La Direttiva NIS2 e la professione dell'Ingegnere ICT

di Alessandro Fontana

LO SCENARIO NORMATIVO EUROPEO

La spinta verso la digitalizzazione dei processi di business, con la Transizione 4.0 ormai prossima ad evolvere in Transizione 5.0, ha imposto alle imprese una sempre maggiore integrazione dei processi aziendali e interaziendali. In futuro, la disponibilità delle tecnologie e la necessità di tracciare tutti i processi, con particolare riguardo alla supply chain e agli stakeholders, richiederanno una tanto maggiore capacità di resistenza a qualsiasi evento perturbativo e distruttivo, quanto più l'ecosistema aziendale sarà esteso e ramificato all'interno di esso e legato al cyberspazio

Si tratta di una rivoluzione, di un cambio di paradigma che coinvolgerà un numero crescente di realtà, per le quali diventerà vitale la capacità di ideare e governare processi sempre più virtuali ed articolati, di comprenderne le minacce e le implicazioni di carattere regolatorio e sanzionatorio, ma anche di coglierne opportunità e occasioni di crescita.

La Direttiva UE 2022/2555 Network and Information Systems (NIS 2) [1] fa parte di una strategia europea che sta definendo un nuovo paradigma, un nuovo approccio coordinato ed articolato al problema della continua evoluzione da un lato della dipendenza delle nostre Società dal digitale, dall'altro dalla crescente pericolosità e sofisticatezza delle minacce. Accanto alla Direttiva NIS 2, possono essere citati:

- La rete europea EU-CyCLONe (coordinamento europeo per i grandi incidenti) [2]
- Il Cyber Resilience Act (sicurezza dei prodotti con elementi digitali)[3]
- Il Regolamento 2022/2556 (DORA, Digital Operational Resilience Act - sicurezza del sistema finanziario)[4]
- La Direttiva 2022/2557 (Direttiva CER - Resilience of Critical Entities)[5]

Un quadro di certificazione a livello europeo, ancora in corso di elaborazione da parte di ENISA[6], fornirà un insieme completo di norme, requisiti tecnici, norme e procedure che avrà l'obiettivo di armonizzare i sistemi di certificazione adottati dagli Stati Membri (Cybersecurity Certification Framework Europeo)[7] . Si tratta di un progresso estremamente interessante: infatti, avvenendo la

[1] EUR-LEX https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2557

[2] ENISA https://www.enisa.europa.eu/topics/incident-response/cyclone

[3] Commissione Europea https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[4] EUR-LEX https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2556

[5] EUR-LEX https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2557

[6] https://www.enisa.europa.eu/

[7] Commissione Europea https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

certificazione per paese membro, avere un insieme di regole armonizzate consente una più agevole ri-certificazione in seno a un altro paese nel caso vi si vada ad operare.

PRINCIPI ISPIRATORI DELLA NIS2

Una prima impressione che si coglie leggendo la Direttiva è una forte analogia con le norme sulla sicurezza sul lavoro: si mira a proteggere i sistemi con criteri analoghi a quelli adottati per i lavoratori, tenendo naturalmente presenti le differenze, in particolare la mobilità dell'oggetto della norma, la cui continua evoluzione impone un inedito livello di elasticità e sofisticatezza nell'approccio e nella gestione.

Una seconda positiva impressione riguarda la presa di coscienza che condivisione e coordinamento sono indispensabili e devono coinvolgere quanti più livelli possibile: come vedremo, questo è uno dei motivi dell'inclusione della supply chain nel processo di gestione della sicurezza.

Sullo sfondo, è chiara la volontà di evitare norme eccessivamente generiche, che rischiano di creare atteggiamenti lassisti (peggio, opportunistici) che producono l'effetto opposto. Quanto rischio? Ci sono controlli? Sanzioni? Responsabilità per danni? Si tratta di distorsioni che si sono verificate con la precedente versione della Direttiva (NIS), una fra tutte la "Valutazione d'impatto", che è stata spesso trattata come puro adempimento formale.

Confrontiamo quindi i "pilastri" su cui poggiano le due versioni della NIS.

I tre pilastri della NIS (2016)

- Prevenzione: i soggetti obbligati devono mettere in atto misure per prevenire gli attacchi informatici;
- Rilevamento: i soggetti obbligati devono essere in grado di individuare tempestivamente gli attacchi informatici;
- Mitigazione: i soggetti obbligati devono essere in grado di ripristinare rapidamente i propri servizi in caso di attacco informatico.

I sei pilastri della NIS 2 (2023)

- Identificazione e valutazione dei rischi: i soggetti obbligati devono identificare e valutare le vulnerabilità delle loro reti e dei loro sistemi informativi, e i rischi per la sicurezza.
- Gestione dei rischi: essi devono mettere in atto misure per gestire le vulnerabilità e i rischi identificati.
- Controlli di sicurezza: devono mettere in atto controlli per prevenire e rilevare attacchi informatici.
- Gestione degli incidenti: devono essere in grado di gestire gli incidenti di sicurezza delle loro reti e dei loro sistemi informativi in modo da ridurre danni, rischi per la privacy degli utenti e interruzioni ai servizi.
- Cooperazione: devono lavorare insieme per prevenire, rilevare e gestire incidenti di sicurezza.
- Informazione e formazione: devono assicurare che il personale coinvolto nella gestione della sicurezza delle loro reti e dei loro sistemi informativi sia adeguatamente informato e formato.

PRINCIPALI NOVITA' INTRODOTTE

La Direttiva entrerà in vigore il 18 ottobre 2024. La Direttiva, a differenza dei Regolamenti, dovrà essere recepita dagli ordinamenti degli Stati Membri entro il 17 ottobre 2024, con l'obbligo di rispettarne gli obiettivi. Indipendentemente quindi dalle declinazioni nazionali, introdurrà requisiti di governance espliciti, che richiedono al management dei soggetti obbligati di approvare e supervisionare le misure di gestione del rischio cyber e di presidiare la formazione sulla sicurezza delle informazioni.

Cosa altrettanto importante, introdurrà un considerevole ampliamento del numero dei soggetti interessati, pubblici e privati, ma sarà richiesta la gestione dei rischi di terzi, in particolare la supply chain, con il coinvolgimento nel processo anche di soggetti di dimensione inferiore.

Verranno prescritte delle misure e attività minime da mettere obbligatoriamente in atto, ma sarà anche richiesto che le misure siano "appropriate" e "proporzionate" in relazione alla dimensione dei soggetti e all'entità dei rischi (un chiaro riferimento al principio di "accountability" già visto nel caso del GDPR). Sarà richiesto un approccio risk-based, con un'attenzione particolare alla notifica alle Autorità competenti, come vedremo in seguito.

Come in altri casi, compreso il GDPR, anche in caso di violazione della NIS2 sono previste sanzioni pesanti, che possono arrivare fino ad un massimo di 10 M€ o il 2% del totale del fatturato mondiale globale per i soggetti essenziali. Per quelli importanti si scende a 7 M€ e 1.7% nell'anno fiscale precedente, qualunque dei due sia il più grande. Si tratta quindi di cifre più che ragguardevoli.

I SOGGETTI OBBLIGATI

Concludiamo questa veloce panoramica elencando i soggetti obbligati, che la Direttiva distingue in "soggetti essenziali" e "soggetti importanti":

Sono considerati "soggetti essenziali" gli operatori dei seguenti settori:

- Energia: elettricità, petrolio, gas naturale, teleriscaldamento, idrogeno
- Acqua potabile, acque reflue
- Trasporti: aerei, treni, navi, strade
- Banche (eccetto le banche centrali)
- Infrastrutture del mercato finanziario
- Salute: ospedali, cliniche
- Infrastrutture Digitali: Internet Exchange Point, DNS, registry TLD, cloud, data center, identificazione, servizi di comunicazione
- Amministrazioni pubbliche centrali e regionali
- Manifattura di prodotti farmaceutici (e vaccini)
- ICT Business-to-Business
- Industria spaziale

La vigilanza su questi soggetti potrà essere effettuata a seguito di un incidente, ma anche preventivamente, come attività di sorveglianza..

Sono considerati “soggetti importanti” gli operatori dei seguenti settori:

- servizi postali e corrieri
- gestione dei rifiuti
- produzione e distribuzione di prodotti chimici
- produzione, lavorazione e distribuzione di alimenti
- produzione di apparecchiature medicali
- fornitori digitali (provider di motori di ricerca online, servizi di social network, e-commerce…)

Per questi soggetti la sorveglianza è prevista soltanto a seguito di un incidente.

L’APPROCCIO BASATO SUL RISCHIO

Leggendo l’art. 21 della Direttiva, si ha un quadro chiaro di come l’obiettivo della norma sia centrato sulla gestione e sul governo dei processi che comportano un rischio cyber. Le misure destinate a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti, secondo la Direttiva, dovranno comprendere almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

GLI OBBLIGHI DI NOTIFICA

Un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti da sistemi informatici e di rete o accessibili attraverso di essi.

L'art. 23 della Direttiva NIS definisce un meccanismo di notifica degli incidenti relativi alla cybersicurezza che ha l'obiettivo di coordinare le risposte a livello degli Stati Membri e di Unione Europea. L'obiettivo è chiaro: le minacce informatiche provenienti dalle organizzazioni criminali e dai gruppi sponsorizzati da Stati a noi ostili sono di tipo transnazionale e possono contare su grandi risorse economiche, tecnologiche ed informative. Risulta quindi sempre più utopistico pensare di proteggersi a livello di singola Organizzazione o anche di singolo Stato Membro. Per questo motivo, risulta necessario un sistema di escalation e di messa in comune delle informazioni sull'entità, identità e gestione degli incidenti.

Ai sensi del comma 3, un incidente è considerato significativo e va notificato se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli

A fronte di un incidente, il Soggetto obbligato deve aver predisposto, accanto al normale piano di risposta all'incidente, una procedura di notifica che preveda:

1. Un preallarme entro 24 ore dall'accertamento dell'incidente, per indicare la natura dell'atto e il potenziale impatto transfrontaliero.
2. Una notifica completa entro 72 ore, con una valutazione iniziale della gravità e dell'impatto, oltre agli eventuali indicatori di compromissione disponibili.
3. Relazioni aggiornate su richiesta di un CSIRT o di un'autorità competente, seguite da un rapporto finale entro un mese dall'incidente, dettagliando la gravità, l'impatto, le cause, le misure di mitigazione adottate, e l'impatto transfrontaliero, se pertinente.

Un'ulteriore novità negli obblighi di notifica degli incidenti sarà richiesta la notifica dei "near miss", ossia di eventi che avrebbero potuto compromettere la sicurezza[8] dei dati conservati, trasmessi o elaborati dai sistemi informatici, ma che è stato efficacemente evitato o non si è verificato.

L'IMPORTANZA DELLA GOVERNANCE

La storia degli incidenti degli ultimi anni ci dice che nella gran parte dei casi, sia il verificarsi dell'incidente in sé, sia soprattutto l'ampiezza dell'impatto, sono dovuti più a una inadeguatezza di misure di sicurezza anche fondamentali, che a fattori non controllabili esterni all'azienda. La Direttiva NIS 2 interviene in modo molto pesante sul ruolo della Direzione nel governare la cyber security

[8] Intesa come conservazione delle caratteristiche di disponibilità, autenticità, integrità e riservatezza.

vista come un processo di gestione del rischio, aspetto tanto fondamentale quanto finora trascurato. Le principali conseguenze di questo salto di qualità sono:

a) il coinvolgimento dei livelli direttivi, che sono chiamati a governare il processo e a rispondere in caso di incidenti;
b) l'inclusione della valutazione dei rischi derivanti dai rapporti con la catena di fornitura, i clienti e gli stakeholders.

Per quanto riguarda il punto (a), l'art. 32 della Direttiva chiede che gli Stati Membri "secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto". Può essere anche disposta la sospensione di certificazioni ed autorizzazioni.

Il punto (b) è una naturale conseguenza di un approccio basato sulla gestione del rischio, e i numerosi incidenti informatici causati da fornitori con sistemi vulnerabili o compromessi stanno a dimostrare l'assoluta necessità di tenerne conto.

PROSPETTIVE PER GLI INGEGNERI

Il recepimento della Direttiva imporrà uno sforzo di adeguamento che potrebbe rivelarsi impegnativo per le organizzazioni precedentemente escluse dalla NIS, in particolare per quelle che rientreranno nella categoria dei "soggetti essenziali", ma soprattutto per la loro supply chain e gli stakeholders, che la NIS 2 (correttamente) include nel perimetro soggetto a verifica di conformità.

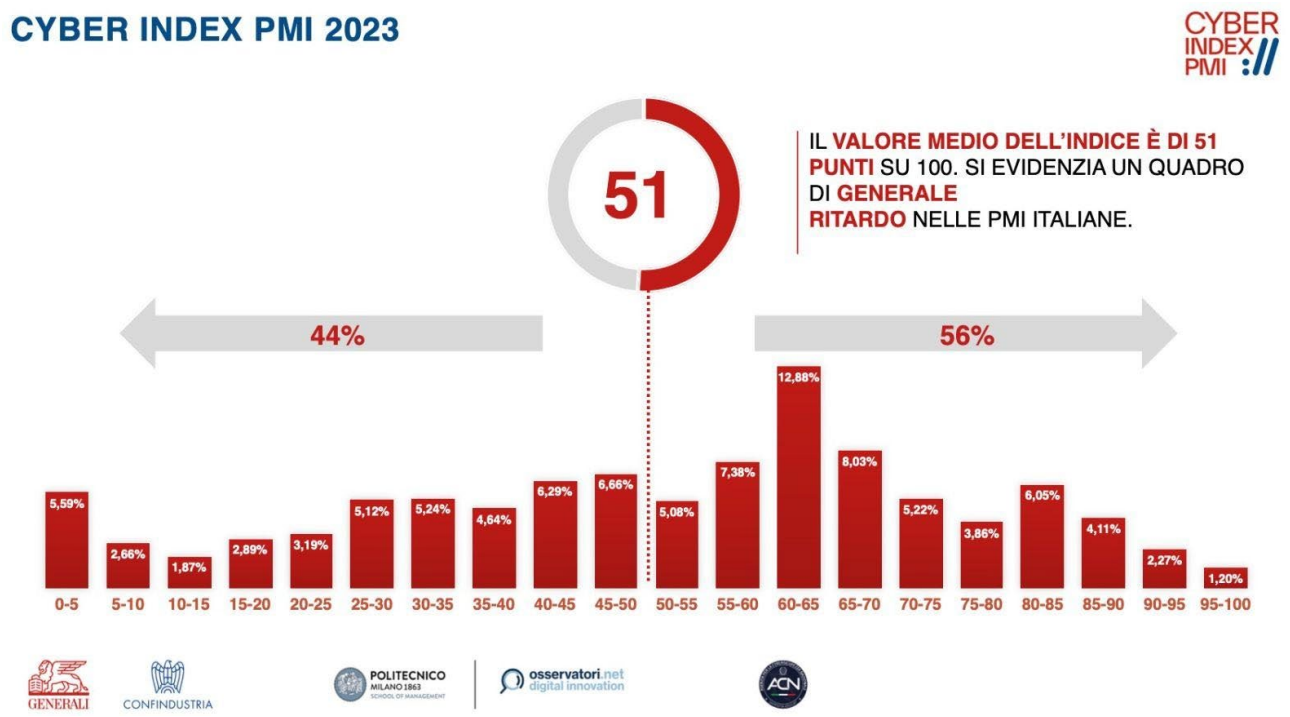
Ipotizzando, come è probabile, che i requisiti di conformità saranno ispirati alle norme esistenti, in particolare le ISO 27K, ma anche ad esempio ISA/IEC 62443 o NIST 800.82 per i sistemi industriali, o ISO 22301 per il Disaster Recovery e la Business Continuity, è chiaro che si apre un discreto spazio di opportunità per gli Ingegneri professionisti, in particolare quelli dell'Informazione. Si apriranno infatti interessanti spazi nel campo della progettazione e della conduzione dei sistemi di cybersecurity, su cui però esiste una sovrapposizione evidente con altre professionalità, cosa che (vexata quaestio) impedisce la creazione di una riserva di legge.

Un aspetto su cui gli Ingegneri potrebbero al contrario giocare un ruolo specifico è quello di "tecnici della compliance", di facilitatori nella valutazione dello stato attuale e degli obiettivi che è necessario fissare per adeguarsi alla norma, nonché di auditors e di consulenti del board. In questo senso, si tratta da un lato di un'attività congeniale al professionista, abituato a confrontarsi con le norme e obbligato per Legge a mantenersi aggiornato. Soprattutto, il professionista iscritto all'Ordine ha la possibilità di porsi in una condizione di terzietà rispetto alle aziende e agli Enti di controllo.

Qui si celano, a parere ed esperienza di chi scrive, un grave pericolo per le organizzazioni ed una grossa opportunità per gli Ingegneri dell'Informazione: in cybersecurity uno dei pericoli più grandi è la convinzione di essere "a posto così", spesso legittimamente coltivata nei livelli operativi, con il rischio che sia mal visto un intervento della Direzione che, in definitiva, mette in discussione lo status quo. In questo senso, può essere risolutiva la presenza di una figura terza dotata di una base

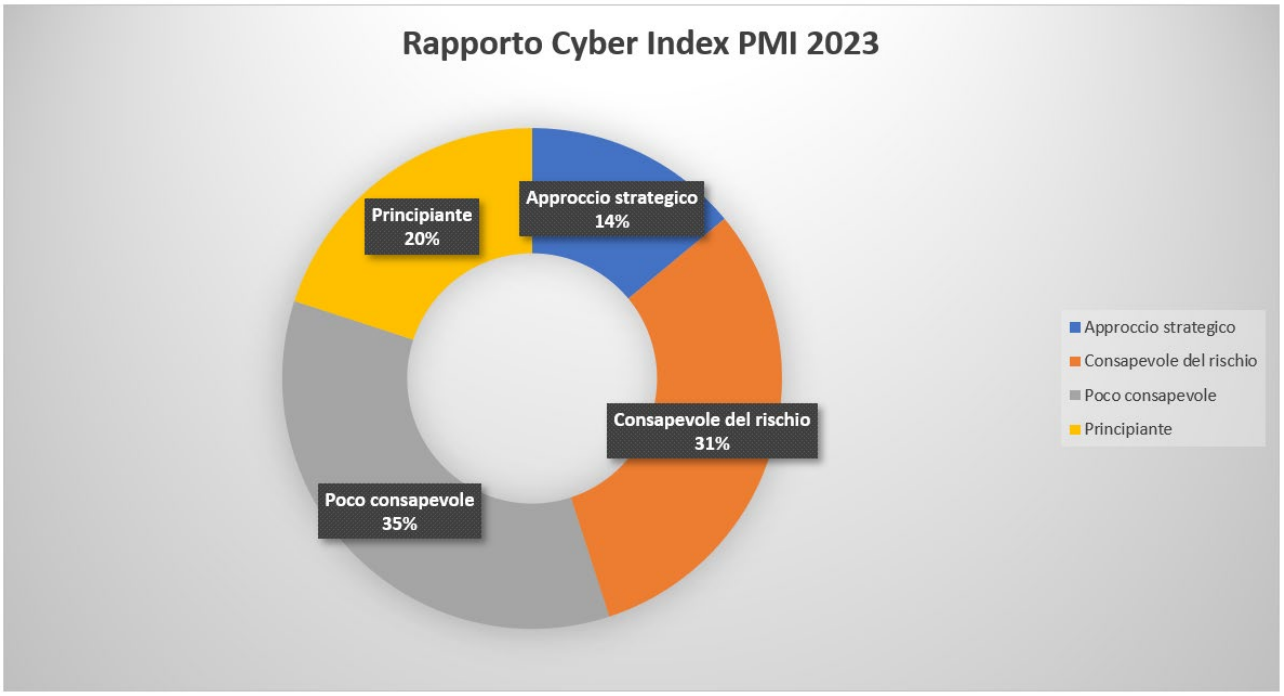
culturale più ampia rispetto al puro tecnico informatico, perché incaricata non soltanto di controllare, ma anche di spiegare, coinvolgere e se necessario mediare, costruendo un percorso di compliance condiviso che eviti conflitti. Una figura di questo livello non sarà un semplice consulente o auditor, ma, in quanto terzo per definizione, potrà essere proposto dalla Direzione come facilitatore nei rapporti tra i vari livelli aziendali coinvolti dalla Direttiva che, ricordiamo, non riguarda solo i livelli operativi, ma responsabilizza pesantemente anche (oserei dire soprattutto) quelli dirigenziali.

Questo aspetto non va sottovalutato in particolare per le PMI, che saranno in molti casi soggette alla Direttiva come conseguenza dell'estensione dell'ambito di azione alla supply chain, non soltanto perché nelle PMI i livelli operativi sono meno numerosi e definiti (il che rende i conflitti più probabili), ma soprattutto per il motivo seguente:



L'indice è frutto di una ricerca su 700 PMI curata da Confindustria, Agenzia per la Cybersicurezza Nazionale e Generali e sviluppato con il contributo dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano[9]. Il risultato è abbastanza sconfortante, perché solo il 51% delle aziende intervistate dimostra di possedere una sufficiente consapevolezza in merito alla cyber security. Di questo 51%, però, solo il 14% ha sviluppato un approccio strategico, mentre il 55% ammette di essere molto in ritardo in tale percorso che, con l'entrata in vigore della Direttiva, diventerà obbligatorio ed urgente per quelle (molte) di loro che rappresentano un elemento della supply chain oppure uno stakeholder:

[9] https://www.generali.it/iniziative/iniziative-commerciali/cyber-index-pmi



Le PMI avranno la necessità di essere orientate e seguite nella valutazione dello stato di fatto e del percorso di adeguamento, nella definizione delle procedure, nel monitoraggio dei processi di adeguamento e mantenimento, nel coinvolgimento della Direzione, nella formazione e nell'aggiornamento continuo del personale (compresi i Dirigenti). Sullo sfondo, l'organizzazione ordinistica potrebbe giocare un ruolo fondamentale nella formazione e disseminazione presso gli iscritti e le aziende, ma anche nel supporto ai colleghi sul campo, attraverso una rete che vedrebbe le Commissioni Ingegneria dell'Informazione attive nel coordinamento di tali attività sul territorio, con le Fondazioni come braccio formativo ed informativo e il coordinamento nazionale affidato al C3i. Molti considereranno tale "visione" piuttosto utopistica, ma in realtà la volontà di fare rete è forte e la sua implementazione è iniziata in diverse realtà territoriali.

Questo articolo fa parte di un'iniziativa della Commissione C3 e della Fondazione Ingegneri di Padova che ha precisamente lo scopo di stimolare lo sviluppo di tale rete.

L'AUTORE

Alessandro Fontana, grande appassionato di meccanica e di informatica sin dai gloriosi tempi della Guzzi due valvole e del Commodore 64, ha trovato nell'Ingegneria Industriale il connubio ideale tra le due passioni e nel paradigma Industria 4.0 la loro naturale evoluzione.

Ha al suo attivo, come singolo e come esperto di informatica in uno staff di Colleghi, circa 50 perizie e diversi progetti relativi ad Industria 4.0 e digital factory, nonché alcune realizzazioni di interfacce MES atte ad implementare il requisito obbligatorio dell'integrazione.

Crede fermamente che la transizione digitale delle aziende possa essere un "game changer" per il nostro tessuto produttivo, in particolare per le PMI. Si fa promotore in diversi contesti della cultura

digitale, in particolare della cybersecurity e dell'integrazione digitale dei processi, consapevole che l'essere umano resta l'anello debole della catena della sicurezza, ma anche un elemento chiave della competitività, e che una migliore comprensione delle potenzialità del digitale potrebbe essere il "bootstrap" di cui molte aziende hanno bisogno per fare il salto di qualità.

Attualmente è molto attivo sul fronte della Direttiva Europea NIS 2, che considera una buona risposta alla necessità di alzare il livello di sicurezza informatica dell'Unione a livello di "immunità di gregge" attraverso il coordinamento e la condivisione di criteri di resilienza e di mitigazione dei rischi il più possibile adeguati ed omogenei.