

Le tendenze evolutive della sicurezza fisica informatizzata nel 2020. Le convergenze con una recente indagine internazionale

di Nils Fredrik Fazzini, CEO di Citel SpA

Considerato lo spazio che negli anni è stato riservato da essecome-securindex all'evoluzione informatica in chiave PSIM per la gestione della sicurezza fisica in Italia, **Citel** non poteva non cogliere l'opportunità che si è presentata per un confronto con altri Paesi in occasione della pubblicazione di un interessante documento di **Stanley Security** con il titolo "**2020 Industry Trends Report**". Un'indagine sulle attese, sulle prospettive e sulle criticità, nella vasta platea di utenti ed operatori nel Nord America ed in Europa, tesa soprattutto alla messa a fuoco delle tendenze evolutive tecnico-funzionali in corso nel campo della sicurezza fisica verso nuovi modelli informatizzati

L'occasione per un confronto sull'informatizzazione della sicurezza fisica

Citel si posiziona nel mercato come il produttore di sistemi che ha storicamente lanciato in Italia la struttura in chiave open-PSIM dei sistemi dipartimentali di gestione della sicurezza fisica e che ha poi generato negli anni il più ampio Ecosistema di utenti, di produttori complementari e di integratori in Italia, con un comune riferimento: il modello del *Sistema Informatico Dipartimentale della Sicurezza Fisica*.

L'indagine di Stanley negli USA è pertanto interessante di per sé, considerata la sua ampiezza e profondità, a maggior ragione, nel giudizio di Citel, per il fatto che essa ha portato a risultati fondamentalmente allineati con lo stato dell'arte in Italia e con le tendenze evolutive in corso nel bacino di utenza PSIM di Citel, compresa la naturale convergenza con i moderni modelli dell'informatica gestionale dipartimentale.

Stanley ha focalizzato la rilevazione sulle tecnologie che oggi vengono considerate universalmente rilevanti nell'evoluzione dell'informatica aziendale. Non tutte dello stesso peso ai fini della sicurezza, ma che sono comunque in esercizio oppure oggetto di valutazione anche in Italia e che fanno riferimento alle *innovazioni basate sull'informatizzazione* a tutti gli effetti della gestione della sicurezza fisica, e soprattutto introducendo i moderni modelli orientati alla *dematerializzazione* ed all'*automazione*:

- **Remote Services**
- **Security As A Service (SAAS)**
- **Monitoring Automation**
- **Cloud Technology**
- **Network Security**



Ed anche sui modelli tecnici che utilizzano soluzioni ormai correnti nell'informatica gestionale, già applicate al PSIM e basate sulla gestione di tipo *predittivo e intelligente*:

- **Big Data**
- **Customer Experience Transformation**
- **Machine Learning**
- **Programmatic Evolution**

Infine, rafforzando le pratiche per una gestione più restrittiva della circolazione del personale:

- **Stricter Access Control Requirements.**

Lo stato dell'arte dell'informatizzazione della sicurezza fisica in Italia

L'indagine di Stanley a livello globale si è presentata come un'occasione particolarmente propizia per Citel per fare un parallelo con lo stato dell'arte nel mercato italiano relativamente ai *singoli paradigmi dell'innovazione* informatica, sempre più frequentemente trattati nel settore.

Va peraltro ricordato preliminarmente che il mercato italiano della sicurezza fisica professionale si è distinto nel quadro internazionale come quello più precoce nell'informatizzazione grazie alla diffusa propensione – a differenza di altri Paesi – per i *sistemi aperti multifornitore* e, quindi, di per sé particolarmente evolutivi dietro la spinta della competizione.

Non è infatti un caso che l'Italia sia il mercato che ha generato precocemente il modello *open-PSIM* di Citel, con un corollario di paradigmi come il *sistema informatico dipartimentale della sicurezza fisica* e del *PSIM come progetto permanente*, a supporto di processi gestionali capaci di far fronte ad esigenze crescenti di *profondità* della protezione in considerazione della crescente dematerializzazione delle minacce. E, in definitiva, con la necessità di allinearsi a criteri mirati generati sull'onda del **Change Management settoriale**, coerente con la *Digital Transformation* generalizzata e diffusa.

Le tecnologie informatiche adottate nel settore della sicurezza fisica e sintesi dello stato dell'arte in Italia

La storia di oltre 20 anni di Citel corrisponde a quella dell'informatizzazione nella fascia critica della sicurezza fisica italiana, comprese le particolari spinte generate da un settore bancario penalizzato dalle rapine e dagli attacchi ai caveau; spinte che hanno portato non solo all'evoluzione accelerata delle piattaforme di telegestione al centro e in campo, ma anche all'accumulo ed alla sedimentazione di esperienza utente, realizzando la *condizione necessaria* per lo sviluppo settoriale di *processi intelligenti* di tipo predittivo ed operativo. E non a caso **Big Data, Customer Experience Transformation, Machine Learning, Monitoring Automation, Network Security, Programmatic Evolution, Cloud**, sono i paradigmi dell'informatica corrente, gestionale e industriale, che con la propria indagine Stanley ha sottoposto al mercato della sicurezza fisica per verificarne aspettative e penetrazione.

Si tratta di paradigmi che in campo PSIM si stanno diffondendo, in linea del progresso generale delle tecnologie informatiche gestionali sulle quali un PSIM professionale si fonda per definizione, sempre che sia *consapevolmente* considerato e gestito come un vero e proprio *sistema informatico dipartimentale*. E sempre a condizione che la sistemistica adottata sia costantemente e tempestivamente adeguata alle *dinamiche evolutive settoriali* di utilizzatori e di partner qualificati e reattivi.

Dinamiche evolutive che in Italia hanno storicamente incluso la **Network Security** (la protezione dei dati di gestione della sicurezza trasmessi in rete) e la **Programmatic Evolution**, termine informatico riconducibile all'evoluzione dei processi di gestione degli eventi, da mantenere *funzionalmente* coerenti con l'andamento dei rischi e *tecnicamente* allineati agli sviluppi della tecnologia.

Così come ci si può aspettare l'utilizzo diffuso del **Cloud** in quanto si tratta di una tendenza di fondo in campo informatico per la dematerializzazione dei Server; ma anche perché particolarmente efficace, se non funzionalmente indispensabile, per la fruizione di funzioni software specializzate di gestione video, accessi, di condivisione di basi dati, ecc. Ed anche – e a maggior ragione – per servizi di erogazione di funzionalità *as-a-service*; e in ogni caso per soluzioni tecniche indossabili o portatili che coinvolgono l'uso di telefonia mobile come, ad esempio, lo smartphone combinato a dispositivi IoT .



Più impegnativi sul piano tecnico, ma portatori di un considerevole salto di qualità prestazionali, sono gli sviluppi funzionali legati all'impiego di tecniche come **Big Data, Customer Experience Transformation, Machine Learning, Monitoring Automation**. Sviluppi in cui Citel è pienamente coinvolta perché una gestione PSIM, che è sempre partita dai singoli segnali per pesarli e correlarli per ottenere *eventi e situazioni*, richiede una qualità e profondità delle informazioni indispensabili per generare *funzioni predittive qualificate*. E in tal senso gli sviluppi di Citel in questo campo sono oggetto di collaborazioni già in corso da tempo con specialisti nel settore dell'intelligenza artificiale.

Un peso crescente avrà nel mercato, la **Security As A Service (SAAS)**, vale a dire *servizi di sicurezza da Control Room*, quindi non più i semplici teleallarmi gestiti dalla vigilanza. Si tratta di servizi che hanno una storia particolarmente consolidata in Italia rispetto ad altri mercati, grazie ai protocolli di trasmissione pubblici (quindi aperti) *bidirezionali* secondo la normativa pubblicata dal CEI più di 40 anni fa, con servizi *multimediali e interattivi*, combinati con periferiche intelligenti in campo (dati, voce, video). Con quelle logiche e sistemistica che hanno permesso al mercato italiano – ed a Citel come battistrada – di eccellere nell'anticipazione di tendenze evolutive che solo in un secondo momento si sono diffuse sul piano internazionale.



Citel non ha dubbi sul fatto che la diffusione di questa tipologia di servizi farà da acceleratore all'impiego delle *tecnologie IoT* ed all'integrazione funzionale con il mondo della telefonia mobile. A questo punto, con un salto generazionale rispetto ai servizi tradizionali basati su verifiche dell'evento superficiali (da centro) o costose (sul posto) in virtù anche del consolidamento del passaggio in corso dall'attuale *telegestione di eventi al situation management avanzato*, vale a dire la *gestione dell'evento con le sue dinamiche* grazie anche all'uso di funzioni predittive intelligenti generate dall'accumulo e metabolizzazione dell'esperienza.

Stricter Access Control Requirements

In tutte le previsioni di questo periodo il controllo accessi è destinato ad espandersi; anche in un Paese come l'Italia, più refrattario di altri a questa applicazione; ma proprio per questo con spazi più ampi di crescita. In generale si tende a concordare sul fatto che il telefono cellulare come terminale di applicazioni specializzate avrà certamente un ruolo di rilievo nella sistemistica adottata, insieme ad altre tecnologie basate sul riconoscimento di tipo biometrico. E, in ogni caso, come sottosistema di un sistema gestionale complessivo della sicurezza fisica integrata dell'edificio e/o dell'organizzazione nel suo insieme.

Tutela della resilienza aziendale

Indipendentemente dalla ricerca di Stanley ma a completamento della rassegna delle tendenze evolutive, il paradigma più ampio, che contiene tutti i valori-obiettivo fin qui espressi e che spingerà verso una *integrazione sempre più stretta e intelligente* dei processi per la sicurezza, è quello della *resilienza aziendale*, che sempre più spesso viene considerato il valore complessivo più generale e che coinvolge ovviamente anche la sicurezza informatica. E se si parla di resilienza aziendale è naturale che essa venga considerata il presupposto di un obiettivo *vitale*, che è la *Continuità Operativa* dell'impresa.

Mentre, per completare la rassegna dei paradigmi, si dovrà considerare anche la "gestione dell'*inatteso*", con un richiamo nello scorso anno da parte di **Andrea Chittaro** - Presidente di AIPSA - e con conferme, più indirette che dirette, provenienti dal settore industriale.

Per concludere, tutte queste considerazioni non fanno che confermare la possibilità di cogliere con sempre maggiore convinzione le possibilità offerte dall'evoluzione dell'informatica e, in particolare, quelle classificate nella *Digital Transformation*, ormai mature sul piano della tecnologia; ma anche tali da rendere sempre più funzionali con l'accumulazione e la metabolizzazione dei valori di esperienza utente in un ambito di apertura multifunzionale e multifornitore gestita in una visione di progetto permanente.



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