



*Catalogo dei corsi offerti dal centro
di trasferimento tecnologico
“Puglia Innovation Center for
Safety and Security - PICS2”*

Sommario

Cyber sicurezza per Imprese e Pubbliche Amministrazioni	3
CY1: Cybersecurity Awareness	3
CY2: Cyber Security e Digital Transformation.....	3
CY3: Information Security Management: Governance, Risk e Compliance	4
CY4: Security Program Management & Operations	5
CY5: Tutela delle informazioni strategiche	6
CY6: Security Assessment & Risk Management.....	7
CY7: IoT Security.....	8
CY8: Cybersecurity issues in food and beverage industry: stato dell'arte e prospettive future.....	9
CY9: Il Building Information Modelling (BIM) ed i connessi aspetti di cyber sicurezza: stato dell'arte e prospettive future	10
CY10: Advanced Cybersecurity	11
Formazione sulla Sicurezza: Corsi e Aggiornamenti per un Ambiente di Lavoro Protetto	13
SA1: Safety Management nei processi industriali	13
SA2: Safety Management nell'Industria 4.0	14
SA3: Prevenzione e Gestione degli Incidenti	14
SA4: Digital Safety Monitoring.....	15
SA5: Robotica collaborativa e Safety.....	15
SA6: Safety Data Analysis	16
SA7: Cloud Safety Management System	16
SA8: Data Protection Officer	17
SA9: Antiriciclaggio, anticorruzione e tutela dei dati	18
Digitalizzazione ed Innovazione: Tecnologie Emergenti, Benessere Digitale e Sostenibilità.....	19
DI1: Introduzione al Machine Learning ed al Deep Learning	19
DI2: Advanced Artificial Intelligence	19
DI3: Realtà aumentata e virtuale.....	20
DI4: Robotica Avanzata	20
DI5: Digitalizzazione dei processi aziendali	21
DI6: Digital Twinning.....	22
DI7: Internet of Things	22
DI8: Firma elettronica digitale.....	23
DI9: Il sistema cloud.....	23
DI10: Introduzione alla Psicologia della Digitalizzazione	23
DI11: Benessere Digitale e Gestione dello Stress Tecnologico.....	24
DI12: Competenze Digitali e Pensiero Critico nell'Era dell'Informazione.....	24
Competenze Manageriali	26
CM1: Progettazione europea.....	26
CM2: Responsabile Servizio Export (livello base)	26
CM3: Responsabile Servizio Export (livello avanzato)	27
CM4: Comunicazione non verbale	28

CM5: Comunicazione aziendale	29
CM6: Design Thinking	29
I corsi di formazione per le Pubbliche Amministrazioni	30
PA1: Contratti pubblici	30
PA2: I contratti sottosoglia.....	30
PA3: La gestione ed il recupero dei crediti nelle amministrazioni pubbliche	31
PA4: Il diritto di accesso ai documenti amministrativi	31
PA5: Il risarcimento del danno a carico della P.A. in sede amministrativa e civile	32
PA6: Guida alla gestione del contenzioso nei contratti pubblici.....	33
PA7: Governance e politiche per la trasformazione digitale nella PA.....	34
PA8: Project Management per la PA Digitale.....	35
PA9: Open Data per la PA digitale.....	36
PA10: Project Financing per la PA digitale	37
PA11: Comunicazione Digitale e Orientamento al Cittadino nella PA.....	38
PA12: I Processi della PA nell'Economia Digitale	39
PA13: Le tecnologie abilitanti per la PA digitale	39
PA14: Misurazione Performance e KPI per la PA Digitale	40
PA15: Organizzazione della PA digitale.....	41
PA16: Il Public Procurement nella PA digitale.....	42

Cyber sicurezza per Imprese e Pubbliche Amministrazioni

CY1: Cybersecurity Awareness

Obiettivi del corso	Questo corso propone un'introduzione sull'importanza del fattore umano nella sicurezza informatica. Ai partecipanti verranno introdotti i concetti di dati e informazioni, al fine di poter comprendere a pieno i motivi per cui è importante la loro protezione. Verranno quindi spiegati i principali metodi di attacco e i meccanismi di difesa e protezione atti a contrastarli. Oltre ai meccanismi di difesa solitamente implementati per difendere i dati, verrà poi evidenziato il ruolo fondamentale dell'essere umano, e come un comportamento non idoneo può rendere vane anche le difese più strutturate. Saranno quindi illustrati tutti i comportamenti potenzialmente rischiosi per la sicurezza dei dati, in maniera tale che gli studenti a fine corso siano in grado di riconoscere ed evitare le principali trappole del mondo cyber.
A chi si rivolge	<ul style="list-style-type: none"> - Responsabili IT: Professionisti che gestiscono l'infrastruttura tecnologica e devono garantire la sicurezza dei dati e dei sistemi informatici. - Dipendenti delle imprese: Personale di aziende di diverse dimensioni che necessita di conoscenze fondamentali sulla sicurezza informatica per proteggere le informazioni aziendali. - Operatori della Pubblica Amministrazione: Funzionari e impiegati pubblici che trattano dati sensibili e devono essere preparati a prevenire e gestire eventuali attacchi informatici. - Dirigenti e Manager: Decision-makers che devono comprendere le minacce alla sicurezza informatica per implementare adeguate politiche di sicurezza aziendale. - Piccoli imprenditori: Titolari di piccole e medie imprese (PMI) che desiderano proteggere le proprie attività da cyber minacce. - Personale non tecnico: Lavoratori che, pur non essendo specialisti IT, devono adottare buone pratiche di sicurezza per contribuire alla protezione complessiva dell'organizzazione.
Contenuti	<p>Introduzione alla Cybersecurity</p> <p>Il ruolo dell'essere umano nella cybersecurity</p> <p>Definizione di dati e informazioni</p> <p>Phishing e spear phishing</p> <p>Firewall e sistemi di rilevamento delle intrusioni (IDS)</p> <p>Consapevolezza e formazione del personale</p> <p>Uso di password deboli e gestione delle password</p> <p>Identificazione delle email di phishing</p> <p>Analisi di casi di successo e fallimento nella sicurezza informatica</p> <p>Sintesi delle principali tematiche trattate</p>
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY2: Cyber Security e Digital Transformation

Obiettivi del corso	Questo corso offre una panoramica completa sulla trasformazione digitale e sulla cybersecurity, con un focus particolare sull'impatto delle tecnologie digitali nelle imprese e nella Pubblica Amministrazione (PA). I partecipanti acquisiranno una
----------------------------	--

A chi si rivolge	<p>comprensione approfondita delle tecnologie dell'industria 4.0 e delle sfide della sicurezza informatica, esplorando tematiche fondamentali per proteggere i dati e ottimizzare i processi aziendali.</p> <ul style="list-style-type: none"> - Dirigenti e Manager: Responsabili aziendali e amministrativi che devono comprendere l'importanza della trasformazione digitale e della cybersecurity per implementare strategie efficaci e sicure. - Responsabili IT e Professionisti del Settore Tecnologico: Personale tecnico che necessita di aggiornamenti sulle ultime tecnologie dell'industria 4.0 e sulle pratiche di cybersecurity per proteggere le infrastrutture informatiche. - Dipendenti della Pubblica Amministrazione: Funzionari e impiegati che gestiscono dati sensibili e devono essere informati sulle nuove tecnologie e sui rischi informatici per garantire la sicurezza delle informazioni pubbliche. - Piccoli Imprenditori e Start-up: Titolari di piccole e medie imprese che desiderano adottare tecnologie digitali per migliorare l'efficienza aziendale e proteggere le loro attività da minacce informatiche. - Professionisti della Sicurezza: Esperti di sicurezza fisica e logica che vogliono approfondire la loro conoscenza della cybersecurity e delle tecniche di protezione contro attacchi informatici. - Personale non Tecnico: Lavoratori di vari settori che, pur non avendo una formazione tecnica, devono comprendere le basi della trasformazione digitale e della sicurezza informatica per contribuire alla protezione complessiva dell'organizzazione.
Contenuti	<ul style="list-style-type: none"> - Trasformazione Digitale: impatto sulle imprese e PA - Tecnologie digitali dell'industria 4.0: introduzione e vantaggi - Ruolo delle tecnologie digitali sui processi di business - Cybersecurity: una visione generale - Lo spazio: Surface Web, Deep & Dark web - Cosa c'è nel Dark web - Sicurezza fisica e logica - Cos'è la cybersecurity - Cosa sono le reti digitali - IT/OT Security - Social Engineering, Phishing, DDOS, APT, Brute Force Attacks
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY3: Information Security Management: Governance, Risk e Compliance

Obiettivi del corso	<p>Il corso è stato progettato con l'obiettivo di fornire una conoscenza approfondita e completa della gestione dei rischi informatici. In un'epoca in cui la tecnologia digitale è profondamente integrata nella nostra vita quotidiana, è cruciale che i giovani comprendano l'importanza di proteggere le infrastrutture digitali e i dati sensibili da minacce e vulnerabilità sempre più sofisticate.</p> <p>Il modulo introduce i concetti fondamentali della gestione del rischio informatico. I partecipanti impareranno a riconoscere il significato del rischio nel contesto della cybersecurity, comprendendo l'importanza della sua gestione per la protezione delle informazioni e dei sistemi. L'identificazione, la valutazione e l'analisi dei rischi rappresentano un pilastro fondamentale del modulo. I frequentanti approfondiranno le metodologie qualitative e quantitative per identificare e valutare i rischi ed identificare le opportune strategie di mitigazione. Impareranno a utilizzare tecniche di analisi per determinare l'impatto e la probabilità dei rischi; esploreranno diverse misure preventive e protettive progettate per ridurre i rischi informatici.</p>
----------------------------	--

A chi si rivolge	<ul style="list-style-type: none"> - Responsabili della Sicurezza Informatica (CISO) e IT Security Managers: Professionisti che sovrintendono la sicurezza delle informazioni e gestiscono le strategie di sicurezza aziendali. - Risk Managers: Esperti nella valutazione e gestione del rischio, incaricati di identificare, analizzare e mitigare i rischi aziendali. - Compliance Officers: Responsabili della conformità che garantiscono che l'organizzazione aderisca a normative come GDPR, NIST e gli standard della famiglia ISO27000. - IT Auditors: Professionisti che conducono audit di sicurezza, valutano l'efficacia dei controlli e gestiscono le attività di remediation. - Security Operation Center (SOC) Analysts: Analisti che monitorano e rispondono agli incidenti di sicurezza, utilizzando strumenti come SIEM e tecniche di Threat Hunting. - Responsabili della Continuità Operativa e Disaster Recovery: Professionisti che sviluppano e implementano piani per garantire la continuità aziendale e la ripresa dopo disastri. - Network Security Engineers: Ingegneri che si occupano della sicurezza delle reti, del controllo degli accessi e della protezione degli endpoint. - Cloud Security Specialists: Esperti nella sicurezza degli ambienti cloud e virtualizzati, che implementano tecnologie di criptazione e protezione delle applicazioni. - Innovation and Technology Managers: Professionisti che lavorano con nuove tecnologie come l'intelligenza artificiale e la realtà aumentata, garantendo la loro sicurezza nell'ambiente aziendale. - Developers and Application Security Specialists: Sviluppatori e specialisti della sicurezza delle applicazioni, focalizzati sulla protezione delle applicazioni e sull'adozione delle migliori pratiche di sicurezza come quelle fornite da CIS e OWASP.
Contenuti	<ul style="list-style-type: none"> - Governance e Gestione del Rischio. - Rischio: analisi, controllo delle minacce, valutazione e gestione. - Controlli, Conformità e Gestione degli accessi. - Gestione del ciclo di vita dei controlli di sicurezza, monitoraggio e mantenimento. - Conformità: GDPR, NIST e gli standard della famiglia ISO27000. Linee guida e Best Practice: CIS e OWASP. - Tipologie di Audit e gestione delle remediation. - Introduzione ai concetti di gestione e risposta agli incidenti. - Gestione della Business Continuity e Piano di Disaster Recovery. - Security Operation: SIEM, Vulnerability Management, Vulnerability Assessment, Penetration Test e Threat Hunting. Condivisione degli scenari nei diversi ambiti. - Controllo degli accessi, sicurezza fisica, sicurezza delle reti. - Protezione degli endpoint e sicurezza delle applicazioni. - Tecnologie di criptazione, sicurezza degli ambienti virtualizzati e sicurezza del cloud computing. - Nuove tecnologie: intelligenza artificiale, realtà aumentata, ecc.
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY4: Security Program Management & Operations

Obiettivi del corso	Questo corso avanzato offre una comprensione approfondita della pianificazione strategica e della gestione della sicurezza delle informazioni in un'organizzazione. È pensato per
----------------------------	---

A chi si rivolge	professionisti che desiderano sviluppare competenze specialistiche nella creazione e manutenzione di programmi di sicurezza efficaci, proteggendo le informazioni azienda garantendo la continuità operativa. I partecipanti impareranno a gestire gli aspetti finazi legati alla sicurezza, come l'allocazione delle risorse, la definizione delle metriche finan e la gestione del budget. Inoltre, il corso affronta le sfide della gestione dei vendor e di terze parti, insegnando come selezionare, valutare e monitorare i fornitori di servizi pe garantire che rispettino gli standard di sicurezza. Attraverso un approccio teorico e pra corso prepara i partecipanti a implementare strategie di sicurezza sostenibili e ad adat alle specifiche esigenze organizzative, con l'obiettivo di consolidare la protezione delle informazioni aziendali e rafforzare la propria carriera nel settore della sicurezza inform
Contenuti	<p>Il corso si rivolge a professionisti e manager che occupano ruoli chiave nella gestione della sicurezza informatica e nella pianificazione strategica delle organizzazioni. In particolare, è pensato per dirigenti IT, responsabili della sicurezza delle informazioni (CISO), risk manager e professionisti coinvolti nella gestione dei budget e delle risorse per la sicurezza. È indicato anche per coloro che si occupano di compliance e gestione dei fornitori, come i procurement manager e i vendor manager. Il corso è adatto a chiunque desideri sviluppare competenze avanzate nella progettazione e implementazione di programmi di sicurezza, nella gestione delle risorse finanziarie per la sicurezza e nel coordinamento con terze parti e fornitori esterni.</p> <ul style="list-style-type: none"> - Pianificazione strategica. Organizzazione, struttura, obiettivi, stakeholder, aspetti finanziari e piano strategico. - Progettazione, sviluppo e manutenzione di un programma di sicurezza delle informazioni per la propria organizzazione. - Gestione degli aspetti finanziari legati alla sicurezza: risorse, definizione delle metriche finanziarie, rinnovo delle tecnologie, ottenimento e gestione del budget. - Concetti base per la gestione di gare e appalti e servizi gestiti da terzi (TCO, RFI, RFP, SLA, ec...). - Gestione dei vendor e delle terze parti.
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY5: Tutela delle informazioni strategiche

Obiettivi del corso	Il corso fornisce una formazione avanzata sui principi di sicurezza delle informazioni strategiche e delle infrastrutture informatiche. I partecipanti acquisiranno una comprensione approfondita delle autorità, degli organi e degli uffici coinvolti nella gestione delle informazioni sensibili, con particolare attenzione alle autorizzazioni necessarie per trattare dati strategici. Viene analizzato il contesto normativo nazionale relativo alla sicurezza delle informazioni classificate e il ruolo della legislazione nella tutela dei dati. Il corso approfondisce le minacce e i rischi informatici, i modelli di protezione delle infrastrutture strategiche e il compito del security manager. Inoltre, sono trattate le metodologie di analisi del rischio, le misure di sicurezza fisica e le procedure per proteggere le comunicazioni sicure. Si esplorano anche le applicazioni crittografiche per la protezione delle reti e la certificazione dei prodotti per la sicurezza, come gli apparati tempest e le camere anecoiche. Il corso si conclude con una panoramica sulle migliori pratiche di sicurezza per la protezione e il trasporto sicuro di materiali e documenti sensibili.
A chi si rivolge	Il corso si rivolge a professionisti e responsabili della sicurezza delle informazioni, come i security manager, che desiderano acquisire competenze avanzate nella protezione delle informazioni strategiche e sensibili. È pensato per dirigenti e responsabili IT, compliance officers e risk managers che operano in ambienti ad alta sicurezza, sia nel settore pubblico che privato. Inoltre, è adatto a coloro che si

Contenuti	<p>occupano della gestione delle infrastrutture informatiche strategiche, della sicurezza delle comunicazioni e della protezione dei dati, come responsabili della protezione dei dati (DPO) e analisti della sicurezza informatica. Il corso è particolarmente utile per chi gestisce documenti e materiali classificati e per operatori economici coinvolti in progetti che richiedono elevati standard di sicurezza.</p> <ul style="list-style-type: none"> - Principi di sicurezza delle informazioni strategiche. - Organizzazione (Autorità, organi e uffici, ocs, sps, organi periferici, operatori economici) classifiche e qualifiche. - Autorizzazioni alla trattazione di informazioni strategiche. - Principi di sicurezza delle infrastrutture informatiche strategiche. - Definizioni e contesto normativo. - Minaccia e rischio informatico. - Modelli di protezione delle infrastrutture informatiche strategiche. - La legislazione nazionale in materia di tutela delle informazioni classificate. - Funzione del security manager. - Definizioni e principi della sicurezza delle comunicazioni. - Metodologie di risk analysis dei sistemi di protezione delle comunicazioni e sicurezza crittografica. - Misure di sicurezza fisica. - Procedure di sicurezza. - Applicazioni alle reti di comunicazioni sicure. - Certificazione di prodotti per la sicurezza (apparati tempest, camere tempest/anecoiche). - Sicurezza delle comunicazioni (materiali e documenti, autorizzazioni e organizzazione, protezione conservazione e trasporto).
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY6: Security Assessment & Risk Management

Obiettivi del corso	<p>Il corso è progettato per fornire ai partecipanti le competenze necessarie per condurre valutazioni della sicurezza e gestire i rischi informatici in modo efficace. Durante il corso, i partecipanti apprenderanno le metodologie e gli strumenti utilizzati per identificare, analizzare e mitigare i rischi associati alle infrastrutture tecnologiche e alle operazioni aziendali.</p> <p>Il programma esplorerà le tecniche di valutazione della sicurezza per rilevare vulnerabilità nei sistemi informatici, nelle reti e nelle applicazioni, nonché le strategie per migliorare le difese contro le minacce esterne e interne. I partecipanti impareranno a sviluppare piani di gestione del rischio che includano l'identificazione dei rischi, la loro valutazione in termini di probabilità e impatto, e la definizione di contromisure adeguate.</p> <p>Il corso tratterà inoltre i concetti di valutazione dell'impatto aziendale e business continuity, con focus su come garantire la resilienza operativa in caso di incidenti di sicurezza. Saranno esplorati anche i principali framework e standard internazionali, come NIST, ISO 27001, e CIS, utili per implementare e monitorare efficaci strategie di gestione del rischio.</p> <p>Infine, il corso fornirà una panoramica delle best practice per implementare una cultura di sicurezza continua, attraverso il monitoraggio, la revisione periodica e l'aggiornamento delle politiche di gestione del rischio.</p>
A chi si rivolge	Il corso "Security Assessment & Risk Management" si rivolge a professionisti e responsabili della sicurezza informatica, come security managers, analisti di sicurezza e

Contenuti	<p>CISO (Chief Information Security Officer), che sono incaricati di proteggere le infrastrutture tecnologiche aziendali e di gestire i rischi informatici. È ideale per responsabili IT, risk managers, consulenti di sicurezza e auditori di sicurezza che devono valutare le vulnerabilità dei sistemi e implementare misure di protezione. Inoltre, il corso è utile a chiunque lavori in ambito compliance e governance della sicurezza, come responsabili della protezione dei dati (DPO) e professionisti della gestione delle crisi. È anche adatto a manager operativi e responsabili delle infrastrutture tecnologiche che vogliono comprendere come proteggere le risorse aziendali da minacce e attacchi informatici, migliorando la resilienza dell'organizzazione.</p> <ul style="list-style-type: none"> - Introduzione alla Sicurezza Informatica: Concetti fondamentali di sicurezza, minacce e vulnerabilità. - Metodologie di Security Assessment: Tecniche per identificare, valutare e mitigare le vulnerabilità nei sistemi informatici. - Framework di Riferimento e Standard: Introduzione a standard internazionali come NIST, ISO 27001, CIS, e le loro applicazioni nella gestione della sicurezza. - Gestione del Rischio: Metodi per l'identificazione, la valutazione e la mitigazione dei rischi informatici. - Risk Assessment: Tecniche per valutare la probabilità e l'impatto dei rischi sui sistemi informatici e sulle operazioni aziendali. - Business Impact Analysis (BIA): Metodologie per analizzare l'impatto delle minacce sulle operazioni aziendali e sulla continuità del business. - Contromisure e Strategie di Mitigazione del Rischio: Soluzioni pratiche per ridurre il rischio attraverso controlli tecnici, amministrativi e fisici. - Gestione delle Risorse e Prioritizzazione del Rischio: Come allocare risorse per la gestione del rischio e come stabilire priorità in base al rischio. - Piani di Contingenza e Business Continuity: Sviluppo di piani per garantire la resilienza e la ripresa in caso di incidenti di sicurezza. - Monitoraggio e Reporting del Rischio: Tecniche per monitorare continuamente i rischi e per produrre report di gestione del rischio efficaci. - Gestione delle Crisi e Incident Response: Come gestire e rispondere agli incidenti di sicurezza informatica in modo efficace. - Best Practices di Risk Management: Approcci strategici e operativi per integrare la gestione del rischio nella cultura aziendale.
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY7: IoT Security

Obiettivi del corso	<p>Il corso "IoT Security" offre una formazione completa sulla protezione dei dispositivi e delle reti IoT. I partecipanti esploreranno le vulnerabilità comuni dei dispositivi IoT e delle reti ad essi connesse, imparando a implementare soluzioni di sicurezza per proteggere i dati e prevenire attacchi come DDoS e botnet. Il corso coprirà tecniche di protezione come la crittografia, l'autenticazione sicura, la gestione delle vulnerabilità e l'uso di firewall specifici per IoT. Verranno anche trattati aspetti normativi come il GDPR e l'impatto delle leggi sulla sicurezza dei dati. Al termine, i partecipanti saranno in grado di applicare best practices e rispondere efficacemente a minacce IoT.</p>
A chi si rivolge	<p>Il corso "IoT Security" si rivolge a professionisti e responsabili della sicurezza informatica, come security managers, CISO, analisti di sicurezza e tecnici IT, che desiderano acquisire competenze specifiche sulla protezione dei dispositivi IoT e delle reti ad essi collegate. È indicato per chi gestisce infrastrutture IT, reti aziendali e sistemi IoT in contesti aziendali o industriali. Inoltre, il corso è utile per ingegneri di sistema, sviluppatori di software e specialisti in sicurezza delle reti che lavorano con dispositivi IoT o soluzioni connesse. È anche adatto a professionisti della compliance che devono affrontare le normative e le sfide legali relative alla sicurezza dei dati nell'ambito IoT.</p>

Contenuti	<ul style="list-style-type: none"> - Introduzione all'IoT e alle sue vulnerabilità: Comprensione dei dispositivi IoT, delle reti e delle potenziali minacce a cui sono esposti. - Minacce e attacchi nell'IoT: Analisi degli attacchi comuni come DDoS, botnet, malware, e vulnerabilità dei dispositivi IoT. - Principi di sicurezza IoT: Fondamenti per la protezione di dispositivi IoT e reti connesse, inclusi concetti di riservatezza, integrità e disponibilità dei dati. - Crittografia e protezione dei dati: Tecniche per proteggere i dati scambiati dai dispositivi IoT tramite la crittografia e altre tecnologie di protezione. - Gestione dell'autenticazione e dell'autorizzazione: Best practices per l'autenticazione sicura e la gestione dei permessi nei dispositivi IoT. - Reti IoT sicure: Protezione delle reti IoT tramite firewall, segmentazione delle reti e monitoraggio delle comunicazioni. - Gestione delle vulnerabilità IoT: Tecniche per identificare, valutare e risolvere le vulnerabilità nei dispositivi IoT. - Normative e compliance: Conformità con le leggi e le normative, come il GDPR, relative alla protezione dei dati nell'IoT. - Sicurezza nelle applicazioni IoT: Protezione delle applicazioni che gestiscono dispositivi IoT, compresa la gestione degli aggiornamenti software. - Soluzioni avanzate di sicurezza: Uso di tecnologie emergenti come l'intelligenza artificiale per rilevare minacce IoT e ottimizzare la sicurezza. - Risposta agli incidenti e monitoraggio della sicurezza: Gestione degli incidenti di sicurezza e l'importanza del monitoraggio continuo per rilevare comportamenti anomali nei dispositivi IoT.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY8: Cybersecurity issues in food and beverage industry: stato dell'arte e prospettive future

Obiettivi del corso	<p>Il corso mira a fornire una panoramica completa delle attuali sfide di sicurezza informatica specifiche per il settore alimentare e delle bevande. Gli obiettivi includono l'analisi delle minacce e vulnerabilità presenti nelle infrastrutture digitali di questo settore, l'approfondimento delle tecnologie e delle pratiche di sicurezza attualmente adottate e la valutazione delle normative e degli standard di conformità pertinenti. Inoltre, il corso esplorerà le tendenze emergenti e le innovazioni tecnologiche che potrebbero influenzare la sicurezza informatica nel futuro, preparando i partecipanti a sviluppare strategie di difesa efficaci per proteggere le loro organizzazioni da potenziali attacchi.</p>
A chi si rivolge	<p>Il corso si rivolge a professionisti e responsabili della sicurezza informatica all'interno dell'industria alimentare e delle bevande. È ideale per IT managers, CISO (Chief Information Security Officers), responsabili della qualità e compliance officers che necessitano di una conoscenza approfondita delle minacce informatiche specifiche del settore. Inoltre, il corso è adatto a consulenti di sicurezza informatica, analisti di rischio e dirigenti aziendali che desiderano comprendere meglio come proteggere le infrastrutture digitali e i dati sensibili. Anche i professionisti della supply chain e gli ingegneri di sistema troveranno utile questo corso per sviluppare strategie di sicurezza robuste e conformi alle normative.</p>
Contenuti	<ul style="list-style-type: none"> - Panoramica delle minacce informatiche nel settore alimentare e delle bevande: Analisi delle principali minacce e vulnerabilità che colpiscono l'industria. - Tecnologie e pratiche di sicurezza attualmente adottate: Esplorazione delle soluzioni di sicurezza utilizzate per proteggere le infrastrutture digitali. - Normative e standard di conformità: Studio delle leggi e delle regolamentazioni specifiche che influenzano la sicurezza informatica nel settore.

Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

- Casi di studio e analisi di incidenti reali: Esame di esempi concreti di attacchi informatici e delle risposte adottate dalle aziende.
- Metodologie di valutazione del rischio: Tecniche per identificare, valutare e mitigare i rischi informatici specifici del settore.
- Tendenze emergenti in cybersecurity: Discussione delle innovazioni tecnologiche e delle nuove minacce che potrebbero influenzare il settore in futuro.
- Strategie di difesa e risposta agli incidenti: Sviluppo di piani per la prevenzione, rilevamento e risposta agli attacchi informatici.
- Protezione dei dati sensibili: Approcci per garantire la sicurezza dei dati dei clienti, dei fornitori e delle operazioni aziendali.
- Sicurezza della supply chain: Analisi delle vulnerabilità e delle soluzioni per proteggere l'intera catena di approvvigionamento.

CY9: Il Building Information Modelling (BIM) ed i connessi aspetti di cyber sicurezza: stato dell'arte e prospettive future

Obiettivi del corso	Il corso offre una panoramica completa delle sfide di sicurezza informatica legate all'uso del BIM nel settore delle costruzioni. I partecipanti esploreranno l'integrazione tra BIM e cybersecurity, analizzando le vulnerabilità specifiche dei modelli digitali e delle piattaforme collaborative utilizzate nella progettazione e gestione delle costruzioni. Il corso tratterà le tecnologie e le pratiche di sicurezza attualmente adottate, le normative e gli standard di conformità, e le tendenze emergenti che potrebbero influenzare il futuro della sicurezza nel BIM. L'obiettivo è fornire ai partecipanti le competenze necessarie per proteggere efficacemente le infrastrutture digitali e sviluppare strategie di difesa avanzate contro le minacce informatiche.
A chi si rivolge	Il corso si rivolge a professionisti nel settore delle costruzioni e della progettazione, come ingegneri, architetti e project managers, che utilizzano il BIM nei loro progetti e sono responsabili della protezione delle informazioni digitali. È ideale per IT managers e CISO (Chief Information Security Officers) che operano all'interno delle aziende di costruzione e necessitano di una conoscenza approfondita delle sfide di sicurezza legate al BIM. Inoltre, il corso è utile per consulenti di sicurezza informatica, specialisti in gestione dei dati e responsabili della conformità che desiderano comprendere come integrare efficacemente le pratiche di cybersecurity nel contesto del BIM. Anche i professionisti della gestione delle infrastrutture e delle facility che utilizzano il BIM per la manutenzione e l'operatività degli edifici troveranno il corso particolarmente rilevante.
Contenuti	<ul style="list-style-type: none"> - Introduzione al Building Information Modelling (BIM): Principi fondamentali del BIM, utilizzo e importanza nel settore delle costruzioni. - Panoramica della cybersecurity nel BIM: Analisi delle minacce informatiche specifiche per i modelli BIM e le piattaforme collaborative. - Tecnologie di sicurezza per il BIM: Strumenti e tecniche per proteggere i dati e le informazioni all'interno dei modelli BIM. - Gestione delle vulnerabilità del BIM: Identificazione e mitigazione delle vulnerabilità nei processi BIM e nelle infrastrutture IT correlate. - Normative e standard di conformità: Studio delle normative e degli standard di sicurezza applicabili al BIM. - Best practices di cybersecurity nel BIM: Approcci e pratiche consigliate per garantire la sicurezza dei dati BIM. - Casi di studio: Analisi di incidenti di sicurezza nel BIM e delle strategie di risposta adottate.

	<ul style="list-style-type: none"> - Integrazione della sicurezza nel ciclo di vita del BIM: Come incorporare la sicurezza in ogni fase del ciclo di vita del progetto BIM, dalla progettazione alla gestione operativa. - Future trends in BIM cybersecurity: Esplorazione delle tendenze emergenti e delle tecnologie innovative che influenzeranno la sicurezza informatica nel BIM nei prossimi anni.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CY10: Advanced Cybersecurity

Obiettivi del corso	<p>Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita della sicurezza offensiva, distinguendo tra sicurezza difensiva e offensiva e analizzando i principi e gli obiettivi dell'offensive security. Si esplorerà l'intero ciclo di vita di un attacco informatico, dalle fasi iniziali di ricognizione e scansione fino alla post-sfruttamento e alla generazione di report. Il corso approfondirà il Vulnerability Assessment, mostrando come eseguire scansioni automatizzate e manuali per identificare vulnerabilità nelle reti, nonché l'introduzione al Penetration Testing, esplorando tecniche di attacco come SQL Injection e Buffer Overflow. Saranno fornite anche esperienze pratiche su come eseguire attacchi, utilizzare strumenti come Metasploit, e configurare sistemi di rilevamento delle intrusioni, come IDS/IPS, per monitorare e prevenire minacce.</p>
A chi si rivolge	<p>Il corso si rivolge a professionisti della sicurezza informatica, come penetration tester, security analysts, CISO (Chief Information Security Officers), IT managers e responsabili della sicurezza delle reti, che desiderano acquisire competenze pratiche nella sicurezza offensiva e nelle tecniche di attacco. È ideale anche per consulenti di sicurezza e esperti di IT che lavorano nella protezione delle infrastrutture digitali e vogliono approfondire le proprie conoscenze in vulnerability assessment e penetration testing. Inoltre, il corso è adatto a chiunque sia coinvolto nella gestione dei rischi informatici e nella protezione delle reti aziendali o istituzionali.</p>
Contenuti	<p>Introduzione alla Sicurezza Offensiva</p> <ul style="list-style-type: none"> - Definizione e importanza della sicurezza offensiva - Differenze tra sicurezza difensiva e offensiva - Obiettivi e principi dell'offensive security <p>Comprendere il Ciclo di Vita di un Attacco Informatico</p> <ul style="list-style-type: none"> - Fasi di un attacco informatico: Reconnaissance, Scanning, Exploitation, Post-Exploitation, Reporting - Analisi dei principali attacchi e delle relative tecniche <p>Introduzione al Vulnerability Assessment (VA)</p> <ul style="list-style-type: none"> - Definizione e obiettivi del Vulnerability Assessment - Strumenti e tecniche per la scansione automatizzata e semi-automatizzata - Verifiche manuali delle vulnerabilità <p>Esecuzione di Vulnerability Assessment</p> <ul style="list-style-type: none"> - Configurazione degli strumenti di VA (es. Nessus, OpenVAS) - Analisi dei risultati delle scansioni - Pratica guidata: esecuzione di un Vulnerability Assessment su una rete simulata <p>Introduzione al Penetration Testing (PT)</p> <ul style="list-style-type: none"> - Definizione e obiettivi del Penetration Testing - Differenze tra VA e PT

	<ul style="list-style-type: none">- Fasi del Penetration Testing: Planning, Discovery, Exploitation, Reporting
	Tecniche di Attacco e Sfruttamento delle Vulnerabilità
	<ul style="list-style-type: none">- Esempi di tecniche di attacco: SQL Injection, Cross-Site Scripting (XSS), Buffer Overflow- Strumenti utilizzati nel PT (es. Metasploit, Burp Suite)- Identificazione e sfruttamento delle vulnerabilità note e oDay
	Pratica di Penetration Testing
	<ul style="list-style-type: none">- Esecuzione pratica di un Penetration Testing su una rete simulata- Utilizzo di tecniche di attacco per accedere a informazioni riservate- Reporting e documentazione dei risultati
	Metodologie di Scoperta delle Intrusioni
	<ul style="list-style-type: none">- Tecniche per il rilevamento delle intrusioni- Strumenti di Intrusion Detection System (IDS) e Intrusion Prevention System (IPS)- Implementazione pratica di un IDS/IPS su una rete simulata
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

Formazione sulla Sicurezza: Corsi e Aggiornamenti per un Ambiente di Lavoro Protetto

SA1: Safety Management nei processi industriali

Obiettivi del corso	Il corso ha l'obiettivo di fornire una solida comprensione delle pratiche e delle normative necessarie per gestire la sicurezza nei contesti industriali. I partecipanti acquisiranno competenze nella valutazione dei rischi e nella gestione della sicurezza per garantire ambienti di lavoro sicuri e conformi alle leggi. Il corso esplorerà le tecniche per identificare, prevenire e mitigare i pericoli legati a macchinari, impianti e processi, nonché le metodologie per sviluppare e implementare piani di emergenza efficaci. Inoltre, si affronteranno le migliori pratiche per la formazione del personale e la promozione di una cultura della sicurezza, al fine di ridurre gli incidenti e migliorare la gestione dei rischi all'interno delle industrie.
A chi si rivolge	Il corso si rivolge a responsabili della sicurezza, safety manager, ingegneri e tecnici di sicurezza che operano in contesti industriali e manifatturieri. È ideale anche per dirigenti aziendali, responsabili della qualità, consulenti in materia di sicurezza sul lavoro e formatori che desiderano approfondire le tecniche di gestione della sicurezza nei processi produttivi. Inoltre, il corso è utile per operatori e supervisori che devono implementare e monitorare le misure di sicurezza quotidiane, nonché per professionisti del settore normativo e della compliance impegnati a garantire la conformità alle normative in materia di salute e sicurezza sul lavoro.
Contenuti	<ul style="list-style-type: none"> - Introduzione alla gestione della sicurezza nei processi industriali: Principi e importanza della sicurezza nei contesti industriali, ruoli e responsabilità. - Valutazione dei rischi industriali: Metodologie per identificare e analizzare i rischi legati alle attività industriali, strumenti per la valutazione dei pericoli. - Normative di sicurezza e conformità: Studio delle leggi e regolamenti internazionali, nazionali e locali, come le direttive OSHA, ISO 45001, e le normative europee. - Sicurezza nei processi produttivi: Tecniche di gestione della sicurezza in impianti industriali, gestione di macchinari, attrezzature e impianti per minimizzare i rischi. - Tecniche di prevenzione e mitigazione: Strategie per prevenire incidenti e malattie professionali, implementazione di misure preventive e di controllo. - Gestione delle emergenze industriali: Pianificazione e sviluppo di piani di emergenza, procedure di evacuazione, gestione degli incidenti. - Formazione e sensibilizzazione del personale: Metodologie per formare i dipendenti e promuovere una cultura della sicurezza sul posto di lavoro. - Gestione dei dispositivi di protezione individuale (DPI): Uso e monitoraggio dell'efficacia dei DPI, norme relative all'adozione dei dispositivi di sicurezza. - Tecnologie per la sicurezza industriale: Introduzione agli strumenti tecnologici per la sicurezza, come sensori, sistemi di monitoraggio e automazione. - Audit e monitoraggio della sicurezza: Tecniche per la conduzione di audit di sicurezza, monitoraggio delle performance e miglioramento continuo dei processi di sicurezza.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA2: Safety Management nell'Industria 4.0

Obiettivi del corso	Il corso ha l'obiettivo di fornire una comprensione approfondita dei rischi legati alla sicurezza nei contesti industriali automatizzati e digitalizzati. I partecipanti apprenderanno come valutare i rischi in ambienti automatizzati, comprendere le dinamiche dell'interazione uomo-macchina nei sistemi intelligenti e affrontare le sfide della safety nei processi produttivi interconnessi. Un altro obiettivo chiave è quello di fornire le competenze necessarie per gestire efficacemente le emergenze in impianti digitalizzati, sviluppando strategie per minimizzare i rischi e garantire la sicurezza operativa in scenari complessi. Il corso prepara i partecipanti a implementare soluzioni di sicurezza integrate in ambienti altamente tecnologici.
A chi si rivolge	Il corso si rivolge a professionisti e responsabili della sicurezza industriale, come safety managers, responsabili della produzione, ingegneri di processo e responsabili della gestione dei rischi che lavorano in ambienti automatizzati e digitalizzati. È ideale anche per operatori di impianti automatizzati, tecnici di manutenzione e ingegneri industriali che desiderano approfondire la gestione della safety nei sistemi intelligenti e interconnessi. Inoltre, il corso è utile per i responsabili della gestione delle emergenze e i formatori in ambito safety, che sono coinvolti nella creazione di protocolli di sicurezza e nella gestione dei rischi nelle organizzazioni industriali.
Contenuti	<ul style="list-style-type: none"> - Valutazione rischi in ambienti automatizzati - Interazione uomo-macchina nei sistemi intelligenti - Safety nei processi di produzione interconnessi - Gestione emergenze in impianti digitalizzati
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA3: Prevenzione e Gestione degli Incidenti

Obiettivi del corso	Il corso l'obiettivo di fornire ai partecipanti le competenze necessarie per gestire efficacemente incidenti in vari contesti, dall'emergenza alla gestione della crisi. Gli obiettivi principali sono la formazione su come rispondere rapidamente e in modo organizzato a diversi tipi di incidenti, l'uso degli strumenti adeguati per il supporto alla gestione delle emergenze e la gestione delle comunicazioni durante e dopo l'incidente. Il corso mira anche a sviluppare le capacità di analisi post-incidente per migliorare la preparazione futura, a garantire che i piani di risposta siano sempre aggiornati e verificati, e a fornire una comprensione delle procedure di analisi forense e della catena di custodia. Infine, l'obiettivo è affrontare le diverse tipologie di incidenti, fornendo una preparazione pratica per la gestione di situazioni critiche in modo sistematico e sicuro.
A chi si rivolge	Il corso si rivolge a responsabili della sicurezza, emergency manager, responsabili delle operazioni aziendali, team di risposta alle emergenze, consulenti di gestione del rischio e professionisti della gestione delle crisi. È ideale per chi lavora in contesti ad alta criticità come industria, sanità, servizi pubblici e settore pubblico, e che ha la responsabilità di prevenire, rispondere e gestire gli incidenti, sia a livello operativo che strategico. Il corso è anche adatto a supervisori e coordinatori di team, che devono implementare e verificare i piani di risposta agli incidenti, nonché a chiunque desideri acquisire una preparazione approfondita nella gestione delle crisi e nella protezione delle risorse aziendali e istituzionali.
Contenuti	<ul style="list-style-type: none"> - Gestione e Risposta agli incidenti. - Strumenti a supporto. - Gestione delle comunicazioni. - Analisi Post-Incident.

	<ul style="list-style-type: none"> - Verifica dei piani di risposta. - Procedure e gestione della crisi. - Analisi forense e catena di custodia. - Affrontare le diverse tipologie di incidenti
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA4: Digital Safety Monitoring

Obiettivi del corso	Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita dell'utilizzo dei sistemi IoT (Internet of Things) per migliorare la sicurezza in tempo reale. I partecipanti impareranno come monitorare la sicurezza utilizzando dispositivi IoT avanzati, come sensori smart, per prevenire incidenti e raccogliere dati utili per l'analisi dei rischi. Inoltre, il corso esplorerà come utilizzare le dashboard per visualizzare e analizzare i dati di sicurezza in tempo reale, permettendo una risposta rapida e informata. Un altro obiettivo importante è comprendere come implementare la manutenzione predittiva per prevenire guasti e ottimizzare le operazioni di sicurezza, riducendo i rischi e migliorando l'efficienza operativa.
A chi si rivolge	Il corso si rivolge a professionisti e responsabili della sicurezza industriale e aziendale, come safety managers, responsabili della manutenzione e ingegneri di sicurezza, che desiderano implementare soluzioni IoT per il monitoraggio e la prevenzione degli incidenti. È anche utile per IT managers e data analysts che lavorano con sistemi di raccolta e analisi dati, nonché per tecnici di manutenzione predittiva e operatori industriali che vogliono integrare tecnologie avanzate per migliorare la sicurezza operativa. Il corso è adatto anche a chi è coinvolto nella progettazione e gestione di sistemi intelligenti per la sicurezza, come ingegneri e consulenti del settore IoT.
Contenuti	<ul style="list-style-type: none"> - Sistemi IoT per il monitoraggio della sicurezza - Dashboard e analisi dati safety in tempo reale - Sensori smart per la prevenzione incidenti - Manutenzione predittiva per la sicurezza
Durata	16 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA5: Robotica collaborativa e Safety

Obiettivi del corso	Gli obiettivi del corso con i contenuti indicati sono fornire ai partecipanti una comprensione approfondita delle normative e delle best practices per la gestione della sicurezza nei sistemi automatizzati e nei cobot. I partecipanti impareranno a configurare e implementare barriere di sicurezza smart, a programmare e gestire le safe zones (zone di sicurezza) per garantire un'interazione sicura tra operatori e robot, e a definire e applicare protocolli di emergenza efficaci per i sistemi robotizzati. Il corso mira a sviluppare competenze pratiche e teoriche per proteggere gli ambienti di lavoro automatizzati, minimizzando i rischi legati all'uso di tecnologie avanzate come i cobot, e garantendo la conformità alle normative di sicurezza industriale.
A chi si rivolge	Il corso si rivolge a professionisti e tecnici che lavorano nell'ambito dell'automazione industriale, come ingegneri di automazione, tecnici di robotica, responsabili della

Contenuti	<p>sicurezza industriale, safety manager e operatori di produzione. È ideale anche per project managers e responsabili della manutenzione che gestiscono o supervisionano l'integrazione di sistemi robotizzati e cobot in ambienti di lavoro. Inoltre, il corso è utile a consulenti di sicurezza e a chi è coinvolto nella progettazione, configurazione e gestione di impianti automatizzati, con un focus particolare sulla sicurezza e la gestione del rischio legato all'uso di tecnologie robotiche.</p> <ul style="list-style-type: none"> - Normative per cobot e sistemi automatizzati - Configurazione barriere di sicurezza smart - Programmazione safe zones - Protocolli di emergenza per sistemi robotizzati
Durata	16 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA6: Safety Data Analysis

Obiettivi del corso	<p>Gli obiettivi del corso sono fornire ai partecipanti le competenze per raccogliere e analizzare i dati relativi alla sicurezza, al fine di identificare indicatori predittivi di rischio che possano anticipare possibili incidenti o vulnerabilità. I partecipanti impareranno a integrare tecniche di machine learning per migliorare la capacità di prevenire incidenti, utilizzando algoritmi avanzati per analizzare modelli e comportamenti rischiosi. Inoltre, il corso si concentrerà sull'automatizzazione dei processi di reporting per la gestione della sicurezza, permettendo la generazione di KPI (Key Performance Indicators) sulla sicurezza in modo efficiente e tempestivo. In sintesi, il corso mira a migliorare le capacità di analisi e gestione del rischio attraverso l'uso di tecnologie avanzate, rendendo più efficiente la gestione della sicurezza aziendale.</p>
A chi si rivolge	<p>Il corso si rivolge a professionisti della sicurezza informatica, data analysts, responsabili della sicurezza e IT managers che desiderano utilizzare strumenti avanzati di analisi dei dati per migliorare la gestione della sicurezza aziendale. È particolarmente utile per analisti di rischio, esperti di machine learning, responsabili della compliance e chiunque sia coinvolto nella prevenzione e gestione degli incidenti di sicurezza in ambito aziendale. Inoltre, il corso è adatto a chi lavora con sistemi di monitoraggio della sicurezza e a chi è responsabile del reporting e della gestione delle performance aziendali in materia di sicurezza.</p>
Contenuti	<ul style="list-style-type: none"> - Raccolta e analisi dati sicurezza - Indicatori predittivi di rischio - Machine learning per prevenzione incidenti - Reporting automatizzato safety KPI
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA7: Cloud Safety Management System

Obiettivi del corso	<p>Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita delle soluzioni tecnologiche moderne per la gestione della sicurezza aziendale, focalizzandosi sull'uso delle piattaforme cloud per ottimizzare la gestione della sicurezza. Gli studenti apprenderanno come digitalizzare e gestire la documentazione relativa alla sicurezza, migliorando l'efficienza e la conformità alle normative. Inoltre, il</p>
----------------------------	--

A chi si rivolge	Il corso esplorerà l'utilizzo di app mobili per la segnalazione dei rischi, offrendo strumenti pratici per coinvolgere il personale nel monitoraggio della sicurezza. Verranno trattati anche gli aspetti dell'integrazione di queste tecnologie con i sistemi ERP aziendali, per garantire un flusso di informazioni continuo e centralizzato nella gestione della sicurezza aziendale.
Contenuti	Il corso si rivolge a professionisti e responsabili della sicurezza aziendale, come safety managers, security officers e responsabili della compliance, che desiderano aggiornare le proprie competenze nell'uso di tecnologie avanzate per la gestione della sicurezza. È ideale anche per IT managers e responsabili dei sistemi informativi che si occupano di integrare piattaforme digitali con i sistemi aziendali, nonché per consulenti di sicurezza che vogliono specializzarsi nell'implementazione di soluzioni cloud e digitali per la gestione dei rischi aziendali. Inoltre, il corso è adatto a chiunque lavori nell'ambito della digitalizzazione dei processi aziendali, come project managers e professionisti ERP, con particolare focus sulle soluzioni di sicurezza.
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA8: Data Protection Officer

Obiettivi del corso	Il corso si propone di formare la figura del Data Protection Officer (DPO), prevista dal Regolamento (UE) 2016/679, trasferendo ai discenti le competenze specialistiche richieste per svolgere con efficacia ed autonomia le proprie funzioni. Il corso approfondisce sul piano teorico e applicativo la normativa nazionale ed europea sulla privacy, cogliendo le novità connesse con le opportunità ed i rischi della digitalizzazione. Il percorso formativo risponde alla domanda di esperti in grado di tracciare i percorsi di transizione digitale al passo con le tecnologie innovative, garantendo la conformità al GDPR.
A chi si rivolge	Il corso è rivolto a Responsabili Privacy, Incaricati del Trattamento Dati Personali, Security Manager, Risk Manager, Responsabili IT, Responsabili Affari Legali, Addetti e Responsabili della funzione HR e Marketing, Professionisti, Consulenti e neolaureati.
Contenuti	<ul style="list-style-type: none"> - Il quadro normativo europeo ed italiano in materia di protezione dei dati. Il Codice in materia di protezione dei dati personali - Le autorità per la protezione dei dati. Il Garante privacy - Il trattamento dei dati personali. I soggetti coinvolti nelle operazioni di trattamento. Il Responsabile della Protezione dei dati personali (Data Protection Officer). - Ruolo, compiti, funzioni e responsabilità - Il trattamento dei dati personali in ambito lavorativo. Il trattamento di particolari categorie di dati personali: i dati genetici. La protezione dei dati in ambito bancario - Tutela dei dati e nuove tecnologie. La relazione fra GDPR e cyber security - La privacy in Internet: diritto all'oblio nei confronti dei siti sorgente e nei confronti dei motori di ricerca. Le determinazioni del Garante privacy e le principali pronunce della giurisprudenza
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

SA9: Antiriciclaggio, anticorruzione e tutela dei dati

Obiettivi del corso	Gli obiettivi del corso sono fornire ai partecipanti una comprensione approfondita delle normative in materia di anticorruzione, antiriciclaggio e privacy, esplorando i profili di responsabilità legale e le modalità di protezione degli individui e delle organizzazioni. Il corso intende offrire un approccio metodologico chiaro per l'implementazione delle best practice e per l'attuazione delle normative pertinenti in queste aree, con particolare attenzione agli strumenti di compliance operativi. Viene anche affrontato il ruolo strategico della Digital Transformation nel favorire la trasparenza e la partecipazione diffusa, e come essa possa essere un asset per garantire la compliance. Inoltre, il corso analizza il ruolo dell'internal audit, della compliance e del risk management attraverso l'adozione di best practice, e fornisce una panoramica sulle funzioni degli organi di vigilanza e controllo, come ANAC, UIF e Guardia di Finanza, nell'ambito della supervisione e applicazione delle normative.
A chi si rivolge	Il Master è rivolto a manager e dipendenti pubblici, amministratori, <i>compliance specialist</i> , consulenti e liberi professionisti che vogliono aumentare il proprio bagaglio di conoscenze per contribuire efficacemente alle fasi di definizione, organizzazione, realizzazione e monitoraggio di sistemi di compliance in enti pubblici e privati.
Contenuti	<ul style="list-style-type: none"> - Inquadramento normativo anticorruzione, antiriciclaggio e privacy: profilo di responsabilità e protezione - Approccio metodologico, best practice e profili attuativi della normativa in materia di antiriciclaggio, anticorruzione e privacy - La trasparenza come asset della compliance e strumento di partecipazione diffusa: il ruolo strategico della "Digital Transformation" - Internal audit, compliance e risk management: best practice e profili attuativi - Il ruolo istituzionale degli Organi di vigilanza e controllo: ANAC, UIF e Guardia di Finanza
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

Digitalizzazione ed Innovazione: Tecnologie Emergenti, Benessere Digitale e Sostenibilità

DI1: Introduzione al Machine Learning ed al Deep Learning

Obiettivi del corso	Il corso si propone di indagare le potenzialità delle tecnologie del Machine Learning e Deep Learning, evidenziando la maturità tecnologica raggiunta nel calcolo computazionale e nella capacità di analisi in real-time di enormi quantità di dati.
A chi si rivolge	Responsabili IT e digital, Data Analyst e Data Scientist, Software Developer, programmatori, Software Engineer di aziende manifatturiere, del settore terziario, di istituzioni pubbliche e del settore sanitario
Contenuti	<ul style="list-style-type: none"> - La trasformazione digitale nei processi organizzativi - L'evoluzione delle competenze nell'Industry 4.0 - I processi della supply chain e la loro evoluzione - Performances e tecnologie abilitanti
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI2: Advanced Artificial Intelligence

Obiettivi del corso	<p>Il Corso intende fornire conoscenze scientifiche e tecnologiche riguardanti l'intelligenza artificiale e le sue applicazioni industriali. Il corso, dopo una breve introduzione sui principi fondamentali dell'intelligenza artificiale, intende illustrare ai destinatari le principali caratteristiche dei processi di apprendimento, le principali metodologie di data mining e di machine learning e come tali metodologie possono essere implementate con successo seguendo una strategia ben definita. Particolare attenzione sarà rivolta agli approcci caratterizzanti il Deep Learning e le sue applicazioni nel campo industriale.</p> <p>Il percorso formativo consente di colmare i gap di conoscenze in materia tecnologica e digitale, che tiene distanti i lavoratori dalle esigenze del mercato del lavoro. Infatti il corso mira a formare profili tecnici altamente specializzati destinati ad operare in realtà industriali ad elevato contenuto tecnologico e digitale.</p>
A chi si rivolge	Il corso si rivolge a professionisti del settore industriale, come ingegneri, tecnici e data scientists, che desiderano acquisire competenze avanzate nell'intelligenza artificiale e nelle sue applicazioni pratiche. È adatto a responsabili IT, sistemi di automazione, project manager e consulenti tecnologici che operano in ambienti industriali ad alto contenuto tecnologico, e che intendono implementare soluzioni di AI, machine learning e deep learning. Inoltre, il corso è pensato per profili tecnici che desiderano colmare le lacune di conoscenza nelle tecnologie digitali e data-driven per rispondere alle esigenze moderne del mercato del lavoro e dell'innovazione tecnologica.
Contenuti	o
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI3: Realtà aumentata e virtuale

Obiettivi del corso	Il corso ha l'obiettivo di fornire ai partecipanti una comprensione solida delle tecnologie AR e VR, delle loro applicazioni e dei benefici che possono portare in diversi settori, tra cui l'industria, l'educazione e l'intrattenimento. I partecipanti apprenderanno le differenze tra AR e VR, esploreranno gli strumenti e le piattaforme principali per lo sviluppo di contenuti immersivi e acquisiranno competenze pratiche su come progettare e implementare soluzioni AR/VR. Il corso mira a far acquisire familiarità con le potenzialità di queste tecnologie per migliorare esperienze utente, ottimizzare processi produttivi e formativi, e introdurre innovazioni in vari contesti professionali. Inoltre, si tratteranno anche gli aspetti legati all'integrazione della realtà aumentata e virtuale con altre tecnologie emergenti come l'intelligenza artificiale e l'Internet of Things (IoT).
A chi si rivolge	Il corso si rivolge a professionisti del settore tecnologico, come sviluppatori software, designer, ingegneri e progettisti, che desiderano acquisire competenze nelle tecnologie immersive. È adatto a responsabili IT, project manager e consulenti tecnologici che vogliono esplorare l'applicazione delle tecnologie AR e VR nei loro progetti o aziende. Inoltre, il corso è utile per professionisti del marketing e della comunicazione, che desiderano comprendere come queste tecnologie possono essere utilizzate per migliorare l'interazione con i clienti, e per formatori e educatori interessati a integrare AR/VR nei processi educativi. Il corso è ideale anche per imprenditori e startupper che vogliono esplorare nuove opportunità di business legate a queste tecnologie emergenti.
Contenuti	<ul style="list-style-type: none"> - Introduzione alla Realtà Aumentata e Virtuale: Definizione, differenze e panoramica delle tecnologie AR e VR, storia e evoluzione. - Tecnologie di base: Fondamenti hardware e software necessari per AR e VR, dispositivi come visori, occhiali e controller. - Sistemi e piattaforme AR/VR: Panoramica delle principali piattaforme e strumenti di sviluppo, come Unity, Unreal Engine, ARKit, ARCore. - Applicazioni della Realtà Aumentata: Utilizzo dell'AR in vari settori come retail, medicina, manutenzione industriale, marketing e turismo. - Applicazioni della Realtà Virtuale: Uso della VR in simulazioni, formazione, videogiochi, progettazione architettonica e visualizzazione di dati. - Progettazione e sviluppo di contenuti AR/VR: Tecniche di design per esperienze immersive, progettazione dell'interazione utente, sviluppo di applicazioni e ambienti 3D. - Integrazione AR/VR con altre tecnologie: Come combinare AR e VR con IoT, intelligenza artificiale (AI) e machine learning per creare soluzioni avanzate. - Sfide e limiti della Realtà Aumentata e Virtuale: Problemi tecnologici, costi, resistenza dell'utente e questioni etiche e di privacy. - Trend e futuro delle tecnologie immersive: Analisi delle tendenze emergenti, come la mixed reality (MR), e le previsioni sul futuro delle tecnologie AR e VR.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI4: Robotica Avanzata

Obiettivi del corso	Il corso si propone di fornire ai partecipanti una comprensione pratica e teorica delle tecnologie robotiche moderne e delle loro applicazioni industriali. Gli obiettivi principali includono l'apprendimento delle basi della robotica, l'acquisizione di competenze nell'uso di robot industriali avanzati e la gestione di sistemi automatizzati. Il corso si concentrerà su come i robot interagiscono con i sistemi di controllo, sui principi di
----------------------------	---

A chi si rivolge	programmazione e sulle tecniche di ottimizzazione delle performance dei robot in ambienti industriali complessi. Inoltre, i partecipanti esploreranno le sfide legate all'integrazione dei robot nei processi produttivi e come sfruttare al meglio le tecnologie per migliorare l'efficienza e la sicurezza nelle operazioni industriali.
Contenuti	<p>Il corso si rivolge a professionisti del settore industriale, come ingegneri meccanici, ingegneri elettronici e tecnici di automazione, che desiderano approfondire le proprie competenze nella programmazione e gestione di robot industriali avanzati. È adatto anche a specialisti in manutenzione e operatori che lavorano con sistemi robotici e automatizzati nelle linee di produzione. Inoltre, il corso è rivolto a ricercatori e sviluppatori nel campo della robotica e dell'automazione, nonché a project manager e responsabili IT che devono integrare soluzioni robotiche nei processi aziendali e industriali.</p> <ul style="list-style-type: none"> - Introduzione alla robotica avanzata: Panoramica sulle tecnologie robotiche moderne, evoluzione dei robot industriali e loro applicazioni. - Architettura e componenti dei robot industriali: Analisi dei principali componenti hardware, come sensori, attuatori, motori, e controller. - Sistemi di controllo robotici: Studio dei sistemi di controllo per la gestione e la programmazione dei robot, incluse le architetture di controllo centralizzato e distribuito. - Programmazione dei robot: Tecniche di programmazione dei robot industriali, con focus su linguaggi di programmazione specifici (es. Python, C++) e interfacce uomo-macchina (HMI). - Robotica e automazione nei processi industriali: Integrazione dei robot nelle linee di produzione e nei sistemi automatizzati, con esempi pratici di applicazioni. - Ottimizzazione delle prestazioni dei robot: Tecniche per migliorare l'efficienza, la velocità e la precisione dei robot in contesti industriali. - Sicurezza e manutenzione dei robot industriali: Gestione della sicurezza nei sistemi robotici, pratiche di manutenzione preventiva e risoluzione dei problemi. - Tecniche avanzate di robotica: Esplorazione di approcci come la robotica collaborativa (cobot), robotica mobile e robotica autonoma. - Sfide e tendenze future nella robotica industriale: Discussione delle sfide tecnologiche e delle innovazioni emergenti nella robotica avanzata, come l'intelligenza artificiale applicata ai robot.
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI5: Digitalizzazione dei processi aziendali

Obiettivi del corso	Il corso si propone di indagare le potenzialità della Smart Factory strutturata in modo modulare all'industria 4.0, all'interno della quale i sistemi cyber-fisici controllano i processi fisici, creano una copia virtuale del mondo fisico, prendono decisioni decentrate e attraverso l'IoT cooperano tra loro. Inoltre, attraverso l'Internet dei servizi, sia i servizi interni che quelli trasversali vengono offerti e utilizzati dai partecipanti della catena di valore.
A chi si rivolge	Imprenditori, Direttori di produzione, R&D Manager, Plant manager, Responsabili della logistica, ICT Manager, Innovation manager, Marketing manager.
Contenuti	<ul style="list-style-type: none"> • Industry 4.0 • La trasformazione digitale nei processi organizzativi • L'evoluzione delle competenze nell'Industry 4.0 • I processi della supply chain e la loro evoluzione • Performances e tecnologie abilitanti

Durata	18 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI6: Digital Twinning

Obiettivi del corso	Il corso ha l'obiettivo di fornire una comprensione approfondita del processo di trasformazione digitale nelle aziende, con un focus sull'analisi del modello aziendale e l'assessment digitale. I partecipanti apprenderanno come sviluppare una roadmap per l'innovazione continua e come implementare tecnologie avanzate come il Digital Twin e le realtà estese (XR) per ottimizzare i processi aziendali. Saranno esplorati i benefici del Digital Twin nell'affrontare le sfide aziendali, con particolare attenzione ai fattori di business che influenzano le decisioni tecnologiche. Il corso si concentrerà anche sulle best practice e sulla selezione delle soluzioni digitali più adatte per le specifiche esigenze aziendali.
A chi si rivolge	Il corso si rivolge a responsabili dell'innovazione digitale, dirigenti aziendali, manager di progetto e consulenti tecnologici che desiderano implementare soluzioni avanzate di trasformazione digitale nelle loro organizzazioni. È ideale per professionisti del settore IT, come CTO, ingegneri e specialisti in sistemi digitali, che vogliono approfondire l'uso di tecnologie come il Digital Twin e le realtà estese (XR). Inoltre, il corso è adatto a responsabili delle operazioni aziendali e a chi si occupa della pianificazione strategica, interessati a migliorare l'efficienza e l'innovazione attraverso l'adozione di strumenti digitali avanzati.
Contenuti	<ul style="list-style-type: none"> - Analisi del modello aziendale e Assessment digitale - Miglioramento continuo e roadmap dell'innovazione digitale - Il Digital Twin [DT] e le realtà estese [XR] - Come il Digital Twin è utile alle necessità delle aziende - Fattori di Business - Le best practice e la scelta della migliore soluzione per le proprie attività
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI7: Internet of Things

Obiettivi del corso	Il seminario presenta le caratteristiche tecnologiche e le architetture di una soluzione IoT, per poi passare ai contesti applicativi e ai possibili scenari di business.
A chi si rivolge	Professional che desiderano acquisire una conoscenza di base e una visione armonica delle tematiche trattate.
Contenuti	Principi e fondamenti del concetto di IoT
Durata	6 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI8: Firma elettronica digitale

Obiettivi del corso	Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita dei benefici e delle tecniche legate alla dematerializzazione dei documenti e all'uso della Firma Elettronica Digitale. I partecipanti apprenderanno come ottimizzare i processi aziendali attraverso la digitalizzazione dei documenti, migliorando l'efficienza operativa e riducendo i costi. Inoltre, il corso si concentra sull'utilizzo della firma elettronica digitale come strumento per semplificare e rendere sicuri i processi burocratici, garantendo la validità legale dei documenti e una gestione più agile delle pratiche amministrative.
A chi si rivolge	Professionisti e personale amministrativo con conoscenze minime di informatica
Contenuti	<ul style="list-style-type: none"> - Dematerializzazione dei documenti per poter sfruttare al meglio i vantaggi che essa offre - Gestire la Firma Elettronica Digitale e utilizzarla al meglio come strumento di semplificazione.
Durata	6 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI9: Il sistema cloud

Obiettivi del corso	Il modulo introduce le idee fondamentali dietro il paradigma cloud, i principali servizi e i vantaggi per le aziende.
A chi si rivolge	Professionisti, junior, dipendenti pubblici che intendono approfondire le tematiche trattate
Contenuti	<ul style="list-style-type: none"> - Fondamenti di Cloud - Applicazioni e potenzialità
Durata	4 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI10: Introduzione alla Psicologia della Digitalizzazione

Obiettivi del corso	Il corso è pensato per fornire una comprensione approfondita dei cambiamenti psicologici e sociali causati dalla digitalizzazione. Gli obiettivi principali sono due: in primo luogo, esplorare come la digitalizzazione influisce sulla mente e sul comportamento delle persone, in particolare degli adolescenti; in secondo luogo, identificare sia i rischi che le opportunità che il mondo digitale presenta per questa fascia d'età. Durante il modulo, gli studenti impareranno a riconoscere le sfide e i benefici dell'interazione con le tecnologie digitali, acquisendo strumenti utili per navigare nel contesto digitale in modo consapevole e sicuro.
A chi si rivolge	Il corso "Introduzione alla Psicologia della Digitalizzazione" si rivolge a professionisti delle risorse umane, manager, formatori e consulenti che desiderano comprendere l'impatto della digitalizzazione sulle persone e sui comportamenti all'interno delle organizzazioni. È adatto a chiunque lavori nell'ambito del cambiamento organizzativo o nella gestione del cambiamento tecnologico, come leader aziendali, responsabili della trasformazione digitale e psicologi del lavoro. Il corso è utile anche a studenti e neolaureati in psicologia, sociologia e gestione aziendale che vogliono approfondire le

Contenuti	<p>dinamiche psicologiche legate all'introduzione di tecnologie digitali nel contesto lavorativo.</p> <ul style="list-style-type: none"> - Panoramica dei cambiamenti socio-psicologici nell'era digitale; - Impatto della tecnologia sullo sviluppo cognitivo e sociale degli adolescenti; - Dipendenza da internet e social media: riconoscere i segnali.
Durata	5 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI1: Benessere Digitale e Gestione dello Stress Tecnologico

Obiettivi del corso	<p>Il corso "Benessere digitale e gestione dello stress tecnologico" si propone di aiutare gli studenti a riconoscere i fattori di stress associati all'uso della tecnologia e a sviluppare strategie per promuovere un uso equilibrato e sano dei dispositivi digitali. Gli obiettivi principali sono identificare gli elementi che causano stress tecnologico e insegnare metodi efficaci per gestire e ridurre tale stress, favorendo un rapporto più armonioso con la tecnologia nella vita quotidiana.</p>
A chi si rivolge	<p>Il corso si rivolge a professionisti e studenti che utilizzano quotidianamente dispositivi digitali, come lavoratori in smart working, manager, insegnanti, operatori sanitari, e chiunque dipenda in modo significativo dalla tecnologia per svolgere il proprio lavoro o studio. È utile anche per genitori che desiderano gestire meglio l'uso della tecnologia nelle famiglie e promuovere il benessere digitale dei propri figli. Inoltre, il corso può essere vantaggioso per consulenti aziendali e coach che lavorano sul miglioramento del benessere psicologico e dell'efficienza lavorativa, cercando di ottimizzare l'uso della tecnologia e prevenire il burnout digitale.</p>
Contenuti	<ul style="list-style-type: none"> - Concetto di benessere digitale; - Impatto dello stress tecnologico sulla salute mentale; - Strategie per la disconnessione e il digital detox; - Promozione di abitudini digitali sane tra gli studenti.
Durata	5 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

DI2: Competenze Digitali e Pensiero Critico nell'Era dell'Informazione

Obiettivi del corso	<p>Il corso si propone di far comprendere l'importanza delle competenze digitali nel contesto educativo e di sviluppare strategie per promuovere il pensiero critico online. Gli studenti impareranno a navigare e utilizzare le risorse digitali in modo efficace e sicuro, acquisendo strumenti per valutare criticamente le informazioni trovate su internet. Inoltre, il modulo mira a sensibilizzare gli studenti sull'importanza di un uso responsabile e consapevole della tecnologia, favorendo un approccio riflessivo e critico alle informazioni e ai contenuti digitali.</p>
A chi si rivolge	<p>Il corso "Competenze Digitali e Pensiero Critico nell'Era dell'Informazione" si rivolge a professionisti, studenti, lavoratori e dirigenti aziendali che desiderano sviluppare le competenze necessarie per affrontare le sfide della digitalizzazione e dell'informazione nell'era moderna. È particolarmente utile per chiunque abbia bisogno di migliorare le proprie capacità di analisi critica delle informazioni, navigazione digitale e gestione dei dati. Il corso è indicato anche per educatori, formatori e consulenti che desiderano integrare il pensiero critico e le competenze digitali nel proprio lavoro quotidiano o nelle attività di formazione e consulenza.</p>

Contenuti	<ul style="list-style-type: none">- Alfabetizzazione digitale e sua importanza nel 21° secolo;- Fake news e disinformazione: impatti psicologici e sociali;- Strategie per insegnare il pensiero critico nella valutazione delle fonti online;- Integrazione delle competenze digitali nel curriculum scolastico.
Durata	5 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

Competenze Manageriali

CM1: Progettazione europea

Obiettivi del corso	Il corso ha l'obiettivo di fornire una panoramica completa del funzionamento delle politiche e dei finanziamenti europei, con particolare attenzione al PNRR e alla gestione dei fondi strutturali. I partecipanti apprenderanno come utilizzare efficacemente il project management per la gestione di progetti finanziati dall'Unione Europea, compreso il ruolo del Responsabile Unico del Procedimento (RUP). Il corso si concentrerà anche sulla europrogettazione, guidando i partecipanti attraverso il processo di redazione e gestione di proposte per ottenere finanziamenti europei. Infine, sarà trattata la valutazione dei progetti e la corretta rendicontazione delle risorse, per garantire la piena conformità e l'efficacia nell'utilizzo dei fondi.
A chi si rivolge	Il corso si rivolge a professionisti e manager coinvolti nella gestione di progetti pubblici e privati, in particolare a coloro che operano nel settore pubblico, nelle istituzioni e nelle organizzazioni che partecipano a bandi e programmi europei. È indicato per responsabili di progetto, europrogettisti, funzionari pubblici, consulenti e consulenti finanziari che desiderano approfondire le modalità di accesso e gestione dei fondi europei. Inoltre, il corso è utile per amministratori locali, dirigenti pubblici e professionisti del settore della programmazione e rendicontazione dei progetti europei.
Contenuti	<ul style="list-style-type: none"> - Unione Europea, policies, programmazione e PNRR - Il bilancio europeo e i fondi strutturali - Il Project management. Il RUP / Responsabile Unico del Procedimento - L'Europrogettazione - La valutazione dei progetti e la rendicontazione
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CM2: Responsabile Servizio Export (livello base)

Obiettivi del corso	Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita delle problematiche relative al commercio estero, migliorando le competenze nella gestione degli aspetti operativi e legali delle transazioni internazionali. Si pone l'accento sull'accelerazione dei tempi di incasso, sulla riduzione dei rischi commerciali e di scambio, e sull'uso delle procedure doganali agevolate. Il corso mira a rendere i partecipanti esperti nella gestione degli ordini e nella conoscenza dei documenti di esportazione, facilitando l'archiviazione e la ricerca dei documenti. Inoltre, si affrontano le problematiche legate alle controversie sulle consegne e vengono sviluppate competenze organizzative per gestire eventi internazionali come fiere e riunioni. Infine, il corso fornisce le conoscenze necessarie per comprendere e gestire i contratti di trasporto e i contratti internazionali d'impresa.
A chi si rivolge	Il corso si rivolge a responsabili e addetti all'export, operatori commerciali, manager delle vendite internazionali, logistici e spedizionieri che operano nel settore del commercio estero e desiderano migliorare la loro preparazione in materia di gestione delle operazioni internazionali. È ideale per chi si occupa di gestione ordini, procedure doganali e contratti internazionali, nonché per professionisti delle risorse umane che gestiscono la formazione in ambito internazionale. Inoltre, il corso è utile per consulenti aziendali e imprenditori che vogliono acquisire competenze pratiche nella gestione di

Contenuti	<p>attività commerciali con l'estero, comprese le procedure legali e organizzative legate al commercio internazionale.</p> <p>Modulo 1. Identificare le tappe di un'operazione export e determinare il ruolo dei diversi attori (4 ore)</p> <ul style="list-style-type: none"> - Comprendere i mutamenti dell'ambiente internazionale, conoscere le zone di libero scambio (UE, ALENA, ASEAN, MERCONSUR...) - Valutare l'interesse di un mercato estero per l'azienda - Conoscere gli aiuti all'esportazione - Comprendere il ruolo e la funzione del servizio export <p>Modulo 2. Analizzare gli adempimenti amministrativi legati alle esportazioni (6 ore)</p> <ul style="list-style-type: none"> - Le condizioni di resa internazionali - Gli obblighi del venditore, gli obblighi dell'acquirente <p>Modulo 3. Scegliere i mezzi di pagamento più sicuri (6 ore)</p> <ul style="list-style-type: none"> - Assegni, effetti, rimesse documentarie - Vantaggi e svantaggi, costi delle diverse formule - Impatti sulla tesoreria e sulla gestione clienti - Crediti di prefinanziamento <p>Modulo 4. Rispondere ad una richiesta di offerta internazionale (6 ore)</p> <ul style="list-style-type: none"> - Conoscere i vincoli tecnici e normativi (licenze, norme..) - Elaborare le clausole principali del contratto commerciale - Difendere gli interessi dell'azienda
Durata	22 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CM3: Responsabile Servizio Export (livello avanzato)

Obiettivi del corso	<p>Il corso si propone di fornire una solida preparazione sulle principali problematiche del commercio estero, con particolare attenzione all'ottimizzazione dei tempi di incasso e alla gestione dei rischi commerciali e di scambio. I partecipanti apprenderanno come applicare le procedure doganali agevolate e gestire correttamente l'IVA nelle operazioni internazionali. Il corso si concentrerà anche sulla gestione degli ordini, la corretta gestione della documentazione di esportazione e l'utilizzo di metodologie di archiviazione per una più facile classificazione e ricerca dei documenti. Un focus particolare sarà dedicato alla prevenzione e gestione delle controversie relative alle consegne, nonché allo sviluppo delle competenze organizzative per la gestione di eventi internazionali come fiere e riunioni. Infine, si approfondiranno gli aspetti legati ai contratti di trasporto nazionali e internazionali, così come i contratti internazionali d'impresa.</p>
A chi si rivolge	<p>Il corso si rivolge a responsabili e addetti all'export, operatori commerciali, manager delle vendite internazionali, logistici e spedizionieri che operano nel settore del commercio estero e desiderano migliorare la loro preparazione in materia di gestione delle operazioni internazionali. È ideale per chi si occupa di gestione ordini, procedure doganali e contratti internazionali, nonché per professionisti delle risorse umane che gestiscono la formazione in ambito internazionale. Inoltre, il corso è utile per consulenti aziendali e imprenditori che vogliono acquisire competenze pratiche nella gestione di attività commerciali con l'estero, comprese le procedure legali e organizzative legate al commercio internazionale.</p>

Contenuti	<p>Modulo 1. I contratto di trasporto nazionali e internazionali (8 ore)</p> <ul style="list-style-type: none"> - Identificare le basi di un sistema di trasporto nazionale e internazionale: aspetti tecnici, giuridici e commerciali - principali contratti rilevanti in ordine al trasporto di merci: contratto di compravendita, contratto di deposito, contratto di spedizione, contratto di trasporto - Analisi della normativa inerenti le modalità di trasporto settore marittimo, stradale, ferroviario, aereo, multimediale o combinato - Conoscere i principali titoli di trasporto - Saper gestire una contestazione, assicurazione, imballaggio, consegne - Sottoscrivere una polizza assicurativa in funzione dei rischi potenziali - Trarre vantaggio dalle facilities doganali: funzioni di stoccaggio, di trasformazione, di utilizzazione; crediti e cauzioni. <p>Modulo 2. I contratti internazionali d'Impresa (12 ore)</p> <ul style="list-style-type: none"> - Problematiche connesse alla stipula di contratti internazionali di impresa - La negoziazione di un contratto internazionale - I documenti precontrattuali: le lettere di intenti - La redazione dei contratti internazionali - La struttura di un contratto internazionale - Contratti tipici e atipici nell'ordinamento giuridico nazionale e internazionale
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CM4: Comunicazione non verbale

Obiettivi del corso	<ul style="list-style-type: none"> - Sviluppare la consapevolezza dell'impatto della comunicazione non verbale nelle interazioni professionali - Migliorare l'efficacia comunicativa nei contesti aziendali chiave (presentazioni, negoziazioni, colloqui) - Potenziare la capacità di lettura dei segnali non verbali di colleghi, clienti e partner - Allineare la comunicazione verbale e non verbale per aumentare la propria credibilità professionale - Gestire lo stress e le emozioni attraverso il controllo consapevole della cnv
A chi si rivolge	<ul style="list-style-type: none"> - Manager e team leader - Professionisti delle vendite e account manager - Specialisti delle risorse umane - Personale addetto alle relazioni con i clienti - Professionisti che tengono presentazioni regolarmente - Dipendenti interessati a migliorare le proprie competenze comunicative
Contenuti	<p>Modulo 1: Fondamenti della comunicazione non verbale</p> <p>Modulo 2: Il corpo come strumento di comunicazione</p> <p>Modulo 3: Applicazioni nel contesto aziendale</p> <p>Modulo 4: Gestione emotiva e Stress</p>
Durata	20 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CM5: Comunicazione aziendale

Obiettivi del corso	Il corso si propone di sviluppare e potenziare le competenze comunicative dei partecipanti nell'ambito professionale, con l'obiettivo di migliorare l'efficacia delle interazioni, rafforzare la capacità di lavorare in team, e accrescere la propria immagine e credibilità all'interno dell'organizzazione. Particolare attenzione verrà data all'allineamento tra comunicazione verbale e non verbale, alla gestione delle riunioni e delle presentazioni, nonché alla risoluzione costruttiva dei conflitti.
A chi si rivolge	Il corso è pensato per diverse figure professionali all'interno del contesto aziendale, tra cui: manager, team leader, specialisti delle risorse umane, addetti alle vendite e alle relazioni con i clienti, nonché per tutti i dipendenti interessati a migliorare le proprie abilità comunicative e di collaborazione.
Contenuti	Modulo 1: Fondamenti della comunicazione efficace Modulo 2: Comunicazione non verbale in azienda Modulo 3: Comunicazione assertiva e gestione dei conflitti Modulo 4: Comunicazione interna e presentazioni efficaci
Durata	16 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

CM6: Design Thinking

Obiettivi del corso	Il corso di Design Thinking mira a fornire ai partecipanti una metodologia strutturata per affrontare e risolvere problemi complessi, focalizzandosi sull'utente finale e sviluppando soluzioni innovative. Al termine del percorso, i partecipanti saranno in grado di: <ul style="list-style-type: none"> - Padroneggiare le fasi e gli strumenti chiave del processo di Design Thinking - Applicare un approccio centrato sull'utente per identificare e comprendere le reali esigenze - Sviluppare soluzioni creative e prototipare idee innovative - Comunicare efficacemente i risultati e coinvolgere le parti interessate
A chi si rivolge	Il corso si rivolge a professionisti di diverse funzioni aziendali, tra cui: <ul style="list-style-type: none"> - Manager e team leader - Dipendenti di reparti R&S, marketing e innovazione - Consulenti e progettisti - Responsabili dello sviluppo prodotto - Chiunque desideri acquisire competenze in Design Thinking
Contenuti	Modulo 1: Introduzione al Design Thinking Modulo 2: Empatia e Comprensione dell'utente Modulo 3: Ideazione e generazione di idee Modulo 4: Prototipazione e sperimentazione
Durata	16 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

I corsi di formazione per le Pubbliche Amministrazioni

PA1: Contratti pubblici

Obiettivi del corso	Il Corso mira a formare figure professionali che operano nel settore degli appalti e contratti pubblici. Il corso fornisce una panoramica approfondita della Legislazione vigente e una disamina esaustiva dell'intero settore. Ogni sessione, della durata di 8 ore, è dedicata ad un tema specifico come da programma allegato.
A chi si rivolge	Il Corso è indirizzato a tutti i professionisti operanti a qualsiasi titolo nel settore degli appalti pubblici. In particolare, si rivolge a rappresentanti di uffici gare, esperti e consulenti in materia di appalti e contratti pubblici, manager di imprese svolgenti pubblici servizi, di enti economici, di società a partecipazione pubblica, dirigenti di società di certificazione e attestazione nel settore edilizio, dirigenti e funzionari pubblici.
Contenuti	<ul style="list-style-type: none"> - Modulo I – Il quadro normativo di riferimento - Modulo II – Le stazioni appaltanti e le attività pre-gara - Modulo III – Le procedure di gara - Modulo IV – I partecipanti alle procedure di affidamento - Modulo VI – La gestione della gara - Modulo VII – L'aggiudicazione e la stipula del contratto - Modulo VIII – La gestione del contratto e del contenzioso
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA2: I contratti sottosoglia

Obiettivi del corso	Il corso analizza le diverse fasi del “contratto sotto soglia” sulla base della modulistica degli atti (accertamento, selezione, aggiudicazione, etc.) e analizzando le responsabilità degli operatori, dal RUP al segretario, etc., in conformità con le indicazioni di ANAC. Parte integrante del seminario saranno le simulazioni delle procedure.
A chi si rivolge	Il Corso è indirizzato a tutti i professionisti operanti a qualsiasi titolo nel settore degli appalti pubblici.
Contenuti	<ul style="list-style-type: none"> - Modulo I – Il quadro normativo di riferimento - Modulo II – Instaurazione della procedura di affidamento - Modulo III – Gli accertamenti della stazione appaltante - Modulo IV – Analisi delle offerte e aggiudicazione
Durata	24 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA3: La gestione ed il recupero dei crediti nelle amministrazioni pubbliche

Obiettivi del corso	Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita delle normative e delle procedure relative alla gestione dei crediti nelle amministrazioni pubbliche. Si propone di migliorare le competenze nella gestione delle riscossioni e nel recupero dei crediti, affrontando le problematiche legate ai ritardi nei pagamenti, all'identificazione dei crediti inesigibili e alle soluzioni per ridurre i crediti deteriorati. Il corso mira a fornire gli strumenti necessari per attuare strategie efficaci di recupero, con particolare attenzione agli aspetti legali, amministrativi e fiscali. Inoltre, si focalizzerà sull'ottimizzazione dei processi interni e sulla gestione della relazione con i creditori, puntando al miglioramento dell'efficienza e alla riduzione dei rischi di contenzioso.
A chi si rivolge	Il corso si rivolge a responsabili e operatori finanziari delle amministrazioni pubbliche, gestori dei servizi di riscossione e addetti agli uffici tributi e riscossione crediti. È particolarmente utile per dirigenti e funzionari coinvolti nella gestione economica e amministrativa all'interno di enti pubblici, come comuni, regioni, ministeri e altre pubbliche amministrazioni. Il corso è indicato anche per consulenti fiscali e legali che si occupano di recupero crediti e contenzioso nelle amministrazioni pubbliche, nonché per chi lavora nella gestione delle entrate e nell'ottimizzazione dei flussi finanziari.
Contenuti	<ul style="list-style-type: none"> - Normative e principi legali: Le principali leggi e regolamenti che disciplinano la gestione dei crediti nelle amministrazioni pubbliche, inclusi i riferimenti normativi nazionali e europei. - Processi di gestione dei crediti: Tecniche e procedure per la gestione efficace dei crediti, dall'identificazione dei crediti esigibili alla pianificazione dei flussi di incasso. - Riscossione dei crediti: Strategie e metodi di riscossione dei crediti, inclusi i meccanismi di pagamento e le modalità di sollecito. - Gestione dei crediti deteriorati: Identificazione e trattamento dei crediti inesigibili o problematici, compresi gli strumenti per il recupero e la gestione delle situazioni di insolvenza. - Tecniche di recupero crediti: Approcci per il recupero stragiudiziale e giudiziale dei crediti, incluse le azioni legali da intraprendere in caso di mancato pagamento. - Ottimizzazione dei processi: Strumenti e metodologie per migliorare l'efficienza e ridurre i tempi di riscossione, con particolare attenzione alle soluzioni digitali e all'automazione dei processi. - Contratti e accordi con i creditori: Gestione delle relazioni con i creditori e definizione di piani di pagamento concordati, inclusi gli aspetti relativi ai piani di rateizzazione e dilazione. - Aspetti fiscali e contabili: Implicazioni fiscali del recupero crediti, contabilizzazione dei crediti e adempimenti fiscali connessi al recupero. - Prevenzione delle problematiche finanziarie: Strategie per evitare l'accumulo di crediti insoluti e garantire una gestione sostenibile delle entrate nelle amministrazioni pubbliche.
Durata	22 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA4: Il diritto di accesso ai documenti amministrativi

Obiettivi del corso	Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita delle normative e delle procedure relative al diritto di accesso ai documenti amministrativi, con un focus sull'applicazione pratica di tali diritti. I partecipanti apprenderanno le modalità di richiesta e le condizioni per l'accesso ai documenti, sia per i cittadini che per le aziende, nonché le limitazioni e le eccezioni previste dalla legge. Inoltre, il corso esplorerà le implicazioni legali e i possibili ricorsi in caso di diniego dell'accesso,
----------------------------	---

A chi si rivolge	formando i partecipanti sulle responsabilità degli enti pubblici nella gestione delle richieste e sulla trasparenza amministrativa. L'obiettivo è fornire competenze pratiche e teoriche per gestire correttamente le richieste di accesso ai documenti e applicare correttamente la normativa vigente.
Contenuti	<p>Il corso si rivolge a professionisti del settore pubblico, come dipendenti di enti e amministrazioni pubbliche, responsabili della trasparenza, dirigenti e funzionari che gestiscono le pratiche amministrative e devono garantire l'accesso ai documenti. È utile anche per avvocati, consulenti legali, professionisti del diritto amministrativo e esperti in compliance normativa che desiderano approfondire la normativa sull'accesso agli atti pubblici. Inoltre, il corso è rivolto a giornalisti e attivisti per la trasparenza che necessitano di comprendere come operare nell'ambito del diritto di accesso agli atti per garantire la corretta informazione e la tutela dei diritti civili.</p> <ul style="list-style-type: none"> - Introduzione al diritto di accesso ai documenti amministrativi: Definizione e principi fondamentali del diritto di accesso, con riferimento alla trasparenza amministrativa e alla legge 241/1990. - Normativa di riferimento: Analisi delle leggi e dei regolamenti che disciplinano l'accesso ai documenti, inclusi la legge sulla trasparenza (legge 150/2009) e il regolamento europeo sulla protezione dei dati personali (GDPR). - Modalità di richiesta di accesso: Procedura per fare una richiesta di accesso ai documenti amministrativi, e i diritti e doveri di chi presenta la richiesta e degli enti coinvolti. - Limitazioni e eccezioni al diritto di accesso: Studio delle situazioni in cui l'accesso può essere negato o limitato, come la protezione di segreti di stato, dati sensibili, o altre esigenze di riservatezza. - Risposte alle richieste e obblighi delle amministrazioni: Termini e modalità di risposta da parte delle amministrazioni, e le possibili conseguenze in caso di inadempimento. - Ricorsi e contenzioso: Come e quando è possibile impugnare il diniego o il silenzio dell'amministrazione, e le procedure per il ricorso al TAR o altre autorità competenti. - Accesso ai documenti e privacy: Esame dell'interazione tra diritto di accesso e protezione dei dati personali, inclusi i principi di bilanciamento tra trasparenza e riservatezza. - Accesso e digitalizzazione: Approfondimento sulle tecnologie e sulle piattaforme digitali utilizzate per la gestione delle richieste di accesso, e sugli strumenti online per semplificare l'accesso ai documenti.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA5: Il risarcimento del danno a carico della P.A. in sede amministrativa e civile

Obiettivi del corso	Il corso si propone di fornire una comprensione approfondita delle normative e delle pratiche relative al risarcimento dei danni causati dalla Pubblica Amministrazione. Gli obiettivi principali includono l'analisi delle modalità di risarcimento del danno sia in sede amministrativa che civile, fornendo ai partecipanti le conoscenze necessarie per distinguere i diversi ambiti giuridici e le relative procedure. Il corso mira a spiegare i fondamenti legali, le responsabilità della P.A., e le forme di indennizzo previste dalla legge, oltre a illustrare gli strumenti a disposizione per i cittadini e le imprese danneggiate. L'obiettivo finale è quello di fornire competenze pratiche per affrontare efficacemente le controversie relative al risarcimento del danno, sia attraverso la via amministrativa che tramite il ricorso al sistema giuridico civile.
A chi si rivolge	Il corso si rivolge a professionisti legali come avvocati specializzati in diritto amministrativo e civile, giudici, consulenti legali e responsabili della gestione dei

Contenuti	<p>contenziosi legali all'interno di enti pubblici. È adatto anche a funzionari della Pubblica Amministrazione che si occupano di responsabilità e risarcimento dei danni, nonché a professionisti coinvolti nella mediazione e risoluzione di controversie legate alla P.A. Il corso è utile anche a imprese e cittadini che desiderano acquisire conoscenze specifiche sui propri diritti e le modalità di ottenere il risarcimento per danni causati dalla Pubblica Amministrazione.</p> <ul style="list-style-type: none"> - Responsabilità della Pubblica Amministrazione: analisi delle diverse forme di responsabilità civile della P.A. (diritto amministrativo e civile) e delle relative implicazioni legali. - Procedura di risarcimento del danno in sede amministrativa: esame delle modalità di presentazione delle richieste di risarcimento, i procedimenti amministrativi, e le competenze degli organi pubblici nella gestione delle domande di risarcimento. - La responsabilità extracontrattuale della P.A.: approfondimento sulla responsabilità civile della Pubblica Amministrazione per danni derivanti da atti illeciti, omissioni o negligenze. - Danno patrimoniale e non patrimoniale: differenza tra i vari tipi di danno, con particolare attenzione al danno emergente, lucro cessante e danno morale. - Le azioni risarcitorie in sede civile: esame del processo civile per il risarcimento del danno subito a causa di atti della P.A., inclusa la distinzione tra danno diretto e indiretto. - Il risarcimento in caso di danno da pubblica amministrazione: procedure per chiedere il risarcimento del danno in ambito civile, con riferimento a sentenze e orientamenti giurisprudenziali. - Il risarcimento dei danni da provvedimenti amministrativi illegittimi: studio del risarcimento per danni causati da provvedimenti amministrativi illegittimi, come sanzioni o ordinanze non correttamente emesse. - La tutela giurisdizionale e il ricorso al giudice ordinario: analisi dei ricorsi contro atti amministrativi e le modalità di intervento del giudice civile per ottenere il risarcimento dei danni. - Compensazione e conciliazione: esame delle soluzioni alternative al contenzioso per il risarcimento del danno, tra cui mediazione e conciliazione. - Caso pratico e studio di giurisprudenza: analisi di casi pratici e sentenze significative relative al risarcimento del danno nei confronti della P.A., per comprendere le dinamiche legali e l'applicazione delle normative in contesti reali.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA6: Guida alla gestione del contenzioso nei contratti pubblici

Obiettivi del corso	<p>Il corso ha l'obiettivo di fornire ai partecipanti una solida comprensione delle problematiche legate alla gestione e risoluzione delle controversie nei contratti pubblici. I partecipanti apprenderanno le tecniche e le best practice per affrontare il contenzioso, con particolare attenzione alla prevenzione delle controversie e alla gestione delle problematiche legali durante l'esecuzione del contratto. Il corso esplorerà le modalità di risoluzione alternativa delle dispute, come la mediazione e l'arbitrato, e approfondirà gli aspetti legali e procedurali previsti dalla normativa nazionale ed europea. L'obiettivo finale è sviluppare competenze per gestire efficacemente le controversie, ridurre i rischi legali e garantire l'efficienza nella gestione dei contratti pubblici.</p>
A chi si rivolge	<p>Il corso si rivolge principalmente a professionisti del settore legale, come avvocati, consulenti legali e giuristi, che operano nel campo dei contratti pubblici e nella risoluzione di controversie legate agli appalti. È anche adatto a responsabili degli appalti e manager di contratti all'interno di enti pubblici e privati, dirigenti pubblici e</p>

Contenuti	<p>funzionari amministrativi che gestiscono o supervisionano contratti pubblici. Inoltre, il corso è pensato per project manager e professionisti dell'amministrazione pubblica che desiderano approfondire le proprie competenze nella gestione dei contenziosi e nella prevenzione di problematiche legali nei contratti con la pubblica amministrazione.</p> <ul style="list-style-type: none"> - Principi e normative dei contratti pubblici: Panoramica sulle normative nazionali e internazionali che regolano i contratti pubblici, con focus sulla legislazione italiana e le direttive europee. - Identificazione e prevenzione del contenzioso: Tecniche per individuare e prevenire potenziali conflitti nelle fasi di gara e nell'esecuzione del contratto. - Le cause comuni di contenzioso nei contratti pubblici: Analisi delle principali problematiche che causano conflitti, come ritardi, inadempimenti e vizi di conformità. - Le fasi del contenzioso: Dalla pre-contenziosa alla gestione vera e propria del conflitto, comprendendo la negoziazione e le azioni legali necessarie. - Risoluzione alternativa delle dispute (ADR): Approfondimento su mediazione, conciliazione e arbitrato, come strumenti per risolvere le controversie senza ricorrere ai tribunali. - Gestione del contenzioso nei contratti pubblici: Strategie pratiche e operative per affrontare il contenzioso, incluse le tecniche di gestione e la documentazione legale da produrre. - Il ruolo della giurisprudenza: Esame dei principali precedenti giuridici che influenzano la gestione del contenzioso nei contratti pubblici. - Risoluzione dei conflitti nelle fasi di esecuzione del contratto: Tecniche per risolvere le problematiche relative a modifiche, varianti, e ritardi nell'esecuzione dei contratti pubblici. - Aspetti procedurali e legali delle gare d'appalto: Come gestire le controversie che sorgono durante la fase di gara e nell'assegnazione dei contratti. - Best practices e casi studio: Analisi di casi reali e studio di best practices per la gestione del contenzioso, con un focus sulla tutela degli interessi pubblici e privati.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA7: Governance e politiche per la trasformazione digitale nella PA

Obiettivi del corso	<p>Il corso si propone di fornire una comprensione approfondita dei principi e delle pratiche fondamentali per guidare la trasformazione digitale all'interno delle pubbliche amministrazioni. Gli obiettivi principali includono l'acquisizione delle competenze necessarie per sviluppare e implementare politiche digitali efficaci, la creazione di una governance che integri l'innovazione tecnologica nei processi amministrativi, e la gestione del cambiamento organizzativo in un contesto pubblico. Il corso mira a preparare i partecipanti a progettare e applicare soluzioni digitali che migliorino l'efficienza, la trasparenza e l'accessibilità dei servizi pubblici, con particolare attenzione alla gestione delle risorse, al rispetto delle normative e alla protezione dei dati. Inoltre, il corso affronta le sfide legate alla digitalizzazione nella PA, inclusi aspetti di gestione del rischio e di coinvolgimento dei cittadini.</p>
A chi si rivolge	<p>Il corso si rivolge a dirigenti e funzionari della pubblica amministrazione, responsabili IT e direttori di dipartimenti digitali, che desiderano acquisire competenze per gestire la digitalizzazione nei loro enti. È ideale per responsabili di progetti di trasformazione digitale, policy maker, consulenti e manager che operano nel settore pubblico e sono coinvolti nella progettazione, implementazione e gestione di politiche digitali. Inoltre, il corso è adatto a chiunque sia interessato a comprendere come applicare le tecnologie digitali per migliorare l'efficienza e l'accessibilità dei servizi pubblici, inclusi giovani</p>

Contenuti	<p>professionisti e esperti di digitalizzazione che vogliono sviluppare la loro carriera nella pubblica amministrazione.</p> <ul style="list-style-type: none"> - Introduzione alla trasformazione digitale nella pubblica amministrazione: analisi delle sfide e opportunità legate alla digitalizzazione nel settore pubblico. - Governance della trasformazione digitale: modelli di governance per gestire l'innovazione digitale, con un focus sulla leadership e il coordinamento interistituzionale. - Politiche digitali e normative: le principali politiche, leggi e regolamenti che influenzano la digitalizzazione nella PA, inclusi la strategia nazionale per la digitalizzazione e le normative relative alla protezione dei dati (GDPR). - Pianificazione e gestione della digitalizzazione: approcci strategici per l'adozione delle tecnologie digitali nei processi pubblici, la gestione del cambiamento e l'implementazione di progetti digitali. - Digitalizzazione dei servizi pubblici: come digitalizzare i servizi per i cittadini, migliorare l'accessibilità, la trasparenza e la partecipazione civica. - Tecnologie emergenti nella PA: l'uso delle tecnologie emergenti (come l'intelligenza artificiale, il cloud computing e la blockchain) per ottimizzare i processi pubblici e migliorare l'efficacia dei servizi. - Gestione dei dati e sicurezza: l'importanza della protezione dei dati, della cyber sicurezza e della gestione sicura delle informazioni nella digitalizzazione della PA. - Valutazione dei progetti di digitalizzazione: metodi di valutazione dell'efficacia dei progetti di trasformazione digitale nella pubblica amministrazione. - Casi studio e best practices: esempi concreti di digitalizzazione di successo nella pubblica amministrazione, con analisi delle best practices applicate in vari contesti.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA8: Project Management per la PA Digitale

Obiettivi del corso	<p>Il corso "Project Management per la PA Digitale" ha l'obiettivo di fornire ai partecipanti le competenze necessarie per gestire con successo progetti digitali all'interno della pubblica amministrazione. Gli studenti apprenderanno le metodologie e le best practices del project management, applicandole in contesti pubblici, con particolare attenzione alla gestione dei progetti di trasformazione digitale e innovazione tecnologica. Il corso mira a sviluppare abilità nella pianificazione, monitoraggio e gestione di progetti digitali, con un focus su gestione dei team, budgeting, tempistiche e compliance normativa. Inoltre, si esploreranno le tecniche per garantire l'efficacia e l'efficienza dei processi digitali nella pubblica amministrazione, affrontando le sfide legate alla gestione di progetti complessi e al miglioramento continuo dei servizi pubblici attraverso l'adozione di tecnologie digitali.</p>
A chi si rivolge	<p>Il corso si rivolge a professionisti della pubblica amministrazione che sono coinvolti nella gestione di progetti digitali e di trasformazione tecnologica, come project manager, responsabili IT, coordinatori di progetto e dirigenti. È ideale per funzionari pubblici che desiderano acquisire competenze specifiche nella gestione dei progetti digitali e specialisti di digitalizzazione che lavorano in enti pubblici o in organizzazioni governative. Inoltre, il corso è adatto a consulenti e formatori che operano nel settore pubblico e che vogliono approfondire le metodologie di project management applicate alla digitalizzazione della pubblica amministrazione.</p>
Contenuti	<ul style="list-style-type: none"> - Introduzione al Project Management: Fondamenti e principi del project management applicati alla pubblica amministrazione, con focus sulle metodologie tradizionali e agili.

<p>Durata</p> <p>Costo</p> <p>Modalità</p>	<ul style="list-style-type: none"> - Gestione dei progetti digitali nella PA: Come progettare e implementare iniziative digitali, dalla fase di ideazione alla realizzazione, all'interno degli enti pubblici. - Pianificazione e gestione delle risorse: Tecniche di pianificazione dei progetti digitali, gestione dei team, allocazione delle risorse e gestione del tempo. - Gestione del budget e dei costi: Principi di budgeting, monitoraggio delle spese, controllo dei costi e gestione delle risorse finanziarie in progetti digitali. - Normative e compliance nella PA digitale: Analisi delle normative vigenti, come il GDPR, le leggi sulla digitalizzazione della PA e le politiche di sicurezza dei dati. - Gestione dei rischi e delle criticità: Identificazione dei rischi, tecniche di gestione delle criticità e delle emergenze, come il recupero dei progetti in caso di ritardi o fallimenti. - Tecnologie per la digitalizzazione della PA: Analisi delle tecnologie emergenti (cloud, big data, IA) e il loro impatto nella gestione dei servizi pubblici digitali. - Monitoraggio e controllo del progetto: Metodologie di controllo avanzate per garantire la qualità e il successo del progetto, con focus su KPI e reportistica. - Gestione del cambiamento e comunicazione: Strategie di gestione del cambiamento per l'adozione delle tecnologie digitali, con particolare attenzione alla comunicazione interna ed esterna. - Casi studio e best practices: Esempi pratici di progetti digitali di successo nella pubblica amministrazione e analisi di casi studio per comprendere le sfide e le soluzioni adottate. <p>15 ore</p> <p>Informazione fornita su richiesta</p> <p>In modalità sincrona, in presenza ed a distanza (su specifica richiesta)</p>
---	--

PA9: Open Data per la PA digitale

<p>Obiettivi del corso</p>	<p>Il corso ha l'obiettivo di fornire ai partecipanti le competenze necessarie per comprendere e utilizzare i dati aperti (open data) all'interno della pubblica amministrazione. I partecipanti apprenderanno come raccogliere, gestire, e pubblicare i dati in modo trasparente e accessibile, seguendo le normative vigenti e le migliori pratiche internazionali. Il corso mira a formare figure capaci di promuovere la digitalizzazione e l'innovazione all'interno della PA, migliorando l'efficienza dei processi e la partecipazione dei cittadini attraverso l'uso di dati aperti. Si focalizzerà sull'importanza degli open data per migliorare i servizi pubblici, stimolare la trasparenza, e facilitare la creazione di politiche pubbliche basate su dati concreti e accessibili.</p>
<p>A chi si rivolge</p>	<p>Il corso si rivolge a dipendenti pubblici e responsabili della digitalizzazione che lavorano all'interno della pubblica amministrazione e desiderano acquisire competenze nell'utilizzo degli open data. È ideale per dirigenti, manager e tecnici coinvolti nella progettazione e gestione dei servizi digitali, nonché per responsabili IT, data manager e specialisti di policy pubbliche. Inoltre, il corso è utile anche per consulenti digitali, professionisti della trasparenza e esperti di gestione dei dati, che vogliono approfondire il potenziale degli open data per migliorare i servizi pubblici e promuovere l'innovazione nelle istituzioni pubbliche.</p>
<p>Contenuti</p>	<ul style="list-style-type: none"> - Introduzione agli Open Data: Definizione, caratteristiche e importanza degli open data nella pubblica amministrazione. Panoramica su normative e linee guida internazionali e locali. - Gestione e Pubblicazione dei Dati: Tecniche per raccogliere, strutturare, e pubblicare i dati in formato aperto. Standard di interoperabilità e piattaforme di open data. - Strumenti e Tecniche di Accesso ai Dati: Strumenti per l'accesso, la visualizzazione e l'analisi dei dati aperti, inclusi software di visualizzazione, API e altre tecnologie. - Sicurezza e Privacy nei Dati Aperti: Gestione della sicurezza, della privacy e della protezione dei dati sensibili, in linea con le normative vigenti (GDPR e altre regolazioni locali).

	<ul style="list-style-type: none"> - Best Practices per l'Implementazione degli Open Data nella PA: Approcci per integrare gli open data nei processi decisionali, nel miglioramento dei servizi pubblici e nella partecipazione civica. - Open Data e Innovazione nei Servizi Pubblici: Applicazioni pratiche degli open data per creare politiche pubbliche più trasparenti e inclusive, stimolando la collaborazione tra cittadini e amministrazioni. - Monitoraggio e Valutazione dell'Impatto degli Open Data: Come monitorare e misurare i benefici derivanti dall'utilizzo degli open data nella pubblica amministrazione.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA10: Project Financing per la PA digitale

Obiettivi del corso	<p>Il corso ha l'obiettivo di fornire ai partecipanti le competenze necessarie per sviluppare e gestire progetti complessi in ambito pubblico, con particolare focus sulla gestione delle risorse finanziarie per l'innovazione digitale. I partecipanti acquisiranno una comprensione approfondita delle metodologie e degli strumenti di finanziamento pubblico e privato applicabili ai progetti digitali, imparando a strutturare soluzioni sostenibili che rispondano alle esigenze della pubblica amministrazione. Inoltre, il corso si concentra sull'identificazione delle opportunità di finanziamento, sulla redazione di piani finanziari efficaci e sulla gestione dei rischi, al fine di garantire l'efficacia e la sostenibilità dei progetti di trasformazione digitale nel settore pubblico.</p>
A chi si rivolge	<p>Il corso si rivolge a professionisti della pubblica amministrazione coinvolti nella pianificazione, gestione e finanziamento di progetti digitali, come responsabili dei settori IT, project manager, analisti finanziari e funzionari pubblici che operano nell'ambito della gestione di risorse e fondi pubblici. È adatto anche a consulenti e esperti di finanza che collaborano con enti pubblici per progettare soluzioni finanziarie per l'innovazione, nonché a responsabili di progetti digitali in enti locali, regioni e ministeri. Il corso è utile anche a imprenditori o professionisti privati che desiderano collaborare con la pubblica amministrazione nella realizzazione di progetti tecnologici, acquisendo conoscenze specifiche sul project financing nel contesto della digitalizzazione della PA.</p>
Contenuti	<ul style="list-style-type: none"> - Introduzione al Project Financing nella PA digitale: Principi di base del project financing e applicazioni specifiche nel contesto della pubblica amministrazione digitale. - Struttura e modelli di finanziamento: Analisi delle diverse tipologie di finanziamento (pubblico, privato e misto) per progetti digitali nella PA, e come scegliere il modello più adatto. - Gestione dei fondi pubblici e delle risorse: Come pianificare e gestire correttamente le risorse finanziarie, monitorare i flussi e garantire la sostenibilità economica. - Valutazione e selezione dei progetti digitali: Criteri per la selezione dei progetti e valutazione delle opportunità di finanziamento, inclusi la fattibilità economica e i benefici a lungo termine. - Normative e regolamenti: Le leggi e le normative che regolano il project financing nella pubblica amministrazione, con focus sulla conformità e le linee guida per i progetti digitali. - Redazione del piano finanziario: Tecniche per sviluppare un piano finanziario efficace che integri le risorse disponibili, i costi e gli obiettivi di progetto. - Gestione dei rischi: Come identificare, valutare e gestire i rischi finanziari, operativi e legali nei progetti digitali finanziati tramite project financing.

	<ul style="list-style-type: none"> - Monitoraggio e rendicontazione: Strategie per monitorare l'avanzamento dei progetti, la gestione del budget e la rendicontazione delle spese. - Casi studio e best practices: Analisi di progetti di successo e insuccesso nella PA digitale, con focus sulle lezioni apprese e le best practices.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA11: Comunicazione Digitale e Orientamento al Cittadino nella PA

Obiettivi del corso	Il corso ha l'obiettivo di migliorare le competenze comunicative dei dipendenti pubblici, fornendo strumenti e strategie per un'interazione efficace e trasparente con i cittadini attraverso canali digitali. Mira a potenziare l'uso delle tecnologie digitali per facilitare l'accesso ai servizi pubblici, migliorare la qualità delle informazioni fornite e favorire una partecipazione attiva e consapevole dei cittadini. Il corso intende anche promuovere una cultura di orientamento al cittadino, incentrata sull'ascolto delle esigenze, la risoluzione dei problemi e l'efficienza dei processi comunicativi.
A chi si rivolge	Il corso si rivolge a dipendenti e funzionari della pubblica amministrazione che operano nei settori della comunicazione, del servizio al cittadino e della gestione dei servizi digitali. È ideale per responsabili della comunicazione, addetti agli sportelli informativi, social media manager, responsabili dell'innovazione digitale, e dirigenti che desiderano migliorare l'interazione con i cittadini e ottimizzare l'uso delle tecnologie digitali nei processi comunicativi. Inoltre, il corso è utile per professionisti IT e consulenti che collaborano con enti pubblici per la digitalizzazione dei servizi e la promozione di una cultura orientata al cittadino.
Contenuti	<ul style="list-style-type: none"> - Principi della comunicazione digitale: Fondamenti e best practices per una comunicazione efficace attraverso i canali digitali. - Strumenti digitali per la comunicazione: Uso di piattaforme social, siti web istituzionali, newsletter e altri strumenti per informare e interagire con i cittadini. - Strategie di engagement: Tecniche per coinvolgere i cittadini, promuovere la partecipazione attiva e raccogliere feedback. - Accessibilità e inclusività: Creazione di contenuti digitali accessibili a tutti i cittadini, compresi quelli con disabilità. - Normative e regolamenti: Conoscenza delle leggi e dei regolamenti relativi alla comunicazione digitale nella pubblica amministrazione, inclusa la gestione della privacy e dei dati personali. - Gestione delle crisi comunicative: Tecniche per affrontare e gestire situazioni di crisi e comunicazioni sensibili. - Analisi e monitoraggio: Utilizzo di strumenti di analisi per monitorare l'efficacia della comunicazione digitale e migliorare le strategie in base ai risultati ottenuti. - Formazione e aggiornamento del personale: Metodologie per formare i dipendenti sull'uso delle tecnologie digitali e sulle pratiche di comunicazione. - Case studies: Analisi di casi di studio reali su comunicazione digitale e interazione con i cittadini nella pubblica amministrazione. - Progettazione e implementazione di campagne digitali: Sviluppo di campagne di comunicazione mirate, dalla pianificazione alla realizzazione.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA12: I Processi della PA nell'Economia Digitale

Obiettivi del corso	Il corso ha l'obiettivo di fornire una comprensione approfondita di come le pubbliche amministrazioni possono sfruttare le tecnologie digitali per migliorare l'efficienza e la trasparenza dei loro processi. I partecipanti apprenderanno come ottimizzare i flussi di lavoro attraverso l'uso di strumenti digitali, ridurre i tempi di risposta e migliorare l'accessibilità dei servizi pubblici. Inoltre, il corso mira a fornire le competenze necessarie per gestire i dati in modo sicuro e conforme alle normative vigenti, e per implementare soluzioni innovative che favoriscano la partecipazione e l'interazione con i cittadini. L'obiettivo finale è di preparare i professionisti della PA a guidare la trasformazione digitale nelle loro organizzazioni, migliorando l'efficacia delle operazioni quotidiane e la qualità dei servizi offerti.
A chi si rivolge	Il corso si rivolge a funzionari e dirigenti delle pubbliche amministrazioni, responsabili dei servizi digitali, manager IT e responsabili della trasformazione digitale che operano all'interno delle istituzioni pubbliche. È ideale per consulenti e professionisti del settore pubblico che si occupano di migliorare l'efficienza dei processi amministrativi attraverso l'adozione di tecnologie digitali. Inoltre, il corso è adatto a project manager, analisti di processo e sviluppatori di soluzioni digitali che lavorano a stretto contatto con le amministrazioni pubbliche per implementare progetti di digitalizzazione e innovazione. Anche i policy maker interessati a comprendere le sfide e le opportunità dell'economia digitale nel contesto della pubblica amministrazione possono trarre beneficio dalla partecipazione a questo corso.
Contenuti	<ul style="list-style-type: none"> - Introduzione alla digitalizzazione nella PA: Panoramica delle tecnologie digitali applicabili alle pubbliche amministrazioni e dei benefici della digitalizzazione. - Ottimizzazione dei flussi di lavoro: Tecniche e strumenti per migliorare l'efficienza e la trasparenza dei processi amministrativi attraverso la digitalizzazione. - Gestione dei dati e sicurezza: Strategie per la gestione sicura dei dati, conformità alle normative sulla privacy e sicurezza informatica nelle amministrazioni pubbliche. - Servizi digitali al cittadino: Sviluppo e implementazione di servizi digitali per migliorare l'interazione e la partecipazione dei cittadini. - Tecnologie emergenti nella PA: Introduzione a tecnologie come l'intelligenza artificiale, la blockchain e l'Internet delle cose (IoT) e il loro potenziale applicativo nelle amministrazioni pubbliche. - Casi di studio e best practice: Analisi di esempi di successo di digitalizzazione in diverse pubbliche amministrazioni e le migliori pratiche adottate. - Gestione del cambiamento: Tecniche per gestire il cambiamento organizzativo necessario per una transizione efficace verso l'economia digitale. - Normative e compliance: Panoramica delle principali normative europee e nazionali relative alla digitalizzazione della PA e alla gestione dei dati. - Strumenti di e-government: Utilizzo di piattaforme e strumenti di e-government per la gestione dei servizi pubblici digitali. - Sviluppo di competenze digitali: Formazione e sviluppo delle competenze digitali per il personale delle pubbliche amministrazioni.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA13: Le tecnologie abilitanti per la PA digitale

Obiettivi del corso	Il corso mira a fornire ai partecipanti una comprensione approfondita delle tecnologie chiave che facilitano la trasformazione digitale nella Pubblica Amministrazione. Gli obiettivi includono l'acquisizione di competenze per implementare soluzioni tecnologiche innovative, migliorare l'efficienza dei servizi pubblici e aumentare la trasparenza e l'accessibilità delle informazioni. I partecipanti impareranno a utilizzare
----------------------------	--

A chi si rivolge	<p>strumenti digitali per ottimizzare i processi amministrativi, gestire dati in modo sicuro e conforme alle normative, e promuovere la partecipazione digitale dei cittadini. Inoltre, il corso intende sviluppare una cultura digitale all'interno delle organizzazioni pubbliche, facilitando la gestione del cambiamento tecnologico e migliorando la collaborazione intersettoriale.</p> <p>Il corso si rivolge a funzionari e dirigenti della Pubblica Amministrazione, responsabili IT, professionisti delle risorse umane e progettisti di servizi pubblici digitali. È adatto anche a consulenti e esperti di trasformazione digitale che collaborano con enti pubblici per l'implementazione di soluzioni tecnologiche. Inoltre, il corso è utile per amministratori locali, policy maker e ricercatori interessati a comprendere e promuovere l'innovazione digitale nei servizi pubblici.</p>
Contenuti	<ul style="list-style-type: none"> - Fondamenti della trasformazione digitale nella Pubblica Amministrazione: Introduzione ai concetti chiave e alle strategie di digitalizzazione nei servizi pubblici. - Tecnologie abilitanti: Analisi delle tecnologie essenziali come cloud computing, intelligenza artificiale, blockchain, Internet of Things (IoT) e big data, con esempi di applicazioni pratiche. - Infrastrutture digitali: Progettazione e gestione delle infrastrutture IT per supportare servizi digitali efficienti e sicuri, includendo aspetti di scalabilità e resilienza. - Gestione dei dati e normativa GDPR: Tecniche per la raccolta, analisi, gestione e protezione dei dati, con particolare attenzione alla conformità con le normative sulla privacy. - Sviluppo e implementazione di servizi digitali: Metodologie per creare e ottimizzare servizi digitali che migliorino l'efficienza operativa e l'accessibilità per i cittadini. - Cybersecurity: Principi e pratiche di sicurezza informatica per proteggere dati e servizi digitali da minacce e vulnerabilità. - Interoperabilità e standard aperti: Utilizzo di standard aperti per garantire l'interoperabilità tra sistemi diversi e migliorare la collaborazione tra enti pubblici. - Cittadinanza digitale e partecipazione: Strategie per coinvolgere i cittadini nell'uso dei servizi digitali e promuovere la loro partecipazione attiva nei processi pubblici. - Gestione del cambiamento: Approcci per gestire il cambiamento organizzativo e culturale necessario per una trasformazione digitale efficace, inclusi aspetti di formazione e sviluppo delle competenze. - Case studies e best practices: Analisi di casi reali di successo nella digitalizzazione della Pubblica Amministrazione, con condivisione delle migliori pratiche e lezioni apprese.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA14: Misurazione Performance e KPI per la PA Digitale

Obiettivi del corso	<p>Il corso ha l'obiettivo di fornire ai partecipanti gli strumenti necessari per misurare e valutare l'efficacia delle attività e dei processi nella Pubblica Amministrazione digitale. Si focalizzerà sull'identificazione e l'analisi dei KPI (Key Performance Indicators) più rilevanti per monitorare e ottimizzare le performance dei servizi pubblici digitalizzati. I partecipanti apprenderanno come definire obiettivi misurabili, monitorare i risultati attraverso indicatori chiave e utilizzare questi dati per migliorare l'efficienza operativa e la qualità dei servizi. Un altro obiettivo importante sarà quello di acquisire competenze nella gestione e nella comunicazione dei risultati, supportando le decisioni strategiche attraverso un approccio basato sui dati.</p>
A chi si rivolge	<p>Il corso si rivolge a responsabili della gestione e della digitalizzazione all'interno della Pubblica Amministrazione, come manager, dirigenti e responsabili dei servizi digitali. È</p>

Contenuti	<p>ideale anche per funzionari e tecnici che si occupano di monitoraggio e valutazione delle performance, analisti di dati e project manager impegnati nella progettazione e implementazione di soluzioni digitali per il settore pubblico. Inoltre, il corso è utile per consulenti e formatori che lavorano con enti pubblici e che desiderano approfondire l'uso dei KPI per ottimizzare i processi e migliorare i servizi digitali offerti alla cittadinanza.</p> <ul style="list-style-type: none"> - Introduzione alla misurazione delle performance nella PA digitale: definizione, importanza e contesto. - Identificazione e selezione dei KPI: come scegliere gli indicatori più appropriati per misurare l'efficienza e l'efficacia dei servizi digitali pubblici. - Tecniche di raccolta e analisi dei dati: metodi per raccogliere, analizzare e interpretare i dati relativi alle performance. - Monitoraggio e reporting: come monitorare in tempo reale e creare report efficaci per la gestione delle performance. - Ottimizzazione dei processi attraverso i KPI: come utilizzare i dati raccolti per migliorare i processi e i servizi digitali nella PA. - Tecnologie di supporto alla misurazione delle performance: strumenti e piattaforme per il monitoraggio delle performance. - Case study e best practices: esempi di applicazione dei KPI nella PA digitale per ottimizzare le operazioni e il servizio pubblico. - Comunicazione dei risultati e decisioni basate sui dati: come utilizzare i KPI per supportare decisioni strategiche nella pubblica amministrazione.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA15: Organizzazione della PA digitale

Obiettivi del corso	<p>Il corso ha l'obiettivo di fornire ai partecipanti una comprensione approfondita dei principi e delle pratiche necessarie per gestire e ottimizzare i processi digitali all'interno della pubblica amministrazione. I partecipanti acquisiranno competenze nel progettare e implementare soluzioni digitali per migliorare l'efficienza operativa, favorire l'integrazione tra i diversi sistemi e garantire la trasparenza e la fruibilità dei servizi pubblici. Inoltre, il corso esplorerà le normative e le tecnologie emergenti che supportano la digitalizzazione, con un focus sull'adozione di strumenti tecnologici innovativi e sulla gestione del cambiamento organizzativo in un contesto pubblico. L'obiettivo finale è formare professionisti capaci di guidare la trasformazione digitale nel settore pubblico, garantendo la qualità dei servizi e il rispetto delle normative.</p>
A chi si rivolge	<p>Il corso si rivolge a dirigenti e funzionari pubblici, responsabili della digitalizzazione e gestori di progetti tecnologici all'interno della pubblica amministrazione. È ideale per amministratori pubblici, tecnici informatici e project manager coinvolti nella gestione di processi digitali o nell'implementazione di soluzioni tecnologiche in enti pubblici. Inoltre, il corso è destinato a consulenti e professionisti che desiderano acquisire competenze per supportare la digitalizzazione della pubblica amministrazione, nonché a responsabili della compliance e della sicurezza informatica in ambito pubblico.</p>
Contenuti	<ul style="list-style-type: none"> - Digitalizzazione nei servizi pubblici - Ottimizzazione dei processi amministrativi tramite tecnologie digitali - Gestione dei dati pubblici e loro protezione - Sicurezza informatica nella pubblica amministrazione - Normativa sulla gestione digitale della PA - Trasparenza e accessibilità dei dati pubblici - Tecnologie emergenti (intelligenza artificiale, machine learning)

	<ul style="list-style-type: none"> - Gestione del cambiamento organizzativo nella PA - Adozione di soluzioni cloud per la PA - Collaborazioni interistituzionali per la digitalizzazione - Buone pratiche per l'implementazione della digitalizzazione nel settore pubblico
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)

PA16: Il Public Procurement nella PA digitale

Obiettivi del corso	Il corso ha l'obiettivo di fornire una comprensione approfondita del processo di acquisto pubblico nel contesto della digitalizzazione della pubblica amministrazione. I partecipanti apprenderanno come integrare le tecnologie digitali nei processi di procurement, migliorando l'efficienza, la trasparenza e la sostenibilità delle gare pubbliche. Si focalizzerà sull'utilizzo di strumenti digitali per semplificare le procedure di acquisto, ottimizzare la gestione dei contratti pubblici e garantire la compliance alle normative vigenti. Inoltre, il corso esplorerà le sfide e le opportunità della digitalizzazione per la gestione degli appalti pubblici, con un focus sulle best practice e sugli strumenti tecnologici che supportano il settore.
A chi si rivolge	Il corso si rivolge a professionisti della pubblica amministrazione, come responsabili degli acquisti, gestori di appalti, funzionari pubblici e project manager che si occupano di gestione dei contratti pubblici e processi di procurement. È utile anche per consulenti e avvocati specializzati in normativa pubblica e appalti, nonché per professionisti IT coinvolti nella digitalizzazione dei processi amministrativi. Inoltre, il corso è adatto a dirigenti e manager che lavorano nel settore pubblico e che desiderano acquisire competenze per affrontare le sfide della digitalizzazione nella gestione degli appalti.
Contenuti	<ul style="list-style-type: none"> - Introduzione al public procurement e al suo ruolo nella pubblica amministrazione. - Il processo di acquisizione digitale: tecnologie e strumenti utilizzati per digitalizzare il procurement pubblico. - Le normative vigenti nel settore degli appalti pubblici e la loro evoluzione con la digitalizzazione. - Il ruolo della trasparenza e della concorrenza nei processi di acquisto digitali. - Piattaforme digitali e strumenti tecnologici per la gestione delle gare e degli appalti. - E-procurement e la gestione elettronica dei contratti pubblici. - La gestione dei dati e delle informazioni nella pubblica amministrazione attraverso strumenti digitali. - Le sfide e opportunità legate alla digitalizzazione del public procurement. - La gestione del monitoraggio, controllo e reporting degli appalti tramite soluzioni digitali. - Best practice e casi di studio sulla digitalizzazione degli appalti pubblici.
Durata	15 ore
Costo	Informazione fornita su richiesta
Modalità	In modalità sincrona, in presenza ed a distanza (su specifica richiesta)