essecome ONLINE 01/21

Periodico digitale di informazione di security & safety

2021 · ANNO XLI

Sommario Interattivo

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

Febbraio 2021: essecome compie 40 anni

Cari lettori,
ho il piacere di informarvi che, all'inizio del 2021, essecome ha compiuto 40 anni di pubblicazione ininterrotta.
"esse come sicurezza", come venne denominata all'inizio la rivista tecnica specializzata dedicata alla sicurezza fisica contro i reati predatori, ideata e diretta da Paolo Tura, era stata infatti pubblicata per la prima volta a Bologna nel febbraio del 1981.
Pur con gli inevitabili avvicendamenti della direzione e in redazione in tanti anni di attività, essecome è sempre stata mantenuta nella linea originaria tracciata dal fondatore: informare in modo corretto gli stakeholder della filiera della sicurezza privata e creare occasioni di incontro tra loro per sviluppare il lavoro e condividere le competenze, promuovendo la crescita di un settore che diventava sempre più importante per l'intera società.

"Quanto sta avvenendo per effetto della pandemia ci porta a considerare un preciso dovere della stampa specializzata garantire un corretto e puntuale servizio di informazione a supporto di chi lavora per dare sicurezza"

essecome è stata via via adeguata alle innovazioni che nel tempo hanno rivoluzionato il mondo della comunicazione. Fin dal 1997, la rivista cartacea è stata affiancata dal sito www.securindex.com, che ha presto unito all'iniziale funzione di motore di ricerca quella di portale di informazione, diventando progressivamente la piattaforma multimediale che oggi raccoglie e divulga le notizie più importanti provenienti da tutto il mondo e fornisce servizi specialistici di comunicazione, marketing e formazione utilizzando ogni strumento disponibile, digitale e non.
Nella nostra visione, abbiamo sempre considerato l'adeguamento all'innovazione tecnologica una priorità costante per mantenere il ruolo di testimoni credibili del cambiamento continuo del mondo della sicurezza e di partner affidabili per chi in quel mondo ci lavora e vuole far sapere cosa fa.
In questo percorso di innovazione continua, abbiamo tuttavia conservato ed anzi impreziosito la rivista storica, che dal 2019 viene pubblicata con cadenza trimestrale con una grafica elegante ed una stampa di alta qualità su carta con certificazione ecologica per sottolineare il valore dei contenuti pubblicati, rispondendo alle richieste dei lettori più affezionati alla carta stampata.
Quanto sta avvenendo per effetto della pandemia a partire dalla primavera 2020, ci porta a considerare un preciso dovere della stampa specializzata garantire un corretto e puntuale servizio di informazione a supporto di chi lavora per dare sicurezza, nel momento in cui questa non riguarda più solamente la protezione da furti e rapine dei beni materiali ma anche la tutela delle persone e della loro salute.
Un cambio di paradigma che, con ogni probabilità, proseguirà anche dopo l'emergenza sanitaria, imponendo nuove soglie di competenza e nuove responsabilità agli operatori che vorranno rimanere sul mercato.
Saranno sfide impegnative per tutti, anche per essecome che le affronterà con l'orgoglio e la forza dei suoi 40 anni di storia.
Grazie per l'attenzione e la fiducia con cui seguite il nostro lavoro.

Raffaello Juvara
editore e direttore responsabile di essecome-securindex

RisControl
Tastiera Touchscreen

RisControl è la nuova Tastiera Touchscreen dotata di tecnologia all'avanguardia e dal design elegante, per LightSYS™" e ProSYS™Plus!

Offri ai tuoi clienti una esperienza di utilizzo senza paragoni con la tastiera Touchscreen RisControl. Dispone di un'interfaccia utente intuitiva e simile a quella di uno Smartphone, ideale sia in contesti residenziali sia commerciali.

Grazie al suo aspetto e a funzionalità di semplice fruizione, l'utente può avere con pochi tocchi sullo schermo lo stato del suo sistema, inserirlo e disinserirlo e accedere a video live o alle registrazioni delle telecamere IP VUpoint.

Video Verifica
Ideale per impianti dotati di Video Verifica dell'allarme in tempo reale, con sensori radio da interno e da esterno con fotocamera integrata, o VUpoint.

Tastiera Touchscreen
Esperienza d'uso senza paragoni, permette il controllo di allarme, video e smart home da una singola interfaccia intuitiva e di semplice utilizzo.

Sicurezza Superibrida
Adatta per installazioni di ogni dimensione con le centrali ibride di RISCO, da 8 a 512 zone, Grado 2 e Grado 3.

RISCO GROUP

Per maggiori informazioni visitate il sito **www.riscogroup.it**
RISCO Group S.R.L | Via Robecco, 91 – Cinisello Balsamo (MI)

SAN GIORGIO

Non scherzate con noi.
Conosciamo Kung fu, Karate, Judo
ed altre 27 pericolosissime parole!

LA SOLUZIONE È SAN GIORGIO.

AMBITI

FORMAZIONE PER LE GPG
SICUREZZA SUSSIDIARIA
AVIATION SECURITY
TRAINING SU CBT: X-BAG
FORMAZIONE CONTINUA FINANZIATA
SICUREZZA SUL LAVORO

ALCUNI CORSI

AGGIORNAMENTO DM. 269 E 154
AVSEC TUTTE LE CATEGORIE
COVID-19 PER LA SECURITY
GESTIONE CENTRALE OPERATIVA
TECNICHE DI COMUNICAZIONE PER L'UTENZA
GESTIONE DELLE EMERGENZE
ANTIRAPINA
ARMI ED ESPLOSIVI
ANTITERRORISMO

TRAINING SOLUTIONS

SAN GIORGIO SRL

www.sangiorgioweb.com - formazione@sangiorgioweb.com

La Norma UNI CEI EN 50518:2020 è arrivata. Tutte le novità per le centrali degli istituti di vigilanza

intervista a Diego Dell'Orto - Senior Security Manager UNI 10459:2017

Il decreto dell'11 dicembre 2020 del Capo della Polizia ha acquisito le novità introdotte dalla **Norma UNI CEI EN 50518:2020** al quadro dispositivo che configura le centrali operative degli istituti di vigilanza.
La novazione di uno dei pilastri della riforma introdotta dal **DM 269/2010** e successivi sembra dare un'altra spinta al rinnovo del modello organizzativo degli istituti di vigilanza verso quello di integratori di servizi e di tecnologie sempre più richiesto dal mercato.
Abbiamo chiesto a **Diego Dell'Orto**, esperto riconosciuto del sistema normativo del settore, di riassumere le novità della versione del 2020 della Norma 50518 e di fare il punto della situazione delle certificazioni degli istituti di vigilanza all'inizio del 2021.

Ci può descrivere gli aggiornamenti al DM 115/14 dopo il recepimento della versione 2020 della UN CEI EN 50518?
In estrema sintesi, è stata rielaborata graficamente la **Tabella 1bis**, riferita alla norma UNI 10891:2000 "Servizi di vigilanza" con le variazioni più specifiche per gli auditor incaricati delle verifiche, che prevedono:
- maggior dettagli d'identificazione della licenza e delle figure dell'IVP
- programma triennale rivisto di più facile compilazione
- raggruppamento delle caratteristiche trasversali.
Le tabelle in uso per la 50518 sono state completamente rielaborate in un'unica nuova **Tabella 2bis** in conformità alla nuova norma 2020.
Il 6 Febbraio 2022 sarà il termine ultimo per aggiornare tutti i certificati in corso di validità.
E' comunque possibile certificare le nuove centrali con la versione 2020 ma sarà necessario un audit integrativo per l'adeguamento degli attuali certificati **(vedi la sintesi delle variazioni alle pagine seguenti).**

A fronte degli aggiornamenti della Norma, qual è il livello di preparazione delle risorse umane dedicate alle centrali operative?
Ritengo che, in generale, negli IVP la formazione in riferimento alla norma UNI CEI EN 50518 sia attualmente inadeguata. Considerando il mercato, solo i grandi gruppi hanno dedicato risorse per la formazione specifica.
Ritengo sia inoltre indispensabile aggiornare anche i profili 10459 con corsi di formazione specifica, blog, newsletter e sessioni di aggiornamento dedicate in modo specifico alle nuove circolari.
Trovo che il profilo della "vecchia" GPG armata sia in continua trasformazione, in modo particolare per gli operatori di centrale ai quali sono richieste ormai competenze da tecnico informatico più che da guardia giurata. Per garantire una corretta attività quotidiana è comunque necessaria una formazione tecnica operativa di base seguita da un approfondimento sulla parte legislativa.
Gli utenti sono invece pronti a ricevere servizi di alta tecnologia e richiedono il contatto con un operatore solo nei casi estremi. Si andrà sempre più con interfacce web o app su smartphone che possano gestire la quasi totalità delle segnalazioni, lasciando il contatto umano dell'operatore solamente nei casi di reale emergenza. Per questo serviranno operatori formati a 360°, capaci di ascoltare e di reagire senza lasciare nulla al caso.

Dal suo punto di osservazione, quali sono stati gli effetti della pandemia sul sistema?
Lo scenario è piuttosto articolato. In generale, il periodo COVID-19 non ha aiutato a proseguire nel percorso di certificazione degli IVP. Diverse aziende si sono trovate in grandissima difficoltà, come gli istituti che operano nei servizi di classe C "assistenza allo spettacolo" che non hanno potuto erogare alcun servizio, ma hanno dovuto sottostare a certificazioni e obblighi onerosi. L'appello al Ministero è prestare attenzione a questa parte del settore.
Per quanto riguarda invece il processo di certificazione, le circolari di Accredia hanno consentito il proseguo di tutte le attività in modalità da remoto.
Se questo ha aiutato a mantenere il settore ad alti livelli di controllo, sarà necessario valutare in futuro attività in modalità "ibrida" da remoto e in presenza, ottimizzando costi e aumentando il livello di capillarità dei controlli nei servizi in campo.

LE NOVITÀ DEL DM 115/14 CONSEGUENTI AL RECEPIMENTO DELLA NORMA UNI CEI EN 50518:2020

Rif.4.1 Categorie
La norma suddivide in due categorie le tipologie di ARC *(Alarm Receiving Center – Centro Ricezione Allarmi)*:
a) La categoria 1 - SECURITY prevede un maggior livello di protezione ed è dedicata agli ARC che gestiscono messaggi dalle applicazioni di sicurezza, nello specifico:
- allarmi provenienti da sistemi antintrusione e anti-rapina
- sistemi di controllo accessi
- videosorveglianza nelle applicazioni di sicurezza che richiedono una risposta d'emergenza
- monitoraggio dei lavoratori solitari per applicazioni di security
- sistemi di tracciamento degli oggetti vigilanza satellitare GPS per applicazioni di security
- messaggi di allarme provenienti da ARC di 2°categoria
- combinazioni dei sistemi di cui sopra.

b) La categoria 2 - NON SECURITY riguarda la tipologia di ARC che ricevono solo allarmi riferiti alle seguenti specifiche:
- sistemi di allarme automatico antincendio
- allarmi manuali antincendio
- sistemi di allarme sociale (telesoccorso sanitario non security)
- impianti citofonici/videocitofonici
- videosorveglianza in applicazioni non di sicurezza (ad esempio flusso di traffico)
- monitoraggio dei lavoratori solitari per applicazioni non security
- sistemi di tracciamento degli oggetti vigilanza satellitare GPS per applicazioni non security
- impianti di emergenza ascensori
- combinazioni dei sistemi di cui sopra.

Rif.5.2.1 Sezioni Guscio
E' possibile ridurre le dimensione delle sezioni del 50% considerando un ARC collocato in un piano superiore al piano terra, ma superiore a 4 metri da terra o da altro piano adiacente.
Lo spessore per l'eventuale impiego di lamiere 8 mm può essere ridotto del 50 % se l'ARC è collocato in un ambiente non direttamente accessibile dal pubblico.

Rif.5.3. - 6.1.3 Serramenti
Invariate per serramenti perimetrici le richieste di resistenza balistica FB3 e antisfondamento RC3 ma con richiesta di specifica riferibilità a certificazioni o a test da parte di terzi. Le stesse potranno essere apribili solo in caso di evacuazione in emergenza o manutenzioni con invio di segnalazione di allarme.

Rif.5.4.1. Vetrate
Rimane invariata la caratteristica balistica BR3-S EN1063 ma varia la richiesta di resistenza agli attacchi fisici P5A EN356. In effetti, la resistenza di effrazione P5A è indicata per la protezione di ambienti a minor rischio, dove anche la resistenza balistica viene considerata come "non importante". Per chiarire la differenza, si specifica che la caratteristica del vetro P5A viene testata con la tenuta all'impatto con una sfera in caduta da una determinata altezza mentre la tipologia di vetro P6B viene testata con colpi d'ascia. Ad oggi, il vetro P5A non risulta reperibile presso i principali produttori.
È previsto che le finestre e vetri debbano garantire una resistenza al fuoco e al fumo non inferiore a 30 minuti.

Rif.5.5 Resistenza al fuoco ed al fumo
La Norma esclude le aree vetrate, contraddicendo quanto previsto al rif. 5.4.1 della stessa Norma 50518:2020. In questo caso, la tabella 2bis redatta dal Ministero riporta solo resistenza al fuoco non minore di 30 minuti secondo la norma EN 13501-2. Sul punto è necessario avere un chiarimento dal Ministero.

Rif.5.7.5 Ventilazione
Nella tabella 2bis si riscontra che il Ministero non riporta i dettagli ma sembra una svista in quanto nei punti successivi viene più volte richiamato il riferimento 5.7.5.
In effetti, il rif. 5.7.5 della norma 50518:2020 prevede una semplificazione, non richiedendo più filtri e controlli di qualità dell'aria esterna e interna, ma solamente flaps ermetici di chiusura con comando manuale e automatico.
Rimane da chiarire se il Ministero aggiornerà con integrazioni.

Rif.5.8.1.1 – 8.1 Locale processamento dati (CED)
Si definisce quali sono gli apparati obbligatoriamente necessari all'interno del CED; inoltre, viene richiesta una dichiarazione di conformità rilasciata da un progettista in conformità alla norma EN50136-1.

Rif.5.8.1.3 CED presso sito remoto
E' previsto che i locali adibiti per l'attrezzatura di processamento dati (CED) possano venire realizzati anche in un sito remoto, ma con evidenza di certificazione in conformità alla norma EN50600 o altro ARC di categoria 1. Questa disposizione dovrà essere chiarita dal Ministero perché non è coerente con quanto previsto dal DM269/10 aggiornato al DM56/15 rif.4.1.2.
Da questo ultimo si evince infatti che, nel caso di un IVP operante nell'ambito territoriale 5, sono necessarie: 1) una centrale conforme alla norma EN 50518; 2) un'ulteriore centrale a norma EN 50518 ovvero ulteriori una o più centrali di cui all'all.to E tipologia C che devono operare in backup tra loro ed entrambi presidiate sulle 24 ore da guardie giurate.

Rif.6.1.7 Allarme aggressione
La norma definisce il posizionamento vicino ad ingressi uscite e postazioni operatori.

Rif.6.1.10 Sistemi videosorveglianza
Devono essere conformi alla nuova norma EN62676-4. Si sottolinea la necessità di consentire l'identificazione delle persone in entrata e uscita dall'ARC e chi utilizza il passa-documenti.

Rif.7.1.1 Fonte energia
In caso di attivazione della fonte energetica d'emergenza, sono richiesti una segnalazione luminosa e un avviso acustico.

Rif.7.2.1 Gruppo d'emergenza
La richiesta di potenza del gruppo d'emergenza viene ora indicata in 1,2 volte il carico richiesto, rispetto a 1,5 volte della precedente versione.

Rif.8.2 Sincronizzazione temporale dei dispositivi
La Norma modifica la richiesta al sistema di riferimento ad UTC e stabilisce inoltre che, per variazioni superiori a 5 secondi di discostamento, deve essere generata un'anomalia nel sistema di controllo.

Rif.8.4 Conservazione dei dati
Tutti i dati riferiti alla gestione degli allarmi devono essere mantenuti per almeno 3 anni

Rif.da 9.1.1 a 9.1.23 – 10.5.2. PROCEDURE
Vengono richieste molteplici procedure dedicate riferite ai seguenti argomenti:
- operatività dell'intero iter di gestione degli eventi
- modifica ed eliminazione servizi utenti e clienti
- gestione dei segnali
- gestione di eventi in riferimento alla comunicazione di risposta anche verso FF.OO. e referenti degli utenti
- servizi forniti dell'ARC
- verifica degli allarmi
- aumento inatteso dei segnali di allarme
- anomalie del sistema di trasmissione di allarme
- controlli di mantenimento della qualità del servizio
- installazione, manutenzione, protezione, rimozione e ripristino di dispositivi sotto il controllo dell'ARC
- monitoraggio e test dei dispositivi-attrezzature
- gestione e report anomalie
- gestione dell'informazioni
- gestione backup dati
- riservatezza e classificazione delle informazioni
- rapporti con fornitori essenziali
- amministrazione gestione vendite e rapporti con clienti e fornitori
- accesso fisico all'ARC
- accesso in remoto
- continuità operativa emergenze
- evacuazione
- rientro d'emergenza
- indicatori di prestazione

Inoltre al punto Rif.10.5.2 viene richiesta una procedura di SECURITY con controllo di sicurezza di tutte le persone che accedono all'ARC.

Rif.9.1.11 Monitoraggio e test
Le cadenze delle verifiche sono variate in: quotidiane, mensili e annuali.

Rif.10.4 Sistema di gestione
Sono previsti:
- analisi documentata e aggiornata delle politiche e dei piani per aspetti riferiti alla gestione dei rischi di resilienza, business continuity e disaster recovery secondo la norma ISO 31000
- approfondimento della redazione e della pianificazione delle procedure operative e di sicurezza informatica in conformità alla norma ISO 27001.
E' necessario inoltre dimostrare una certificazione del profilo dell'ICT Management System ai sensi della norma ISO27001 edizione corrente.

SFR&L 2021: gli spostamenti che hanno cambiato la sicurezza delle Cose

a cura di Raffaello Juvara

Seguendo l'evoluzione dei rischi ai quali sono esposti i beni materiali nell'era digitale, si possono individuare due fenomeni di "spostamento" che, per quanto fossero iniziati ben prima della pandemia, si stanno completando nella nuova normalità con effetti pesanti per l'intero comparto della sicurezza fisica ma, anche, con notevoli opportunità per coloro che saranno in grado di coglierle.

Lo spostamento del contante dalle banche

Come noto, il sistema bancario italiano è stato per decenni il principale utilizzatore di tecnologie e servizi di sicurezza per difendere le proprie filiali dalla criminalità predatoria. Dal 2007, l'anno del picco delle rapine in banca, il sistema ha iniziato compatto una propria "war on cash" seguendo due direttrici che, nel tempo, hanno portato a risolvere il problema alla radice. La prima è stata la riduzione al minimo indispensabile della presenza di banconote nelle filiali, affidando la movimentazione, il trattamento e la custodia alle società di trasporto valori. La seconda è stata la spinta determinata nei confronti dei clienti a utilizzare i pagamenti digitali che, nell'ultimo periodo, stanno arrivando ai livelli europei grazie ai lockdown e, in parte, alle campagne di comunicazione del governo.
La conseguente quasi totale scomparsa del contante dalle banche, peraltro sempre meglio protette, ha convinto ladri e rapinatori a migrare seguendo le sue tracce verso supermercati, tabaccherie e farmacie ed è fattuale che, almeno fino al 2019, le curve in discesa degli attacchi alle banche si siano incrociate con le curve in salita degli attacchi a questi altri settori. Probabilmente ha concorso a favorire questa "migrazione predatoria" anche il fatto che nei loro punti vendita si trovino sia il denaro che articoli appetibili da rubare, mentre non possono venire blindati come le filiali di banca.

Lo spostamento delle Cose dai negozi

Tra i vari effetti secondari della pandemia c'è stata anche la diffusione di massa degli acquisti online che, oltre ad aver accelerato i pagamenti digitali, hanno cambiato i flussi tradizionali delle merci, che non devono più venir portate nei negozi in attesa di venderle a compratori che le portino via ma vengono recapitate direttamente a casa loro dai corrieri dell'ultimo miglio che le prelevano dai magazzini della logistica su input delle piattaforme di e-commerce.
Questa "semplice" variazione di flusso sta comportando che:

1. *i negozi non siano più pieni di merce come prima ma la sicurezza dev'essere estesa dalla protezione degli articoli a quella dei clienti, che esigono esperienze rassicuranti innanzitutto in materia sanitaria*

2. *le merci vengano attaccate sempre più spesso da bande organizzate durante le fasi di trasferimento e di sosta sia a bordo dei mezzi di trasporto che nei magazzini, che agiscono su commissione per rivenderle a prezzi di svendita sulle piattaforme di e-commerce parallele, provocando un doppio danno a produttori e retailer*

3. *il picco improvviso all'inizio del 2020 delle consegne a domicilio ha messo in crisi il sistema dei corrieri last mile, con forti carenze di personale selezionato e l'arrivo di operatori "opachi" che potrebbero comportare infiltrazioni di criminalità diverse da quelle predatorie e la conseguente diffusione di reati di maggior allarme sociale.*

Questi i temi trattati nel ciclo di tavole rotonde digitali **SFR&L 2021** nei tre appuntamenti organizzati da securindex formazione con la partecipazione di **AXIS Communications** e **Cittadini dell'Ordine**:
2 dicembre 2020: New normal, l'evoluzione della domanda di sicurezza nello store
19 gennaio 2021: Sicurezza nei trasporti e nelle aree di parcheggio: aspetti legali di responsabilità e strumenti tecnici di tutela
17 febbraio 2021: Sicurezza della logistica urbana, vecchi e nuovi rischi

Ringraziamo in modo particolare **Franco Fantozzi**, coordinatore scientifico di SFR&L 2021, ed i relatori **Jerome Bertrume, Stefano Colombo, Franco Isola, Massimo Marciani, avv. Barbara Michini, Alessandro Peron, prof. Michele Riccardi, Eleonora Santarelli, Marco Stratta, Pietro Tonussi.**

Autotrasporto, serve integrare security e safety per la tutela di autisti, merci e vettori

intervista all'avv. Barbara Michini – Studio Gianni & Origoni

Qual è l'orientamento della giurisprudenza in relazione alle responsabilità dei datori di lavoro in caso di lesioni agli autisti in occasione di rapine subite in viaggio?
In tema di furti e rapine perpetrati durante lo svolgimento delle operazioni di trasporto, l'orientamento consolidato della giurisprudenza è piuttosto severo per ciò che concerne la configurabilità della responsabilità dei vettori.
Secondo la giurisprudenza, il mero verificarsi del furto o della rapina, considerati rischi tipici delle attività di autotrasporto, non consente di assolvere il vettore dalla propria responsabilità contrattuale, essendo necessario, a tal fine, verificare che tali eventi si siano presentati o si siano svolti con aspetti e modalità talmente atipici, abnormi ed inconsueti da doversi ritenere del tutto imprevedibili e inevitabili a priori; o che, in ordine agli stessi, non siano esigibili attività di prevenzione che determinino costi sproporzionati al rischio del loro verificarsi, o alla natura ed alle dimensioni dell'impresa.
L'autotrasporto viene qualificato come un'attività intrinsecamente pericolosa, in cui la sottrazione illecita delle merci è considerata, per lo più, evento prevedibile ed evitabile. In tale ottica, anche la responsabilità datoriale per gli infortuni sul lavoro subiti dagli autisti vittime di "atti predatori" viene valutata in termini rigorosi in tutti quei casi in cui il giudice ritenga violato, da parte dell'impresa di trasporto, il cd. "obbligo di prevenzione".
Il datore di lavoro può essere ritenuto responsabile verso il proprio dipendente per le lesioni dal medesimo subite, allorchè risultasse accertato, in modo oggettivo (con una valutazione cd. "ex ante" e non "ex post"), che l'evento criminoso non si sarebbe verificato se il personale e gli

strumenti di lavoro fossero stati dotati di adeguati strumenti di protezione (e prevenzione). Ad esempio, le aggressioni ai danni di un autista durante la perpetrazione di un evento criminoso possono essere considerate ascrivibili alla responsabilità dell'impresa di autotrasporto per non avere preventivamente dotato il mezzo di sistema di antifurto idoneo a scongiurare la rapina.

Se le lesioni subite per atti predatori durante il viaggio vengono considerate come effetti di infortunio sul lavoro, quali misure deve adottare il datore per la sicurezza degli autisti per evitare sanzioni ai fini del Dlgs 81/08?
La tutela degli infortuni sul lavoro nell'autotrasporto è principio di ispirazione dell'intero impianto normativo che disciplina il settore, avendo il legislatore - nazionale e comunitario - premura di garantire la sicurezza nella circolazione stradale a beneficio della incolumità sia degli utenti della strada che degli stessi autisti che guidano i mezzi adibiti al servizio di merci per conto terzi.

L'art. 2087 del codice civile dispone che *"l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro"*. Tuttavia, da detta norma – sostiene la giurisprudenza - non può desumersi la prescrizione di un obbligo assoluto di rispettare ogni cautela possibile ed innominata diretta ad evitare qualsiasi danno, con la conseguenza di ritenere automatica la responsabilità del datore di lavoro ogni volta che il danno si sia verificato, occorrendo, invece, che l'evento sia riferibile a sua colpa.
La colpa, quindi, costituisce l'elemento della responsabilità contrattuale del datore di lavoro. La responsabilità del datore, come delineata dall'ampio contenuto della norma di cui all'art.2087 c.c., non può essere dilatata fino a comprendere ogni ipotesi di danno verificatosi a carico dei dipendenti; se così fosse – cioè se il datore di lavoro fosse ritenuto responsabile sempre e comunque - sarebbe ipotizzabile una sorta di "responsabilità oggettiva", viceversa non configurabile.
La stessa Corte di Cassazione ha più volte statuito che l'infortunio del lavoratore alla guida non è un'ipotesi di responsabilità oggettiva del datore di lavoro. La responsabilità del datore di lavoro sussiste nei casi di violazione degli obblighi di comportamento "imposti" non solo dalle norme di fonte legale (come appunto il D. Lgs. 81/2008), ma anche "suggeriti" dalle conoscenze sperimentali e tecniche del momento.
Il datore di lavoro ha, dunque, l'obbligo di adeguarsi alla migliore tecnologia e ai più sofisticati presidi antiinfortunistici. La valutazione dei rischi – esterni ed interni all'ambiente del lavoro – è un processo dinamico, tant'è che il Testo Unico sulla Sicurezza impone la rielaborazione dei DUVRI in relazione alla evoluzione della tecnica della prevenzione e della protezione. Non è, quindi, possibile individuare in modo assoluto quali siano le misure precauzionali da adottare, ma ogni protocollo di sicurezza deve essere rapportato al "tempo" e al "luogo" in cui le mansioni dell'autista vengono svolte.

Una riflessione di chiusura: se non può accollarsi al datore di lavoro l'obbligo di garantire un ambiente di lavoro a "rischio zero", è anche vero che non possono nemmeno escludersi casi in cui sia lo stesso autista ad essere "il colpevole" e a dover risarcire l'impresa al servizio della quale lavora; il Contratto collettivo nazionale contempla, infatti, la responsabilità dell'autista del mezzo per i casi in cui gli eventi dannosi dipendano dalla sua condotta negligente, essendo egli tenuto alla custodia del carico che gli viene affidato e, in generale, ad attenersi ai protocolli operativi di sicurezza previsti dall'azienda. Ne consegue che il fattivo spirito di cooperazione tra autista e datore di lavoro costituisce lo strumento di tutela più efficace per la prevenzione dei crimini su strada.

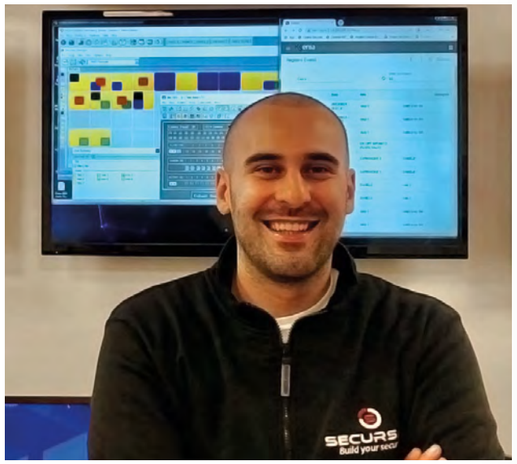
Dal punto di vista assicurativo, quali sono le prescrizioni in generale per coprire i rischi di furto e rapina in relazione al valore del trasportato?
I rischi - pressocchè fisiologici – di eventi criminosi durante lo svolgimento dei servizi di trasporto terrestre possono essere oggetto di un'efficace tutela assicurativa non solo in relazione al danneggiamento ed alla perdita delle merci, ma anche con riferimento alla salute dei prestatori di lavoro. In quest'ultimo caso, oltre alle assicurazioni obbligatorie di legge, possono essere stipulate dall'impresa specifiche polizze integrative a favore dei propri dipendenti. Va da sé che tali ulteriori forme d'indennizzo non opereranno nei casi in cui l'autista si fosse reso causa (anche in via indiretta) del verificarsi dell'evento criminoso, ad esempio, parcheggiando incautamente il mezzo carico di merce in un'area non custodita, non illuminata, non recintata e priva di sistemi d'allarme.
Molte polizze prevedono, tra le condizioni di operatività della garanzia assicurativa, l'assunzione obbligatoria di una serie di misure di sicurezza e prevenzione, positivamente identificate. Inoltre, occorre sempre prestare attenzione alla condotta da tenere nelle immediatezze del sinistro, così come prescritta in polizza, che richiede, come primo passo da compiere, la denuncia tempestiva dell'accaduto alle competenti Autorità.

Secursat: le linee guida per la progettazione di un Security Operation Center

intervista a Alessio Cino, security project & design account presso il Business Development Secursat

Un *Security Operations Center* (SOC) può essere il cuore nella gestione della sicurezza e può essere pensato e progettato come luogo di raccolta di dati e di informazioni utili alla protezione del business, tanto quanto al management aziendale, per orientare scelte e decisioni. Non sempre l'aumento dei perimetri comporta il necessario aumento di risorse per la gestione, la tecnologia deve essere orientata guardando al futuro ed ai possibili cambiamenti di scenario.

Alessio Cino, security project & design account all'interno del team di **Business Development Secursat**, condivide l'approccio da seguire nella progettazione di un SOC pensato come hub di governance tecnologica.



Quali sono le linee guida che regolano la progettazione di un Security Operation Center ed in che modo può essere pensato come un hub tecnologico?

La struttura, il guscio, i sistemi di protezione, la o le piattaforme di integrazione e gestione, risorse e postazioni di lavoro, sono a grandi linee le scelte che le aziende si trovano ad affrontare per la progettazione di un Security Operation Center (SOC), o come viene definito dalla norma UNI CEI EN 50518:2020, Alarm Receiving Center (ARC). Nel dettaglio, la normativa di riferimento regola e guida le aziende nella scelta delle caratteristiche infrastrutturali e tecniche, dei sistemi di allarme ed alimentazione elettrica, nonché nelle modalità operative attraverso le quali devono essere gestiti gli allarmi e le segnalazioni, al fine di realizzare un luogo idoneo, e certificabile, per la gestione ed il monitoraggio dei sistemi di safety e security. Secondo Secursat, la necessità di rispettare queste linee guida deve essere orientata da un approccio integrato con gli obiettivi non solo della security ma del management in generale, per seguire il percorso di digitalizzazione ed innovazione nella gestione dei processi già ampiamente diffuso nelle organizzazioni.

La risposta alla pandemia ha, infatti, reso ancora più evidente la necessità di accelerare l'adozione di modalità di gestione dei processi snelle ed efficaci, di sistemi capaci di collezionare dati ed informazioni puntuali per superare l'incertezza e stabilizzare il business attraverso un'azienda "più "intelligente" e, nel nostro caso, anche attraverso una security "più intelligente".

Una security intelligente, secondo Secursat, in questa fase implica più che l'adozione di nuove tecnologie, il revamping dei sistemi in campo o la ricerca di nuovi prodotti, un cambio di direzione radicale nella gestione dei processi di security ripensando il Security Operation Center come luogo chiave nella gestione dei sistemi.

Il SOC deve dunque essere progettato per essere agile, resiliente e capace di cambiare continuamente. Non una struttura rigida basata sul controllo, ma un luogo di gestione dinamica di eventi di security e safety e di segnalazioni tecniche ed operative.

L'obiettivo è dunque progettare un "ARC" certificabile ai sensi della normativa, laddove necessario, uscendo dalla tradizionale concezione di gestione generica degli allarmi da parte di guardie particolari giurate, per invece progettare un SOC strategico dove, attraverso competenze tecniche, di security e di analisi, è possibile monitorare e gestire da un lato segnalazioni tecnologiche ed operative e attività legate all'infrastruttura IT (rete, sistemi ed applicazioni), dall'altro eventi ed informazioni di security e safety per garantire la protezione dei siti, dei beni e delle persone dell'azienda o dei clienti. Secondo questo approccio il SOC diventa non solo il luogo dove monitorare in real-time eventi e situazioni, ma anche un centro di raccolta dati ed informazioni utili per prevenire scenari di evoluzione del rischio, studiare modelli di automazione dei sistemi, fornire risposte per ottimizzare le risorse ed implementare l'efficacia delle attività.

Adottare un modello diverso di gestione della sicurezza attraverso il SOC può aiutare piccole e grandi organizzazioni a mitigare i rischi, automatizzare le attività di routine attraverso modelli *human+machine* ma anche a ridurre i costi tradizionalmente associati alle attività extra, rivedendo il ruolo della security nell'organizzazione aziendale.

Per realizzare questo modello, secondo il nostro approccio, utilizzato sia nella progettazione dei nostri *Security Operation Centers* certificati, sia in progetti di supporto alla progettazione di SOC o alla scelta delle piattaforme da parte dei nostri clienti, in primo luogo è necessario partire dall'analisi della *capacity*.

Il nostro team si basa sull'analisi dei dati relativi alle segnalazioni dei sistemi presenti in campo, classificandole e studiandone il comportamento, nonché analizza e comprende la tipologia dei siti da connettere per uscire dall'equivoco che un numero maggiore di siti e collegamenti debba necessariamente comportare un aumento degli investimenti in risorse. Il team Secursat, grazie ad un mix di competenze di analisi, tecniche dei sistemi tradizionali e IT, aiuta dunque a comprendere le migliori scelte tecnologiche e definisce la *road-map* per rimodulare le caratteristiche delle piattaforme di integrazione. L'obiettivo è consentire un monitoraggio evoluto dei sistemi e delle segnalazioni con un impatto diretto sulla riduzione dei costi associati alle attività extra, nonché standardizzare il modello di gestione degli eventi, classificandone la tipologia, per disporre di dati da fornire al management per monitorare KPI e processi.

Un altro aspetto, non meno importante, interessa invece la capacità del SOC di garantire la *business continuity* nella gestione delle attività nonché *backup* e *disaster recovery*, tutte attività rivelatesi strategiche soprattutto durante la pandemia dove il SOC, nel nostro caso, è diventato il luogo per continuare a garantire la continuità operativa dei nostri clienti da remoto. Il nostro team, parallelamente alle scelte infrastrutturali e relative alle piattaforme, contribuisce a ripensare l'infrastruttura di rete ed i modelli di collegamento, basandosi su soluzioni cloud-based e guardando agli standard di sicurezza internazionale, nonché includendo nei ragionamenti complessivi anche valutazioni relative alla protezione dei server e degli apparati hardware necessari per garantire il buon funzionamento del SOC e anche la sicurezza delle informazioni processate.

Per ultimo, nel pensare alla realizzazione di un SOC, occorre analizzare risorse e competenze necessarie nonché definire procedure e regole di comportamento delle persone come dei sistemi, in modo da garantire da un lato il rispetto delle procedure aziendali, dall'altro ridurre la discrezionalità degli operatori. Seguendo il percorso tracciato nella progettazione di un SOC, secondo Secursat, pensare alle risorse in maniera innovativa significa abbandonare i tradizionali processi decisionali *top-down*, e formare team con un mix di competenze tecniche e tecnologiche, relative ai più diffusi sistemi di security e safety presenti sul mercato per monitorare gli eventi ma anche gestire le segnalazioni operative, con competenze di security e di analisi per l'utilizzo di piattaforme utili per il monitoraggio degli scenari internazionali come dei viaggiatori dell'azienda o dei clienti.

Il SOC dovrebbe dunque essere popolato da team responsabilizzati con obiettivi e regole chiare nella gestione dei sistemi, guidati e supportati dai dati e dalla tecnologia, secondo logiche *end-to-end*, per una maggiore e migliore velocità di risposta e gestione. In questo senso

il team Secursat aiuta dunque a definire le modalità di implementazione delle piattaforme di gestione dei sistemi, di travel security, di localizzazione, etc. e le modalità di utilizzo delle stesse da parte degli operatori. L'obiettivo è garantire che la gestione degli eventi garantisca a sua volta risposte rapide, prevedendo la formazione delle risorse, per identificare nuovi talenti e competenze capaci di rispondere alle esigenze di gestione degli eventi, nonché l'affiancamento delle stesse nelle fasi di avvio e start-up del progetto.

In conclusione, le *guide-lines* brevemente rappresentate definiscono un modello dove gli investimenti in tecnologia e nelle modalità di applicazione della stessa garantiscono una reale riduzione dei costi fissi e delle attività extra, privilegiando la qualità delle risorse umane alla quantità. Secondo questo approccio il SOC diventa un luogo dove monitorare i rischi legati alla *business continuity*, gestire gli improvvisi cambiamenti nelle necessità, prendere decisioni real-time prevedendo e mitigando i rischi di sicurezza, fornire dati ed informazioni utili all'intera organizzazione, grazie ad un insieme di tecnologie e competenze che garantiscono una buona reazione alle crisi, oggi, e che saranno utili anche nel prossimo futuro per una vera capacità di resilienza da parte della security.

Una progettazione che segue le esigenze e le normative attualmente in essere, cercando allo stesso tempo di prevedere un punto di rottura definitiva in cui la linea di demarcazione tra sicurezza fisica e virtuale, sarà completamente intangibile, ponendo le basi per consentire la futura evoluzione dei nostri "tradizionali" centri di monitoraggio in *Network Operation Center* (NOC) o *Global Security Control Room* (GSCR) capaci di superare i confini territoriali, sincronizzare le esigenze della *physical-security* con quelle IT ed adottare logiche di *machine-learning*.

SECURSAT
Build your security

Contatti:
Secursat
Tel. +39 0141 33000
www.secur-sat.com

Citel annuncia Centrax-open-BMS

di Nils Fredrik Fazzini, CEO di CITEL spa

In un settore come quello della Building Automation, l'architettura di sistema chiusa è stata la regola in base alla quale i grandi nomi della climatizzazione e dell'elettrotecnica negli USA, in Germania e in Francia hanno potuto contare negli anni sull'accettazione da parte degli utenti di soluzioni e di sistemistica chiuse e quindi **monofornitore** degli impianti per i grandi edifici.
Essendo specializzata sulla gestione informatizzata della supervisione, Citel ha potuto progettare soluzioni di discontinuità con il passato rispetto a quel quadro di mercato ingessato, puntando sulle **architetture aperte** destinate inizialmente ai grandi sistemi centralizzati per la sicurezza fisica, bancaria e non, per poi passare al consolidamento del PSIM come **sistema dipartimentale di gestione Informatizzata della sicurezza fisica**, anche come strumento a supporto per la gestione delle crescenti responsabilità dei Security Manager nelle grandi e medie organizzazioni.

Il progetto della sistemistica aperta di building automation è sempre stato attivo, dando luogo a importanti realizzazioni per utenti di prestigio; ma solo ora sta passando al lancio ufficiale del sistema BMS completo e aperto, con la disponibilità, oltre alla gestione strutturata della sicurezza fisica nelle diverse tecnologie (intrusione, accessi, videosorveglianza, emergenze), di nuovi moduli applicativi per le funzioni che riguardano l'**area tecnica** e la relativa impiantistica per la climatizzazione, l'incendio, l'accesso e la circolazione delle persone, più qualsiasi altro sistema, necessari per ottenere una sistemistica integrata basata sulla combinazione:

- delle funzioni di Centrax-open-PSIM per la gestione complessiva mirata, guidata, monitorata di **sicurezza e safety** basati su moduli applicativi specializzati anche multi fornitore;
- di tutte le funzionalità di **gestione tecnologica** classificate nella definizione corrente di Building Automation;

- di processi di gestione basati sull'**interoperabilità multifornitore** tra sistemi adottati autonomamente dall'utente;
- di **processi esperti** a scopi predittivi.

Non a caso, il nome del sistema dipartimentale del modello descritto è **Centrax-*open*-BMS** ed è il risultato della collaborazione tra Citel e una società europea leader di mercato, specializzata nei sistemi aperti per la gestione degli impianti tecnologici degli edifici. La combinazione permette diversi assetti, mettendo a disposizione numerose funzionalità e un grande numero di integrazioni con apparati in campo nelle applicazioni di Building Automation che ora si aggiungono a quelli già elevati del catalogo Centrax-open-PSIM per le applicazioni di sicurezza fisica e safety.
Centrax-*open*-BMS è configurabile in diversi assetti:

- BMS dedicato ad un **singolo edificio** con tutte le funzioni gestionali *in loco*;
- sistema BMS al servizio di una **pluralità di edifici in un comprensorio**;
- sistema PSIM centralizzato in **Control Room aziendale** e sottosistemi BMS e security in edifici nel territorio;
- la variante del precedente centralizzata presso **Società di Servizi per la sicurezza**.

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

L’evoluzione delle unità di deposito contante nei punti vendita: Gunnebo guarda al futuro del Retail

a cura della Redazione

Nelle prossime settimane, **Gunnebo** presenterà al mercato europeo e, quindi anche in Italia, la nuovissima **High Speed D6**, un’unità di deposito di banconote e monete metalliche per **Retailer, Grande Distribuzione e Centri Commerciali** progettata con tecnologie che pensano già al futuro.

La nuova unità **HS D6** avrà infatti a bordo un evoluto validatore certificato in base agli standard BCE, in grado di eseguire il riconoscimento completo delle banconote, la lettura e la storicizzazione del numero seriale in conformità alla recente normativa della Banca Centrale Europea in materia di anti riciclaggio già in vigore oggi.

Il nuovo validatore sarà multi-valuta, con una velocità di deposito di oltre 300 banconote al minuto, ideale quindi per gestire rapidamente volumi medio/alti di contante.

L’unità **HS D6 è il primo prodotto della famiglia High Speed che evolve ed integra nativamente la nuova interfaccia di comunicazione Easy Modular Assisted (EMA)** per la gestione remota, comune a tutti i prossimi prodotti Gunnebo. L’interfaccia **EMA** permetterà di aggiornare i software di bordo, semplificare il service e assicurare il supporto all’utenza finale, il tutto in tempo reale.

La famiglia **HS D6** è completata con un ampio display touch da 7” per una migliore interazione tra l’utente e il prodotto e le sue numerose funzioni.

La **HS D6 nasce per interagire** e, per questa ragione, integra diverse tipologie di collegamento per integrazioni bancarie e/o CIT, anche mediante l’utilizzo di modem/router opzionali. Nativamente, è in grado di gestire due canali indipendenti VPN e separare i dati amministrativi da quelli tecnologici.

La struttura del mezzo forte sarà disponibile in due versioni: **UL (244 kg) e CEN IV (364 kg)**.

PESI E DIMENSIONI

Peso	CEN IV kg. 364 | UL Type kg. 244
Altezza	mm. 995
Larghezza	mm. 440
Profondità /con maniglia	CEN IV mm. 573 / 653 | UL Type mm. 570 / 615

Il deposito delle banconote avverrà all’interno di un sacco termo-saldabile, disponibile nelle modalità “free fall” o “Semi Stack” con capacità comprese tra 2.500 e 10.000 banconote a seconda delle dimensioni del mezzo forte usato e dalle tecnologie di deposito.

E’ possibile integrare il deposito con un accettatore di monete opzionale le quali, una volta accettate e contabilizzate, vengono depositate all’interno di un sacco dedicato.

La famiglia HS D6 è disponibile dall’1 febbraio 2021.

GUNNEBO®
For a safer world

Contatti:
Gunnebo Italia SPA
Tel. +39 02267101
info.it@gunnebo.com
www.gunnebo.it

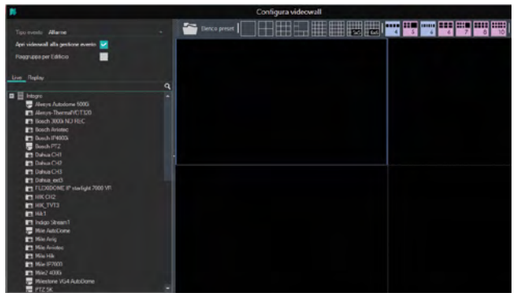
Intègro, la soluzione di supervisione e gestione adatta a tutte le esigenze di sicurezza e oltre

comunicato aziendale

Intègro è una piattaforma innovativa e completa in grado di integrare tutti i sistemi di sicurezza in un unico ambiente semplice, intuitivo e produttivo.
Grazie alle mappe grafiche, è possibile ricreare completamente l'ambiente da supervisionare, visualizzando contemporaneamente tutte le sorgenti hardware e i punti di rilevamento.
"La sicurezza non è fatta di un singolo prodotto ma di un processo di azioni e decisioni"
La facilità d'uso e di configurazione è una delle caratteristiche principali di **Intègro**, peculiarità che lo rende utilizzabile anche da figure del settore sicurezza non prettamente tecniche o con skills informatiche.
Alesys offre inoltre un supporto multivendor definendosi, sin dalla sua fondazione, azienda indipendente e autonoma.
Gli oltre 40 drivers proprietari disponibili, ed in continuo aumento, rendono **Intègro** una delle piattaforme più complete sul mercato in termini di integrazione e sviluppi.
L'architettura Client-Server è modulare e scalabile a seconda delle necessità dell'utente.
L'interfaccia utente è user friendly e graficamente ideata dal nostro team interno per facilitare il cliente nell'utilizzo day to day.

È possibile utilizzare il software in modalità multi-monitor e, all'interno della pagina principale di gestione, inserire mappe sia AutoCAD che Bitmap per creare successivamente delle viste personalizzabili e perfettamente definite anche in caso di zoom e mappe dettagliate e complesse.
Grazie alla configurazione "Punta e Clicca", è possibile posizionare, con un paio di click, i sensori sulla mappa inserita. I sensori possono essere: punti allarme, telecamere, rivelatori incendio, sensori di controllo accessi, ma anche una serie di sensori tecnologici quali misuratori di temperatura, elettricità, ecc. connessi tramite Modbus o driver proprietari.
La configurazione dei sensori è identica per qualunque tipo di hardware si voglia inserire in mappa, ciò facilita sia la gestione che la manutenzione, permettendo cambiamenti e nuovi inserimenti in modo estremamente rapido.
Un pratico menu a tendina dà la possibilità di scegliere il tipo di sensore da integrare, il brand del prodotto, l'icona da visualizzare in mappa, ecc.
L'intero processo di configurazione avviene in pochi secondi per poter agevolare anche le grandi soluzioni con presenza di centinaia o migliaia di punti così come i sistemi multi-sito.
Un pratico pannello notifiche, molto simile a quello di uno smartphone, permette di visualizzare in tempo reale ed in modo intuitivo lo stato di ogni dispositivo. Si potranno, a colpo d'occhio, verificare i sensori in allarme, quelli in blocco, ecc.
Al pannello di notifiche si aggiunge poi il grande dettaglio degli allarmi dove si possono visualizzare sia i nuovi allarmi sia quelli la cui gestione deve ancora essere completata.
I dispositivi sono raggruppabili in aree indipendenti e la gestione è unificata per tutti i sistemi di sicurezza, video e tecnologici. Gli eventi su allarme hanno un monitoraggio continuo e la visione delle telecamere si attiva automaticamente con registrazioni e/o output a seconda di come vengono customizzati dall'utente.
Le notifiche operatore sono personalizzabili con procedure operative a seconda delle necessità interne. Il log allarmi ed eventi è evoluto e prevede una reportistica relativa da cui è possibile estrarre file Pdf ed Excel per ulteriori verifiche. Inoltre, una prossima configurazione di statistiche permetterà la visione di grafici ed informazioni utili a fini commerciali e di marketing, per ampliare il concetto di sicurezza e rendere **Intègro** una piattaforma unica per gestione, manutenzione e business management

In termini di sistemi di videosorveglianza, **Intègro** si interfaccia con decine di dispositivi tra telecamere e VMS di vari brand. Le interazioni prevedono visione delle immagini live su videowall personalizzabile, registrazioni, esportazione e supporto dei metadati forniti dalle stringhe delle telecamere con particolare attenzione alla regolamentazione GDPR.
È possibile, inoltre, impostare la registrazione pre e post allarme automatica, inserendo un timing specifico per sensore. **Intègro** supporta apparati triplo-stream e comandi telecamere dome e PTZ.
Infine, di grande importanza, il servizio incluso di diagnostica che verifica in tempo reale lo stato delle telecamere ed eventuali manutenzioni o controlli da eseguire.



Per quanto concerne il controllo accessi, invece, **Intègro** permette innumerevoli interazioni tra cui la lettura dei transiti e degli accessi, nonché la gestione degli utenti con dettagli a seconda delle centrali supportate.
Inoltre, con pochissimi clic, è possibile posizionare i varchi sulla mappa e gestirli da remoto senza necessità di verifica a campo. Grazie all'accesso alle telecamere, gli addetti sono in grado di attivare input e output su eventi di accesso e guasti.
I vantaggi della soluzione **Intègro**, così come descritti, sono molteplici. Tra i principali, ricordiamo la semplicità di configurazione ed utilizzo, l'interfaccia unica per installatore ed operatore disponibile su tutti i dispositivi e l'integrazione di prodotti dei marchi più importanti, consultabile sul sito **Alesys**.
La gestione guidata e semplificata degli eventi di allarme così come l'architettura modulare e la scalabilità della soluzione completano la presentazione di **Intègro**, la soluzione di supervisione e gestione adatta a tutte le esigenze di sicurezza e oltre.

ALESYS
SECURITY MADE SIMPLE

Contatti:
Alesys
Tel. +39 0331 219436
www.alesys.it

Rilevazione presenze e controllo degli accessi con i terminali dormakaba 97 00 e 96 00

comunicato aziendale

Le nuove versioni dei terminali per la rilevazione presenze ed il controllo degli accessi **dormakaba 97 00** e **96 00** sono ancora più flessibili ed efficienti dal punto di vista energetico rispetto alle versioni precedenti. I terminali, ampliabili grazie alla struttura modulare, sono un punto di riferimento in materia di funzionalità e design e sono la base per una rilevazione presenze semplice e moderna, nonché per una gestione degli accessi intelligente e una comunicazione mirata tra i dipendenti.

I terminali **dormakaba 97 00** e **96 00** possono essere personalizzati grazie a nuovi layout, colori e icone standard.

E' possibile configurare liberamente l'interfaccia utente, in ogni suo singolo elemento, rendendolo ancora più unico e con la possibilità di adattare il display al corporate design aziendale includendo: logo, icone, sfondi e documenti in pdf.

Le imprese possono creare in modo semplice e rapido l'interfaccia più in linea con la loro identità aziendale. I terminali offrono anche la possibilità di monitoraggio e controllo delle porte, nonché di collegamento di componenti porta digitali.

Grazie al suo touchscreen da 7", il terminale **dormakaba 97 00** offre la massima libertà nella gestione personalizzata del display. Quando non viene utilizzato, il terminale con sensore di prossimità si avvia in modalità standby. Questa modalità oltre a garantire l'efficienza in fase di raccolta dati di presenza e controllo accessi presenta un miglioramento in termini di consumi energetici.

Il terminale **dormakaba 96 00** presenta solidi punti di forza quali le sue dimensioni compatte, il brillante touchscreen da 4" e l'affidabile protezione di grado IP65 dalla polvere e dall'acqua.

I partner **dormakaba** possono anche integrare le loro app nel terminale per eventuali personalizzazioni.

dormakaba

Contatti:
dormakaba Italia
Tel. +39 051 41 78311
Tel. +39 02 494842
info.it@dormakaba.com
www.dormakaba.it

RisControl: la tastiera touchscreen di RISCO Group per un'esperienza d'uso intuitiva e personalizzata

comunicato aziendale

RisControl è la nuova tastiera touchscreen dal design moderno di **RISCO Group** – azienda indipendente leader a livello globale nel mercato della sicurezza e specializzata nello sviluppo, nella produzione e nella commercializzazione di un'ampia gamma di soluzioni di sicurezza integrate – che abilita un'esperienza d'uso senza paragoni sia in ambito residenziale che commerciale.

Il display ad alta risoluzione da 8 pollici di RisControl, infatti, offre un'interfaccia davvero intuitiva: grazie a icone simili a quelle di uno smartphone, l'utente ha la possibilità di controllare lo stato del sistema di sicurezza, inserire o disinserire l'allarme e accedere a video live o alle registrazioni delle telecamere **IP VUpoint** in tutta semplicità, per un controllo e una sicurezza senza eguali.

Inoltre, RisControl consente di personalizzare la visualizzazione fornendo accesso rapido alle funzioni più utilizzate dall'utente ed è integrata nel Cloud di RISCO, con cui comunica attraverso la rete wi-fi. Il collegamento con la centrale avviene, invece, tramite **RISCO Bus**.

La nuova tastiera touchscreen è progettata per favorire un'installazione e un cablaggio semplificati e veloci grazie a una staffa di montaggio e a un connettore rimovibile. RisControl fornisce inoltre sicurezza e controllo avanzati consentendo agli utenti di visualizzare facilmente e rapidamente video dal vivo e registrazioni dalle telecamere IP VUpoint e dalla soluzione NVR.

RisControl è supportata dalla versione 1.4 del firmware **ProSYS Plus**, oltre a essere certificata Grado 3, e sarà a breve rilasciato un firmware per **LightSYS** che la supporterà.

A breve la tastiera consentirà di gestire, grazie all'integrazione con il Cloud RISCO, il campanello elettronico con telecamera **Doorbell**, per permettere all'utente di beneficiare del pieno controllo della propria abitazione o del proprio ufficio, ovunque si trovi, e di interagire con gli ospiti.

"Con la nuova tastiera RisControl, RISCO Group offre agli utenti la possibilità di personalizzare la propria interfaccia con icone ad accesso rapido per controllare con semplicità il sistema di sicurezza, la gestione video e l'automazione domestica" ha dichiarato **Ivan Castellan**, Branch Manager di **RISCO Group Italia**. *"La nuova soluzione dell'azienda è in grado di soddisfare le esigenze di semplicità e chiarezza sempre più richieste da installatori e utenti finali grazie a una gestione grafica davvero intuitiva e attuale che ricorda quella degli smartphone: basta, infatti, un tocco sullo schermo per inserire o disinserire l'impianto o attivare uno degli scenari programmati in centrale".*

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

DIAS presenta la gamma VESTA di CLIMAX

DIAS SRL
(+39) 02 38036901
www.dias.it

I sistemi **VESTA** offerti da **DIAS** tramite la rete dei propri partner distributori rappresentano una linea completa di prodotti di ultima generazione per la sicurezza antintrusione e la domotica, particolarmente ideali in ambito residenziale e commerciale.

Con la possibilità di gestire fino a 160 dispositivi, le centrali VESTA offrono un elevato livello di sicurezza e affidabilità unito a funzioni innovative, design moderno dei componenti e degli accessori – a partire dall'elegante tastiera touchscreen 7" TSP-3 a colori ad alta risoluzione con fotocamera da 2 MP incorporata per riconoscimento utenti.

Caratteristiche di grande valore della gamma VESTA sono l'utilizzo delle più recenti tecnologie di comunicazione wireless, di integrazione domotica con tecnologia **Z-Wave** e **Zigbee** e la possibilità di video verifica, anche on demand, tramite i sensori con telecamera integrata e attraverso l'integrazione con telecamere di terze parti, e una linea completa di sensori via radio tra i più affidabili presenti sul mercato.

Di grande interesse è la comoda e avanzata app **XProHome** – gratuita e disponibile per iOS e Android - con la quale è possibile controllare e gestire in modo semplice e intuitivo il sistema di sicurezza e la domotica, quest'ultima gestibile con assistenti vocali quali Alexa e Google Home.

Elementi di spicco della gamma sono inoltre il convertitore da zone cablate a radio e il ripetitore, che consente il collegamento fino a 60 dispositivi o 8 Pircam, con ripetizione tra loro e raggiungendo distanze superiori a 2 km.

HE-130/HE-131: gli eccellenti rivelatori effetto tenda a doppia tecnologia con antimascheramento

HESA SPA
(+39) 02 380361
www.hesa.com

I rivelatori **Serie HE-130** e **HE-131** a doppia tecnologia con antimascheramento sono stati progettati per fornire una valida protezione perimetrale esterna creando una barriera verticale a fasci multipli che rileva la presenza di un intruso prima che faccia irruzione negli ambienti interni. Questi rivelatori offrono una portata massima di 9 metri con un'apertura di 7,5° e sono ideali per la protezione di porte, finestre e vetrate. Disponibili sia nella versione cablata (HE-130) che in quella a basso assorbimento (HE-131), offrono in questa seconda versione un ampio vano interno che garantisce la possibilità di alloggiare tutti i trasmettitori senza fili disponibili sul mercato. L'elettronica di tutte le versioni è protetta da un robusto contenitore plastico IP54.

Il led (escludibile) sul sensore fornisce l'indicazione luminosa di quale tecnologia ha segnalato l'allarme.

La funzione "risparmio energetico" assicura una durata della batteria particolarmente lunga nel modello a basso assorbimento.

Caratteristiche e prestazioni

- Ideale per la protezione di porte, finestre e vetrate
- Possibile installazione nel vano di finestre e porte
- Portata 9 metri, angolo 7.5°
- Funzione antimascheramento con IR attivi
- Regolazione sensibilità antimascheramento
- Portata microonda e sensibilità PIR regolabili
- Fornito con staffa montaggio destra/sinistra e tettuccio opzionale
- Compatibile con tutti i trasmettitori
- Disponibile nei colori bianco e marrone
- Disponibile in versione cablata e a basso assorbimento

Nuova Termocamera Bi-Spectrum per il rilevamento della temperatura

HANWHA TECHWIN EUROPE LTD
(+39) 02 36572 890
www.hanwha-security.eu/it

La nuova Termocamera **Bi-Spectrum** di **Hanwha Techwin** è in grado di rilevare il calore e misurare la temperatura con un grado di precisione molto elevato, fornendo al contempo una verifica visiva delle persone all'interno del campo di visione.
La **Wisenet TNM-3620TDY** è un dispositivo multicanale bi-spettro che incorpora una termocamera di classe QVGA e una videocamera di videosorveglianza da 2 MP.
Grazie al supporto della funzionalità di rilevamento dei volti basata su Deep Learning, la **TNM-3620TDY** è in grado di misurare in tempo reale la temperatura di fino a 10 persone a una distanza di 3 m, lasciando agli operatori la scelta se visualizzare le immagini termiche o le immagini standard ad alta definizione.
Per effetto dell'elevato range entro cui avviene il rilevamento della temperatura, la nuova telecamera puó essere utilizzata anche, ad esempio, per il controllo di impianti di gestione rifiuti e discariche oltre che per la rilevazione in tempo reale di eventuali eventi in ambienti come impianti industriali e produttivi o magazzini di stoccaggio alimentare, dove un cambiamento della temperatura potrebbe essere indice di un problema.

- Telecamera a doppia tecnologia, termografica e visibile, con sensore termico QVGA e telecamera 2 MP con analisi video **AI Deep Learning**
- Precisione fino a **±0.3°C** con utilizzo Black Body
- Diverse modalità di utilizzo: misurazione **temperatura corporea** 30~45°C/ ±0.3°C, misurazione standard -20~130°C/±5°C(≤100°C), ±20%(>100°C)
- **Certificazione IEC 60601**, per utilizzo in ambito medicale

essecome ONLINE

n. 1/2021
Anno XLI
Periodico fondato da Paolo Tura

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

HA COLLABORATO A QUESTO NUMERO
Nils Fredrik Fazzini

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

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

REGISTRAZIONE
Tribunale di Milano n. 21 del 31 gennaio 2018

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
lilian@lilastudio.it