono di soluzioni che hanno funzionato e di altre che invece sono andate male. Spesso si impara molto di più da queste conversazioni che da un corso. Investire sulle persone resta l'investimento con il ritorno più alto in termini di sicurezza reale».

Le piccole e medie imprese italiane rappresentano spesso l'anello più vulnerabile dal punto di vista cyber. Quali consigli darebbe alle Pmi per migliorare la propria resilienza digitale senza affrontare costi insostenibili?

«Vorrei partire da un equivoco da chiarire subito: la sicurezza non è prima di tutto una questione di soldi, è una questione di metodo. Mi è capitato di vedere piccole aziende, con budget davvero modesti, proteggersi meglio di realtà molto più grandi e ben finanziate. Il motivo era semplice: avevano lavorato con ordine, definendo priorità chiare, invece di inseguire l'ultima novità presentata in fiera. Ai piccoli imprenditori darei quattro indicazioni pratiche».

Ovvero?

«La prima è capire cosa si possiede e cosa va davvero protetto. Dati dei clienti, know-how, sistemi gestionali, magari progetti che sono il cuore del valore aziendale. Sembra una banalità, ma molte Pmi questo esercizio



IN UNA PICCOLA AZIENDA OGNI DIPENDENTE, DALL'AMMINISTRATIVA AL MAGAZZINIERE, È DI FATTO UN PEZZO DEL SISTEMA DI DIFESA. SE NON LO SA, È ANCHE IL PRIMO PUNTO DEBOLE DA CUI PUÒ ENTRARE UN ATTACCO. PER QUESTO È NECESSARIA LA FORMAZIONE

non l'hanno mai fatto, e finiscono per difendere tutto allo stesso modo, cioè male. La seconda riguarda quella che chiamerei "igiene digitale". Sono comportamenti di base che, da soli, bloccano la stragrande maggioranza degli attacchi: tenere aggiornati sistemi e applicazioni, attivare l'autenticazione a più fattori dove è possibile, fare backup periodici e, soprattutto, verificarli ogni tanto, perché un backup mai testato non è un backup, è una speranza. E poi gestire bene chi può accedere a cosa: non tutti devono poter fare tutto. La terza è formare le persone. In una piccola azienda ogni dipendente, dall'amministrativa al magazziniere, è di fatto un pezzo del sistema di difesa. Se non lo sa, è anche il primo punto debole da cui può entrare un attacco».

Infine?

«La quarta è prepararsi a quando qualcosa andrà storto, perché purtroppo prima o poi succederà. Avere un piano minimo di risposta agli incidenti, sapere chi chiamare, dove sono i contatti utili, cosa fare nelle prime ore: la differenza tra un'azienda che reagisce con metodo e una che si fa prendere dal panico è enorme, anche in termini economici. Aggiungo una nota concreta. Oggi esistono strumenti messi a disposizione dall'ACN, l'Agenzia per la Cybersicurezza Nazionale, e da diverse iniziative europee, spesso gratuiti

o a costi davvero contenuti. Le Pmi dovrebbero conoscerli meglio e utilizzarli di più. E quando serve un aiuto specifico, il mio consiglio è di rivolgersi a un consulente competente per un intervento mirato, piuttosto che spendere soldi in soluzioni complesse che poi nessuno sarà in grado di gestire davvero».

In futuro quali saranno le principali minacce informatiche emergenti e come dovrà evolversi il ruolo dei professionisti della cybersecurity in Italia?

«Ci sono diversi fronti aperti che mi preoccupano, e che meritano attenzione fin da oggi. Il primo è quello dell'intelligenza artificiale, che è davvero un'arma a doppio taglio. Da una parte ci sta dando strumenti potentissimi per difenderci meglio, dall'altra mette nelle mani degli attaccanti capacità che fino a poco fa erano riservate a pochissimi. Mi riferisco a campagne di phishing personalizzate, costruite su misura sul singolo destinatario; a deepfake che ingannano anche professionisti esperti; a malware che si adatta da solo al sistema che sta attaccando. Poi c'è il tema quantistico, che a molti sembra ancora fantascienza, ma non lo è del tutto. Quando i computer quantistici raggiungeranno una potenza concretamente utilizzabile, una parte importante della crittografia che usiamo oggi smetterà di essere

sicura. Le organizzazioni dovrebbero iniziare a ragionarci adesso, perché certe transizioni richiedono anni di lavoro, non si improvvisano in poche settimane. Un terzo fronte critico è quello delle supply chain digitali. Sempre più spesso gli attaccanti non colpiscono direttamente l'obiettivo finale, ma arrivano attraverso un fornitore, un partner tecnologico, un software di terze parti che l'azienda utilizza ogni giorno senza pensarci. È un meccanismo subdolo, perché l'attacco entra da un canale che si considerava affidabile. E infine c'è il capitolo delle infrastrutture critiche e dei sistemi industriali. Qui un attacco non si traduce solo in dati rubati: può fermare una linea produttiva, bloccare un servizio essenziale, avere ricadute concrete sulla vita delle persone. Il livello di rischio è di un'altra natura».

Quali sono le sue conclusioni?

«In uno scenario del genere, il mestiere del professionista della cybersecurity sta cambiando in profondità. Le competenze tecniche restano importanti, ovviamente, ma da sole non bastano più. Servono persone che sappiano dialogare con il management, che riescano a tradurre il rischio in termini economici e normativi, che siano capaci di muoversi dentro la complessità crescente di normative come NIS2, Dora, AI Act. Serve insomma più visione d'insieme, più capacità di comunicare, più attitudine a stare in mezzo a discipline diverse. La cybersecurity sta diventando sempre più una professione di frontiera, dove tecnologia, diritto, economia e fattore umano si incontrano. E credo che proprio per questo sia oggi una delle professioni più affascinanti, e più necessarie, per il futuro del nostro Paese».

•Gaia Santi

Selezionare le giuste tecnologie

Massimo Fanton e Lorenzo Patron raccontano la visione di Brinthesis: un modello di open innovation pensato per aiutare le grandi imprese a integrare Ai, cloud, resilienza operativa e governance del rischio attraverso una cybersecurity concreta, modulare e misurabile

La cybersecurity oggi non è più soltanto una questione tecnologica. È una sfida di governance, resilienza e capacità decisionale. Le grandi organizzazioni si muovono in ecosistemi sempre più frammentati, dove cloud, Ai, supply chain, compliance e identità digitali si intrecciano in modo continuo. In questo contesto, il vero vantaggio competitivo non nasce dall'accumulare strumenti ma dalla capacità di scegliere le tecnologie giuste, integrarle con intelligenza e trasformarle in risultati concreti. È da questa visione che nasce Brinthesis, una realtà italiana guidata da Massimo Fanton e Lorenzo Patron, specializzata nella cybersecurity enterprise attraverso un approccio basato sull'open innovation.

Brinthesis si definisce “cacciatrice di idee innovative”. Cosa significa concretamente?

Massimo Fanton: «Significa che il nostro lavoro inizia molto prima della vendita di una tecnologia. Osserviamo costantemente l'evoluzione globale della cybersecurity, analizziamo startup, piattaforme emergenti e nuovi modelli operativi per individuare quelle innovazioni in grado di generare valore concreto per le grandi organizzazioni. Operiamo attraverso un modello di open innovation: dialoghiamo costantemente con aziende primarie, analisti, venture capital e sviluppatori di tecno-



Massimo Fanton e Lorenzo Patron, alla guida di Brinthesis

logie per selezionare soluzioni realmente efficaci. Il nostro obiettivo è consentire alle imprese di anticipare l'accesso a innovazioni realmente rilevanti per la cybersecurity enterprise, accelerandone l'adozione nei contesti operativi reali».

Oggi il mercato della cybersecurity è estremamente affollato. Dove si crea davvero valore?

Lorenzo Patron: «Il valore non nasce dall'aggiungere continuamente nuove piattaforme. Le grandi organizzazioni dispongono già di ecosistemi tecnologici estremamente complessi. Il punto non è sostituire ciò che esiste, ma rendere più efficace ciò che esiste già. Per questo non proponiamo piattaforme monolitiche, ma tecnologie specialistiche capaci di in-

tegrarsi con l'esistente e di rafforzare concretamente capacità operative, governance e visibilità».

Quali sono oggi le principali priorità dei ciso?

M.F.: «Direi tre. La prima è la riduzione del rischio reale. Oggi molte organizzazioni sono sommerse da alert, vulnerabilità ed esposizioni tecniche. Ma non tutto ha lo stesso impatto. Occorre capire quali percorsi di attacco possono realmente compromettere gli asset critici e concentrare lì le priorità. La seconda è la resilienza operativa. Gli ambienti cloud e ibridi evolvono continuamente: automazione, rilasci veloci, workload dinamici richiedono una sicurezza più contestuale e integrata nei processi operativi. La terza riguarda la prote-

zione dei nuovi domini critici: dati, Ai, software factory, supply chain, terze parti, identità digitali e rischio umano. Ambiti profondamente interconnessi che non possono più essere gestiti separatamente».

Avete scommesso sull'integrazione tra tecnologie diverse.

L.P.: «È fondamentale. Una cybersecurity efficace non può essere dispersiva. Ogni ambito può essere affrontato singolarmente, ma il valore aumenta quando i diversi moduli dialogano tra loro.

Integrare gli strumenti esistenti significa trasformare eventi tecnici in decisioni operative: ticket, Sla, responsabilità, workflow di remediation, evidenze per audit e compliance. È qui che la sicurezza smette di essere soltanto difesa tecnica e diventa governo operativo del rischio».

Dora e Nis2 stanno cambiando il modo di affrontare la sicurezza?

M.F.: «Assolutamente sì. Le nuove normative europee richiedono un approccio molto più profondo rispetto alla semplice adozione di controlli tecnologici. Servono governance continua, tracciabilità, gestione del rischio Ict, presidio dei fornitori e capacità dimostrabile di resilienza operativa. La compliance non può più essere trattata come un esercizio documentale separato dalla sicurezza. Deve diventare il risultato naturale di processi e controlli integrati nella gestione quotidiana del rischio digitale».

L'intelligenza artificiale è la nuova frontiera della cybersecurity?

L.P.: «L'Ai rappresenta una discontinuità enorme. Non è soltanto una nuova tecnologia da proteggere: cambia la superficie d'attacco, il modo in cui si sviluppa il software, la gestione del dato e persino la natura della frode digitale. Per questo riteniamo che la sicurezza dell'Ai debba essere affrontata lungo tre direttrici fondamentali: visibilità, protezione e validazione».

Ce le spiegate meglio?

M.F.: «La prima è la visibilità: le aziende devono sapere quali modelli, agenti Ai, datastore e pipeline siano realmente presenti, anche quando emergono fuori dai processi ufficiali, nel fenomeno della cosiddetta shadow Ai. La seconda è la protezione: servono controlli capaci di affrontare minacce nuove, che non si basano solo su vulnerabilità tecniche tradizionali, ma anche su manipolazione del linguaggio naturale, abuso degli agenti Ai ed esposizione dei dati. La terza è la validazione continua. I modelli Ai devono essere verificati costantemente in termini di robustezza, affidabilità, sicurezza e conformità lungo tutto il loro ciclo di vita». • **Guido Anselmi**



L'AI CAMBIA LA SUPERFICIE D'ATTACCO, IL MODO IN CUI SI SVILUPPA IL SOFTWARE, LA GESTIONE DEL DATO E PERSINO LA NATURA DELLA FRODE DIGITALE. LA SICUREZZA DELL'Ai VA AFFRONTATA LUNGO TRE DIRETTRICI FONDAMENTALI: VISIBILITÀ, PROTEZIONE E VALIDAZIONE

VISIONE, APPROCCIO, PORTFOLIO

La visione di Brinthesis si fonda su un modello di cybersecurity modulare best of breed, nel quale ogni soluzione opera come componente specializzato, contribuendo al tempo stesso a una postura di sicurezza più solida e coerente attraverso integrazione, governance e visibilità condivisa.

L'approccio di open innovation consente di evolvere continuamente il portfolio con tecnologie selezionate, complementari e ad alto valore aggiunto, rendendo l'innovazione concretamente adottabile anche nei contesti enterprise più complessi e soggetti a requisiti regolamentari sempre più stringenti.

Il portfolio copre in modo integrato i principali domini della cybersecurity enterprise moderna, supportando programmi end-to-end orientati al controllo, alla prioritizzazione e alla riduzione del rischio digitale.

Pronti per il bis

Tra intelligenza artificiale, semplificazione amministrativa e competenze digitali: la visione del direttore generale dell'AgID Mario Nobile nel nuovo mandato che segna la sua conferma fino al 2029

La conferma di Mario Nobile alla guida dell'AgID fino al 2029 segna un passaggio inedito nella storia dell'innovazione pubblica italiana. Per la prima volta, il direttore generale dell'Agenzia viene confermato per un secondo mandato triennale, in un contesto in cui la trasformazione digitale della Pubblica amministrazione diventa sempre più centrale nell'agenda del Paese. Sotto la sua guida, e nel quadro della strategia digitale promossa dal governo con il supporto del sottosegretario all'Innovazione Alessio Butti, la Pa ha iniziato a sperimentare l'intelligenza artificiale come leva per migliorare servizi e processi. Restano però aperte sfide strutturali importanti: dalla complessità burocratica ai tempi ancora lunghi per procedure chiave come l'apertura di un'impresa.

La sua conferma fino al 2029 rappresenta un caso unico nella storia di AgID. Qual è la priorità assoluta del suo secondo mandato per accelerare davvero la trasformazione digitale dell'Italia?

«La priorità indicata dal sottosegretario Alessio Butti è chiara: in questi anni abbiamo realizzato e consolidato importanti infrastrutture come le piattaforme abilitanti (Spid, Cie, PagoPA, l'app Io, Anpr, Psn, Pdnd), la migrazione al cloud e l'interoperabilità tra i sistemi. Adesso bisogna evolvere creando un ecosistema in grado di farle funzionare insieme in modo coerente, assicurando la piena interoperabilità tra le banche dati, accelerando sull'adozione dell'IT Wallet, lavorando sulla qualità del dato come asset strategico e accompagnando le amministrazioni nella governance dell'intelligenza artificiale».

Sotto la sua guida e con la strategia promossa da Alessio Butti, la Pubblica amministrazione ha iniziato a sperimentare l'intelligenza artificiale. In quali ambiti concreti l'ia può migliorare entro pochi anni la vita quotidiana di cittadini e imprese?

«Il primo e più immediato ambito è quello che riguarda l'assistenza e il supporto ai cittadini e alle imprese, e la semplificazione dei processi amministrativi. Oggi un cittadino- ma anche un'impresa- che vuole accedere a un servizio o completare un adempimento amministrativo si trova spesso di fronte a procedure che richiedono tempi lunghi e conoscenze burocratiche. Sistemi di ia ben progettati possono fungere da intermediari intelligenti, guidando il cittadino anche in modo proattivo, traducendo il linguaggio burocratico in istruzioni comprensibili, riducendo gli errori nelle domande e quindi i tempi di lavorazione. Questo è già tecnicamente possibile e alcune amministrazioni stanno già sperimentando in questa direzione. Per non parlare della capacità di questi sistemi, ormai consolidata, di parlare tutte le lingue del mondo. Un altro ambito nel



DALL'ANALISI PREDITTIVA PER LA GESTIONE DELLE LISTE D'ATTESA ALLA LETTURA ASSISTITA DI IMMAGINI DIAGNOSTICHE, L'IA PUÒ ALLEVIARE IL CARICO DI LAVORO DEL PERSONALE SANITARIO E AMMINISTRATIVO, DISTRIBUIRE IN MODO PIÙ EFFICIENTE LE RISORSE DISPONIBILI E MIGLIORARE LA TEMPESTIVITÀ DELLE DIAGNOSI

quale l'ia può avere un forte impatto è quello della sanità pubblica: dall'analisi predittiva per la gestione delle liste d'attesa alla lettura assistita di immagini diagnostiche, l'ia può alleviare il carico di lavoro del personale sanitario e amministrativo, distribuire in modo più efficiente le risorse disponibili e migliorare la tempestività delle diagnosi».

Molti imprenditori lamentano ancora tempi lunghi e procedure burocratiche complesse, ad esempio per l'apertura di una nuova impresa. Quali ostacoli frenano oggi la piena digitalizzazione della Pa e cosa serve per superarli definitivamente?

«Il problema principale è che spesso la digitalizzazione si ferma alla superficie: si è digitalizzato il punto di contatto con il cittadino o l'impresa, senza però mettere in discussione i processi interni alle amministrazioni. In realtà, digitalizzare significa prima di tutto semplificare i processi, eliminando passaggi inutili e riducendo la complessità, non limitarsi a trasferire online procedure pensate per il cartaceo. E questo è ancora più vero se applichiamo le tecnologie emergenti, come la Agentic AI. Il primo ostacolo è, quindi, culturale. Un altro ostacolo è rappresentato dalla frammentazione: l'Italia ha oltre 20.000 enti pubblici, ciascuno con i propri sistemi, i propri processi, spesso i propri applicativi sviluppati

negli anni in modo disomogeneo. Raggiungere la piena interoperabilità in questo contesto è un lavoro enorme, che richiede non solo tecnologia ma anche capacità di coordinamento. Infine, c'è un problema di tipo normativo. Ci sono norme che impongono adempimenti ridondanti, vincoli procedurali pensati per un mondo cartaceo che sopravvivono nell'era digitale».

L'Italia ha spesso mostrato eccellenze tecnologiche ma difficoltà nell'esecuzione su larga scala. Come immagina il futuro digitale del Paese nel 2030 e quali risultati misurabili vorrebbe lasciare come eredità del suo mandato?

«I risultati che considero davvero importanti sono la riduzione dei tempi burocratici, la crescita dell'utilizzo dei servizi digitali, una maggiore interoperabilità tra amministrazioni, la diminuzione dei costi amministrativi per le imprese e un aumento delle competenze e della fiducia dei cittadini nei confronti dello Stato digitale. I risultati vanno misurati sui numeri della infrastruttura digitale pubblica, che crescono in maniera evidente: più di 40 milioni di identità digitali, più di 17 milioni di caselle Pec, più di 35 milioni di certificati di firma digitale».

La trasformazione digitale richiede non solo infrastrutture e piattaforme, ma anche competenze. Come può l'Italia colmare il di-

vario digitale nella Pubblica Amministrazione e tra i cittadini, evitando che innovazioni come l'intelligenza artificiale aumentino le disuguaglianze?

«Nessuna trasformazione digitale può funzionare senza persone preparate ad accompagnare il cambiamento. In Italia, solo una persona su due ha competenze digitali di base e il numero di laureati in Ict è ancora troppo basso. L'intelligenza artificiale non aumenterà le disuguaglianze se sapremo costruire un ecosistema in cui tutti abbiano gli strumenti per parteciparvi. Non in modo eguale- non serve trasformare ogni dipendente in un programmatore- ma in modo equo: garantendo a ognuno una base di accesso, di comprensione, di tutela. Su questo abbiamo appena stipulato un accordo con la Crui, la Conferenza dei rettori delle Università italiane, proprio per dispiegare su tutto il territorio nazionale azioni di formazione e addestramento». •Gloria Martini



Mario Nobile, direttore generale AgID

Un acceleratore di business

Zerobyte offre un approccio integrato alla trasformazione digitale che unisce infrastrutture It, cybersecurity, software e marketing per supportare la crescita e la continuità operativa delle imprese

La capacità di governare sistemi informativi complessi, proteggere i dati e integrare soluzioni digitali non rappresenta più un vantaggio competitivo opzionale, ma un requisito essenziale per la sopravvivenza e la crescita nel mercato contemporaneo. Aspetto ben chiaro a Zerobyte, realtà che interpreta il digitale non come un insieme di strumenti isolati, ma come un ecosistema integrato in grado di accompagnare le aziende lungo tutte le fasi della loro evoluzione tecnologica.

Con sede a Veduggio, in provincia di Treviso, l'azienda si propone come partner strategico per imprese e studi professionali, adottando un approccio che supera il concetto tradizionale di fornitura It. L'obiettivo dichiarato è quello di rendere la tecnologia un acceleratore di business, attraverso un modello strutturato e multidisciplinare che unisce consulenza, infrastruttura, sicurezza e comunicazione.

La sicurezza informatica rappresenta uno dei pilastri fondamentali dell'offerta, in un contesto in cui le minacce cyber sono sempre più sofisticate e pervasive. L'azienda promuove una visione della cybersecurity come investimento strategico e non come semplice voce di costo, ponendo l'accento sulla necessità di proteggere la continuità operativa oltre che i dati sensibili.

Per Zerobyte la sicurezza informatica non può più essere considerata un elemento accessorio dell'infrastruttura It, ma deve essere integrata fin dall'inizio nei processi aziendali come componente strutturale del business. Una protezione efficace dei sistemi passa necessariamente attraverso la comprensione della triade fondamentale della sicurezza: confidenzialità, integrità e disponibilità dei dati.

La confidenzialità garantisce che le informazioni siano accessibili esclusivamente agli utenti autorizzati, evitando qualsiasi



La sede di Zerobyte

forma di esposizione non controllata dei dati sensibili. L'integrità assicura che le informazioni aziendali non vengano alterate in modo non autorizzato, mantenendo coerenza e affidabilità nel tempo. La disponibilità, infine, rappresenta la capacità dei sistemi di essere sempre operativi e accessibili quando l'azienda ne ha bisogno, perché anche pochi minuti di fermo possono tradursi in perdite operative significative e impatti economici rilevanti. L'approccio adottato è fortemente orientato alla prevenzione, con strumenti che permettono di individuare le vulnerabilità prima che possano essere sfruttate. Tra questi si colloca il security check, un'analisi tecnica approfondita che consente di monitorare infrastrutture, reti e dispositivi attraverso un'osservazione prolungata nel tempo. Il sistema consente di individuare criticità legate a configurazioni errate, password deboli o falle nei sistemi, resti-

LA SICUREZZA INFORMATICA NON PUÒ PIÙ ESSERE CONSIDERATA UN ELEMENTO ACCESSORIO DELL'INFRASTRUTTURA IT, MA DEVE ESSERE INTEGRATA FIN DALL'INIZIO NEI PROCESSI AZIENDALI COME COMPONENTE STRUTTURALE DEL BUSINESS

tuendo una fotografia completa dello stato di sicurezza dell'infrastruttura aziendale. La fase di analisi iniziale rappresenta un momento cruciale perché permette di trasformare la percezione del rischio in dati concreti e misurabili. Attraverso il security check è possibile osservare il comportamento reale della rete aziendale in condizioni operative quotidiane, senza interventi invasivi, e costruire successivamente un piano di miglioramento mirato che tenga conto delle priorità di sicurezza e delle esigenze organizzative del cliente. Questo approccio consente di passare da una gestione reattiva del rischio a una strategia proattiva, in cui la prevenzione diventa il vero elemento distintivo. Sul piano tecnologico, la protezione viene realizzata attraverso soluzioni integrate e partnership con player consolidati del settore, come Bitdefender per la sicurezza degli endpoint e Timenet per la connettività. L'integrazione con i servizi di rete consente di implementare sistemi di difesa che agiscono anche a livello infrastrutturale, bloccando minacce e traffico malevolo prima che raggiungano i sistemi aziendali.

Un ulteriore elemento distintivo è rappre-

sentato dal modello Msp (managed service provider), che si traduce nel servizio "Sorveglianza & Agisco". In questo caso, la gestione It non è più episodica ma continua, con un monitoraggio costante delle infrastrutture e interventi tempestivi in caso di anomalie o vulnerabilità. "La gestione continuativa dei sistemi informatici rappresenta oggi una necessità imprescindibile per le piccole e medie imprese che non dispongono di un reparto It interno strutturato: attraverso il modello Msp, l'azienda diventa un'estensione del team interno del cliente, garantendo presidio costante, aggiornamenti regolari, backup strutturati e piani di disaster recovery che consentono di ridurre drasticamente i tempi di inattività e di proteggere il patrimonio informativo aziendale in modo sistemico e affidabile.

Infine, grande attenzione viene riservata al fattore umano, riconosciuto come uno degli elementi più critici nella catena della sicurezza informatica. Per questo Zerobyte integra percorsi di formazione specifici per sensibilizzare dipendenti e collaboratori sui rischi legati a phishing, social engineering e comportamenti non sicuri. •

Beatrice Guarnieri

QUATTRO BUSINESS UNIT

La proposta di Zerobyte si basa su quattro business unit integrate - sicurezza informatica, soluzioni It, sviluppo software e comunicazione e marketing - che coprono l'intero ciclo di vita digitale dell'impresa. Questo modello consente di affrontare in modo strutturato le esigenze aziendali, trasformando la complessità tecnologica in un percorso chiaro e progressivo. Le attività guidano il cliente dalla costruzione dell'infrastruttura alla crescita del brand, passando per la gestione e la protezione dei processi. In particolare, la fase di sviluppo riguarda le fondamentali tecnologiche, mentre quella di gestione si concentra sull'ottimizzazione dei processi aziendali tramite sistemi Erp e soluzioni digitali integrate.

sorveglio & agisco

La soluzione MSP di Zerobyte

Sicurezza Aziendale H24 il reparto IT che non dorme mai

Sorveglio

identifica
il problema H24



Agisco

lo risolve
da remoto
o in sede

- **Monitoraggio:** Controllo continuativo 24/7
- **Aggiornamenti:** Software sempre performanti ed aggiornati
- **Business Continuity:** Continuità operativa garantita
- **Sicurezza:** Massima protezione della tua infrastruttura IT

Chiedi una consulenza gratuita

Zerobyte S.r.l.

Via Vicenza 32, 31050 Veduggio (TV) | Tel. 0423 723001 | www.zerobytesrl.it
assistenza@zerobytesrl.it | commerciale@zerobytesrl.it

Nis2, Privacy e Ai

Con Andrea Paro, ceo di Gemini Consult, scopriamo la nuova frontiera della governance digitale, tra compliance normativa, soluzioni innovative per la protezione dei dati e la gestione del rischio digitale

L'entrata in vigore della direttiva Nis2, l'evoluzione delle normative europee sulla privacy e l'impatto crescente dell'intelligenza artificiale stanno imponendo a enti pubblici e imprese nuovi standard di governance, sicurezza e accountability. In questo contesto di profonda evoluzione normativa e tecnologica si inserisce il lavoro di Gemini Consult, realtà specializzata nella consulenza in materia di protezione dei dati personali, governance It e cybersecurity, guidata da Andrea Paro, consulente privacy certificato Tüv (CDP_26), European Privacy Expert ISDP 10003:2020, ANIP Professional Partner Liv. 5 (Cod. 2685) e componente di Federprivacy e AssoPrivacy.

Con una lunga esperienza maturata sia nel settore pubblico che in quello privato, Paro guida oggi un team composto da professionisti altamente qualificati e certificati. L'attività di consulenza si concentra soprattutto sui temi della governance It, della cybersecurity e dell'adeguamento normativo connesso al D.Lgs 138/2024, noto come Nis2.

«Da anni Gemini Consult opera nel settore della compliance normativa attraverso un approccio fondato su metodologie strutturate e standard internazionali. La società ha sviluppato un sistema proprietario di valutazione del rischio costruito sulle normative applicabili e sui principali framework di riferimento, con l'obiettivo di ridurre al minimo la discrezionalità nelle analisi e nei processi decisionali. Il nostro obiettivo è sempre stato quello di rendere la valutazione del rischio il più possibile oggettiva, ancorandola a standard riconosciuti e a riferimenti normativi precisi» spiega Andrea Paro.

Anche nelle ultime settimane il settore è stato interessato da importanti novità regolamentari. L'Agenzia per la Cybersicurezza Nazionale ha infatti emanato le Determine 127437 del 14 aprile 2026 e 155238 del 20 aprile 2026, introducendo nuovi obblighi per i soggetti



Gemini Consult è specializzata nella consulenza in materia di protezione dei dati personali, governance It e cybersecurity

Nis2, tra cui il censimento dei "fornitori rilevanti" e la caratterizzazione delle aree e dei servizi aziendali.

«Dopo l'emanazione delle Determine ACN siamo stati letteralmente sommersi da richieste di supporto da parte dei clienti, chiamati a rispettare scadenze molto ravvicinate come il caricamento dei fornitori rilevanti entro il 31 maggio 2026 e delle valutazioni d'impatto entro il 30 giugno» racconta Paro.

L'esperienza accumulata nel settore rappresenta uno dei punti di forza della società. Gemini Consult lavora infatti in ambito Nis fin dal 2016, periodo di introduzione della cosiddetta Nis1, sviluppando know-how specifico nella gestione di realtà complesse e strategiche. «L'esperienza maturata con soggetti appartenenti al perimetro Nis1 ci ha consentito di trasferire metodologie e competenze ai

IL NOSTRO SISTEMA CONSENTE DI MISURARE IL RISCHIO SISTEMICO IN MODO DOCUMENTABILE E OPPOIBILE ANCHE IN SEDE GIUDIZIALE, EVITANDO APPROCCI AUTOREFERENZIALI O VALUTAZIONI BASATE ESCLUSIVAMENTE SU SOFTWARE COMMERCIALI

soggetti Nis2, integrando aspetti tecnico-organizzativi con oltre trent'anni di esperienza diretta nel settore It e della sicurezza», sottolinea Andrea Paro.

L'attività del gruppo spazia oggi dalla governance It alle certificazioni Iso/lec 27001, 27017, 27018 e 20000, includendo anche sistemi di qualità Iso 9001 e modelli di Business Continuity Management.

Le consulenze coinvolgono una vasta gamma di settori, dal comparto pubblico alle grandi realtà private. Tra i clienti figurano multiutility, comuni, istituti scolastici, aziende della grande distribuzione, compagnie aeree, multinazionali produttive, cooperative di servizi alla persona, strutture sanitarie e società di servizi. Particolare attenzione viene oggi dedicata anche alle implicazioni normative dell'intelligenza artificiale. Gemini Consult ha infatti elaborato ed accresciuto nel corso del tempo, in collaborazione con lo studio legale Soffientini di Arezzo, un tool dedicato alla valutazione del rischio Ai e alla predisposizione delle Valutazioni d'Impatto (DPIA) richieste sia ai provider sia ai deployer di sistemi di intelligenza artificiale.

«Abbiamo realizzato uno strumento che consente alle organizzazioni di effettuare in modo guidato l'autovalutazione del rischio derivante dai trattamenti Ai, integrando la documentazione tecnica e i regolamenti aziendali

necessari per garantire l'accountability. Il sistema nasce dall'evoluzione di un modello multi-norma sviluppato nel corso degli ultimi quindici anni e oggi in grado di integrare simultaneamente framework e normative differenti, tra cui Nis2, Nist, Gdpr, Iso 27001, Iso 27701, AgID e Whistleblowing. Alla base del modello vi è il Framework Nazionale di Cybersecurity e Data Protection, sviluppato dall'Università La Sapienza di Roma e adottato negli anni come riferimento nazionale. Il nostro sistema consente di misurare il rischio sistemico in modo documentabile e opponibile anche in sede giudiziale, evitando approcci autoreferenziali o valutazioni basate esclusivamente su software commerciali e su questo basare le strategie di compliance da sviluppare poi nell'Organizzazione» precisa Andrea Paro.

Tra gli strumenti adottati dalla società figurano inoltre il Modello Organizzativo Privacy (Mop) e il Modello Organizzativo Nis (Monis), sviluppati internamente in collaborazione con l'avvocato Marco Soffientini e costantemente aggiornati in base all'evoluzione normativa.

«Il vantaggio di sviluppare internamente i modelli organizzativi è la possibilità di adattarli in maniera sartoriale alle esigenze operative e legali dei clienti, assumendoci pienamente la responsabilità del prodotto che proponiamo» conclude Paro. • **Beatrice Guarnieri**

LA CULTURA DELLA PROTEZIONE DEI DATI

A distinguere Gemini Consult è anche una visione che mette al centro la persona, oltre alla competenza tecnica e normativa. Il gruppo partecipa attivamente a realtà professionali come Federprivacy, ANIP, Assoprivacy e Osservatorio679, contribuendo alla diffusione di una cultura della protezione dei dati fondata non soltanto sulla compliance, ma anche sulla tutela concreta della dignità, dei diritti e del valore della persona. Un approccio che si riflette anche nel rapporto quotidiano con collaboratori, clienti e fornitori, attraverso una gestione improntata alla trasparenza, alla responsabilità e alla condivisione delle competenze. La convinzione alla base dell'attività del gruppo è che la protezione delle informazioni non rappresenti soltanto un obbligo normativo o tecnologico, ma un elemento essenziale di fiducia e sostenibilità organizzativa.

*Dal 1919,
Passione Italiana,
Tratto Distintivo.*



*Since 1919,
Italian Passion,
Sign of Distinction.*

*Nel cuore e nelle mani
degli italiani dal 1919.*

DAL 1919 FACCIAMO LE COSE ALLO STESSO MODO, CON LA STESSA IMMUTATA PASSIONE. OGGETTI SENZA TEMPO, BELLI E CONCRETI, COME SOLO NOI ITALIANI SAPPIAMO CREARE. DA OLTRE 100 ANNI, NON SCENDIAMO MAI A COMPROMESSI, SULLA QUALITÀ DEI MATERIALI E SULLE TECNICHE DI LAVORAZIONE. ORGOGLIOSI DI CONTINUARE A SCRIVERE, CON IL MEDESIMO CARATTERE AUTENTICO E APPASSIONATO, LA STORIA DELLO STILE ITALIANO.

Aurora S.r.l - Strada Abbazia di Stura, 200 - 10156 Torino



aurorapenofficial



aurorapenofficial

www.aurorapen.it



aurorapen



AuroraPen

La nuova frontiera delle prove investigative

«Oggi più che mai servono prove, non sospetti»: il titolare dell'Agenzia Investigativa Alpha spiega come tecnologia, analisi forense e rigore legale stiano trasformando la professione dell'investigatore privato

Oggi l'investigazione privata non si limita più all'osservazione sul campo o ai tradizionali servizi di pedinamento e osservazione: è una disciplina multidimensionale che integra analisi forense, intelligence digitale, raccolta documentale e metodologie operative capaci di trasformare indizi frammentari in elementi probatori concreti. La figura dell'Investigatore Privato assume un ruolo sempre più strategico. «Dalla tutela patrimoniale alle indagini aziendali, fino ai delicati procedimenti familiari, il valore di un'attività investigativa si misura oggi nella precisione tecnica, nella legittimità delle procedure e nella capacità di produrre documentazione affidabile» spiega Ennio Tesone, titolare dell'Agenzia Investigativa Alpha, realtà operativa con sedi in diverse città italiane (Salerno, Potenza, Roma) e specializzata in investigazioni private, aziendali, difensive, assicurative e nelle indagini forensi.

Come nasce la vostra realtà professionale e con quale impostazione operativa?

«L'Agenzia Investigativa Alpha nasce dall'idea di costruire una struttura altamente professionale, capace di coniugare esperienza investigativa, innovazione tecnologica e rigore metodologico. Fin dall'inizio abbiamo scelto di operare secondo standard elevati, rivolgendoci sia ai privati al mondo aziendale e in quello legale. Negli anni abbiamo sviluppato una rete operativa strutturata, composta da agenti / collaboratori qualificati e costantemente aggiornati, con l'obiettivo di offrire servizi fondati su tre pilastri fondamentali: riservatezza assoluta, legalità delle procedure e attendibilità probatoria. Oggi chi si rivolge



a un investigatore privato - autorizzato non cerca semplicemente informazioni, ma elementi concreti su cui poter prendere decisioni importanti, spesso anche in sede giudiziaria».

Quali sono oggi le richieste più frequenti che arrivano da parte dei clienti privati?

«L'ambito privato continua a rappresentare una parte significativa del nostro lavoro, ma le esigenze sono profondamente cambiate rispetto al passato. Non si tratta soltanto di accertare una presunta infedeltà coniugale: molto spesso interveniamo in situazioni familiari delicate, dove è necessario raccogliere prove documentate per procedimenti di separazione, affidamento dei minori o revisione assegni di mantenimento delle condizioni economiche

stabilite dal giudice. Ci occupiamo inoltre di indagini pre e post matrimoniali, controllo dei minori, stalking, rintraccio di persone scomparse e verifica di comportamenti potenzialmente lesivi della sicurezza familiare. In tutti questi casi il nostro compito non è alimentare sospetti ma verificare i fatti attraverso attività investigative lecite e tecnicamente fondate».

Le aziende sembrano ricorrere sempre più spesso alle investigazioni private. Per quali motivi?

«Perché oggi il rischio aziendale non riguarda soltanto gli aspetti economici, ma anche quelli reputazionali e organizzativi. Sempre più imprese si rivolgono a noi per affrontare problematiche legate ad assenteismo strategico, falsa malattia, abuso dei permessi previsti dalla Legge 104/92, concorrenza sleale o comportamenti infedeli da parte di dipendenti e soci. Le investigazioni aziendali richiedono competenze molto specifiche, soprattutto perché ogni attività deve essere svolta nel pieno rispetto della normativa sul lavoro e della privacy. Una prova raccolta correttamente può fare la differenza in un contenzioso disciplinare o civile; al contrario, un'attività improvvisata rischia di compromettere l'intero procedimento».

Quanto conta la tecnologia nel vostro lavoro quotidiano?

«La tecnologia è diventata una componente essenziale dell'investigazione moderna. Oggi molte informazioni transitano attraverso dispositivi digitali, piattaforme online e sistemi di comunicazione avanzati. Per questo utiliz-

ziamo strumenti e attrezzature evolute di analisi informatica, attività di digital intelligence, tecniche Osint (Open Source Intelligence) e metodologie di acquisizione documentale che consentono di ricostruire dinamiche e comportamenti con elevata precisione».

Qual è il vostro metodo operativo quando prendete in carico un nuovo caso?

«Ogni indagine richiede un approccio personalizzato e riservato. La prima fase è sempre quella dell'analisi preliminare: ascoltiamo il cliente, studiamo il contesto e definiamo gli obiettivi investigativi. Successivamente, elaboriamo una strategia operativa calibrata sul caso specifico, integrando attività sul territorio, strumenti tecnologici e raccolta documentale. L'ultimo passaggio, spesso sottovalutato ma fondamentale, riguarda la produzione del report investigativo finale. La qualità della relazione conclusiva è determinante, perché rappresenta la sintesi tecnica dell'intera attività svolta corredata di foto e il principale supporto documentale per il cliente o per il legale incaricato».

La figura dell'investigatore privato è molto diversa rispetto all'immaginario tradizionale. Come è cambiata negli anni?

«Profondamente. L'investigatore moderno è un professionista specializzato che lavora all'interno di un sistema complesso, spesso in collaborazione con avvocati, consulenti tecnici e aziende. Il nostro ruolo consiste nel trasformare situazioni poco chiare in elementi oggettivi, verificabili e documentabili. In una società in cui le informazioni sono tante ma spesso confuse o manipolabili, il valore dell'accertamento professionale diventa fondamentale». •Gaia Santi

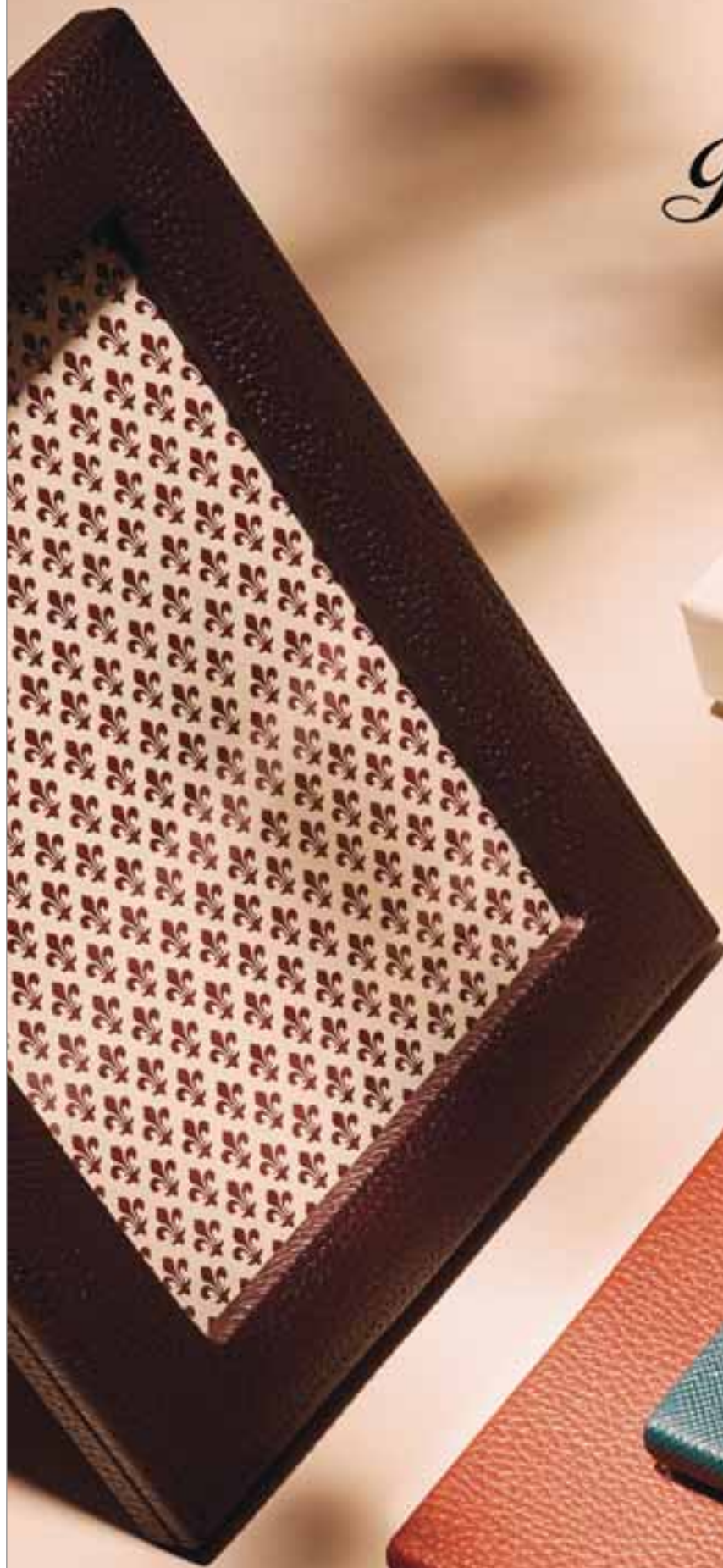
Ennio Tesone, titolare di Alpha Investigazioni



IL VALORE LEGALE DELLE PROVE

La missione dell'Agenzia Investigativa Alpha è fornire strumenti concreti per la tutela di diritti, interessi e patrimoni, attraverso attività investigative finalizzate a consentire decisioni consapevoli basate su fatti accertati e prove verificabili. L'obiettivo è trasformare il dubbio in evidenza documentata, nel pieno rispetto della legalità e delle procedure investigative. «Un'indagine svolta da un'agenzia investigativa autorizzata, regolarmente riconosciuta dalla Prefettura competente e dal Ministero dell'Interno di Roma, e dotata di tesserino identificativo ha valore reale soltanto se le prove raccolte possono essere utilizzate in modo corretto in sede giudiziaria - spiega Ennio Tesone -. Tutte le nostre attività vengono svolte nel pieno rispetto delle normative vigenti, affinché la documentazione prodotta possa avere efficacia probatoria nei procedimenti civili e, in determinati casi, anche in quelli penali. Questo significa adottare procedure rigorose, documentare ogni fase dell'attività investigativa e redigere report dettagliati, chiari e tecnicamente solidi. Oggi il cliente non cerca semplicemente conferme personali: cerca elementi concreti che possano tutelarli legalmente».


Pineider
FIRENZE, 1774



**DOUBLE
YOUR
PERFORMANCE**

 PIQUADRO



GAGGIO MONTANO, ITALY
44°11'14.04"N 10°59'47.58"E

Cybersecurity e trasformazione digitale

Luca Busi racconta l'evoluzione di Gmg net, azienda nata a Genova nel 2000: dalla consulenza web alla costruzione di ecosistemi digitali avanzati, dove tecnologia, sicurezza dei dati e intelligenza artificiale diventano leve strategiche per la competitività delle imprese

Era l'inizio del Duemila e il digitale era ancora agli albori. In quel periodo nasceva a Genova, Gmg net, una realtà che ha attraversato l'intero percorso di quella trasformazione che oggi non è più soltanto una questione tecnologica, ma rappresenta un processo strutturale che coinvolge governance, sicurezza, gestione dei dati, continuità operativa e capacità di interpretare il cambiamento. In un contesto in cui infrastrutture cloud, cybersecurity, intelligenza artificiale e comunicazione convergono sempre di più, Gmg net è uno di quei partner per le imprese in grado non solo di sviluppare strumenti digitali, ma di costruire ecosistemi affidabili, scalabili e sostenibili nel tempo. Abbiamo incontrato il fondatore, Luca Busi.

Quanto è cambiato, dagli anni della fondazione di Gmg net a oggi il ruolo di un partner tecnologico?

«È cambiato radicalmente. Nei primi anni Duemila il digitale veniva percepito principalmente come uno strumento di comunicazione o come un asset per le aziende. Oggi, invece, rappresenta un'infrastruttura strategica che attraversa ogni funzione aziendale: produzione, organizzazione, marketing, gestione dei dati, sicurezza, relazione con i clienti e processi decisionali. Questo significa che il ruolo di un partner tecnologico non può più limitarsi allo sviluppo di un sito o di un software. Oggi serve una visione integrata, capace di mettere in relazione tecnologia, business e governance operativa. Le aziende si trovano a gestire ecosistemi digitali sempre più complessi, dove convivono piattaforme cloud, strumenti di collaborazione, sistemi di cybersecurity, applicazioni personalizzate e flussi continui di dati. Il nostro compito è aiutare le imprese a governare questa complessità, traducendola in soluzioni concrete, sostenibili e sicure nel lungo periodo. La vera evoluzione del settore è proprio questa: passare dalla semplice fornitura tecnologica alla costruzione di architetture digitali coerenti e affidabili».

Il vostro approccio si basa su ascolto, personalizzazione e sviluppo su misura. «Evitiamo modelli standardizzati perché ogni impresa ha dinamiche, obiettivi e criticità differenti. Uno degli errori più frequenti nella trasformazione digitale è pensare che esistano soluzioni universali valide per tutti. In realtà, la tecnologia funziona



davvero solo quando riesce ad adattarsi ai processi aziendali e non il contrario. Per questo ogni progetto parte da una fase molto approfondita di ascolto, analisi e definizione degli obiettivi. Cerchiamo di comprendere non soltanto le esigenze tecniche, ma anche l'organizzazione interna dell'azienda, il livello di maturità digitale, le modalità operative e le prospettive di crescita future. Questo ci permette di progettare piattaforme e infrastrutture realmente utili, capaci di evolvere insieme al business.

La personalizzazione non riguarda solo l'estetica o le funzionalità ma soprattutto la sostenibilità del progetto nel tempo. Una soluzione ben progettata deve essere flessibile, scalabile e facilmente governabile».

Oggi sicurezza informatica e continuità operativa sono diventate priorità strategiche. Come affrontate questi aspetti?

«Oggi cybersecurity e continuità operativa non possono più essere considerate elementi accessori. Sono componenti centrali della stabilità aziendale. Per questo lavoriamo sulla progettazione di ecosistemi tecnologici sicuri fin dalla loro architettura iniziale. Ci occupiamo della gestione delle infrastrutture cloud, del monitoraggio continuo dei sistemi, dell'aggiornamento delle piattaforme e della protezione delle informazioni sensibili. Allo stesso tempo, affrontiamo il tema della sicurezza anche dal punto di vista normativo e organizzativo, supportando le aziende nei percorsi di conformità, nella protezione dei dati e nell'adozione di procedure coerenti con gli

standard attuali. La sicurezza efficace oggi non è soltanto tecnologica: è culturale, organizzativa e strategica».

Uno degli ambiti più innovativi del vostro lavoro riguarda l'intelligenza artificiale privata. Perché avete scelto questo approccio?

«Perché riteniamo che il tema centrale dell'intelligenza artificiale oggi non sia soltanto la potenza degli strumenti, ma il controllo dei dati e la governance delle informazioni. Molte aziende sono interessate all'AI, ma allo stesso tempo hanno forti preoccupazioni legate alla riservatezza dei dati, alla conformità normativa e alla sicurezza delle informazioni aziendali. È qui che nasce il valore delle soluzioni di AI privata. Noi sviluppiamo sistemi basati su infrastrutture dedicate, dove i dati rimangono sotto il pieno controllo dell'azienda. Questo consente di utilizzare modelli di intelligenza artificiale in modo sicuro, senza esporre informazioni sensibili a piattaforme esterne o a processi non governabili. L'obiettivo non è introdurre l'AI come elemento "di moda", ma integrarla concretamente nei processi operativi e decisionali delle imprese. Quando progettata correttamente, l'intelligenza artificiale può migliorare l'efficienza, velocizzare l'accesso alle informazioni, supportare l'analisi dei dati e automatizzare attività ripetitive. Ma tutto questo deve avvenire all'interno di un ecosistema affidabile, trasparente e conforme alle normative europee».

• **Bianca Raimondi**

Luca Busi, founder di Gmg net



LE ATTIVITÀ DI GMG NET

Gmg net integra competenze tecniche, strategiche e operative nella gestione dei progetti digitali, con l'obiettivo di rendere la tecnologia un'infrastruttura affidabile, sicura e funzionale alla continuità operativa delle organizzazioni.

Le attività spaziano dalla definizione di strategie digitali e percorsi di comunicazione alla progettazione di esperienze utente e identità visive, fino allo sviluppo di siti web, piattaforme e-commerce e applicazioni. A queste si affiancano la gestione di infrastrutture cloud, servizi digitali evoluti e attività di marketing online, sviluppate attraverso un approccio orientato all'analisi dei dati, alle performance e alla crescita sostenibile delle imprese.

A Bologna si va sul sicuro

Le nuove tecnologie, simulazioni di rischio e le esperienze più virtuose di wellbeing corporate. Saranno in vetrina dal 26 al 28 maggio ad Ambiente Lavoro, fiera regina per gli operatori della sicurezza nei luoghi professionali

La salute e la sicurezza prima di tutto. È il messaggio ispirato alla costruzione di una cultura collettiva sulla prevenzione che intende rilanciare con forza Ambiente Lavoro, salone d'eccellenza per prodotti e servizi volti a minimizzare i rischi di incidenti e malattie professionali che tornerà in passerella a BolognaFiere dal prossimo 26 maggio fino al 28. Tre giornate che riuniranno all'ombra delle Due Torri operatori e aziende attive nel mondo della sicurezza, dell'ambiente, delle risorse umane e della sostenibilità, presentando le nuove tecnologie e le best practice per promuovere la salute professionale a 360 gradi- equilibrio psicologico e benessere organizzativo inclusi- e per aggiornarsi vicendevolmente sugli ultimi indirizzi normativi in materia.

DPI, IN MOSTRA LE GAMME PIÙ INNOVATIVE SUL MERCATO

In un collaudato scacchiere espositivo che anche nella passata edizione ha incassato il pollice alto di oltre 8 mila visitatori, in primo piano si confermerà Sicur Labor, il salone dedicato ai Dpi e all'abbigliamento professionale. Un'area espositiva che raccoglie le gamme più innovative del mercato, spaziando dalla protezione delle vie respiratorie ai sistemi anticaduta, fino alle nuove soluzioni per il benessere del piede. Uno sguardo speciale sarà rivolto agli aggiornamenti normativi Uni e al loro impatto sull'adozione e sull'utilizzo degli Apvr. Sicur Labor ospiterà inoltre iniziative dedicate alle nuove tendenze del workwear, valorizzandone sia la funzionalità sia l'estetica. Tanto da svelarne persino la dimensione spettacolare nell'ambito della DPI Fashion Week, in cui scarpe, tute, guanti, caschi e molto altro si prenderanno il palcoscenico grazie a sessioni di break dance, improvvisazione teatrale e Rock 'n' Roll acrobatico. Di grande interesse in termini di formazione pratica si preannuncia poi il Campo Prove allestito presso il padiglione 22, dove le aziende potranno mettere in funzione i propri prodotti inserendoli in una simulazione di rischio. Con un'area dedicata alla verifica e debriefing che affiancherà due zone dimostrative: una riservata alla "Movimentazione & Sicurezza Antitaglio", che includerà sistemi anticollisione, sensori intelligenti e dispositivi di assistenza per carrelli elevatori; l'altra ai "Lavori in Quota & Barriere di Sicurezza", che proporrà tra le altre cose simulazioni realistiche dedicate agli spazi confinati e alle procedure di primo soccorso, con stuntman profes-



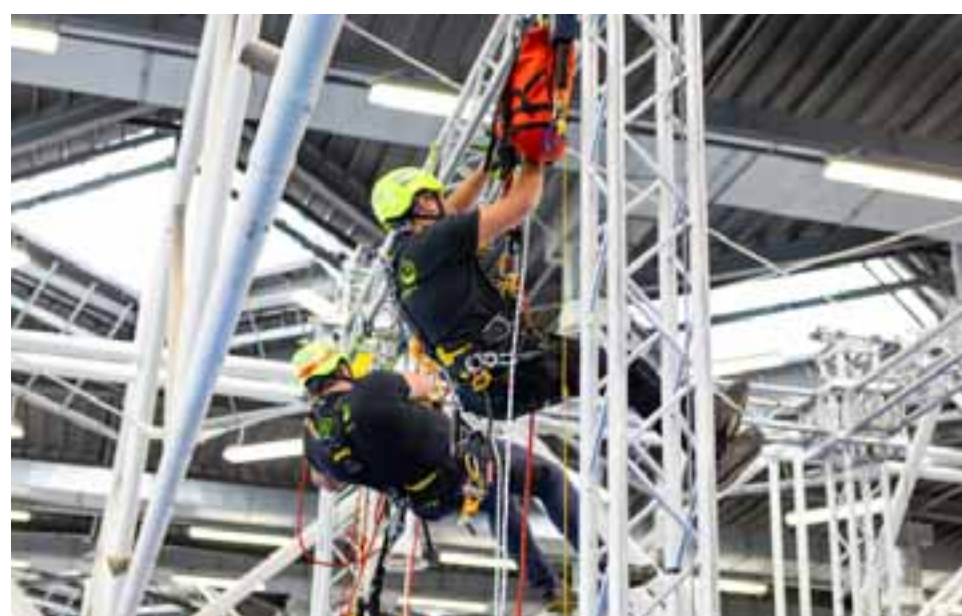
NELLA PRIMA EDIZIONE DEGLI OSCAR DELLA SICUREZZA VERRANNO PREMIATE ESPERIENZE DI SUCCESSO IN FATTO DI PREVENZIONE DI INCIDENTI E MALATTIE PROFESSIONALI, POLITICHE AMBIENTALI E ESG

sionisti e tecnici specializzati che insceneranno cadute dall'alto e casistiche di sovraccarico biomeccanico.

DEBUTTA NEXT, LABORATORIO DI IDEE PER IL MONDO HSE

Sempre di stampo formativo saranno le iniziative messe a punto in partnership con Inail, Aias, fino al Ministero del Lavoro, mentre alla condivisione di buone pratiche si ispirerà il ciclo di workshop Safety Sensei, destinato alle migliori case history di grandi aziende in fatto di tematiche emergenti. Quest'anno, a finire sotto i riflettori saranno le novità per i datori di lavoro e i rischi derivanti dalle differenze di genere e generazionali, posti in risalto da Rspg e Hse manager di grandi realtà indu-

striali che racconteranno le loro esperienze evidenziandone punti deboli e risvolti positivi. Sulla scia del gradimento riscosso nelle passate edizioni, ad Ambiente Lavoro si rinnoverà l'appuntamento con i percorsi di wellbeing corporate, un approccio strategico alla gestione delle risorse umane che mira a promuovere la salute e il benessere dei dipendenti in ufficio o in fabbrica. In questo senso, la Wellbeing Arena allestita nel quartiere fieristico di Bologna sarà il luogo prediletto in cui concedersi una pausa tra le molte attività proposte nelle 72 ore di palinsesto, approfondendo come si può migliorare il clima e il benessere aziendale. Per rafforzare il proprio ruolo di "place to be" culturale oltre che commerciale, quest'anno Ambiente Lavoro lancerà anche Next, il laboratorio di idee che costituirà il think tank della manifestazione. Una piattaforma di elaborazione permanente che coinvolgerà alcune tra le più autorevoli realtà associative e professionali del settore, con affondi sui temi oggi più rilevanti per il mondo Hse. Dal ruolo strategico del facility management nella gestione integrata degli ambienti di lavoro, focus di apertura della prima giornata, alla partecipazione attiva delle persone nei processi di prevenzione di cui si parlerà nell'ultimo incontro organizzato in collaborazione con Hse Excellence Sharing Team. Ancora sotto il cappello di Next, infine, annunciati altri due debutti importanti: Next Safety connection, format relazionale ideato per favorire lo scambio di competenze tra direzioni aziendali e professionisti Hse; la prima edizione degli Oscar della Sicurezza, che premieranno esperienze di successo in fatto di prevenzione di incidenti e malattie professionali, politiche ambientali e Esg. •Gaetano Gemiti



Prestazioni elevate e sviluppo internazionale

Odb Safety accelera sul mercato dei Dpi con nuove referenze, partnership internazionali e un piano di sviluppo focalizzato su innovazione, canali professionali e rafforzamento del brand. Ne parliamo con il ceo Matteo Tuniola

Nel settore dei dispositivi di protezione individuale, la competizione si gioca sempre meno sul solo prodotto e sempre più sulla capacità di costruire un'identità forte, una rete commerciale strutturata e una proposta capace di coprire esigenze differenti del mercato professionale. Ed è proprio qui che si inserisce il percorso di crescita di Odb Safety, azienda friulana con sede a Maniago (Pn) specializzata nella produzione di Dpi, in particolare guanti da lavoro. Una strategia che guarda al consolidamento sul mercato italiano e all'espansione nei canali professionali, anche attraverso appuntamenti di settore come Secure Labor Bologna, dove Odb sarà presente il 27 maggio con incontri dedicati agli operatori della filiera. Abbiamo incontrato il ceo Matteo Tuniola.

Il mercato dei Dpi è sempre più competitivo e strutturato. Su quali leve state costruendo la crescita di Odb Safety?

«La crescita oggi non può basarsi esclusivamente sul prezzo o sulla disponibilità del prodotto. Il mercato richiede visione, specializzazione e soprattutto coerenza. Per questo abbiamo deciso di investire contemporaneamente su tre direttrici: ampliamento della gamma, rafforzamento della rete commerciale e consolidamento del posizionamento del marchio. Negli ultimi mesi abbiamo lavorato molto sulla struttura aziendale per renderla più vicina ai clienti e ai distributori professionali. Parallelamente, abbiamo avviato un importante percorso di rebranding che non riguarda soltanto il logo o l'immagine coordinata, ma il modo in cui vogliamo essere percepiti dal mercato: un partner tecnico affidabile, competente e focalizzato sulle reali esigenze operative degli utilizzatori».



Da sinistra, Matteo Tuniola, ceo, e Gian Paolo Fedrigo, chairman di Odb Safety

La vostra strategia commerciale si fonda sul modello "Good, Better, Best". Come si traduce concretamente?

«Abbiamo scelto una struttura di offerta chiara, che permetta al cliente di individuare rapidamente il livello di protezione e performance più adatto alla propria attività. La logica "Good, Better, Best" ci consente di coprire esigenze molto differenti, mantenendo però una forte coerenza di gamma.

Ci sono aziende che cercano un prodotto affidabile e competitivo per utilizzi general purpose, mentre altre operano in contesti ad altissima complessità tecnica dove il guanto diventa un vero strumento di lavoro. Noi vogliamo essere presenti in entrambe le situazioni. Per questo parliamo anche delle nostre "Ferrari della protezione": modelli sviluppati per garantire prestazioni elevate in termini di resistenza, sensibilità tattile, ergonomia e sicurezza. È un approccio che ci permette di dialogare con mercati diversi senza perdere identità».

Accanto al marchio Odb, state sviluppando anche partnership con grandi player internazionali. Quanto conta questo aspetto nella vostra strategia?

«Conta molto, perché crediamo che oggi il valore si costruisca anche attraverso la capacità di creare sinergie industriali e commerciali solide. Da una parte c'è il nostro marchio proprietario, sul quale continuiamo a investire in termini di ricerca, sviluppo e posizionamento; dall'altra collaboriamo con multinazionali leader del settore come Ansell, combinando la flessibilità di una realtà specializzata con la forza e

strali complessi e ad alto rischio, dove il livello di protezione deve convivere con precisione e comfort operativo. Orma Technocut 18507 offre un livello antitaglio F secondo normativa En 388 ed è stato progettato per lavorazioni molto tecniche.

La combinazione di fibre Uhmwpe, acciaio, nylon e spandex a 18 aghi garantisce un equilibrio particolarmente evoluto tra resistenza meccanica, flessibilità e sensibilità tattile. Anche il rivestimento in nitrile sabbato è stato studiato per assicurare grip affidabile in condizioni operative difficili. Un altro aspetto importante è la certificazione Esd, che rende il prodotto idoneo anche per ambienti Atex e contesti dove il controllo delle scariche elettrostatiche è fondamentale. In pratica non si tratta semplicemente di un guanto protettivo, ma di un dispositivo progettato per diventare parte integrante del processo produttivo».

Anche il segmento general purpose continua però ad avere un peso importante nella vostra offerta.

«Assolutamente sì. Un esempio è il Superlatex 14530, che rappresenta perfettamente la nostra idea di prodotto versatile ma ad alte prestazioni. In molti casi il mercato general purpose viene considerato una fascia standardizzata; noi invece crediamo che anche lì sia possibile portare innovazione e qualità. Il supporto in po-

ABBIAMO SCELTO UNA STRUTTURA DI OFFERTA CHIARA, CHE PERMETTA AL CLIENTE DI INDIVIDUARE RAPIDAMENTE IL LIVELLO DI PROTEZIONE E PERFORMANCE PIÙ ADATTO ALLA PROPRIA ATTIVITÀ. LA LOGICA 'GOOD, BETTER, BEST' CI CONSENTE DI COPRIRE ESIGENZE MOLTO DIFFERENTI MANTENENDO PERÒ UNA FORTE COERENZA DI GAMMA

l'esperienza di gruppi internazionali.

A partire dal 2026 inizieremo inoltre la distribuzione del marchio giapponese Showa, un passaggio strategico che rafforzerà ulteriormente il nostro presidio nel segmento premium e ad alto contenuto tecnico».

Tra i prodotti di punta spicca Orma Technocut 18507. Quali esigenze di mercato intercetta?

«È un prodotto che nasce per ambienti indu-

lietere a 13 aghi e il rivestimento in lattice crinkle permettono di ottenere un'ottima presa mantenendo comfort e flessibilità elevati. Abbiamo lavorato molto anche sull'ergonomia, per ridurre l'affaticamento dell'operatore durante utilizzi prolungati. La resistenza al calore fino a 100°C per 15 secondi amplia ulteriormente i campi applicativi e rende questo modello particolarmente interessante per numerosi contesti industriali e logistici». •Beatrice Guarnieri

OBIETTIVI A BREVE TERMINE

Nei prossimi mesi Odb Safety prevede il lancio di circa dieci nuovi prodotti e proseguirà gli investimenti legati alla crescita e al consolidamento del brand. Un'attenzione particolare è rivolta anche al digitale, con il rafforzamento della presenza su LinkedIn come strumento di relazione con mercato, distributori e partner, oltre all'imminente go live del nuovo sito web aziendale, progettato per rendere più semplice e immediata la consultazione della gamma prodotti e dei contenuti tecnici. A conferma del percorso di crescita intrapreso, l'azienda ha inoltre ricevuto un riconoscimento da Italy-Post, che ha inserito Odb Safety tra le migliori realtà imprenditoriali della provincia di Pordenone, premiandone il percorso di sviluppo, qualità e specializzazione.

People, Product, Process

Sono i tre pilastri su cui 3P Safety costruisce ogni attività. «Crediamo che la sicurezza non possa essere affrontata in maniera frammentata, ma debba nascere dall'integrazione tra competenze umane, qualità tecnica del prodotto e gestione strutturata dei processi». L'analisi di Matteo Pettenuzzo

L'evoluzione tecnologica degli impianti, l'introduzione di nuovi vettori energetici come l'idrogeno e l'adeguamento ai più recenti standard europei impongono oggi competenze altamente specialistiche e un approccio multidisciplinare capace di integrare progettazione, analisi del rischio, certificazione e gestione operativa. In settori complessi come oil & gas, chimico, farmaceutico e manifatturiero avanzato, la conformità alle direttive Atex, Ped e al nuovo Regolamento Macchine Ue 2023/1230 è diventata un fattore decisivo per garantire affidabilità, innovazione e protezione delle persone. 3P Safety, realtà specializzata nella consulenza e certificazione industriale, ha costruito la propria identità su un approccio integrato alla gestione dei processi e dell'innovazione tecnologica. Sotto la guida di Matteo Pettenuzzo, l'azienda ha sviluppato una visione tecnica e strategica capace di trasformare la sicurezza industriale in un autentico valore di sistema, al servizio dell'efficienza, della conformità e dell'evoluzione delle imprese.

3P Safety nasce con una forte specializzazione nella sicurezza industriale: qual è oggi la vostra identità sul mercato?

«3P Safety è una società di consulenza e certificazione che opera nel campo della sicurezza di macchine, impianti e apparecchiature industriali. Il nostro lavoro si concentra soprattutto sugli ambiti Atex, direttiva macchine e Ped, con competenze trasversali che ci permettono di seguire progetti complessi in diversi settori industriali. Il nome stesso dell'azienda sintetizza il nostro approccio: People, Product, Process. Sono i tre pilastri su cui



costruiamo ogni attività. Crediamo che la sicurezza non possa essere affrontata in maniera frammentata, ma debba nascere dall'integrazione tra competenze umane, qualità tecnica del prodotto e gestione strutturata dei processi».

Cosa significa concretamente applicare il modello People, Product, Process?

«Significa affrontare ogni progetto con una visione globale. "People" perché la sicurezza nasce prima di tutto dalle persone: dalla formazione, dalla consapevolezza e dalla capacità di gestire

correttamente i rischi. "Product" perché ogni macchina o impianto deve essere progettato e certificato per garantire affidabilità, conformità normativa ed efficienza operativa. Infine "Process", perché senza procedure strutturate e controlli adeguati non esiste sicurezza duratura. Questo approccio integrato ci permette di accompagnare i clienti lungo tutto il ciclo di vita del prodotto, dalla progettazione fino alla messa in servizio».

Quali sono oggi gli ambiti nei quali siete maggiormente specializzati?

«Operiamo in settori industriali ad alta complessità e ad alto rischio, come chimico, farmaceutico, oil & gas, manifatturiero avanzato e tecnologie energetiche innovative. In particolare ci occupiamo di conformità Atex, classificazione delle zone a rischio esplosione, marcature Ce, analisi dei rischi, fascicoli tecnici e applicazione del nuovo Regolamento macchine Ue 2023/1230. Parallelamente abbiamo sviluppato competenze molto avanzate in ambito Ped per apparecchiature e impianti in pressione, seguendo attività di classificazione, progettazione, certificazione e formazione tecnica».

Negli ultimi anni il tema dell'idrogeno è diventato centrale nella transizione

energetica. Qual è il vostro ruolo in questo settore?

«L'idrogeno rappresenta una delle sfide tecnologiche più importanti dei prossimi anni e richiede standard di sicurezza estremamente elevati. 3P Safety è coinvolta nello sviluppo di importanti progetti legati alle stazioni di compressione e rifornimento H₂, elettrolizzatori fino a 1 MW, forni di processo per acciaierie e sistemi di accumulo a idruri metallici. In questi contesti ci occupiamo di tutti gli aspetti legati alla sicurezza: classificazione Atex, Fire & Explosion Risk Assessment, progettazione dei sistemi di rilevazione gas e incendio, logiche hardware e software di sicurezza, modellizzazione delle esplosioni, attività Fat/Sat e marcature Ce integrate».

Anche il settore Hvac sta vivendo una trasformazione importante, legata ai nuovi refrigeranti infiammabili. Come state affrontando questa evoluzione?

«La transizione verso refrigeranti a basso impatto ambientale come A2L e R290 sta modificando profondamente il settore Hvac. Abbiamo supportato aziende nazionali e multinazionali nella conversione produttiva di chiller, pompe di calore e refrigeratori industriali, affrontando tutte le problematiche legate alla sicurezza di gas infiammabili. In questi progetti la nostra attività comprende analisi Atex, valu-

Matteo Pettenuzzo, amministratore delegato di 3P Safety



tazioni del rischio incendio ed esplosione, progettazione delle aspirazioni di sicurezza, sistemi di rilevazione gas e adeguamento delle logiche di sicurezza degli impianti».

La sicurezza viene spesso percepita come un costo. È ancora così?

«Fortunatamente sempre meno. Le aziende più evolute hanno compreso che la sicurezza è un investimento strategico. Un impianto sicuro è un impianto più efficiente, più affidabile e più competitivo. Ridurre i rischi significa evitare fermi produttivi, aumentare la continuità operativa e proteggere il valore industriale dell'azienda. Oggi la sicurezza è strettamente collegata anche alla sostenibilità e alla reputazione aziendale».

• **Guido Anselmi**

ALTE SPECIALIZZAZIONI

«Oggi non basta conoscere la normativa: servono competenze tecniche, ingegneristiche, impiantistiche e anche legali - sottolinea Pettenuzzo -. I progetti industriali sono sempre più integrati e richiedono figure in grado di dialogare con progettisti, costruttori, responsabili Hse e organismi notificati. Il nostro valore aggiunto è proprio la capacità di mettere insieme competenze diverse all'interno di un unico interlocutore tecnico». 3P Safety può contare su un team tecnico altamente specializzato e su un costante investimento nella formazione continua, fondamentale in un settore in continua evoluzione. L'obiettivo è supportare le imprese nel trasformare gli obblighi normativi in opportunità concrete di crescita, innovazione ed efficienza operativa.

I nostri servizi per le tecnologie basate sull'idrogeno



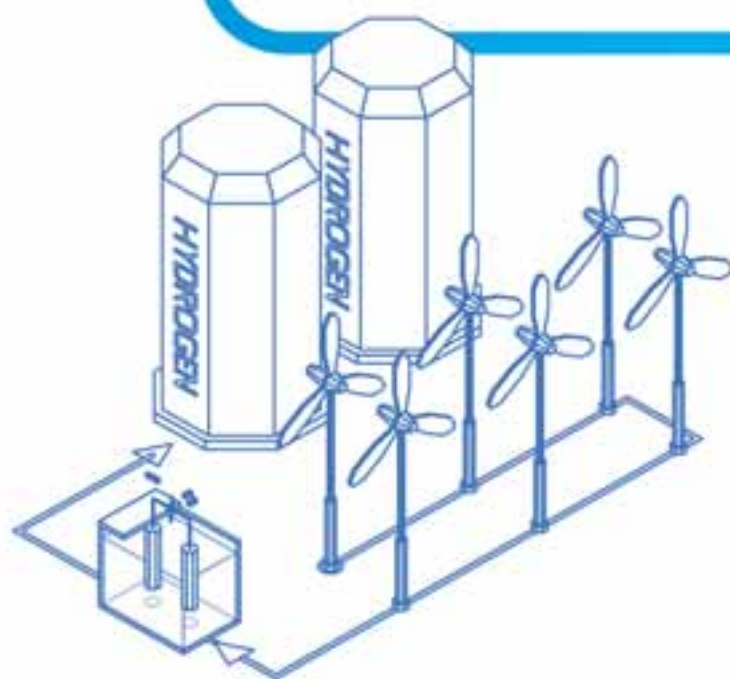
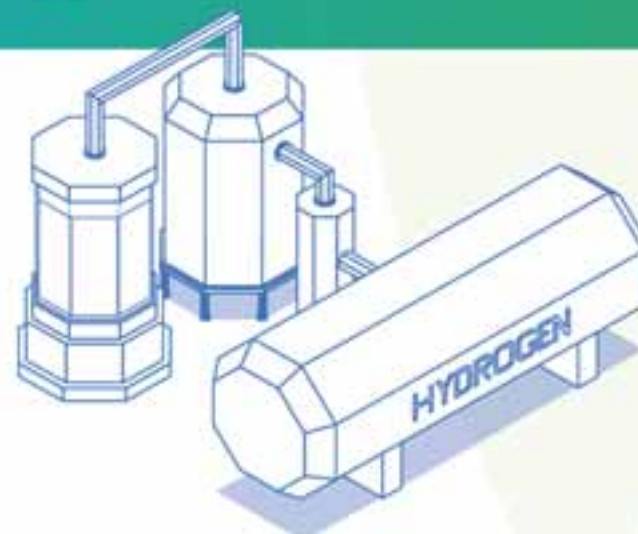
Studi fattibilità

vincoli certificativi e autorizzativi



Zone ATEX

classificazione, modellizzazione
effetti su macchine e impianti



Analisi rischi

ATEX e Process Safety



Progettazione

sistema di sicurezza
ATEX e Fire Protection



Verifica acquisto

apparecchiature
meccaniche, elettriche,
sistemi di protezione



Fascicoli tecnici

prove e collaudi, FAT/SAT
istruzioni per l'uso



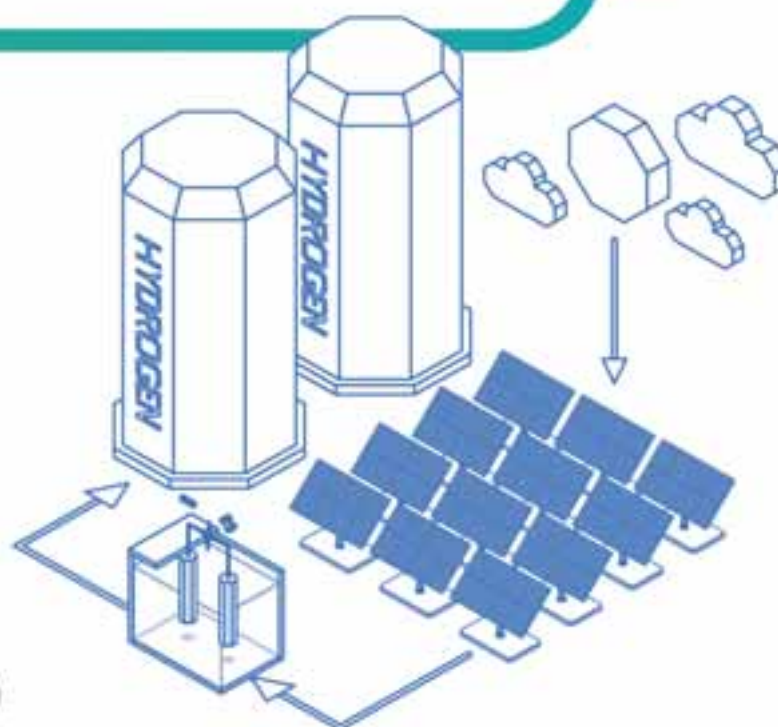
Marcatura CE

Direttive Macchine
2006/42/CE, ATEX e PED



Validazione

Safety Function dei sistemi di
sicurezza EN 13849-1/2 (PL/SIL)



3P SAFETY S.R.L. | People Products Process

Sede legale

Bastioni di Porta Nuova, 21
20121 Milano (MI) Italy
Phone: +39 3480728960

Sede operativa Vicenza

Piazza Pontelandolfo, 6
36100 Vicenza (VI) Italy
Phone: +39 04441453703

Sede operativa Parma

Via G.P. Sardi 14/B
Loc. Alberi - 42124 Parma

3p-safety.it

Un piano d'azione concreto

Dalla legge 198/2025, che premia le aziende virtuose, al ruolo della formazione, dei dati e dell'la, la strategia per rafforzare la cultura della sicurezza. L'analisi del presidente Inail Fabrizio D'Ascenzo

Il 28 aprile si è svolta la Giornata mondiale per la sicurezza e la salute sul lavoro. Un tema su cui l'Italia cerca una svolta, dopo anni di cronicizzazione del fenomeno. Per i primi tre mesi del 2026, calano le morti bianche, ma aumentano gli infortuni (le denunce nel 2025 sono state 416.900) e le malattie professionali. Entriamo nel dettaglio con il presidente dell'Inail, Fabrizio D'Ascenzo.

Presidente, dove risiedono oggi le maggiori criticità del sistema italiano della prevenzione? La nuova Legge 198/2025 può contribuire positivamente?

«Il quadro normativo italiano in materia di salute e sicurezza sul lavoro è tra i più avanzati in ambito europeo. Ma questo purtroppo non basta. Permangono settori di attività - costruzioni, logistica, trasporto - che continuano a registrare un'elevata incidenza infortunistica, confermando la necessità di rafforzare ulteriormente le azioni di prevenzione per incidere sui contesti produttivi più esposti al rischio. Il provvedimento adottato a fine 2025, a cui l'Istituto ha lavorato attivamente per definirne i contenuti in sinergia con il ministero del Lavoro, ha riconosciuto all'Inail un ruolo determinante per contrastare gli infortuni sul lavoro, rafforzandone così la missione sociale. Era dal 2008 che mancavano passaggi legislativi così significativi sul tema della sicurezza».

Può evidenziare le novità più significative?

«Mi riferisco a temi emergenti come i near miss, l'importanza delle campagne formative e informative e la consultazione gratuita di alcune norme UNI rilevanti in materia di salute e sicurezza sul lavoro. In particolare, la nuova normativa si fonda su una logica premiale, che punta a incentivare le imprese virtuose attraverso il potenziamento del bonus per andamento infortunistico favorevole, con aliquote di riduzione del premio assicurativo. Inoltre, l'Inail, con l'oscillazione del tasso medio di tariffa per prevenzione, premia le aziende che eseguono interventi per il miglioramento delle condizioni di salute e sicurezza nei luoghi di lavoro ulteriori rispetto a quelli previsti dalla vigente normativa. La legge prevede, inoltre, la copertura assicurativa in itinere per gli studenti impegnati nei percorsi di formazione scuola-lavoro».

Quanto è importante rendere accessibile la formazione al più ampio numero di imprese possibile?

«La formazione è un pilastro centrale della strategia di prevenzione adottata dall'Istituto. Renderla accessibile al maggior numero di imprese, soprattutto alle Pmi, che rappresentano un segmento molto rilevante del tessuto produttivo italiano, è di fondamentale importanza. Con l'addendum all'accordo del 2023 tra l'Inail e la Conferenza delle Regioni e delle Pro-



vince autonome, sottoscritto a dicembre 2025, si estende a tutto il 2026 l'opportunità per le imprese di accedere alla formazione finanziata in materia di salute e sicurezza attraverso i pro-

Ha definito l'intelligenza artificiale un "alleato strategico" dell'Inail. In quali ambiti nello specifico?

«L'la è uno strumento prezioso in chiave pre-

LA FORMAZIONE È UN PILASTRO CENTRALE DELLA STRATEGIA DI PREVENZIONE ADOTTATA DALL'ISTITUTO. RENDERLA ACCESSIBILE AL MAGGIOR NUMERO DI IMPRESE, SOPRATTUTTO ALLE PMI, CHE RAPPRESENTANO UN SEGMENTO MOLTO RILEVANTE DEL TESSUTO PRODUTTIVO ITALIANO, È DI FONDAMENTALE IMPORTANZA

grammi formativi resi disponibili dalle Regioni e sostenuti dall'Istituto con oltre 10 milioni di euro».

La formazione è al centro anche dell'Accordo sottoscritto il 5 maggio scorso con Federmanager.

«Questa intesa nasce dalla convinzione che il management industriale possa contribuire alla diffusione della cultura della prevenzione, trasferendola lungo tutta la filiera produttiva e trasformandola in azioni concrete. Una leva che può fare la differenza nelle realtà più piccole, dove spesso mancano strutture dedicate e competenze specialistiche per tradurre gli obblighi normativi in pratiche efficaci».

venzionale, ma anche per lo sviluppo di protesi e strumenti riabilitativi; un ambito nel quale Inail collabora con enti di primo piano nel mondo scientifico e accademico. Sul fronte della prevenzione, sono stati avviati progetti per l'adozione di sistemi cognitivi per l'analisi dei dati relativi agli infortuni mortali, i "quasi incidenti" e gli infortuni su strada. L'la è stata trasversalmente integrata in tutte le linee di ricerca Inail: dispositivi di protezione individuale smart che integrano sensori e sistemi di controllo in Dpi tradizionali; oppure abiti intelligenti sensorizzati, realizzati con tessuti ingegnerizzati per monitorare sia i fattori ambientali, sia i parametri fisiologici del lavo-

ratore. L'la può intervenire in alcune problematiche legate all'organizzazione del lavoro, rendendo le informazioni più accessibili e comprensibili. L'Inail sta sperimentando strumenti di comunicazione multilingua, anche attraverso scenari immersivi e avatar virtuali. Sul fronte dell'ambito protesico e riabilitativo, infine, numerose sono le applicazioni per rendere i movimenti delle persone con disabilità più intuitivi, naturali e personalizzati».

In base al Piano triennale della Prevenzione Inail 2025-2027, quali linee di intervento prioritario identifica?

«La Relazione annuale 2024 dell'Inail si chiudeva con una sfida per il futuro: contribuire alla definizione di una strategia nazionale di prevenzione e protezione, accompagnata da un piano d'azione concreto, basato su un approccio sistematico e a rete. In questa direzione, grazie alla fattiva collaborazione con il governo, sono stati compiuti importanti passi in avanti anche attraverso la Strategia nazionale in materia di salute e sicurezza nei luoghi di lavoro 2026-2030 e la legge 198/2025. Con un metodo di lavoro partecipato, l'Istituto intende rafforzare ulteriormente la cultura della sicurezza, sostenendo lavoratori e imprese e investendo nell'innovazione tecnologica e nell'analisi dei dati. Tra gli obiettivi prioritari, rientra il miglioramento delle condizioni di salute e sicurezza in un mondo caratterizzato da rischi nuovi ed emergenti, senza trascurare l'azione di mitigazione dei rischi tradizionalmente noti. In questa prospettiva, la circolarità tra ricerca e prevenzione, fondata su dati ed evidenze, potrà contribuire al miglioramento della qualità della vita dei lavoratori, con riflessi positivi in termini di sostenibilità».

•Francesca Druidi



Fabrizio D'Ascenzo, presidente Inail

Dpi professionali, non solo conformità

Carlo Splendiani, realtà specializzata nella fornitura di soluzioni di antinfortunistica e abbigliamento da lavoro, da oltre 40 anni affianca le aziende con competenza, continuità e un approccio consulenziale

Nel settore della sicurezza sul lavoro, l'evoluzione normativa e tecnologica ha trasformato profondamente il ruolo dei dispositivi di protezione individuale e dell'abbigliamento tecnico professionale. Oggi non si tratta più soltanto di fornire prodotti conformi, ma di progettare sistemi integrati di protezione capaci di garantire sicurezza, ergonomia, comfort operativo e identità aziendale. Esperienza, competenza tecnica e capacità consulenziale diventano elementi decisivi per accompagnare le imprese nella scelta delle soluzioni più adeguate ai diversi contesti produttivi. È proprio su questi valori che la Carlo Splendiani, realtà con sede a Loro Piceno, in provincia di Macerata, ha costruito oltre quarant'anni di attività nel settore dell'antinfortunistica professionale. Fondata dalla visione imprenditoriale di Carlo Splendiani, l'azienda, sotto la guida di Maria Luisa Silveti e Lorella Settembri, ha saputo crescere affiancando imprese, operatori e professionisti con un'offerta altamente specializzata che comprende Dpi, abbigliamento tecnico, sistemi anticaduta, dispositivi antincendio e soluzioni per la sicurezza industriale. Un percorso sviluppato attraverso un'attenta selezione qualitativa dei prodotti, partnership con i principali brand internazionali del settore e una struttura organizzativa costruita per garantire rapidità, affidabilità e supporto tecnico costante.

La vostra azienda nasce oltre quarant'anni fa con una visione molto precisa: mettere la sicurezza al centro del lavoro. Quanto è cambiato questo settore da allora?

«È cambiato radicalmente. Quando abbiamo iniziato, la sicurezza veniva spesso percepita come un obbligo normativo o un costo necessario. Oggi, invece, le aziende hanno una consapevolezza completamente diversa: comprendono che investire nella protezione delle persone significa investire nella qualità del lavoro, nell'efficienza produttiva e nella sostenibilità dell'impresa stessa. Inoltre, oggi c'è un'attenzione maggiore anche all'aspetto estetico e al vestiario utilizzato in azienda ed è anche per questo motivo che noi ci siamo specializzati nella vendita di abbigliamento da lavoro personalizzato».

Quanto conta oggi l'esperienza in un settore così tecnico e normato?

«Conta moltissimo, perché la sicurezza non può essere improvvisata. Ogni ambiente di lavoro presenta criticità specifiche e richie-



NON CI LIMITIAMO A VENDERE PRODOTTI: ANALIZZIAMO ESIGENZE, CONTESTI E RISCHI, ACCOMPAGNANDO IL CLIENTE NELLA SCELTA PIÙ CORRETTA SOTTO IL PROFILO TECNICO E NORMATIVO

de dispositivi adeguati alle reali condizioni operative. La nostra esperienza ci consente di affiancare le aziende in modo concreto, individuando soluzioni affidabili, certificate e realmente efficaci. Non ci limitiamo a vendere prodotti: analizziamo esigenze, contesti e rischi, accompagnando il cliente nella scelta più corretta sotto il profilo tecnico e normativo. È un approccio consulenziale che negli anni ci ha permesso di costruire rapporti solidi e duraturi con molte aziende».

La vostra offerta comprende una gamma molto ampia di soluzioni professionali.

Quali sono oggi i prodotti più richiesti?

«Operiamo con una proposta estremamente articolata che comprende guanti tecnici in pelle, sintetici e speciali, abbigliamento professionale di I, II e III categoria, capi ad alta visibilità, calzature antinfortunistiche cucite e iniettate, dispositivi anticaduta, sistemi di sollevamento, materiale antincendio e prodotti per il primo soccorso. Negli ultimi anni abbiamo registrato una crescente attenzione verso prodotti ad alto contenuto tecnico, in particolare nel campo dell'ergonomia, della traspirabilità e della resistenza dei materia-

li. Oggi il lavoratore cerca protezione, ma anche comfort e libertà di movimento, soprattutto nei contesti operativi più complessi».

Anche l'abbigliamento professionale sembra aver assunto un ruolo diverso rispetto al passato.

«Assolutamente sì. Oggi l'abbigliamento da lavoro non è più soltanto una dotazione tecnica: è diventato parte integrante dell'identità aziendale. Le imprese vogliono capi che garantiscano sicurezza e prestazioni elevate, ma che siano anche coerenti con la propria immagine e con il proprio brand. Per questo proponiamo ampie possibilità di personalizzazione, permettendo alle aziende di coniugare protezione, funzionalità e comunicazione visiva. È un aspetto che negli ultimi anni è cresciuto enormemente».

La qualità dei prodotti è uno dei vostri punti di forza. Come selezionate i marchi e le soluzioni che proponete?

«La selezione qualitativa è sempre stata centrale nella nostra filosofia aziendale. Collaboriamo con alcuni dei principali leader mondiali del settore come Honeywell, BLS, 3M, Exena, U-Power e Payper, realtà che rappresentano standard elevatissimi in termini di innovazione, affidabilità e certificazione. Accanto a questi brand, abbiamo sviluppato anche il nostro marchio, oggi conosciuto in gran parte d'Italia. Ogni prodotto che proponiamo viene scelto sulla base di criteri molto rigorosi legati a qualità, prestazioni e conformità normativa».

• Bianca Raimondi

Alcuni degli articoli di Splendiani



QUALITÀ CERTIFICATA

La certificazione Uni En Iso 9001:2008 rappresenta per l'azienda non soltanto un riconoscimento formale, ma la conferma di un modello organizzativo costruito su efficienza, controllo dei processi e qualità del servizio. In un settore in cui affidabilità e tempestività risultano determinanti, l'attenzione non si concentra esclusivamente sul prodotto finale, ma coinvolge l'intera struttura aziendale: dalla gestione degli ordini all'assistenza al cliente, fino alla logistica e alle tempistiche di consegna. Nel corso degli anni, la società ha sviluppato un'organizzazione interna solida e strutturata, supportata da un magazzino efficiente che consente di gestire anche forniture di significativa entità e di assicurare consegne rapide direttamente attraverso mezzi aziendali. Un approccio operativo che rappresenta oggi uno dei principali punti di forza dell'azienda e un elemento particolarmente apprezzato dal mercato professionale.

L'evoluzione normativa, la crescente complessità organizzativa delle imprese e l'integrazione di nuove tecnologie nei processi produttivi stanno cambiando il ruolo dell'ingegneria applicata alla prevenzione, all'ambiente e alla gestione dei rischi. Oggi le aziende non chiedono soltanto consulenza tecnica, ma modelli organizzativi capaci di integrare conformità normativa, sostenibilità, innovazione tecnologica e valorizzazione delle persone. La sicurezza, infatti, non viene più interpretata esclusivamente come obbligo legislativo, ma come elemento strategico per migliorare qualità del lavoro, competitività e continuità operativa.

In questo quadro si inserisce l'esperienza di Studio Leonardo, realtà guidata da Valter Borgogno, che negli anni ha costruito un modello multidisciplinare fondato sull'integrazione tra ingegneria, formazione, organizzazione aziendale e sviluppo umano.

Studio Leonardo nasce con una visione molto diversa rispetto al tradizionale studio di ingegneria. Qual è stata l'idea di partenza?

«Fin dall'inizio abbiamo sentito l'esigenza di costruire qualcosa che andasse oltre il semplice concetto di consulenza tecnica. Volevamo creare una struttura nella quale competenze professionali, crescita personale e relazioni umane potessero convivere in modo equilibrato. Nel nostro lavoro ci occupiamo di sicurezza, ambiente, organizzazione e gestione dei rischi, ma dietro ogni progetto ci sono sempre persone, aziende, dinamiche umane e responsabilità molto profonde. Per questo abbiamo scelto di sviluppare un modello fondato sulla collaborazione, sul confronto continuo e sulla crescita reciproca tra professionisti, collaboratori e clienti. Ogni incarico rappresenta per noi non solo un'attività tecnica, ma un'occasione per costruire fiducia, cultura organizzativa e consapevolezza».

Quanto è cambiato negli ultimi anni il settore della sicurezza e dell'ingegneria applicata alle imprese?

«È cambiato radicalmente. Oggi le aziende si trovano ad affrontare scenari molto più complessi rispetto al passato. Le normative evol-

Competenze tecniche, organizzative e umane

La visione sistemica di Studio Leonardo integra ingegneria applicata, formazione, ambiente e sviluppo organizzativo per accompagnare le aziende nella trasformazione tecnologica e nella crescita delle persone. L'esperienza di Valter Borgogno



vono rapidamente, i processi produttivi sono sempre più digitalizzati, aumentano le responsabilità organizzative e cresce la necessità di integrare competenze diverse. La sicurezza non può più essere gestita come un comparto isolato o come una semplice attività documentale. Deve diventare parte integrante della strategia aziendale. Questo significa lavorare contemporaneamente su prevenzione, organizzazione, formazione, cultura aziendale e innovazione tecnologica. Le imprese che riescono a sviluppare questa visione integrata sono quelle che oggi costruiscono ambienti di lavoro più efficienti, più sostenibili e anche più competitivi».

La sicurezza resta il cuore dell'attività dello Studio. Come viene interpretata oggi?

«La sicurezza per noi non coincide con il semplice rispetto delle norme. Naturalmente la conformità normativa è fondamentale, ma il vero obiettivo è costruire sistemi di prevenzione realmente efficaci e sostenibili nel tempo. Quando entriamo in un'azienda analizziamo processi, organizzazione, dinamiche operative e fattore umano. Attraverso consulenza, progettazione, analisi dei rischi e formazione aiutiamo le organizzazioni a sviluppare una cultura della prevenzione più consapevole. La sicurezza funziona davvero solo quando diventa parte del comportamento quotidiano delle persone e non un insieme di regole percepite come imposte dall'esterno».

Nel tempo Studio Leonardo si è strutturato in diverse aree operative. Perché questa scelta multidisciplinare?

«Perché le esigenze delle aziende sono diventate multidimensionali. Oggi un'impresa ha bisogno contemporaneamente di competenze tecniche, organizzative, ambientali, forma-

mazione tecnologica, Leonsafety la formazione e la certificazione dei lavoratori, mentre Leoncoach si occupa dello sviluppo delle persone e dei team. Questa struttura ci permette di affrontare progetti complessi con una visione sistemica, evitando approcci frammentati».

Anche innovazione e digitalizzazione sono entrate in modo importante nel vostro lavoro. Come stanno cambiando il settore?

«La trasformazione digitale sta modificando profondamente il modo in cui vengono gestiti sicurezza, organizzazione e processi aziendali. Oggi disponiamo di strumenti molto avanzati per il monitoraggio dei rischi, l'analisi dei dati, la gestione documentale e la formazione. Tuttavia l'innovazione non deve mai essere fine a sé stessa. La tecnologia va interpretata come uno strumento per migliorare qualità del lavoro, efficienza e prevenzione. Attraverso Leontech stiamo lavorando proprio su questo: integrare nuove tecnologie nei processi industriali mantenendo sempre al centro sostenibilità, semplicità operativa e valore umano». •Beatrice Guarnieri



L'INGEGNERIA AL SERVIZIO DELLE PERSONE

Per Studio Leonardo il fattore umano riveste oggi un ruolo centrale anche in un settore fortemente tecnico. La tecnologia è sempre più determinante e continuerà a esserlo, ma senza competenze umane, capacità relazionali e consapevolezza organizzativa non è in grado di produrre risultati realmente efficaci. Alla base dell'approccio dello Studio vi è il principio secondo cui l'ingegneria debba essere al servizio delle persone, con l'obiettivo di progettare sistemi più sicuri, processi più efficienti e ambienti di lavoro migliori, valorizzando al tempo stesso il contributo umano all'interno delle organizzazioni. Le aziende, in questa visione, non sono costituite soltanto da procedure o macchinari, ma da persone che collaborano, prendono decisioni, gestiscono responsabilità e generano risultati concreti.



Valter Borgogno, titolare di Studio Leonardo

LA CULTURA DELLA SICUREZZA

[cul·tù-ra]

1. Quanto concorre alla formazione dell'individuo sul piano intellettuale e morale e all'acquisizione della consapevolezza del ruolo che gli compete nella società. L'etimologia della parola "cultura" deriva dal verbo latino "colere", che significa "coltivare" ma anche altri significati correlati, tra cui "prendersi cura", "adorare" e "ornare".

COSA È

- È un sistema complesso e dinamico, in continua evoluzione;
- È condivisa, appresa e trasmessa all'interno di un gruppo umano;
- È ciò che permette all'uomo di adattarsi all'ambiente e di affrontare le sfide della vita associata.

A COSA SERVE

- Definisce i **comportamenti** e le **modalità di interazione** all'interno di un gruppo;
- Consente di sviluppare un **senso di identità**;
- Permette di acquisire **spirito critico** e di non cadere nel conformismo.

LA CULTURA DELLA SICUREZZA È IL COLLANTE CHE TIENE INSIEME IL SISTEMA DELLA SICUREZZA.

Gli attori che partecipano alla Sicurezza sul Lavoro sono molteplici, tutti hanno delle responsabilità, **ognuno ha un ruolo ben preciso** ed è attraverso la **condivisione** che si crea un **Sistema** efficiente, duraturo, sostenibile. Se tutti gli elementi del Sistema condividono la stessa Cultura allora si costruisce il **Sistema della Sicurezza**: il modo più efficace per garantire protezione, continuità ed economicità.

La Cultura è alla base della nostra società, è il collante che unisce tutti gli elementi del Sistema

IL SISTEMA DELLA SICUREZZA FUNZIONA SE TUTTI GLI ELEMENTI NE RICONOSCONO IL VALORE.

LA CULTURA DELLA SICUREZZA È IL COLLANTE CHE LO ANIMA, LO CONSOLIDA E LO SOSTIENE.

UNIGUM
THE SAFE SIDE

Molto più di un semplice fornitore di DPI e articoli tecnici: un vero partner per la tua azienda.

La fiducia non si compra, si conquista e si guadagna attraverso un continuo processo di comprensione delle esigenze del cliente e rispetto degli accordi.

Il vero valore aggiunto di UNIGUM si trova nella competenza ed esperienza delle sue persone e nella qualità dei servizi erogati.

UNIGUM S.p.A. - Firenze - Italia

☎ 0558968401

✉ info@unigum.it

🌐 www.unigum.it

📍 82C www.unisafety.it

Una svolta necessaria

Vigilare sull'Accordo Stato-Regioni in materia di formazione. Rafforzare il coordinamento nazionale sulla prevenzione e creare uno standard europeo di sicurezza. Le priorità di AIAS indicate dal presidente Francesco Santi

AIAS (Associazione Italiana Ambiente e Sicurezza) è la prima e più importante associazione tecnico-scientifica costituita da professionisti della sicurezza, che nel 2025 ha festeggiato i suoi primi 50 anni e prosegue oggi la sua opera di valorizzazione delle competenze tecniche-professionali. In occasione della fiera Ambiente Lavoro di Bologna, «Oltre agli eventi realizzati con i nostri partner su temi come l'AI applicata alla sicurezza, Vision Zero e il nuovo quadro normativo, l'iniziativa di punta sarà il lancio del Comitato Nazionale di Controllo sull'applicazione dell'Accordo Stato-Regioni», anticipa il presidente Francesco Santi. «Vogliamo che sia un organismo indipendente promosso da AIAS per monitorare le Regioni nel recepimento della riforma della formazione obbligatoria, offrendo supporto tecnico-scientifico agli enti e garantendo che i contenuti innovativi dell'accordo non vengano dispersi nella frammentazione locale».

Tra le battaglie storiche di AIAS, ci sono l'approccio qualitativo alla formazione e la cultura della sicurezza nelle scuole dell'obbligo. Su quali obiettivi si concentra la vostra azione nel prossimo futuro?

«Le nostre priorità si sviluppano su tre assi. Il primo è rafforzare il ruolo di raccordo tra il mondo reale- cantieri, fabbriche, uffici- e le istituzioni, a livello sia regionale che nazionale. AIAS è nata cinquant'anni fa per dare voce tecnica a chi lavora ogni giorno sulla prevenzione, e questa missione è oggi più urgente che mai. Continueremo a organizzare eventi fisici e online per confrontarci su tutti i temi rilevanti. Il secondo asse è promuovere in Italia Vision Zero, la strategia internazionale ora adottata in Europa e in Italia per i prossimi tre anni: lavoriamo perché diventi cultura diffusa tra imprese, lavoratori e istituzioni. Il terzo asse riguarda il recepimento regionale dell'Accordo Stato-Regioni sulla for-



mazione obbligatoria: dobbiamo monitorare le applicazioni regionali. La prima Regione ha legiferato e ha prodotto un testo che rischia di ridurre la formazione a mero adempimento documentale, vanificando le innovazioni dell'accordo. Se le venti Regioni procedessero ciascuna per conto proprio, ne deriverebbero uno spreco enorme di risorse pubbliche e costi insostenibili per le imprese. In questo momento storico, gli italiani non se lo meritano».

Lei presiede non solo AIAS, ma anche la Federazione delle Associazioni ENSHPO. Uno degli obiettivi è portare il Decalogo per la sicurezza, la Carta di Urbino, in Europa. Quali sfide individua a livello europeo?

«ENSHPO riunisce le associazioni professionali di sicurezza e salute sul lavoro di 17 paesi europei, rappresentando circa 50mila professionisti Hse (salute, sicurezza e ambiente). La sfida più grande è culturale prima ancora che normativa: convincere i Paesi membri che la standardizzazione non è una minaccia alle identità nazionali, ma un'opportunità per valorizzare il meglio di ogni esperienza. Purtroppo, ad esempio, i fenomeni sono già standardizzati: il plateau della prevenzione è, infatti, comune a tutti i paesi europei, così come la difficoltà con la prevenzione nelle Pmi. La Carta di Urbino è già un punto di riferimento riconosciuto in tutta Europa, così come l'approccio Vision Zero. Lavorare per la prevenzione in Europa significa lavorare per profili professionali riconosciuti in tutto il continente, percorsi formativi equivalenti e una raccolta dati armonizzata che consenta confronti affidabili tra paesi. Dobbiamo avere il coraggio di abbandonare i localismi e costruire uno standard europeo che unisca le migliori pratiche dei nostri Paesi. La direzione è quella giusta».

Per arginare morti e feriti sul lavoro ha in-

LA TECNOLOGIA OFFRE OPPORTUNITÀ STRAORDINARIE: DAI SISTEMI DI RILEVAMENTO PRECOCE DEI RISCHI FISICI E CHIMICI, AGLI ESOSCHELETRI CHE PROTEGGONO LA SCHIENA DEGLI OPERAI, AI SISTEMI DI RILEVAMENTO DI COMPORTAMENTI ERRATI, AGLI ALGORITMI CHE ANALIZZANO I DATI STORICI DEGLI INFORTUNI PER IDENTIFICARE PATTERN E PREVENIRLI

dicato la necessità di sviluppare un coordinamento nazionale forte, basato su controlli uniformi ed efficaci, formazione standardizzata e raccolta dati integrata. Vede dei passi in avanti verso questa direzione?

«Dopo un anno, le direttrici restano le stesse. Sul fronte dei controlli: abbiamo in Italia decine di enti preposti alla vigilanza con risorse frammentate. Se in Italia ogni giorno muoiono mediamente due persone sul lavoro- una strage silenziosa- è anche perché i controlli non sono né sistematici né preventivi. Se questo fenomeno avesse le caratteristiche della lotta nazionale come fu per il terrorismo, avremmo già un coordinamento centrale. Serve un'agenzia nazionale che unifichi la vigilanza. Sulla formazione, il rischio concreto è che l'applicazione disomogenea dell'Accordo Stato-Regioni faccia sopravvivere gli «attestifici»- chi rilascia certificazioni senza reale valore formativo- e mantenga viva la percezione della formazione come adempimento inutile, spreco di ingenti risorse. Sul fronte dei dati, qualche passo avanti c'è stato: oggi l'Inail dialoga con l'Inps. Ma bisogna accelerare nella costruzione di un completo sistema informa-

tivo nazionale integrato per la prevenzione. L'Inail potrebbe e dovrebbe essere il soggetto guida di questo percorso».

Quali sono i rischi e le opportunità che derivano dalle nuove tecnologie come l'intelligenza artificiale?

«L'intelligenza artificiale e le tecnologie connesse- IoT, wearable, sensori intelligenti- rappresentano una svolta epocale per la sicurezza sul lavoro. I rischi esistono, ma sono legati a un uso distorto: quando la tecnologia è impiegata unicamente per il controllo o la riduzione dei costi, a scapito della centralità e del rispetto delle persone. Le opportunità, invece, sono straordinarie. Penso ai sistemi di rilevamento precoce dei rischi fisici e chimici, agli esoscheletri che proteggono la schiena degli operai, ai sistemi di rilevamento di comportamenti errati, agli algoritmi che analizzano i dati storici degli infortuni per identificare pattern e prevenirli. L'AI ben governata può trasformare la prevenzione da adempimento burocratico a sistema intelligente di tutela reale delle persone».

• **Francesca Druidi**



Francesco Santi, presidente AIAS

Migliorare la qualità del lavoro

Innovazione tecnologica, sostenibilità, ergonomia e gestione del rischio sono da sempre prerogative di Errebian che, con le sue forniture professionali, si conferma un partner strategico per l'efficienza e il benessere delle imprese

C'è qualcosa che racconta davvero l'identità di Errebian: la capacità di evolversi restando fedele al proprio ruolo, non solo come operatore economico ma come attore consapevole nel tessuto sociale e produttivo.

Dal 1968 a oggi, l'azienda ha attraversato profonde trasformazioni del mondo del lavoro, adattandosi ai cambiamenti organizzativi e tecnologici. Un percorso costruito con investimenti costanti in competenze, innovazione e relazioni, guidato da una visione chiara: essere un partner affidabile, capace di semplificare la complessità.

Oggi Errebian è un interlocutore strutturato che interpreta il proprio sviluppo come parte di un ecosistema più ampio, fatto di persone, aziende e territori. Una visione che si traduce in azioni concrete: modelli organizzativi certificati, iniziative a impatto so-



SUL FRONTE DELL'INNOVAZIONE, ERREBIAN HA SVILUPPATO "ERMES", UNA PIATTAFORMA PROPRIETARIA DI INTELLIGENZA ARTIFICIALE CHE INTEGRA SISTEMI GESTIONALI, CRM E CATALOGHI FORNITORI

gno è documentato da certificazioni come Iso 9001, Iso 14001, Sa8000, Uni P.d.R. 125 e Fsc. Inoltre, l'azienda ha adottato volontariamente i principi della Direttiva Nis2, rafforzando il proprio ruolo di partner affidabile nelle catene di approvvigionamento.

Sul fronte dell'innovazione, Errebian ha sviluppato "Ermes", una piattaforma proprietaria di intelligenza artificiale che integra sistemi gestionali, Crm e cataloghi fornitori.

Consente di migliorare l'esperienza d'acquisto, ottimizzare i processi commerciali e supportare la rete vendita con accesso immediato a informazioni su oltre 1,3 milioni di referenze, oltre a rendere più efficaci le attività di marketing.

Nel percorso evolutivo dell'azienda, l'ergonomia occupa un ruolo centrale come leva strategica per migliorare la qualità del lavoro. L'approccio si basa su prevenzione e

integrazione: non singoli prodotti, ma progettazione consapevole degli ambienti. Sedute ergonomiche, arredi regolabili e accessori dedicati favoriscono posture corrette e riducono l'affaticamento, con benefici su salute ed efficienza. La sicurezza sul lavoro rappresenta uno degli ambiti più strategici dell'offerta Errebian, sviluppato con un approccio che va oltre la semplice fornitura di prodotti e si traduce in una consulenza concreta a supporto delle aziende nella gestione del rischio. L'offerta include il brand Elica Safety, linea proprietaria dedicata ad abbigliamento da lavoro, guanti e calzature di sicurezza, pensata per garantire protezione, comfort e durabilità nelle condizioni operative più impegnative. A completare la proposta, una gamma di abbigliamento professionale con linee corporate e capi multinorma, progettati per ambienti che richiedono protezione simultanea da rischi multipli. Errebian si avvale di partnership consolidate con i principali produttori mondiali del settore, garantendo una selezione certificata e conforme alle normative europee vigenti: dalla protezione della testa agli indumenti ad alta visibilità, dalla protezione delle vie respiratorie ai sistemi anticaduta per i lavori in quota. Su quest'ultimo fronte, l'offerta si estende a un servizio integrato che comprende l'analisi dei rischi, la revisione periodica dei Dpi e la formazione del personale, per una gestione completa e conforme del rischio in quota.

Tra le novità di rilievo, Vivest® Pocket, il defibrillatore tascabile che ridefinisce gli standard della cardioprotezione in azienda, e ROOTFIT®, il wearable per il monitoraggio in tempo reale del rischio termico nei lavori in ambienti caldi o all'aperto.

• **Cristiana Golfarelli**

La sede di Errebian a Pomezia



ciali e attenzione alla valorizzazione delle risorse umane.

Questa identità si riflette in un'offerta ampia e integrata: forniture per ufficio, igiene e pulizia, arredo, soluzioni tecnologiche, dispositivi per la sicurezza e il benessere, abbigliamento professionale. Oltre 100.000 referenze pensate per offrire soluzioni coordinate e facili da gestire.

La sostenibilità è oggi un pilastro strategico. Le certificazioni in ambito qualità, ambiente e responsabilità sociale rappresentano un percorso strutturato e misurabile. I principi Esg guidano decisioni e strategie, confermando un impegno trasversale a tutta l'organizzazione.

Innovazione, sostenibilità e affidabilità definiscono il modello Errebian. Questo impe-



Una fase di estremo dinamismo

Grazie a tecnologie più avanzate e una spinta sul piano normativo verso una maggior resilienza aziendale, l'industria della sicurezza fisica e informatica degli edifici allunga la scia della crescita. Il punto di Andrea Monteleone

Con tassi di crescita che superano puntualmente il 10 per cento annuo, già da qualche tempo il mercato fire&security sta vivendo una fase di estremo dinamismo. Registrando un andamento che si può definire anticiclico rispetto alla situazione geopolitica attuale, e decisamente più maturo in termini di cultura aziendale. Specie alla luce dell'introduzione a livello europeo delle nuove normative NIS2, CER e CRA, che per la prima volta puntano a uniformare le regole e rafforzare la resilienza e la sicurezza informatica nei Paesi della Ue. «In questo scenario - sottolinea Andrea Monteleone, presidente di Anie Sicurezza - i settori dell'antincendio e della videosorveglianza risultano i più brillanti in termini di fatturato, grazie a dinamiche che si possono definire strutturali».

In virtù di quali fattori si stanno segnalando come locomotive dell'industria italiana della fire&security?

«Nel caso del fire, la crescita è determinata dall'evoluzione normativa e dalla ricerca sempre più spinta di soluzioni integrate e ad alta affidabilità; per quanto concerne invece la videosorveglianza, il trend positivo è legato alla transizione in atto da un approccio basato sulla "sicurezza" a quello basato sulla "resilienza", frutto anche qui di un nuovo assetto normativo».

Quali dispositivi dominano il panorama della videosorveglianza e in quali ambiti applicativi prevalenti?

«Il termine videosorveglianza, per certi versi, è diventato obsoleto per descrivere un mercato dove sensori termici, ottici, radar, sistemi di analisi automatici, metadati, intelligenza artificiale e computer vision concorrono a comporre sistemi sempre più pervasivi, evoluti e flessibili. Non mi soffermerei quindi su di uno specifico dispositivo,



I SETTORI DELL'ANTINCENDIO E DELLA VIDEOSORVEGLIANZA RISULTANO I PIÙ BRILLANTI IN TERMINI DI FATTURATO, GRAZIE A DINAMICHE CHE SI POSSONO DEFINIRE STRUTTURALI

quanto piuttosto sul fatto che tecnologie più o meno consolidate vengano utilizzate con modalità, finalità e in ambiti differenti rispetto a quanto fatto finora con l'approccio di tipo tradizionale».

La direttiva europea NIS2 sta ridisegnando in modo radicale l'approccio con cui le imprese italiane devono fare e garantire la cybersecurity. Quali sono i nuovi comportamenti che prescrive?

«La NIS2 è uno dei tasselli fondamentali di un quadro normativo molto più ampio e articolato che la Comunità Europea ha introdotto per affrontare in modo coerente e coordinato la complessità all'interno della quale, volenti o nolenti, operiamo. L'approccio della NIS2 è di tipo risk-based e non si li-

mita a definire una serie di prescrizioni tecniche minime da soddisfare, ma impone alle aziende una ridefinizione dei modelli di gestione interna, dell'assegnazione delle responsabilità, della formazione del personale e della scelta e gestione dei fornitori. Inoltre - e questo è un tema molto importante - impone tempi rapidi per la comunicazione di eventuali incidenti informatici alle Autorità preposte, in un'ottica di consapevolezza diffusa e massima collaborazione all'interno del "sistema Paese».

In una cornice regolatoria così mutevole, la formazione dei professionisti è la chiave di volta per rimanere sulla cresta. Quali sono i principali focus tematici dei vostri attuali percorsi formativi?

«La formazione è diventata, se possibile, ancora più essenziale proprio in virtù della complessità richiamata in precedenza e di un contesto normativo sempre più articolato. Il nostro focus è indirizzato alla qualifica dei Tecnici Manutentori in ambito IRAI ed EVAC, alla formazione su CEI 79-3:2025 e DM 37/08 per il mondo dell'antintrusione così come alla divulgazione sulla corretta implementazione della UNI 11988:2025 per i sistemi di allarme vocale per scopi di emergenza. E questa è solo una parte delle attività, perché ci sono molti altri temi che richiedono approfondimenti sempre più mirati, sviluppati ed erogati secondo criteri di eccellenza».

Nel campo della protezione delle infrastrutture critiche, che sviluppi si preve-

dono in termini di convergenza tra sicurezza fisica e digitale?

«Qui il tema meriterebbe una trattazione a parte, data la sua ampiezza. Il concetto di convergenza tra sicurezza fisica e digitale si traduce, in concreto, nell'applicazione di due Direttive europee e dei relativi atti di recepimento nazionali: la NIS2, già citata, per la parte cyber e la meno nota, ma altrettanto rilevante, CER (Critical Entities Resilience Act), da non confondere con le comunità energetiche rinnovabili».

A quali traiettorie evolutive devono prepararsi le imprese?

«La traiettoria che si delinea è quella che porta a governare con consapevolezza i due contesti, mettendo a fattor comune tutte le professionalità disponibili, sia da parte delle entità critiche che da parte di tutte le loro filiere di fornitura, in uno sforzo congiunto e coordinato. Idea all'apparenza utopica, ma ai più attenti non sarà sfuggito che è proprio questo l'obiettivo fissato nei due testi normativi».

• **Gaetano Gemiti**



Andrea Monteleone, presidente di Anie Sicurezza

Verifiche elettriche, misura e conformità

L'ingegnere Corrado De Francesca, partner di MA.DE. Engineering, analizza l'evoluzione delle attività ispettive nel settore elettrico, tra prescrizioni normative, complessità degli impianti e qualità della misura

La sicurezza degli impianti elettrici è un ambito in cui aspetti normativi, tecnici e organizzativi sono strettamente collegati. Nei contesti industriali, sanitari, infrastrutturali e produttivi, la verifica degli impianti non riguarda soltanto il rispetto di un obbligo previsto dalla legge, ma anche la capacità di individuare condizioni di rischio, anomalie di funzionamento e criticità che possono incidere sulla continuità di esercizio.

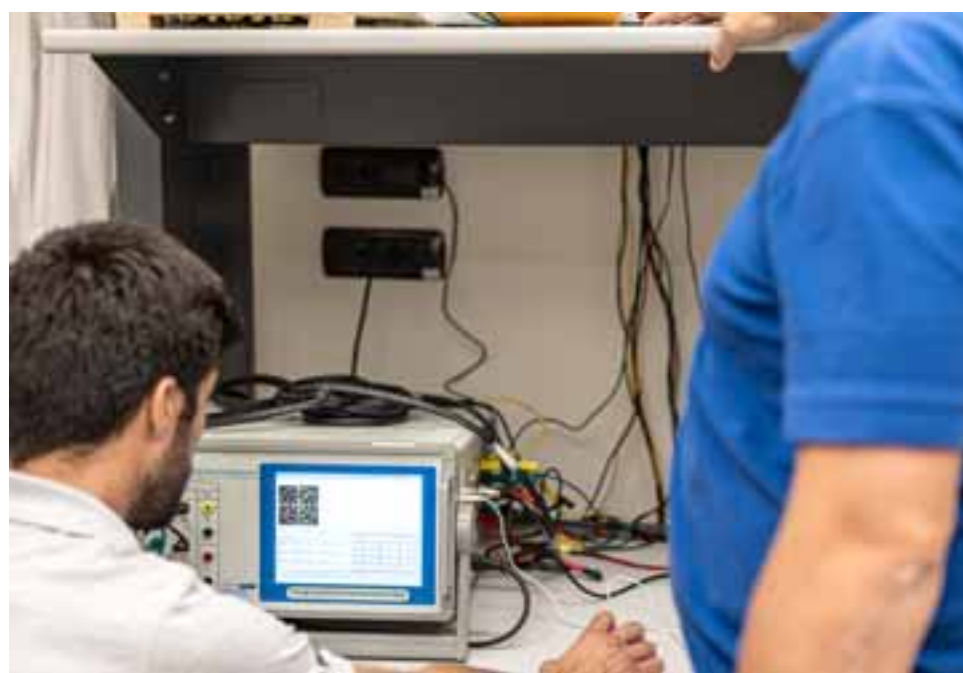
Negli ultimi anni, l'evoluzione delle reti elettriche, l'integrazione di sistemi di generazione distribuita, la diffusione di apparati più complessi e l'aggiornamento delle norme tecniche hanno reso le attività di verifica sempre più articolate. In questo quadro, gli organismi tecnici sono chiamati a operare con procedure definite, strumenti adeguati e competenze specialistiche.

MA.DE. Engineering opera in questo settore dal 1995, dopo un percorso professionale avviato già negli anni Sessanta nell'ambito dell'elettrotecnica e delle reti elettriche. L'esperienza maturata dall'azienda consente di osservare l'evoluzione del comparto da una prospettiva tecnica e operativa.

«Nel tempo il settore è cambiato profondamente - spiega l'ingegnere Corrado De Francesca, partner di MA.DE. Engineering - . Le verifiche non possono più essere considerate attività isolate o puramente documentali. Oggi richiedono conoscenza degli impianti, capacità di interpretare le norme e attenzione alla qualità del dato misurato».

Come è cambiato il tema della sicurezza elettrica negli ultimi anni?

«È cambiato soprattutto il livello di complessità. Gli impianti sono più estesi, più interconnessi e spesso integrano sistemi di automazione, generazione e controllo che richiedono un approccio diverso rispetto al passato. La verifica



deve partire da elementi oggettivi: documentazione disponibile, configurazione reale dell'impianto, misure effettuate, riscontri sul campo. Il punto non è soltanto stabilire se un impianto risponde formalmente a una prescrizione, ma comprendere se le condizioni effettive siano coerenti con i requisiti di sicurezza previsti. In questo senso, l'indipendenza dell'organismo di ispezione ha un ruolo importante. La valutazione deve basarsi su criteri tecnici, non su interpretazioni generiche o su esigenze contingenti del committente».

Quali sono oggi le principali aree di intervento nel settore delle verifiche elettriche?

«Le attività possono essere distinte in ambiti differenti. Un primo ambito riguarda le verifiche previste dal Dpr 462/01, quindi impianti di terra, dispositivi di protezione contro le scariche atmosferiche e impianti elettrici in ambienti con pericolo di esplosione. Sono controlli re-

golati, che interessano direttamente la sicurezza nei luoghi di lavoro. Un secondo ambito riguarda le misure e le verifiche elettriche specialistiche. Qui svolgiamo attività complesse come prove circuitali, verifiche funzionali, analisi dei disservizi e attività di connessione alla rete secondo le norme Cei 0-16 e Cei 0-21. Operiamo su generatori, trasformatori, motori e reti At/Mt con strumentazioni avanzate e personale altamente qualificato, con professionalità sempre riconosciuta dai grandi produttori e distributori di energia elettrica. C'è poi il tema metrologico. La qualità della misura dipende anche dalla qualità dello strumento utilizzato. Per questo la taratura e la conferma metrologica degli strumenti sono aspetti spesso meno visibili, ma fondamentali».

Perché la metrologia è così rilevante nelle attività di verifica?

«Perché ogni valutazione tecnica si fonda su dati misurati. Se lo strumento non è affidabile, anche il risultato della verifica può essere compromesso. La taratura serve a stabilire il comportamento dello strumento rispetto a riferimenti noti e tracciabili. Un elemento importante è l'incertezza di misura. Non basta ottenere un valore: bisogna sapere con quale margine quel valore può essere considerato attendibile. Questo è particolarmente rilevante quando le misure incidono su valutazioni di conformità, decisioni operative o analisi di anomalie. La metrologia, quindi, non è un'attività accessoria. È parte del processo tecnico che consente di dare solidità ai risultati di una verifica».

Quali competenze sono richieste oggi a un

tecnico che opera in questo ambito?

«Le competenze sono più trasversali rispetto al passato. Servono conoscenze sugli impianti elettrici, sulle norme tecniche, sulle procedure ispettive, sugli strumenti di misura e sulla qualità dell'energia. In molti casi il tecnico deve anche saper leggere fenomeni non immediatamente evidenti: squilibri, disturbi, disservizi, comportamenti anomali della rete o degli apparati. La capacità di analisi è diventata centrale. La strumentazione è certamente importante, ma da sola non basta. Il dato va raccolto correttamente, validato e interpretato. È qui che la competenza tecnica fa la differenza».

Quali sono le criticità più frequenti che emergono nelle attività di verifica?

IL NOSTRO OBIETTIVO È CONTRIBUIRE CONCRETAMENTE AL MIGLIORAMENTO DEI PROCESSI AZIENDALI DEI CLIENTI, AIUTANDOLI A OPERARE IN MODO PIÙ SICURO, EFFICIENTE E CONFORME ALLE NORMATIVE

«Una criticità ricorrente riguarda la distanza tra la documentazione disponibile e lo stato reale dell'impianto. Nel tempo gli impianti vengono modificati, ampliati o adattati, ma non sempre la documentazione viene aggiornata con la stessa continuità. Un altro aspetto riguarda la percezione della verifica come adempimento periodico, da svolgere e archiviare. In realtà, l'esito di una verifica dovrebbe essere letto come un'informazione tecnica utile per gestire l'impianto nel tempo. Infine, c'è il tema della manutenzione. Alcune condizioni di rischio non nascono da un errore iniziale di progettazione, ma dal degrado progressivo dei componenti, dall'uso dell'impianto o da modifiche intervenute successivamente».

•Gaia Santi

L'ingegnere Corrado De Francesca, partner di MA.DE. Engineering



DPR 462/01 E ORGANISMI DI ISPEZIONE ACCREDITATI

MA.DE. Engineering è riconosciuta dal Ministero delle Imprese e del made in Italy come organismo abilitato ai sensi del Dpr 462/01. Questo riconoscimento attesta competenze tecniche, indipendenza operativa e conformità a rigorosi standard qualitativi. Le verifiche previste dalla normativa sono fondamentali per garantire la sicurezza degli impianti elettrici nei luoghi di lavoro, inclusi impianti di terra, sistemi di protezione contro le scariche atmosferiche e ambienti a rischio di esplosione. L'accreditamento Accredia secondo la norma Eni Cei En Iso/lec 17020 garantisce inoltre affidabilità, tracciabilità e qualità delle procedure ispettive.

Le persone al centro

Le imprese oggi si trovano ad affrontare sfide sempre più complesse legate alla formazione continua, alla sostenibilità sociale, alla retention dei talenti e alla qualità degli ambienti lavorativi. La consulenza tecnica diventa quindi un'attività strategica che accompagna le aziende non solo nella conformità normativa ma anche nella crescita culturale e organizzativa. È dentro questa trasformazione che prende forma la storia di Rischio Zero e di SempliceMente, due progetti nati da un'intuizione semplice ma ambiziosa: mettere al centro le persone.

La storia comincia nel 2022, lontano dai grandi investimenti iniziali e dai modelli imprenditoriali costruiti a tavolino. A dare vita al progetto è Tommaso Dal Bianco, giovane laureato specializzato in sicurezza e salute sul lavoro, che decide di trasformare competenze tecniche, studio e visione professionale in una realtà concreta. All'inizio non esiste una struttura aziendale, non ci sono uffici moderni né team numerosi. Esiste sol-

La crescita di Rischio Zero e il progetto SempliceMente raccontano un modello imprenditoriale che unisce sicurezza sul lavoro, benessere organizzativo, formazione, inclusione e valorizzazione delle persone



IL PROGETTO SEMPLICEMENTE HA L'OBIETTIVO DI INTRODURRE NELLE AZIENDE UNA NUOVA CULTURA ORGANIZZATIVA CENTRATA SUL BENESSERE DELLE PERSONE, SULLE RELAZIONI INTERNE E SULLA CRESCITA SOCIALE DELLE IMPRESE

tanto una soffitta di casa, trasformata in spazio operativo, dove tra documenti, corsi di formazione e consulenze nascono le prime collaborazioni con le aziende del territorio. Le giornate scorrono tra telefonate, sopralluoghi e pratiche preparate fino a tarda sera. L'obiettivo non è soltanto offrire consulenza tecnica, ma costruire un approccio diverso, più vicino alle imprese e soprattutto più umano. La crescita arriva lentamente, alimentata dal passaparola, dalla fiducia conquistata sul campo e da un metodo di lavoro fondato sulla presenza costante e sull'ascolto delle esigenze reali delle aziende. Dopo pochi mesi, nel progetto entra anche Giada Deganello, scegliendo di lasciare il proprio percorso professionale per dedicarsi completamente a quella che inizialmente appare ancora come una scommessa. È un passaggio decisivo, non solo dal punto di vista operativo, ma anche umano. Insieme, Tommaso e Giada iniziano a costruire l'identità più autentica di Rischio Zero.

La soffitta lascia spazio a un piccolo ufficio condiviso, con una sola scrivania, poche comodità e giornate senza orari definiti. È in quel contesto essenziale che il progetto cambia passo. Crescono le responsabilità, aumentano i clienti e si consolidano le com-

petenze. Ma soprattutto prende forma una filosofia precisa: sicurezza sul lavoro significa tutela concreta delle persone prima ancora che semplice rispetto delle norme. Negli anni successivi Rischio Zero amplia progressivamente i propri servizi, occupandosi oggi di consulenza in materia di sicurezza sul lavoro, incarichi di RSPP esterno, formazione aziendale, valutazione dei rischi e certificazioni aziendali. Parallelamente, cresce anche la struttura organizzativa.

Accanto all'attività legata alla sicurezza prende forma anche SempliceMente, progetto ideato da Giada con l'obiettivo di introdurre nelle aziende una nuova cultura organizzativa centrata sul benessere delle persone, sulle relazioni interne e sulla crescita sociale delle imprese.

L'iniziativa nasce dall'ascolto quotidiano delle esigenze di imprenditori e lavoratori e si sviluppa attraverso servizi HR, percorsi formativi, consulenze organizzative e progetti dedicati alla valorizzazione delle risorse umane. L'idea di fondo è chiara: un'azienda cresce davvero soltanto quando crescono anche le persone che ne fanno parte.

Per questo motivo SempliceMente lavora sui temi della cultura aziendale, dell'inclusione, della comunicazione interna e del benessere

organizzativo, accompagnando le imprese in percorsi concreti di evoluzione culturale. Particolare attenzione viene dedicata anche ai progetti legati alla certificazione della parità di genere, attraverso i quali le aziende vengono supportate nella costruzione di modelli organizzativi più equi, inclusivi e so-

stenibili.

Un'attività che non si limita agli aspetti normativi, ma punta a generare un cambiamento reale all'interno dei luoghi di lavoro, promuovendo maggiore consapevolezza e nuove modalità di gestione delle persone. Grande attenzione viene riservata anche alla formazione delle nuove generazioni. Tommaso e Giada collaborano infatti con scuole e percorsi educativi come docenti e formatori, convinti che la cultura della sicurezza e del benessere debba nascere prima di tutto dalla conoscenza, dalla sensibilizzazione e dall'educazione dei più giovani. Oggi Rischio Zero rappresenta una realtà in continua evoluzione, capace di crescere mantenendo intatto lo spirito degli inizi. Quello di chi ha creduto in un progetto quando esisteva soltanto una scrivania in una soffitta. Quello di chi ha costruito ogni traguardo attraverso sacrificio, notti insonni e scelte coraggiose. Perché ci sono aziende che nascono semplicemente per fare impresa. E altre che scelgono di costruire valore lasciando un segno concreto nelle persone e nei luoghi di lavoro.

•Beatrice Guarnieri

Giada Deganello, socia di Rischio Zero e fondatrice di SempliceMente, e Tommaso Dal Bianco, fondatore di Rischio Zero



UNA REALTÀ IN CRESCITA

Da due anni Rischio Zero opera nella nuova sede di Zanè, uno spazio moderno e strutturato che rappresenta il simbolo tangibile di un percorso costruito passo dopo passo. A rafforzare il team sono arrivate nuove figure professionali come Michela Sauro, responsabile della formazione, e Alessandro Marchioro, impegnato nell'ufficio tecnico a supporto delle attività consulenziali e operative. Attorno al nucleo interno si è sviluppata inoltre una rete composta da circa venti professionisti selezionati, coinvolti per garantire elevati standard qualitativi e un supporto multidisciplinare alle aziende.

Organizzazione e responsabilità

Le morti sul lavoro non sono frutto di mancanze individuali: «serve una cultura della sicurezza sostanziale, non solo burocratica».

L'avvocato Rolando Dubini analizza riforme, criticità e prospettive della prevenzione

È ormai trascorso un anno dall'entrata in vigore dell'Accordo Stato-Regioni sulla formazione in materia di salute e sicurezza sul lavoro. Facciamo il punto con Rolando Dubini, avvocato penalista, cassazionista, docente e formatore esperto in queste materie, sulle principali novità legislative e sui nodi strutturali ancora da affrontare. «L'Accordo, pubblicato in Gazzetta Ufficiale il 24 maggio 2025, conclude il periodo transitorio il 24 maggio 2026. Da tale data, i corsi dovranno essere integralmente conformi alle nuove regole. Per i corsi avviati prima, secondo i previgenti Accordi, vale il principio tempus regit actum».

Quali sono gli elementi più innovativi introdotti dall'Accordo Stato-Regioni? E quali profili di criticità invece riscontra?

«Sono quattro le innovazioni principali. Innanzitutto, l'obbligo formativo per il datore di lavoro (16 ore), che colma un vuoto rilevante: prima del 2025, il datore non Rspp (Responsabile servizio prevenzione e protezione) non aveva un percorso definito, mentre ora deve acquisire "competenze organizzative, gestionali e giuridiche", superando "una visione formale della materia a favore di una visione sostanziale". Poi la verifica obbligatoria dell'apprendimento contest, colloqui e prove pratiche: non basta più la mera frequenza. Quindi la verifica di efficacia durante la prestazione lavorativa, con analisi infortunistica, questionari e check list, da riportare nella riunione periodica. Infine, il rafforzamento dei contenuti pratici: rapporto docente/discendente massimo 1:6 e metodologie didattiche attive obbligatorie (lavori di gruppo,



casi di studio, simulazioni, realtà virtuale). La criticità riguarda l'entrata in vigore: l'Accordo la fissa alla pubblicazione in G.U. (24 maggio), ma il Ministero ha diffuso indicazioni che la ancorano al 19 maggio. Cinque giorni di scarto possono incidere su scadenze e validità di atti, generando incertezza applicativa».

Come valuta le novità della L. 198/2025 su formazione, tracciabilità e near miss, ossia mancati infortuni?

«La L. 198/2025 prosegue il rafforzamento avviato dalla L. 215/2021. Sul fronte tracciabilità, accelera il fascicolo elettronico ex art. 14D.Lgs. 150/2015, già richiamato dall'art. 37 comma 14 D.Lgs. 81/2008: gli organi di vigilanza verificano in tempo reale gli adempimenti formativi. La Cassazione (sentenza 16865/2024) ha chiarito che la formazione deve precedere l'adibizione alle mansioni e non può essere surrogata dal "Travaso di conoscenza tra lavoratori". Quando sarà operativa la tracciabilità digitale, renderà questo principio finalmente verificabile in modo oggettivo, impedendo regolarizzazioni retroattive. Sul near miss, la legge introduce un obbligo strutturato di rilevazione e analisi, sistematizzando quanto l'Accordo Stato Regioni 2025 già prevede includendo i "mancati infortuni" tra gli indicatori dell'analisi infortunistica aziendale. L'approccio è corretto: il near miss è il più potente predittore dell'infortunio. Resta il nodo culturale: se le segnalazioni non si traducono in azioni correttive, il sistema è inefficace. Serve una cultura organizzativa che valorizzi chi segnala».

Come si integrano D.Lgs. 81/2008 (Testo Unico Sicurezza sul lavoro) e la?

cordo sindacale o autorizzazione INL: la Cassazione (sent. 38882/2018) ha affermato che "il consenso del lavoratore, in qualsiasi forma prestato, non vale a scriminare la condotta del datore di lavoro". Serve dunque un bilanciamento: l'la è lecita se trasparente, proporzionata e accompagnata da supervisione umana».

Ha scritto che le morti bianche non sono frutto di disattenzioni individuali, sono conseguenza di disorganizzazione aziendale e di omissioni negli obblighi di legge. Quali restano le fragilità della cultura della sicurezza e della prevenzione nel nostro Paese?

«Le fragilità persistono. La sicurezza è ancora percepita come costo e non come investimento. Troppe aziende si fermano alla compliance cartolare: il Dvr (Documento Valutazione rischi) formalmente completo ma inattuato; formazione erogata ma non

L'INTELLIGENZA ARTIFICIALE OFFRE GRANDI OPPORTUNITÀ: ANALISI PREDITTIVA DEI RISCHI INCROCIANDO DATI SU INFORTUNI E NEAR MISS; MONITORAGGIO REAL-TIME CON SENSORI IOT E ALERT AUTOMATICI; FORMAZIONE IMMERSIVA CON REALTÀ VIRTUALE, SENZA ESPOSIZIONE A RISCHI REALI; ASSISTENZA AI PREPOSTI NELLA VIGILANZA TRAMITE COMPUTER VISION

Quali sono i rischi e le opportunità nell'applicare questa tecnologia alla sicurezza sul lavoro?

«L'integrazione è governata dal Regolamento Ue 2024/1689 (Ai Act), che classifica ad alto rischio i sistemi di monitoraggio dei lavoratori, e dalla L.132/2025, che impone all'la di essere "sicura, affidabile, trasparente" e vieta che operi "in contrasto con la dignità umana". L'la offre grandi opportunità: analisi predittiva dei rischi incrociando dati su infortuni e near miss; monitoraggio real-time con sensori IoT e alert automatici; formazione immersiva con realtà virtuale, senza esposizione a rischi reali; assistenza ai preposti nella vigilanza tramite computer vision. Ma la posizione di garanzia è del datore (Cass. pen. 4361/2015: "è costituito garante dell'incolumità fisica dei prestatori di lavoro") e non è delegabile a un algoritmo. Chi si affida ciecamente all'la senza verificarne l'affidabilità risponde penalmente. Inoltre, sistemi di videosorveglianza pervasiva violano l'art. 4 dello Statuto Lavoratori se installati senza ac-

verificata; preposti nominati ma senza effettivi poteri di intervento. Le Pmi spesso non dispongono delle risorse per implementare sistemi di gestione adeguati e di segnalazione: in troppi contesti chi identifica un pericolo è percepito come elemento problematico».

In quale direzione attuare il necessario cambio di passo?

«Serve il passaggio dalla compliance formale a quella sostanziale, con controlli ispettivi che accertino l'effettività e non solo l'esistenza dei documenti; l'integrazione tra sicurezza e organizzazione aziendale; la promozione di una cultura della prevenzione che parta dalla formazione scolastica e accompagni il lavoratore per tutta la vita lavorativa, interiorizzando la sicurezza come valore e non come vincolo. La Cassazione (sent. 2084/2024) ha affermato che la tutela del lavoratore "non ammette sconti in ragione di fattori quali ineluttabilità, fatalità, fattibilità economica e produttiva". Le scelte organizzative devono essere valutate per il loro impatto prevenzionale» • **Francesca Druidi**



Rolando Dubini, avvocato penalista e cassazionista

Potenziare l'attività dell'operatore in officina

Evomach introduce soluzioni avanzate per la lavorazione della lamiera integrando tecnologie innovative come gli esoscheletri industriali che supportano il lavoro umano e migliorano i processi produttivi. Ne parliamo con Renato Gastaldo e Pietro Merlino

Nella lavorazione della lamiera e nella meccanica industriale, l'innovazione non riguarda più solo le macchine, ma l'intero ecosistema produttivo: dalla configurazione degli impianti fino alla sicurezza e al benessere degli operatori. Sotto la guida di Renato Gastaldo e Pietro Merlino, Evomach affianca le aziende non come semplice rivenditore, ma come partner tecnico nella scelta di soluzioni su misura per la produzione e per la salute in officina.

Evomach si presenta come un operatore "non tradizionale" nel settore della lavorazione della lamiera. Qual è la vostra differenza sostanziale rispetto a un rivenditore classico?

Renato Gastaldo: «La differenza sta nell'approccio, che non è mai orientato al prodotto ma al processo. Un rivenditore tradizionale parte da una macchina e cerca il cliente giusto. Noi facciamo l'opposto: partiamo dal cliente, dal suo flusso produttivo reale, da come entra la materia prima e da come esce il pezzo finito. Analizziamo ogni fase, inclusi i passaggi spesso trascurati come movimentazione, finitura, preparazione alla saldatura e logistica interna. Questo ci permette di evitare soluzioni standardizzate che, nella maggior parte dei casi, generano inefficienze nascoste. Se una macchina non è coerente con il processo, semplicemente non la proponiamo. È una scelta controcorrente, ma nel medio periodo crea più valore per l'azienda cliente».

In questo modello di consulenza avanzata, dove si inserisce il tema dell'esoschele-



tro industriale?

Pietro Merlino: «Si inserisce in modo naturale, perché il nostro concetto di impianto non si limita alla macchina ma include l'operatore. L'Ekso EVO sviluppato da Ekso Bionics rappresenta proprio questo passaggio: considerare il corpo umano come parte integrante del sistema produttivo. In molte lavorazioni della lamiera - penso alla piegatura, alla saldatura, alla verniciatura o alla movimentazione dei pezzi - l'operatore è sottoposto a carichi ripetitivi e posture non sempre ottimali. L'esoscheletro non sostituisce nulla, ma redistribuisce lo sforzo, riduce il carico articolare e muscolare e permette di mantenere prestazioni costanti lungo tutta la giornata. È importante chiarire che non stiamo parlando di un concetto futuristico, ma di una tecnologia già applicabile oggi, con benefici misurabili in termini di fatica percepita e continuità operativa».

Dal punto di vista applicativo, in quali contesti avete visto i risultati più interessanti?

R.G.: «I risultati più evidenti emergono nei lavori ripetitivi e prolungati, soprattutto dove l'operatore lavora con le braccia sollevate o in posizioni statiche. Nella lavorazione della lamiera questo accade spesso: penso alla verniciatura, alla saldatura su grandi carpenterie o alla manipolazione di componenti prima e dopo la piegatura. Abbiamo osservato che, quando l'operatore riduce lo sforzo fisico, aumenta la precisione nei gesti e diminuisce la variabilità del risultato. Questo ha un impatto diretto sulla qualità del prodotto finito. Inoltre, il beneficio non è solo individuale ma orga-

nizzativo: meno affaticamento significa meno pause non programmate e maggiore continuità del ciclo produttivo».

In Italia, però, queste tecnologie fanno ancora fatica a essere adottate. Da cosa dipende questa resistenza?

P.M.: «Ci sono due fattori principali. Il primo è culturale: l'idea che un supporto tecnologico possa "aiutare" l'operatore viene ancora percepita, in alcuni contesti, come una diminuzione del ruolo professionale. In realtà è il contrario, perché riduce il margine di errore e migliora la qualità del lavoro manuale. Il secondo fattore è economico, ma spesso male interpretato. Un esoscheletro viene visto come costo aggiuntivo, mentre dovrebbe essere valutato come investimento sulla continuità operativa e sulla riduzione del rischio di fermo legato a infortuni o affaticamento cronico. Nei sistemi produttivi moderni, il costo vero non

è l'acquisto ma l'inefficienza».

L'Ekso EVO è anche certificato e inquadrato come Dpi. Quanto conta questo aspetto per le aziende?

R.G.: «È molto importante, perché rende lo strumento immediatamente integrabile nei sistemi aziendali senza ambiguità normative. Essendo certificato secondo la Direttiva Europea 2016/425 come dispositivo di protezione individuale, può essere inserito nei protocolli aziendali di prevenzione.

Inoltre, rientrare in strumenti di incentivazione come i bandi Inail Isi significa trasformare una scelta tecnologica in una decisione anche fiscalmente sostenibile. Questo accelera l'adozione, ma soprattutto aiuta le aziende a vede-

IL NOSTRO CONCETTO DI IMPIANTO NON SI LIMITA ALLA MACCHINA MA INCLUDE L'OPERATORE. L'EKSO EVO SVILUPPATO DA EKSO BIONICS CONSIDERA IL CORPO UMANO COME PARTE INTEGRANTE DEL SISTEMA PRODUTTIVO

re il progetto nella sua interezza, non come un accessorio».

Guardando avanti, pensa che questi sistemi diventeranno parte integrante delle officine?

P.M.: «Sì, ma non in modo immediato e non in modo uniforme. Succederà per gradi. Le aziende più strutturate e quelle con maggiore pressione produttiva saranno le prime ad adottarli, perché vedono subito il ritorno in termini di stabilità operativa. Nel medio periodo, però, credo diventerà difficile immaginare alcune lavorazioni manuali senza supporti ergonomici. Non perché la tecnologia sostituirà il lavoro umano, ma perché renderà sostenibile ciò che oggi è sempre più complesso mantenere nel tempo». •Beatrice Guarnieri

Renato Gastaldo e Pietro Merlino, soci di Evomach



TECNOLOGIE ADATTE A REQUISITI SPECIFICI

Evomach si fonda sull'esperienza trentennale dei soci, Renato Gastaldo e Pietro Merlino, nel settore dei macchinari per la lavorazione della lamiera.

L'obiettivo è quello di differenziare e innalzare il livello del servizio rispetto al tradizionale fornitore di macchine piegatrici, affiancandosi ai clienti come partner tecnico e consulenziale. Nessuna soluzione viene proposta senza una preventiva analisi approfondita delle esigenze e uno studio di fattibilità. L'approccio è orientato all'individuazione della tecnologia più adatta a soddisfare requisiti specifici, risolvere criticità operative e semplificare l'attività lavorativa quotidiana.



MEDIWORK
SICUREZZA E SALUTE NEI LUOGHI DI LAVORO



**WORK
SAFETY**

MEDIWORK, PROFESSIONISTI AL FIANCO DELLE AZIENDE

Società di consulenza aziendale specializzata in sicurezza sul lavoro, formazione, medicina del lavoro, privacy e gestione documentale.

Dal 1999 affianchiamo imprese, datori di lavoro e professionisti nella gestione degli adempimenti previsti dal D.Lgs. 81/08, con un approccio tecnico, concreto e orientato alla continuità operativa. Offriamo soluzioni integrate per la prevenzione dei rischi nei luoghi di lavoro: valutazione dei rischi, redazione DVR, incarichi RSPP, sopralluoghi tecnici, procedure aziendali, piani di emergenza, formazione obbligatoria, sorveglianza sanitaria e supporto nella scelta dei dispositivi di protezione individuale.

La nostra attività nasce da un principio semplice: la sicurezza non deve essere solo un obbligo normativo, ma uno strumento di organizzazione, controllo e crescita aziendale.

Mediwork punta su competenza, aggiornamento normativo e digitalizzazione dei processi, per rendere la gestione della sicurezza più chiara, accessibile e misurabile.

Dalla consulenza alla formazione, dalla medicina del lavoro alla gestione delle scadenze: un unico partner per aziende più sicure, organizzate e consapevoli.

Mediwork srl

📍 Sede legale e operativa
Via della Regione 9/A
90041 Balestrate (PA)

✉ info@mediwork.it
☎ 0918945079
🌐 www.mediwork.it

Innovazione, prevenzione e cultura del rischio

Abbiamo incontrato Jacopo Marchese, fondatore dell'azienda HSEGAS – Gestione Ambiente Sicurezza, per approfondire visione, metodologia e sfide future di un settore sempre più strategico per il sistema produttivo italiano: la gestione di sicurezza, salute e ambiente

HSEGAS – Gestione Ambiente Sicurezza è specializzata nell'analisi, prevenzione e gestione dei rischi lavorativi e ambientali attraverso un approccio multidisciplinare che integra competenze tecniche, scientifiche e organizzative. L'azienda opera su scala nazionale sviluppando soluzioni personalizzate per imprese pubbliche e private, con l'obiettivo di semplificare processi complessi e trasformare gli obblighi normativi in strumenti di efficienza aziendale. Dall'applicazione del D.Lgs. 81/08 ai modelli organizzativi previsti dal D.Lgs. 231/01, fino alla gestione ambientale e alla medicina del lavoro, HSEGAS costruisce percorsi su misura capaci di armonizzare prevenzione, formazione, innovazione tecnologica e governance, come spiega il fondatore Jacopo Marchese.

HSEGAS nasce in un settore altamente tecnico e normativamente articolato. Qual è stata la visione iniziale che ha guidato la creazione dell'azienda?

«La nostra realtà nasce da un'esperienza familiare che affonda le proprie radici nel 1976. Da sempre la nostra famiglia opera nel campo della prevenzione e della sicurezza negli ambienti di lavoro, inizialmente all'interno degli enti di controllo e, successivamente, nell'attività di supporto e consulenza alle organizzazioni. Abbiamo ereditato una visione costruita attraverso il diretto confronto con gli organi di vigilanza e accompagnata da una profonda conoscenza dell'evoluzione normativa italiana in materia di sicurezza sul lavoro. Un percorso che parte dal D.P.R. 547 del 1955, una delle prime grandi normative di riferimento per la prevenzione e la sicurezza in Italia, fino ad arrivare all'attuale Decreto Legislativo 81 del 2008. Nel corso degli anni abbiamo seguito da vicino l'evoluzione delle norme e la loro applicazione concreta all'interno delle organizzazioni, maturando competenze trasversali nei diversi settori produttivi. Questa esperienza ci ha permesso di sviluppare un approccio fondato non solo sulla conformità normativa, ma anche sulla capacità di interpretare le esigenze delle aziende e accompagnarle nella costruzione di ambienti di lavoro sempre più sicuri ed efficienti».

Qual è il vostro approccio alla sicurezza e alla tutela della persona?

«Oggi continuiamo a operare in un conte-



sto fortemente regolamentato, caratterizzato da normative prescrittive che rappresentano un riferimento imprescindibile per tutte le organizzazioni. Tuttavia, ciò che le aziende stanno vivendo è anche un importante cambiamento culturale: il rispetto della norma non è più percepito come un semplice adempimento, ma come il punto di partenza di un percorso più ampio orientato al benessere della persona».

Questo cosa comporta?

«La tutela della salute e il miglioramento delle condizioni di lavoro, vanno oltre la sola ottemperanza normativa. Il vero obiettivo è creare valore aggiunto per il lavora-

tore, accompagnandolo durante tutta la propria esperienza professionale e contribuendo al suo equilibrio complessivo, sia all'interno sia all'esterno dell'ambiente lavorativo. Oggi il concetto di sicurezza si integra sempre più con quello di promozione della salute, in una visione estesa che coinvolge non soltanto il luogo di lavoro ma l'intero contesto di vita quotidiana. Temi come l'alimentazione corretta, la conciliazione tra vita privata e professionale, la mobilità sostenibile e il benessere psicofisico stanno assumendo un ruolo centrale nelle politiche aziendali moderne. L'individuo viene quindi considerato nella sua globalità: il contesto lavorativo non si

limita a imporre regole e procedure, ma può diventare uno strumento capace di favorire stili di vita più sani e consapevoli. Un approccio che non si esaurisce all'interno del perimetro aziendale ma che si riflette anche nella quotidianità e nelle relazioni familiari, contribuendo a diffondere una cultura della salute e del benessere sempre più ampia e condivisa».

Parlate spesso di “soluzioni personalizzate”. In termini operativi, cosa significa realmente per un'azienda cliente?

«Significa abbandonare definitivamente il modello standardizzato. Ogni realtà produttiva presenta dinamiche differenti: cambiano i processi, le esposizioni al rischio, l'organizzazione interna, la cultura aziendale e persino il rapporto con il territorio. Il nostro lavoro parte sempre da un'analisi tecnica approfondita. Studiamo i cicli produttivi, valutiamo i fattori di rischio, analizziamo gli aspetti ambientali e individuiamo le criticità organizzative. Solo successivamente sviluppiamo misure di prevenzione e protezione realmente coerenti con il contesto specifico. Personalizzare significa anche rendere sostenibili le procedure. Una misura tecnicamente perfetta ma impossibile da applicare nella pratica quotidiana è inefficace. Noi lavoriamo molto sulla semplificazione dei processi e sulla costruzione di modelli operativi concreti, facilmente integrabili nella vita aziendale».

• **Bianca Raimondi**

Jacopo Marchese, fondatore di HSEGAS



LAVORARE SULLA CONSAPEVOLEZZA

HSEGAS attribuisce un ruolo determinante alla cultura della sicurezza all'interno delle organizzazioni aziendali. Secondo l'approccio sviluppato dall'azienda, la sicurezza non può essere garantita esclusivamente da procedure o dispositivi di protezione. Serve una cultura condivisa, costruita attraverso informazione, formazione e addestramento continuo. «Molto spesso gli incidenti derivano da sottovalutazione del rischio, cattive abitudini operative o mancanza di consapevolezza. Per questo motivo i nostri percorsi formativi non sono mai puramente teorici. Cerchiamo di coinvolgere direttamente i lavoratori, di far comprendere il senso delle procedure e di sviluppare un approccio responsabile alla prevenzione» afferma Jacopo Marchese. Tale consapevolezza si traduce, sul piano organizzativo, in una riduzione degli infortuni e in un miglioramento complessivo dell'efficienza e dell'affidabilità dei processi aziendali.



UN MONDO DI LUCE BEGHELLI

Illuminare razionalmente, limitando gli sprechi di energia

Un Mondo di Luce è il progetto Beghelli che prevede la sostituzione "a costo zero" degli impianti di illuminazione presenti negli edifici con apparecchi di nuova generazione ad altissima efficienza. Una soluzione "chiavi in mano" e "a costo zero" grazie al risparmio energetico ottenuto, garantito contrattualmente, con possibilità di ottenimento anche dei Certificati Bianchi e accesso agli incentivi legati al piano di Transizione 5.0.

Ad oggi sono stati realizzati oltre 6.750 impianti, con 1.290.000 apparecchi installati.

L'efficiamento energetico Beghelli è il risultato della combinazione di più variabili: sistemi di illuminazione con tecnologia elettronica all'avanguardia, fotosensori per compensazione con la luce naturale, comfort visivo, rilevazione presenza di persone, programmazione e gestione da remoto degli impianti.

Per industria, logistica, retail, GD, centri commerciali, uffici, ospedali, scuole, parcheggi e aree esterne.



AUDIT
ENERGETICO



CALCOLO
ILLUMINOTECNICO



ANALISI
COSTI-BENEFICI



INSTALLAZIONE
SENZA PENSIERI



RISPARMIO ENERGETICO
GARANTITO



MANUTENZIONE
INCLUSA

beghelli.it | numero verde 800 626 626

Beghelli
IDEE PIENE DI VITA

Serve un cambio di mentalità

Sicurgroup affianca le aziende nella gestione di sicurezza, formazione, ambiente e organizzazione del lavoro con un approccio integrato e personalizzato che unisce consulenza tecnica, servizi specialistici e cultura della prevenzione. Ne parliamo con il fondatore Gianfranco Ingenito

Oggi si parla molto di sicurezza sul lavoro, ma spesso la percezione è ancora quella di un obbligo burocratico, invece è fondamentale cambiare mentalità. Per troppo tempo la sicurezza è stata vista esclusivamente come un insieme di obblighi normativi da rispettare per evitare sanzioni mentre, in realtà, rappresenta un investimento sul valore umano dell'azienda. «Un ambiente di lavoro sicuro migliora la qualità della vita delle persone, aumenta la produttività, rafforza il senso di appartenenza e riduce in maniera significativa i rischi e i costi derivanti da incidenti o problematiche sanitarie – sottolinea Gianfranco Ingenito, fondatore di Sicurgroup, realtà che accompagna le imprese in un percorso che unisce competenza tecnica, organizzazione e sensibilizzazione, trasformando la sicurezza da semplice adempimento burocratico a vero valore aziendale condiviso -. Noi di Sicurgroup lavoriamo proprio su questo aspetto culturale. Cerchiamo di trasmettere alle aziende l'idea che la sicurezza non debba essere vissuta come un peso, ma come una responsabilità condivisa e come uno strumento di crescita. La sensibilizzazione e la formazione continua sono elementi decisivi perché permettono ai lavoratori di diventare parte attiva del sistema di prevenzione. Quando una persona comprende realmente i rischi e sa come affrontarli, cambia completamente il modo di vivere il proprio lavoro».

Qual è la filosofia che guida Sicurgroup nel rapporto con le aziende?

«La nostra filosofia parte da un concetto molto semplice: ogni azienda è diversa e necessita di soluzioni personalizzate. Non esistono modelli standard validi per tutti. Per questo abbiamo costruito una struttura composta da professionisti spe-

cializzati in diversi settori, capaci di lavorare in sinergia e di seguire il cliente a 360 gradi. Noi non ci limitiamo alla semplice consulenza tecnica. Affianchiamo concretamente il datore di lavoro nella gestione quotidiana delle problematiche legate alla sicurezza, all'organizzazione aziendale, alla formazione e agli aspetti ambientali. Vogliamo essere un punto di riferimento stabile, presente e affidabile. Il nostro obiettivo è creare ambienti lavorativi sani, sicuri e anche più sereni dal punto di vista organizzativo. Quello che ci distingue è probabilmente il rapporto umano. Dietro la professionalità ci sono persone appassionate che credono realmente nel valore del proprio lavoro. Questo approccio permette di instaurare relazioni di fiducia durature con le aziende».

Qual è oggi il valore aggiunto di un'azienda come Sicurgroup nel supporto alle imprese sul tema della sicurezza?

«Noi abbiamo una visione forse un po' distorta rispetto a quello che è oggi il quotidiano nel mondo della safety. Siamo perfettamente consapevoli che gli imprenditori, molto più rispetto a qualche decennio fa, si trovano a gestire una quantità enorme di impegni e responsabilità che gravano sulle loro spalle, indipendentemente dalla dimensione o dalla capacità dell'azienda.

La sicurezza sul lavoro, che un tempo poteva essere demandata senza particolare attenzione o competenza, oggi non può più essere affrontata in questo modo. Per questo abbiamo cambiato radicalmente approccio: non ci limitiamo a fornire un servizio ma ci affianchiamo concretamente alle aziende. Abbiamo la fortuna di seguire realtà molto diverse tra loro, dalle multinazionali alle più piccole imprese familiari, ed è proprio questa una delle no-



CERCHIAMO DI TRASMETTERE ALLE AZIENDE L'IDEA CHE LA SICUREZZA NON DEBBA ESSERE VISSUTA COME UN PESO, MA COME UNA RESPONSABILITÀ CONDIVISA E COME UNO STRUMENTO DI CRESCITA

stre forze. Non ci fossilizziamo su un unico modello, ma abbracciamo tutte le forme di attività, così da conoscere davvero il territorio ed essere costantemente presenti».

E questo cosa comporta?

«Quando affianchiamo un'impresa lo facciamo con una convinzione precisa: oggi l'imprenditore non ha più bisogno del sin-

golo consulente che prepara un documento il sabato o organizza una formazione veloce solo per "mettersi a posto". Le aziende hanno bisogno di strutture professionali solide, capaci di offrire un supporto continuo e integrato, finalizzato alla tutela concreta dell'azienda e dei lavoratori. Questa, per noi, è la vera carta vincente. Oggi siamo organizzati per accompagnare le imprese italiane in un percorso di crescita e consapevolezza. Per esempio, la nuova normativa prevede il corso per il datore di lavoro, ma le statistiche ci dicono che il 95 per cento dei datori di lavoro sceglie di seguirlo in Fad. Questo significa che spesso manca ancora la giusta consapevolezza: si tende a viverlo come un semplice adempimento da svolgere in maniera asincrona, quando si ha tempo, senza la necessaria attenzione. Noi crediamo che non sia questa la direzione giusta. Il nostro obiettivo è diventare parte integrante della struttura aziendale, ed è anche per questo che siamo organizzati in diversi reparti specializzati: per garantire alle imprese un supporto reale, continuo e competente sotto ogni aspetto della sicurezza e della prevenzione».

• Gaia Santi

UN SUPPORTO CONCRETO ALLE IMPRESE

Sicurgroup opera oggi in diversi ambiti: dalla consulenza in materia di sicurezza sul lavoro all'igiene industriale, dalla medicina del lavoro alla formazione specialistica, fino alla consulenza ambientale, ai sistemi antincendio e alla gestione Haccp. Nel corso degli anni l'azienda ha consolidato una reputazione fondata su competenza, tempestività e affidabilità, diventando un punto di riferimento per numerose realtà imprenditoriali. L'approccio multidisciplinare e la capacità di affiancare le aziende con soluzioni personalizzate hanno contribuito a costruire un rapporto di fiducia duraturo con clienti e partner. Un impegno costante verso qualità, aggiornamento normativo e innovazione che distingue Sicurgroup nel panorama della consulenza integrata alle imprese.



Gianfranco Ingenito, fondatore di Sicurgroup

Futuro in corso.

**Da oltre 140 anni,
siamo impegnati per il progresso
e la sicurezza energetica del Paese.
Anche adesso, anche qui.**

Puntiamo su fonti rinnovabili e tecnologie innovative
per garantire un sistema energetico stabile
e affidabile, al servizio delle generazioni future.

📍 Impianto eolico Edison, provincia di Foggia.



Diventiamo l'energia che cambia tutto.

Verbali Asl e corretta gestione dei macchinari

«Una macchina sicura è una macchina che lavora meglio, riduce gli errori e tutela sia il datore di lavoro sia gli operatori». Antonio Salvati e Francesca Paduano, fondatori di SSafety srls, spiegano come rispondere alle emergenze ispettive salvaguardando la produttività in fabbrica

L'evoluzione delle normative europee, l'aumento dei controlli da parte degli organi ispettivi e la necessità di garantire ambienti produttivi efficienti hanno spinto le aziende a investire non solo nella conformità documentale, ma soprattutto nella sicurezza concreta dei macchinari industriali. È inevitabile la richiesta di competenze altamente specializzate, capaci di intervenire su macchine nuove e datate, integrando aspetti tecnici, normativi e produttivi. Fondata da Antonio Salvati e Francesca Paduano, SSafety srls è oggi una delle poche realtà del Sud Italia specializzate esclusivamente nella sicurezza dei macchinari industriali. Un modello operativo che punta su specializzazione tecnica, rapidità d'intervento e soluzioni progettuali concrete.

Perché avete scelto di specializzarvi esclusivamente nella sicurezza dei macchinari?

Antonio Salvati: «La nostra scelta nasce da un'esigenza precisa: la sicurezza dei macchinari è una materia estremamente complessa e non può essere affrontata in modo generico. Molti consulenti trattano contemporaneamente decine di aspetti della sicurezza sul lavoro, mentre noi abbiamo deciso di concentrarci esclusivamente sulle macchine industriali. Questo ci permette di essere più rapidi, più efficaci e soprattutto più competenti nella gestione delle criticità tecniche».

In cosa consiste concretamente il vostro lavoro?

Francesca Paduano: «Non ci limitiamo a produrre documenti standardizzati. Il nostro obiettivo è studiare come rendere realmente sicuro un macchinario. Ogni intervento parte da un'analisi tecnica approfondita: valutiamo i rischi, progettiamo i sistemi di protezione e individuiamo le soluzioni più adatte al contesto produttivo. La sicurezza non deve rallentare il lavoro, ma integrarsi nel processo produttivo».

Quali sono i servizi più richiesti dalle aziende?

A.S.: «Ci occupiamo principalmente di consulenza sulla marcatura Ce e dei macchinari industriali, valutazione dei rischi, revamping e retrofit di vecchie macchine, manuali d'uso e manutenzione, istruzioni operative e gestione dei verbali Asl. Proprio quest'ultimo aspetto è uno degli ambiti nei quali veniamo coinvolti più frequentemente».

Perché la gestione di un verbale Asl è così delicata?

F.P.: «Perché molte aziende sottovalutano le conseguenze di una prescrizione. Quando arriva un verbale, spesso la reazione immediata è cercare una soluzione veloce per chiudere il problema nel minor tempo possibile. Il rischio, però, è affidarsi a interventi improvvisati che non risolvono realmente la criticità».

Qual è l'errore più comune che vedete nelle aziende?

A.S.: «Molte imprese pensano che basti installare un riparo o un sensore per rendere conforme una macchina. In realtà una protezione progettata male può persino introdurre nuovi rischi operativi. Inoltre, se dopo un intervento non corretto dovesse verificarsi un infortunio, la posizione del datore di lavoro potrebbe aggravarsi anche dal punto di vista penale».

In che modo intervenite quando c'è una prescrizione dell'Asl?

F.P.: «Il nostro approccio non consiste nel 'tappare il buco'. Quando riceviamo un incarico eseguiamo una nuova analisi dei rischi del macchinario e studiamo un intervento completo che permetta sia di rispondere correttamente alla prescrizione sia di migliorare l'efficienza della macchina. L'obiettivo è trasformare un obbligo normativo in un upgrade produttivo».

Avete sviluppato anche un metodo operativo specifico: il Lean Machine Safety. Di cosa si tratta?

A.S.: «È un approccio che unisce l'ingegneria della sicurezza ai principi della Lean Manufacturing. La sicurezza non deve essere un elemento aggiunto successivamente alla



LEAN MACHINE SAFETY: LA SICUREZZA NON DEVE ESSERE UN ELEMENTO AGGIUNTO SUCCESSIVAMENTE ALLA MACCHINA, MA PARTE INTEGRANTE DEL SUO FUNZIONAMENTO

macchina, ma parte integrante del suo funzionamento. Una protezione mal progettata genera rallentamenti, tempi morti e procedure complicate. Una macchina progettata correttamente, invece, permette di lavorare meglio, più velocemente e con meno errori».

Quanto conta la rapidità d'intervento in questo settore?

F.P.: «Conta moltissimo. Spesso le aziende si trovano in difficoltà perché ricevono assistenza da consulenti che operano a centinaia di chilometri di distanza e intervengono dopo mesi. Noi lavoriamo su un territorio circoscritto del Sud Italia e riusciamo a effettuare il primo sopralluogo generalmente entro una settimana. Quando c'è di mezzo un verbale Asl, la velocità diventa fondamentale».

Antonio Salvati e Francesca Paduano, fondatori di SSafety



tale».

Oltre alla consulenza tecnica, investite molto anche nella divulgazione. Perché?

A.S.: «Oggi la normativa è molto complessa e gli imprenditori hanno bisogno di comprendere davvero i rischi che corrono. Per questo condividiamo casi pratici e contenuti informativi attraverso il nostro portale e il canale YouTube. Crediamo che un imprenditore informato possa prendere decisioni migliori e prevenire problemi molto seri».

Che consiglio darebbe a un'azienda che riceve una prescrizione su un macchinario non conforme?

F.P.: «La prima cosa è non perdere tempo e non affidarsi a soluzioni improvvisate. Bisogna verificare che chi interviene abbia una competenza specifica nella sicurezza dei macchinari industriali, soprattutto quando si parla di macchine datate o modificate nel tempo. Ogni intervento deve essere progettato e documentato correttamente per evitare ulteriori contestazioni e garantire la reale tutela dei lavoratori».

Qual è oggi la vostra visione della sicurezza industriale?

A.S.: «La sicurezza non deve essere percepita come un costo o come un ostacolo alla produzione. Se progettata bene, diventa uno strumento per migliorare organizzazione, efficienza e affidabilità dell'azienda. Una macchina sicura è una macchina che lavora meglio, riduce gli errori e tutela sia il datore di lavoro sia gli operatori».

• BR

ALTA SPECIALIZZAZIONE

SSafety, a differenza dei consulenti generalisti, ha scelto di concentrarsi su un'unica materia per garantire un'elevata competenza tecnica, tempi di intervento rapidi e soluzioni pienamente conformi alle richieste degli organi ispettivi. Grazie all'esperienza maturata e a una presenza mirata sul territorio, è in grado di intervenire con tempestività e di gestire in modo efficace le diverse problematiche legate alla sicurezza dei macchinari industriali.



DIGITAL ENTERPRISE

Accelera la tua trasformazione digitale

Diventa una vera Digital Enterprise, combinando perfettamente il mondo reale e quello digitale.

Raccogliere, comprendere e utilizzare l'enorme quantità di dati creati nell'Industrial Internet of Things (IIoT) è essenziale per diventare un'impresa ancora più sostenibile ed efficiente. La convergenza IT/OT offre la trasparenza necessaria - dal livello più alto al livello di campo - per un processo decisionale basato sull'analisi dei dati. L'integrazione di IT e software nell'automazione sta aprendo la strada per una produzione adattiva che abilita una maggiore flessibilità.

Con Siemens Xcelerator e con Industrial AI ti aiutiamo ad accelerare la tua trasformazione digitale e a diventare una vera Digital Enterprise!

siemens.it/digital-enterprise

SIEMENS

Dalla tutela in cantiere alla robotica indossabile

Il Gruppo Fabbri sviluppa un modello integrato che unisce macchine movimento terra, dispositivi di protezione individuale ed esoscheletri per migliorare il benessere dei lavoratori e supportare le imprese nell'evoluzione dei processi produttivi. Ne parliamo con Antonio Fabbri

Nel mondo della sicurezza sul lavoro, prevenzione e innovazione non sono più concetti separati. Le aziende chiedono soluzioni integrate, capaci di proteggere i lavoratori in ogni fase dell'attività produttiva: dai cantieri industriali fino alle nuove frontiere dell'ergonomia applicata. Aspetti ben chiari Gruppo Fabbri, realtà che attraverso tre anime complementari – Fabbri, Officine Fabbri e Angelo Fabbri Support Devices – ha costruito un ecosistema dedicato alla sicurezza a 360 gradi: macchine movimento terra dotate di sistemi avanzati di prevenzione, dispositivi di protezione individuale altamente specializzati e tecnologie robotiche indossabili per ridurre il sovraccarico biomeccanico dei lavoratori. «La sicurezza non può più essere considerata un insieme di obblighi separati o di semplici adempimenti normativi - afferma il ceo Antonio Fabbri -. Oggi serve una visione integrata, nella quale tecnologia, formazione e prevenzione dialoghino tra loro. È proprio questo il modello che abbiamo costruito come Gruppo Fabbri: accompagnare le aziende in ogni aspetto della tutela del lavoratore, dalla macchina operatrice fino al benessere fisico dell'operatore nel lungo periodo».

Partiamo dal settore delle macchine movimento terra. Quanto conta oggi la sicurezza attiva nei cantieri?

«Conta moltissimo, perché la prevenzione comincia già dalla progettazione dei mezzi. Con l'azienda Fabbri lavoriamo con marchi leader come Kubota, Eurocomach e Mecalac, se-



Antonio Fabbri, ceo del Gruppo Fabbri

lezionando macchine che integrano sistemi di sicurezza avanzati. Penso alle valvole anticaduta sui bracci degli escavatori, ai sistemi di doppia sicurezza idraulica sugli attacchi rapidi, alle retrocamere ad alta definizione per eliminare gli angoli ciechi o alle barre servoassistite che bloccano automaticamente i comandi quando l'operatore scende dal mezzo. Anche la manutenzione è un tema di sicurezza: avere vani motore accessibili da terra significa ridurre sensibilmente il rischio di incidenti durante gli interventi tecnici».

Accanto ai macchinari, resta centrale il tema dei Dpi. Qual è il valore aggiunto di Officine Fabbri?

«Il nostro obiettivo non è semplicemente vendere dispositivi, ma creare una vera cultura della sicurezza. Officine Fabbri propone un catalogo altamente specializzato che comprende sistemi anticaduta, calzature tecniche, guanti professionali e dispositivi per lavorazioni ad alto rischio, collaborando con aziende leader del settore come Delta Plus, Sparco, Base Protection e Kratos Safety. Ma il punto fondamentale è un altro: un Dpi è efficace solo se il lavoratore sa utilizzarlo correttamente. Per questo investiamo molto nella formazione e nell'addestramento pratico, soprattutto per i Dpi di terza categoria, i lavori in quota e gli spazi confinati. Formare significa dare consapevolezza e ridurre concretamente il rischio di errore umano. In quest'ottica, oltre ad aggiornare i nostri dipendenti, teniamo dei veri e propri corsi presso la nostra sede, dedicati alla sicurezza su carrelli elevatori, piattaforme aeree, macchine operatrici che richiedono conoscenze e responsabilità particolari».

Una delle aree più innovative del gruppo riguarda gli esoscheletri occupazionali. Come nasce questo progetto?

«Nasce da una riflessione molto concreta: oggi una delle principali cause di assenza dal lavoro è legata ai disturbi muscolo-scheletrici. Lombalgie, tendiniti, sovraccarichi articolari incidono enormemente sulla salute dei lavoratori e sulla produttività delle aziende. Con Angelo Fabbri Support Devices abbiamo deciso di investire nella robotica indossabile, introducendo esoscheletri occupazionali sviluppati in partnership con realtà internazionali come Auxivo e Comau. Si tratta di dispositivi che supportano il lavoratore durante attività gravose o ripetitive, riducendo il carico biomeccanico sulla co-

lonna vertebrale e sulle articolazioni».

Che impatto hanno concretamente queste tecnologie nelle aziende?

«L'impatto è molto significativo, soprattutto nei settori industriali e logistici. Gli esoscheletri aiutano a mantenere posture corrette, riducono l'affaticamento e contribuiscono alla prevenzione delle patologie professionali. Ma soprattutto cambiano il modo in cui le aziende guardano al benessere del lavoratore. Noi non ci limitiamo a fornire il dispositivo: realizziamo un percorso completo di consulenza, partendo dall'analisi delle aree corporee in sovraccarico fino alla formazione pratica direttamente sul posto di lavoro, coinvolgendo datori di lavoro, Rspg e

IL MODELLO CHE ABBIAMO COSTRUITO COME GRUPPO FABBRI È ACCOMPAGNARE LE AZIENDE IN OGNI ASPETTO DELLA TUTELA DEL LAVORATORE, DALLA MACCHINA OPERATRICE FINO AL BENESSERE FISICO DELL'OPERATORE NEL LUNGO PERIODO

operatori».

Qual è oggi la sfida più importante nel settore della sicurezza?

«Far comprendere che la sicurezza non è un costo, ma un investimento strategico. Un'azienda che protegge i propri lavoratori riduce gli infortuni, migliora il clima interno, aumenta la produttività e diventa più attrattiva sul mercato. La vera sfida è superare la frammentazione: macchine sicure, Dpi adeguati, formazione continua ed ergonomia devono diventare parte di un unico sistema. Solo così possiamo avvicinarci davvero all'obiettivo "zero infortuni"».

•Beatrice Guarnieri



DISTRIBUTORI UFFICIALI DEL MARCHIO AUXIVO

Di recente il Gruppo Fabbri ha acquisito la distribuzione del marchio svizzero Auxivo, specializzato nella produzione di esoscheletri passivi che non richiedono alimentazione elettrica, aria compressa o altre fonti di energia. A differenza della maggior parte degli esoscheletri presenti sul mercato, questi dispositivi sono realmente indossabili: il loro design compatto consente di portarli sotto gli abiti e di operare anche in spazi ristretti, senza aumentare l'ingombro oltre la sagoma del corpo. In particolare "Lift Suit", rappresenta una soluzione progettata per specifiche attività lavorative, che può essere comodamente indossata sotto l'abbigliamento da lavoro, garantendo supporto ergonomico senza limitare i movimenti o la libertà operativa.

The background of the entire advertisement is a high-magnification, close-up photograph of a human eye. The eye is looking directly at the viewer. Within the iris, there is a clear, circular reflection of a lush green agricultural landscape. This landscape features rolling hills, a field of yellow wildflowers in the foreground, and a bright sun shining through a blue sky with scattered white clouds. The reflection is sharp and detailed, contrasting with the organic texture of the eye itself.

syngenta

DA QUI, IL FUTURO È MERAVIGLIOSO

Da 25 anni Syngenta guida l'innovazione in agricoltura, per scoprire dove è possibile fare la differenza e accompagnare le imprese di domani

Grazie all'impegno dei nostri ricercatori, agronomi e innovatori, abbiamo sviluppato tecnologie d'avanguardia per ottimizzare il lavoro degli agricoltori e garantire la sicurezza alimentare alle generazioni future. Dalle sementi di precisione a prodotti più sostenibili per la difesa delle colture, fino alle soluzioni digitali che stiamo mettendo a disposizione delle aziende agricole, il nostro lavoro ha già apportato cambiamenti che sono sotto gli occhi di tutti. Continueremo a investire in ricerca. Perché per Syngenta l'innovazione non è solo ciò che facciamo: è il nostro modo di vedere il mondo.

Imparare a intervenire prima

Analisi predittiva, neuroscienze e consulenza organizzativa trasformano la gestione del rischio in un processo strutturale e su misura per le imprese. Il ceo Cristiano Stevanato spiega l'approccio di Safe Engineering

L'evoluzione normativa, l'introduzione di tecnologie avanzate e la crescente attenzione ai fattori comportamentali stanno spingendo imprese e consulenti verso modelli sempre più integrati, in cui la prevenzione non è più un adempimento formale ma un processo strutturale legato all'organizzazione stessa del lavoro. In questo contesto si inserisce Safe Engineering, società di servizi e consulenza con sede operativa a Martellago, in provincia di Venezia, guidata dall'ingegner Cristiano Stevanato e dall'ingegner Andrea Gambron.

Come sta cambiando oggi il modo di intendere la prevenzione nelle aziende?

«Sta cambiando in modo radicale. Per anni la prevenzione è stata interpretata come un insieme di adempimenti formali, quindi documenti, procedure e obblighi normativi spesso vissuti come un costo o un vincolo burocratico. Oggi questo modello non è più sufficiente perché non riesce a incidere davvero sulla riduzione degli infortuni. Le aziende hanno bisogno di un approccio diverso, più integrato, che entri nei processi produttivi e li migliori concretamente».

Qual è, secondo lei, il limite principale dei modelli attuali?

«Il limite principale è la natura reattiva. Si interviene quasi sempre dopo che l'evento è accaduto. In realtà esistono già segnali prima dell'incidente, come i near miss o le anomalie operative, che però spesso non vengono analizzati in modo strutturato. Il problema è proprio questo: la grande quantità di informazioni non viene trasformata in conoscenza utile».

In che modo l'intelligenza artificiale può cambiare questo approccio?

«L'intelligenza artificiale può fare un salto decisivo perché consente di leggere e collegare dati che oggi restano frammentati. Attraverso algoritmi di machine learning e analisi del linguaggio naturale, è possibile individuare pattern invisibili e correlazioni tra

eventi che sembrano scollegati. Questo permette di costruire modelli dinamici di rischio, quindi non una fotografia del passato ma una previsione del possibile futuro».

Che tipo di applicazioni concrete può avere questo approccio in azienda?

«Significa poter intervenire prima che l'infortunio accada. Se il sistema rileva, ad esempio, una ricorrenza di micro-eventi in determinate turnazioni o condizioni operative, può segnalare un aumento della probabilità di rischio. A quel punto l'azienda può agire in anticipo con manutenzioni, modifiche ai processi o interventi organizzativi mirati».

Un altro tema centrale è quello demografico e della forza lavoro.

«L'età media dei lavoratori aumenta e nei settori più fisici questo comporta un incremento delle patologie muscolo-scheletriche e della fatica. La risposta non può essere quella di escludere i lavoratori senior, che invece rappresentano un patrimonio di competenze. Bisogna riprogettare il lavoro con strumenti come robotica collaborativa ed esoscheletri, che riducono il carico fisico e rendono sostenibile l'attività».

Quanto pesa il fattore umano negli incidenti sul lavoro?

«Pesa moltissimo, spesso più della componente tecnica. Molti incidenti derivano da abitudini consolidate e automatismi. Le persone, con il tempo, tendono a sottovalutare il rischio perché non vedono conseguenze immediate. Gli studi di Kahneman spiegano bene questo meccanismo: il cervello usa scorciatoie mentali che funzionano nella routine, ma che in certi contesti diventano pericolose».

Questo cosa significa per la formazione dei lavoratori?

«Significa che la formazione non può più limitarsi a spiegare le regole. Bisogna lavorare sui comportamenti reali, sugli automatismi quotidiani, e creare contesti che aiutino le persone a mantenere alta la percezione del



IL CONSULENTE DI VALORE È QUELLO CHE SA “CUCIRE” LA SICUREZZA ADDOSSO AL CLIENTE, TROVANDO SOLUZIONI CHE GARANTISCANO IL MASSIMO LIVELLO DI TUTELA SENZA PARALIZZARE I PROCESSI AZIENDALI

rischio. In pratica non basta parlare al pensiero razionale, bisogna agire anche sulle abitudini».

Lei ha parlato anche di formazione scolastica. Perché partire così presto?

«Perché le abitudini si formano prima del mondo del lavoro. Se si interviene solo in azienda, spesso è troppo tardi. Introdurre la cultura del rischio già nelle scuole medie significa sviluppare consapevolezza, responsabilità e capacità di riconoscere i pericoli

nella vita quotidiana. Questo rende più naturale, in futuro, il comportamento corretto anche in ambito lavorativo».

Qual è il problema principale del sistema normativo attuale?

«L'eccesso di burocrazia. Negli anni si è costruito un sistema molto centrato sugli adempimenti formali, che però non sempre produce un miglioramento reale della prevenzione. In molti casi si è creato un sovraccarico documentale che allontana i professionisti dal lavoro sul campo, che invece è quello che fa davvero la differenza. Bisogna valorizzare l'innovazione tecnologica e misurare l'efficacia concreta degli interventi, non solo la conformità formale. Ogni azienda è diversa, quindi servono soluzioni su misura e integrate nei processi produttivi».

Qual è oggi il ruolo del consulente nella gestione della sicurezza in azienda?

«Oggi sempre di più, ogni azienda ha una propria cultura, dimensioni diverse e necessità peculiari. Un approccio rigido e preimpostato è destinato a fallire o, peggio, a diventare un ostacolo alla produttività. Proprio per questo il consulente di valore è quello che sa “cucire” la sicurezza addosso al cliente, trovando soluzioni che garantiscano il massimo livello di tutela senza paralizzare i processi aziendali».

• Gaia Santi

LA MISSION DI SAFE ENGINEERING

Con oltre vent'anni di esperienza maturata nel settore della sicurezza sul lavoro e della formazione professionale, Safe Engineering si è affermata come partner strategico per le imprese, con un approccio orientato a trasformare gli obblighi normativi in strumenti di miglioramento continuo e non in meri costi burocratici. Nel tempo ha sviluppato metodologie consulenziali flessibili, costruite sulle reali esigenze organizzative delle aziende e sui diversi livelli di rischio operativi. L'obiettivo è integrare la prevenzione nei processi produttivi, rendendola parte attiva della gestione aziendale e non un elemento esterno. Questo approccio consente di coniugare conformità normativa, efficienza operativa e tutela concreta dei lavoratori, migliorando la qualità complessiva dell'organizzazione.



Cristiano Stevanato, ceo di Safe Engineering

MUSCOLI E OSSA IL TUO MOTORE

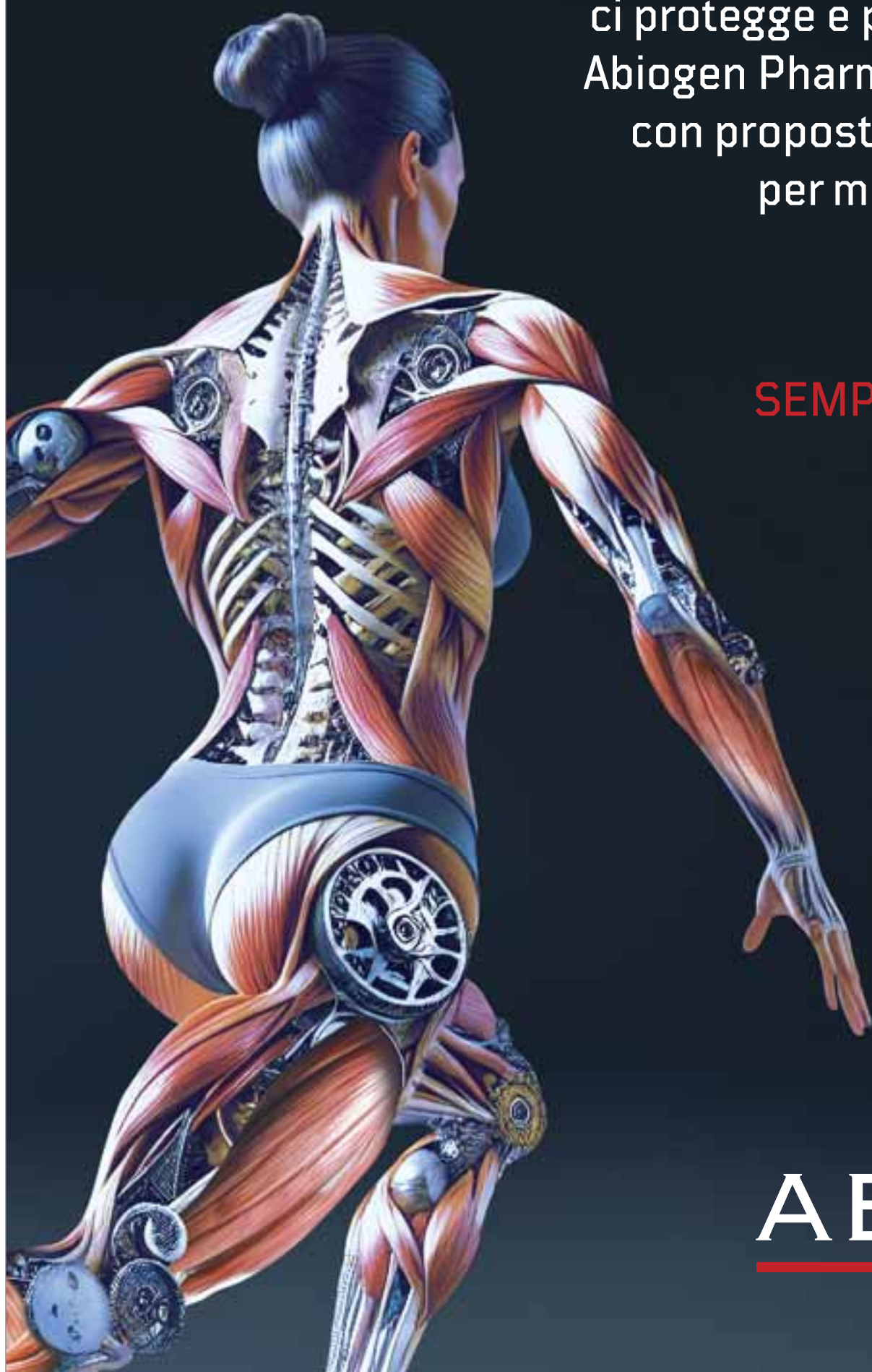
Il sistema muscoloscheletrico ci sostiene,
ci protegge e permette il movimento.
Abiogen Pharma ne cura le patologie
con proposte efficaci e accessibili,
per muscoli e ossa in salute.

ABIOGEN PHARMA
SEMPRE UN PASSO AVANTI

www.abiogen.it



ABIOGEN
PHARMA



La luce che protegge l'industria

Dalla progettazione ottica avanzata alla segnaletica luminosa dinamica: con innovative tecnologie proprietarie, Progtech ridefinisce gli standard della sicurezza industriale a livello internazionale

In molti ambienti industriali la sicurezza non è più soltanto una questione normativa, ma un elemento strutturale che incide direttamente sull'organizzazione degli spazi, sull'efficienza operativa e sulla responsabilità delle imprese. In questo scenario, anche la luce smette di essere un fattore accessorio e diventa uno strumento progettuale: non solo illumina ma segnala, guida, previene. È qui che si inseriscono tecnologie capaci di trasformare la percezione degli ambienti di lavoro, rendendo visibile ciò che spesso, tra polveri, usura e movimentazioni continue, tende a scomparire. È in questo ambito che si colloca Progtech, realtà con sede in provincia di Bergamo che, dal 2008, ha costruito un percorso altamente specializzato nella progettazione e commercializzazione di apparecchi illuminanti a Led per la proiezione della segnaletica di sicurezza.

Oggi, con due sedi operative e un team di quindici persone, Progtech progetta, produce e personalizza internamente i propri dispositivi, esportandoli in circa cinquanta Paesi e consolidando una presenza internazionale significativa. Il tratto distintivo resta quello di un'azienda che mantiene il controllo diretto su tutte le fasi, con un'impronta fortemente orientata al made in Italy e a una fascia di mercato medio-alta.

«Il nostro obiettivo è quello di non fermarci mai sul piano della ricerca e sviluppo, perché è lì che si costruisce il vero vantaggio competitivo - spiega il titolare Michele Rottigni -. La progettazione di nuove soluzioni ottiche, in particolare lo sviluppo di lenti dedicate abbinata a Led di ultimissima generazione, consente di ottenere performance difficilmente replicabili. Questo investimento continuo in R&D ci permette di mantenere un posizionamento avanzato rispetto a concorrenti che spesso si limitano a importare prodotti standardizzati, prevalentemente di origine asiatica, con caratteristiche non comparabili in termini di durata, effi-



Alcune tecnologie sviluppate da Progtech

cienza e precisione».

Questa differenza si riflette direttamente nell'applicazione dei prodotti. I proiettori sviluppati da Progtech sono progettati per replicare fedelmente la segnaletica orizzontale tradizionale - come strisce, percorsi e indicazioni di sicurezza - attraverso una proiezione dall'alto verso il basso. «Il vantaggio è evidente soprattutto in ambienti critici, dove la segnaletica a terra tende a deteriorarsi rapidamente o diventa invisibile - prosegue Rottigni -. Contesti caratterizzati da sporco, superfici irregolari, temperature estreme o traffico intenso di mezzi rappresentano infatti condizioni in cui le soluzioni tradizionali mostrano tutti i loro limiti. In questi casi, la proiezione luminosa garantisce una visibilità costante, contribuendo a migliorare sensibilmente le condizioni di sicurezza e riducendo in modo significativo i costi di manutenzione». L'utilizzo delle soluzioni Progtech si estende a diversi ambiti

namica capace di attivarsi automaticamente in prossimità di incroci o attraversamenti pedonali. Si tratta di un passaggio significativo: la segnaletica non è più statica, ma diventa reattiva, adattandosi in tempo reale alle condizioni operative.

«Il mercato della sicurezza è in forte crescita, anche perché i dati sugli infortuni impongono alle aziende una maggiore attenzione e investimenti sempre più consistenti. In questo contesto, le soluzioni da noi proposte intercettano un'esigenza concreta e trasversale, trovando applicazione in settori molto diversi tra loro ma accomunati dalla necessità di garantire ambienti di lavoro più sicuri. La capacità di personalizzare i prodotti in base alle specifiche esigenze del cliente rappresenta un ulteriore elemento di competitività, consentendo di sviluppare soluzioni mirate e perfettamente integrate nei contesti operativi».

LA PROIEZIONE LUMINOSA GARANTISCE UNA VISIBILITÀ COSTANTE, CONTRIBUENDO A MIGLIORARE SENSIBILMENTE LE CONDIZIONI DI SICUREZZA E RIDUCENDO IN MODO SIGNIFICATIVO I COSTI DI MANUTENZIONE

applicativi: dall'industria pesante alle carriere, dalle vetrerie alla logistica, fino al settore alimentare. I dispositivi possono essere installati, ad esempio, su carroponti o carrelli elevatori, proiettando a terra linee luminose - blu o rosse - che segnalano in anticipo la presenza di mezzi in movimento, aumentando la consapevolezza degli operatori e riducendo il rischio di incidenti. In una logica ancora più evoluta, i sistemi possono essere integrati con sensori e quadri di gestione, dando vita a una segnaletica di-

Accanto alla linea principale, il 2024 ha segnato l'introduzione di una nuova divisione, denominata Fly-Light, che amplia ulteriormente il campo di applicazione delle tecnologie sviluppate. «Si tratta di apparecchi Led brevettati progettati per l'allontanamento dei volatili dagli ambienti industriali. Piccioni e gabbiani rappresentano infatti un problema diffuso in molti capannoni, con implicazioni sia igieniche sia operative. Le soluzioni Fly-Light, interamente progettate e prodotte internamente, stanno registrando riscontri positivi, aprendo nuove prospettive di sviluppo e rafforzando la presenza dell'azienda presso clienti già acquisiti». Dal punto di vista tecnico, tutti i proiettori sono realizzati in Italia e garantiti per cinque anni anche in condizioni di funzionamento continuo, ventiquattro ore su ventiquattro per tutto l'anno. Un aspetto che evidenzia non solo la qualità costruttiva, ma anche l'affidabilità nel lungo periodo, elemento fondamentale in ambito industriale. La recente introduzione di ottiche ancora più performanti, capaci di proiettare linee più lunghe e visibili anche in ambienti ad alta luminosità, rappresenta un ulteriore passo avanti. «Questo si traduce in un costo al metro più competitivo per il cliente e in prestazioni superiori in condizioni difficili».

• Beatrice Guarnieri

PROGETTARE TECNOLOGIE PROPRIETARIE

In un settore dove la concorrenza si dimostra ancora limitata e spesso poco strutturata, la capacità di sviluppare tecnologie proprietarie - come le lenti progettate internamente per la proiezione precisa delle linee - consente di consolidare una posizione distintiva. Più che un semplice produttore di apparecchi illuminanti, Progtech si configura così come un attore tecnologico capace di ridefinire il ruolo della luce negli ambienti industriali, trasformandola in un elemento attivo di sicurezza e organizzazione dello spazio. Un approccio che, unendo progettazione avanzata e applicazione concreta, continua a trovare spazio in un mercato sempre più attento alla prevenzione e all'efficienza.





S-CROSS HYBRID **NEXT LEVEL SUV**



TUTTO DI SERIE, **SENZA SORPRESE.**

Suzuki S-CROSS Hybrid consumo ciclo combinato: da 5,4 a 6,1 l/100km (WLTP). Emissioni di CO₂: da 121 a 141 g/km. Tutti i dettagli sui vantaggi e le promozioni applicabili ai singoli modelli e la loro disponibilità sono disponibili presso le Concessionarie o sul sito suzuki.it. Le immagini delle vetture sono puramente indicative.



HYBRID ALLGRIP SUZUKI connect **3PLUS** SUZUKI 800-452625 **SUZUKI**finance **MOTUL**



Life, uninterrupted.

Secure your mission-critical
infrastructure.

