



excellence in safety

Corsi di formazione 2026

Cybersecurity OT



academy

tec.nicum
Schmersal Group





Bruno Diniz

Managing Director of tec.nicum – Solutions & Services GmbH

Introduzione

La sicurezza funzionale delle macchine è un campo complesso. Esistono requisiti differenti per i vari ruoli nella gestione di macchine e impianti.

Da un lato, i fabbricanti di macchine devono assicurare la conformità a normative e leggi basate su direttive internazionali in materia. Dall'altro lato, gli utilizzatori di tali macchine sono soggetti ai requisiti delle direttive sulle attrezzature di lavoro per la salute, la sicurezza, l'ambiente e a specifici requisiti nazionali, ove applicabili. Ma non solo i fabbricanti e gli utilizzatori sono soggetti a questo obbligo. Anche importatori e distributori di macchine e impianti operano su un terreno delicato, in quanto sono soggetti a specifiche disposizioni di legge. Inoltre, non è raro che macchine in uso vengano ammodernate, autonomamente o con il supporto di integratori, il che comporta una serie di altre complessità con processi ben definiti da rispettare.

Per tali complesse questioni legali e tecniche, un numero sempre maggiore di aziende chiede supporto ad esperti qualificati.

I nostri esperti sviluppano e implementano progetti e soluzioni di sicurezza in tutte le fasi del ciclo di vita, quali sviluppo, produzione, vendita, funzionamento, adeguamento (retrofitting) e dismissione di macchine e impianti, in tutto il mondo.

tec.nicum è la divisione servizi del Gruppo Schmersal. I nostri Functional Safety Engineers e Machinery CE Experts, certificati da TÜV Rheinland, formano una rete di consulenza a livello mondiale, che dispone di una conoscenza approfondita delle direttive, delle leggi e dei regolamenti regionali, nazionali e internazionali applicabili, nonché di un know-how tecnico e di una esperienza pluriennale nella realizzazione di progetti. I servizi sono quindi disponibili in tutto il mondo.

La filosofia di base di tec.nicum è quella di offrire una consulenza indipendentemente dal fabbricante e il più possibile obbiettiva. Il principio guida di tec.nicum è: offrire ai clienti una consulenza competente, indipendente da prodotti e fabbricanti, e supportarli nella analisi di sicurezza e nella progettazione di macchine e ambienti di lavoro.

In questo modo, tec.nicum contribuisce in modo significativo a rendere il mondo più sicuro in ambiente industriale – fedele al motto: excellence in safety – we care!

Bruno Diniz

Offerta di tec.nicum poggia su sei moduli base: academy, consulting, engineering, integration, digitalisation, outsourcing

academy Centro di formazione ■ Corsi di formazione ■ Workshop personalizzati ■ Formazione in-house ■ Corsi certificati (mce.expert e FSE)		consulting Analisi e documentazione ■ Assistenza tecnica ■ Valutazione dei rischi ■ Valutazione della conformità CE ■ Valutazioni di macchine e linee di produzione ■ Documentazione tecnica	
engineering Progettazione e costruzione ■ Pianificazione progettazione tecnica ■ Sviluppo del progetto concettuale ■ Progettazione elettronica e meccanica ■ Gestione del progetto		integration Applicazione pratica ■ Soluzioni chiavi in mano ■ Installazione ■ Retrofit	
digitalisation Integrazione software ■ tec.ps (Product Service System) ■ tec.ssm (Schmersal Smart Machine) ■ tec.cvs (AI and Computational Vision Solutions) ■ tec.dloto (Digital Lockout Tagout) ■ tec.ems (Energy Monitoring System)		outsourcing Soluzioni complete ■ Prodotti Plug & Play ■ ETO (Engineer to Order) ■ Sistemi e quadri di controllo	
tec.nicum			

academy: trasmissione di competenze

La tec.nicum academy offre, in tutto il mondo, un programma completo di formazione e seminari sul tema della sicurezza dei macchinari e degli impianti. Dai corsi introduttivi di base agli argomenti specifici, i contenuti della formazione vengono accuratamente adattati alle esigenze dei clienti di tec.nicum.

Un team internazionale di docenti, composto da esperti di sicurezza certificati con una esperienza pratica pluriennale, garantisce una trasmissione di competenze di alta qualità.

La tec.nicum academy supporta, con il know-how necessario, i fabbricanti e gli utilizzatori per la applicazione delle disposizioni di legge per la sicurezza delle macchine e dei luoghi di lavoro, in modo mirato al cliente, con formazione in presenza in uno dei centri di formazione presenti in tutto il mondo, con seminari in loco o comodamente alla scrivania nel formato online.

I programmi aggiornati dei corsi delle sedi nazionali della tec.nicum academy possono essere consultati qui: **www.tecnicum.com**

Per maggiori informazioni riguardanti i servizi tec.nicum academy non esitate a contattarci all'indirizzo e-mail: tecnicum-it@schmersal.com

Corsi sulla sicurezza informatica di macchine ed impianti proposti a catalogo:

SEM-DG01 – Corso Security OT Base

SEM-DG02 – Corso Security OT Avanzato (include Corso Security OT Base)

SEM-DG03 – Corso Secure PLC Programming (da effettuare dopo il Corso Security OT Avanzato o Base)

SEM-DG04 – NIS2 con riferimenti a norma ISO 27001

SEM-DG05 – ISA/IEC 62443-2 con riferimenti alla NIS2

SEM-DG06 – ISA/IEC 62443-2-4: Requisiti per i Fornitori di Servizi IACS

SEM-DG07 – ISA/IEC 62443-3-3: Requisiti di sicurezza dei sistemi

SEM-DG08 – ISA/IEC 62443-4-1: Ciclo di Vita dello Sviluppo del Prodotto

SEM-DG09 – Introduzione al Cyber Resilience Act

SEM-DG10 – Introduzione a GDPR e Data Act

SEM-DG11 – Introduzione al Regolamento “macchine” 2023/1230

Catalogo Corsi

Codice	Titolo	Durata		
		4 h	6 h	8 h
SEM-DG01	Corso Security OT Base			X
SEM-DG02	Corso Security OT Avanzato			X
SEM-DG03	Corso Secure PLC Programming			X
SEM-DG04	NIS2 con riferimenti a norma ISO 27001	X		
SEM-DG05	ISA/IEC 62443-2 con riferimenti alla NIS2	X		
SEM-DG 06	ISA/IEC 62443-2-4: Requisiti per i Fornitori di Servizi IACS	X		
SEM-DG07	ISA/IEC 62443-3-3: Requisiti di sicurezza dei sistemi	X		
SEM-DG08	ISA/IEC 62443-4-1: Ciclo di Vita dello Sviluppo del Prodotto	X		
SEM-DG09	Introduzione al Cyber Resilience Act	X		
SEM-DG10	Introduzione a GDPR e Data Act		X	
SEM-DG11	Introduzione al Regolamento “macchine” 2023/1230	X		

Nota:

I corsi sono erogati sia in modalità sincrona online che presso sede Clienti.

SEM-DG01:

Contenuti Dei Corsi

Security OT Base

Scopo del corso:

Dedicato alla sicurezza informatica delle apparecchiature OT/ICS, fornisce le nozioni di base per il personale coinvolto nella progettazione e gestione degli impianti.

SEM-DG02:

Security OT Avanzato

Scopo del corso:

Dedicato alla sicurezza informatica delle apparecchiature OT/ICS come risultato di oltre 20 anni di esperienza su sistemi SCADA, PLC, DCS. Affronta in modo approfondito i temi della cybersecurity applicata al contesto industriale.

SEM-DG03:

Corso Secure PLC Programming

Scopo del corso:

Comprendere gli aspetti della cybersecurity specifici per le applicazioni OT, Individuare i potenziali rischi cyber di un impianto di automazione, etc.

SEM-DG04:

NIS2 con riferimenti a norma ISO 27001

Scopo del corso:

Tale modulo formativo si propone di fornire una comprensione approfondita della Direttiva NIS2 (UE 2022/2555). Viene presentata un'introduzione alla direttiva, specificandone gli obiettivi principali, il contesto normativo e storico, e trattando l'entrata in vigore e il recepimento nel quadro giuridico nazionale tramite il DLGS 138/2024. Un elemento cardine è l'identificazione dei soggetti obbligati e dei settori e attività interessati dalla direttiva. Il corso esamina quindi argomenti di natura operativa, quali la gestione del rischio e degli incidenti informatici, illustrando le metodologie di valutazione e gestione.

Vengono descritte le misure tecniche, operative e organizzative da implementare, i piani di risposta agli incidenti, nonché le procedure di notifica e gestione delle crisi. Vengono inoltre esaminati i requisiti minimi di sicurezza, la protezione della supply chain, e la sicurezza dei sistemi informativi. Di rilevanza sono i criteri per la valutazione della gravità degli incidenti e gli obblighi di comunicazione e notifica, incluse le procedure e lo scambio di informazioni tra autorità, unitamente alla collaborazione con i CSIRT (Computer Security Incident Response Teams). Aspetti sanzionatori e legali sono altresì considerati, con riferimento alle sanzioni per violazioni della direttiva e alle implicazioni legali per le organizzazioni.

SEM-DG05:

ISA/IEC 62443-2 con riferimenti alla NIS2

Scopo del corso:

Questo corso offre un'analisi dettagliata della serie di standard ISA/IEC 62443. La sezione IEC 62443-2-1 verte sui requisiti e le definizioni relative al sistema di gestione della sicurezza della rete IACS (Industrial Automation and Control Systems), includendo le responsabilità degli utenti e dei proprietari dei dispositivi. Un obiettivo centrale, allineato con la NIS2, è l'adozione di misure.

proporzionate ai rischi, basate su una valutazione che tenga conto del servizio essenziale, configurando un approccio "Risk Based". Nello specifico, vengono trattate le politiche di analisi dei rischi e di sicurezza dei sistemi informatici, la gestione degli incidenti, le procedure e gli strumenti per la notifica, con l'obiettivo, compatibile con la NIS2, di predisporre un piano per il contenimento degli incidenti e coordinarsi con le autorità preposte. Vengono discussi i temi della continuità operativa e della gestione del backup in caso di disastro, in linea con l'obiettivo NIS2 di garantire la ripresa ottimale dell'erogazione del servizio. Un altro tema fondamentale è la sicurezza della supply chain, orientata a gestire in sicurezza la catena dei fornitori per minimizzare il rischio di attacco, in coerenza con un obiettivo compatibile NIS2. Il corso affronta anche la sicurezza nell'acquisizione, nello sviluppo e nella manutenzione dei sistemi, inclusa la gestione e la divulgazione delle vulnerabilità, aspetti cruciali per la gestione della sicurezza nel cambiamento e la protezione dalle vulnerabilità.

SEM-DG06:

ISA/IEC 62443-2-4: Requisiti per i Fornitori di Servizi IACS

Scopo del corso:

Questo corso esplora il ruolo dei system integrator, dei fornitori di servizi e degli OEM (Original Equipment Manufacturers) nell'ecosistema IACS. Vengono esaminati i requisiti specifici per i fornitori di servizi lungo il ciclo di vita del servizio sicuro e vengono definiti ruoli e responsabilità per l'erogazione di servizi sicuri in ambito OT (Operational Technology). Un aspetto pratico trattato è la gestione della sicurezza durante le fasi di delivery, includendo le attività richieste per la messa in servizio e la manutenzione sicura, e i controlli per la gestione delle credenziali, configurazioni, patch e aggiornamenti. Il corso sottolinea l'importanza di integrare i requisiti di sicurezza nei contratti e negli SLA (Service Level Agreements) e le best practice per la collaborazione tra cliente e fornitore al fine del mantenimento della sicurezza. Vi è un chiaro allineamento con il framework NIS2, considerando la valutazione del fornitore quale parte della supply chain critica e le evidenze e gli audit richiesti per dimostrare la conformità.

SEM-DG06:

ISA/IEC 62443-3-3: Requisiti di sicurezza dei sistemi

Scopo del corso:

In questo contesto, si distinguono i Functional Requirements, che descrivono le specifiche funzioni che un sistema deve espletare per garantire la sicurezza, e i Security Requirements, requisiti più generali che definiscono le caratteristiche di sicurezza che un sistema deve possedere, quali la protezione dei dati, il

controllo degli accessi, la crittografia e la gestione delle vulnerabilità. Un concetto fondamentale introdotto è il Target Security Level (SL-T), che rappresenta il livello di sicurezza desiderato per una determinata soluzione di automazione, indicando la protezione necessaria per salvaguardare il sistema, la zona o il condotto. Per conseguire tale livello, si utilizza il processo di valutazione del rischio, essenziale per identificare, valutare e trattare i rischi al fine di ridurli a un livello tollerabile, processo che include la modellazione delle minacce, l'analisi delle vulnerabilità e la valutazione dell'impatto. Dopo l'implementazione delle misure di sicurezza, si valuta l'Achieved Security Level (SL-A), il livello di sicurezza effettivamente raggiunto dal sistema, tramite test e verifiche per assicurare che soddisfatti i requisiti definiti. Il corso illustra altresì il Security Level Capability (SL-C), che rappresenta le contromisure tecniche di sicurezza native disponibili in un sistema o componente, le quali possono essere integrate e configurate per proteggere la soluzione di automazione senza ulteriori misure compensative.

SEM-DG07: **ISA/IEC 62443-4-1: Ciclo di Vita dello Sviluppo del Prodotto**

Scopo del corso:

Questa norma è destinata ai fornitori di prodotti, software e componenti per l'automazione industriale. L'elemento centrale del corso è il processo di Secure Development Lifecycle (SDL), spiegando come integrarlo nei processi di sviluppo aziendali esistenti. Vengono presentati i requisiti chiave della norma, coprendo aspetti quali la gestione della sicurezza (SM-1), la specifica dei requisiti di sicurezza (SR-1), la sicurezza by design (SD-1, SD-2), l'implementazione e verifica (DM-1, DM-2), i test di sicurezza (TA-1), la gestione dei problemi di sicurezza (MA-1), gli aggiornamenti e le patch (SU-1) e la guida alla sicurezza per l'integrazione (SI-1). Si discutono le evidenze richieste e la conformità alla norma, con esempi di documentazione e processi, e la valutazione della maturità del processo tramite audit. È significativo notare il collegamento tra l'applicazione di questa norma e il soddisfacimento dei requisiti normativi europei quali la NIS2 e il Cyber Resilience Act (CRA) in materia di sicurezza dei prodotti digitali.

SEM-DG08: **Introduzione al Cyber Resilience Act**

Scopo del corso:

Questo corso illustra inizialmente cos'è il CRA e quali sono i suoi obiettivi: migliorare la sicurezza e garantire la resilienza dei prodotti digitali. Esamina il contesto normativo e il rapporto con altre normative UE, come il GDPR. Vengono chiariti i prodotti che rientrano nell'ambito di applicazione (quelli con una componente digitale, connessi a Internet o a reti) e quelli esclusi. Vengono descritti dettagliatamente gli obblighi per i produttori, che includono la valutazione dei rischi di sicurezza, l'integrazione di misure di sicurezza nel ciclo di vita del prodotto, la documentazione, e la gestione del ciclo di vita (progettazione sicura, test, aggiornamenti, monitoraggio, gestione incidenti).

Ulteriori obblighi cruciali concernono la comunicazione e la trasparenza (notifica di incidenti e vulnerabilità) e la responsabilità del produttore per la sicurezza del prodotto e la mancata conformità. Il corso copre inoltre le misure di sicurezza e resilienza, trattando i principi di sicurezza (confidenzialità, integrità, disponibilità), le tecnologie (machine learning, blockchain, API) e le misure di resilienza (backup, controlli accesso, monitoraggio intrusioni, gestione incidenti). Infine, vengono affrontate le procedure di conformità ed enforcement, incluse la valutazione, la certificazione, i controlli delle autorità e le sanzioni.

SEM-DG09:

Introduzione a GDPR e Data Act

Scopo del corso:

Questo corso è articolato in moduli. Inizia con una introduzione al GDPR, ai suoi principi fondamentali, ruoli e obblighi, e una panoramica sul Data Act, i suoi obiettivi e l'impatto per le aziende, evidenziando differenze e interazioni tra le due normative. Un modulo specifico è dedicato alle misure di sicurezza informatica, illustrando gli obblighi di sicurezza previsti dall'Articolo 32 del GDPR e le misure tecniche e organizzative essenziali quali pseudonimizzazione, crittografia, backup, resilienza dei sistemi e il ruolo degli amministratori di sistema. Vengono altresì analizzati i requisiti di sicurezza introdotti dal Data Act per la condivisione e l'accesso ai dati. Il corso include un modulo sulla valutazione del rischio e la compliance normativa, su come condurre una valutazione, le best practice per la gestione dei rischi informatici, e l'implementazione e documentazione delle misure di sicurezza. L'ultimo modulo è incentrato sulla gestione degli incidenti e delle violazioni dei dati, coprendo le procedure operative e gli obblighi di comunicazione delle violazioni.

SEM-DG10:

Introduzione al Regolamento Macchine

Scopo del corso:

Il nuovo Regolamento Macchine (UE) 2023/1230, sebbene applicabile dal 20 gennaio 2027, è entrato in vigore il 29 giugno 2023 e introduce significative novità in materia di sicurezza delle macchine, con una particolare attenzione alla cybersecurity. Il corso offre una panoramica del regolamento, i suoi obiettivi, ambito di applicazione e definizioni chiave come "macchina" e "quasi-macchina", considerando i componenti digitali e software. Un punto cruciale è l'integrazione della cybersecurity nel ciclo di vita delle macchine, sottolineando che la sicurezza informatica deve essere considerata fin dalla progettazione e per tutta la vita utile della macchina, includendo la valutazione del rischio cyber e l'adozione di misure di mitigazione adeguate. Vengono elencati i requisiti di sicurezza informatica specifici, come la protezione dei dati, il controllo degli accessi e la necessità di aggiornamenti di sicurezza per correggere vulnerabilità. Il corso evidenzia inoltre la responsabilità condivisa tra fabbricanti, importatori, distributori e acquirenti e l'importanza della collaborazione tra tutti gli stakeholder per garantire un adeguato livello di sicurezza informatica.



Qualifica di "Machinery CE Expert"

Esperto in sicurezza delle macchine in soli cinque giorni

La tec.nicum academy ha aggiunto al suo programma una nuova offerta di qualificazione: con un seminario articolato in cinque giorni, i partecipanti possono ottenere la qualifica di "Machinery CE Expert" (MCEexpert®).

Sulla base di una esperienza decennale, Schmersal ha sviluppato questo seminario e i suoi contenuti e lo ha fatto certificare dal TÜV Rheinland. Il corso, con un format compatto, fornisce tutte le competenze necessarie per implementare una procedura di valutazione della conformità CE per macchine e impianti, comprensiva di tutte le relative sottofasi. In questa forma e con questo ampio trasferimento di competenze, il seminario è pressoché unico nel suo genere sul mercato.

Una volta completato con successo, i Partecipanti potranno dimostrare di aver acquisito la Qualifica di Esperto in Sicurezza delle Macchine avvalendosi di un certificato rilasciato da TÜV Rheinland®.

Si è autorizzati a utilizzare il titolo di "Machinery CE Expert with TÜV Rheinland® Certified Qualification". Il titolo è riconosciuto a livello internazionale.

Il database dei certificati online "Certipedia", TÜV Rheinland® fornisce informazioni su tutte le caratteristiche dei prodotti testati, sui servizi, sulle aziende, sui sistemi e sulle certificazioni personali (www.certipedia.com). La descrizione del seminario "Machinery CE Expert" e il numero di identificazione individuale di ciascun esperto possono essere visualizzati e verificati in "Certipedia".

Ulteriori informazioni su:

www.tecnicum.com/mce-expert

mce . expert
Machinery CE Expert

tec.nicum:

Centri di assistenza e ingegneria globali

tec.nicum – Solutions & Services GmbH è una filiale del Gruppo Schmersal. Offre un'ampia gamma di servizi relativi ai macchinari e alla sicurezza sul lavoro. tec.nicum è costituita da una rete di consulenza globale di ingegneri certificati da TÜV Rheinland per la sicurezza funzionale e di esperti CE di macchinari. I servizi possono essere utilizzati in tutto il mondo.

I servizi offerti da tec.nicum si basano su sei elementi: Il trasferimento delle conoscenze nell'area academy, i servizi di consulenza nell'area di consulting, la progettazione di soluzioni di sicurezza nell'area di engineering, l'implementazione pratica nell'area di integration, lo sviluppo di soluzioni software e di nuove tecnologie digitali nell'area di digitalisation e la fornitura di soluzioni complete nell'area di outsourcing.



Italia

Via Molino Vecchio, 206
25010 Borgosatollo (BS)
info-it@tecnicum.com
+39 030 2507411



Europa

Friedrichstraße 65
66459 Kinkel (Germania)
europe@tecnicum.com
+49 6841 77780-0



Asia-Pacifico

Plot No G 7/1, Ranjangaon MIDC
Taluka Shirur, Pune (India)
apac@tecnicum.com
+91 2138 614700



Nord America

8545 Challenger Drive
Indianapolis, IN 46241 (USA)
north-america@tecnicum.com
+1 888 496-5143



America Latina

Av. Brasil, 815 – Jardim Esplanada
CEP 18557-646, Boituva (Brasile)
latam@tecnicum.com
+55 15-32 63-98 00



In tutto il mondo

Möddinghofe 30
42279 Wuppertal (Germania)
global@tecnicum.com
+49 202 6474-932