Ottobre 2023

Sicurezza informatica per la Formazione Professionale e le PMI

CURRICULUM EUROPEO SULLA SICUREZZA INFORMATICA

SVILUPPATO DA META4 INNOVATIONS E. U.

WORK PACKAGE 3 - CURRICULUM EUROPEO SULLA SICUREZZA INFORMATICA

Funded by the European Union

Finanziato dall'Unione europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione europea o dell'Agenzia esecutiva per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili. KA220-VET-C9588303

CONTENUTI

IL PROGETTO

SecureFuture – Sicurezza Informatica per Istituti di Formazione Professionale e le PMI - è un progetto Erasmus+ realizzato tra dicembre 2022 e dicembre 2024. Il progetto è condotto da un consorzio di sei partner provenienti da cinque paesi, tutti con competenze rilevanti nel campo dell'Istruzione e della Formazione Professionale (IFP) e della Sicurezza Informatica.

PAESE	ORGANIZZAZIONE
Turchia	Istanbul Ticaret Universitesi (coordinatore)
Turchia	İstanbul Valiligi
Portogallo	Mindshift Talent Advisory
Spagna	Media Creativa 2020
Italia	Pragma Engineering srl
Austria	Meta4 Innovations

Il consorzio SecureFuture ha rilevato come il livello attuale di preparazione fornita nei percorsi di formazione professionale dell'Unione Europea (UE) non sia all'altezza delle esigenze del mercato del lavoro e come ci siano Paesi che non hanno un livello diffuso di formazione adeguato nel campo della Sicurezza Informatica (CyberSecurity). Inoltre, molte piccole e medie imprese (PMI) non dispongono di personale qualificato per proteggere le loro aziende dalle minacce informatiche e trovare assistenza esterna in materia di Sicurezza Informatica è molto costoso.

Tenendo conto di questi aspetti, il progetto sta sviluppando un curriculum e contenuti formativi sulla Sicurezza Informatica per guidare IFP (Istituti di Formazione Professionale) le PMI che vogliono fornire competenze di Sicurezza Informatica ai loro allievi e dipendenti. Questo documento fa riferimento al Curriculum europeo sulla Sicurezza Informatica.

ABSTRACT

Il Curriculum europeo sulla Sicurezza Informatica proposto è il risultato finale dell'attività 3 del progetto: WP3 - Curriculum europeo sulla Sicurezza Informatica.

Il leader del WP3 - Meta4 Innovations e. U. - ha preparato un piano di lavoro, linee guida e modelli per tutti i partner al fine di facilitare la progettazione e lo sviluppo di una proposta di Curriculum europeo sulla Sicurezza Informatica. Il processo di sviluppo ha previsto che questo Curriculum europeo sulla Sicurezza Informatica fosse modellato sul Framework Europeo delle Qualifiche (EQF) attraverso un confronto delle attuali competenze nazionali e relativi Quadri delle Qualifiche Nazionali sulla Sicurezza Informatica, che è stato sviluppato dai partner.

A luglio 2023 è stata condotta un'indagine in tutti i Paesi partner - Austria, Italia, Portogallo, Spagna e Turchia - in cui un gruppo di 66 esperti ha fornito i propri contributi, al fine di acquisire una panoramica delle rispettive esigenze nazionali in merito al curriculum del progetto. Questi contributi sono stati messi insieme da Meta4 e condivisi con i partner per individuare le Unità Formative che compongono il presente Curriculum Europeo sulla Sicurezza Informatica.

1. INTRODUZIONE AL CURRICULUM

Valutazione ECVET

Considerando l'eterogeneità dell'uso di ECVET nei Paesi partner e i crediti ECVET medi assegnati per ogni ora di formazione, il partenariato del progetto SecureFuture ha concordato quanto segue:

20 ore di formazione = 1 punto ECVET

Il Curriculum Europeo sulla Sicurezza Informatica è composto da 10 moduli per un totale di 120 ore, che corrispondono a 6 punti ECVET.

Unità 1: Introduzione alla tutela della Sicurezza Informatica

Introduzione

L'unità "Introduzione alla tutela della Sicurezza Informatica" introduce al tema della Sicurezza Informatica per le PMI. Questo modulo fornisce ai discenti le conoscenze e le competenze essenziali per difendersi dalle minacce informatiche e proteggere i dati sensibili nell'attuale panorama in costante evoluzione.

Obiettivo

L'obiettivo è quello di fornire ai partecipanti una solida comprensione dei concetti e dei principi fondamentali della Sicurezza Informatica per identificare, mitigare e rispondere efficacemente alle minacce informatiche.

LEARNING OUTCOMES

Conoscenze	K1. Comprendere i principi di base della Sicurezza Informatica e della tutela dei dati. K2. Identificare le minacce informatiche e le vulnerabilità comuni. K3. Comprendere gli aspetti legali ed etici della Sicurezza Informatica.	Competenze	S1. Dimostrare la capacità di analizzare il traffico di rete alla ricerca di attività sospette. S2. Capacità di configurare i firewall contro le minacce e le vulnerabilità. S3. Competenza nella conduzione di test e valutazioni di sicurezza.	Responsabilità e autonomia	RA1. Valutare e dare priorità ai rischi per la sicurezza per sviluppare un piano d'azione personalizzato per la Sicurezza Informatica. RA2. Rispondere efficacemente alle minacce informatiche più comuni, come il malware o il phishing. RA3. Collaborare alle procedure per ridurre al minimo l'impatto degli incidenti di sicurezza.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 2: Protezione dati e privacy

Introduzione

Questa unità fornisce ai discenti le competenze essenziali per la salvaguardia dei dati nell'era digitale. Tratta gli aspetti chiave della protezione dei dati, tra cui la classificazione dei dati, la gestione responsabile delle informazioni sensibili, la privacy, la proprietà intellettuale e le complessità della guerra informatica. Viene data rilevanza al GDPR e alle altre normative sulla protezione dei dati, insieme alla crittografia efficace delle informazioni, alle pratiche di archiviazione sicura e alla risposta agli episodi di violazioni dei dati. Il modulo promuove atteggiamenti che danno priorità alla privacy, all'etica e all'adattabilità nella Sicurezza Informatica, consentendo agli studenti di contribuire attivamente alla difesa digitale e di diventare attenti protettori dei dati e della privacy.

Obiettivo

Fornire le conoscenze, le competenze e le attitudini necessarie per proteggere e gestire efficacemente i dati, assicurando la conformità alle normative sulla protezione dei dati e salvaguardando la privacy nella Sicurezza Informatica.

LEARNING OUTCOMES

Conoscenze	K1. Definire i concetti relativi ai dati, comprese le informazioni sensibili, la proprietà intellettuale e la guerra informatica. K2. Distinguere le normative sulla protezione dei dati personali, i dati digitali e il Regolamento Generale sulla Protezione dei Dati (GDPR). K3. Spiegare l'importanza di promuovere una mentalità che dia priorità alla gestione responsabile dei dati.	Competenze	S1. Utilizzare adeguate tecniche di crittografia in base ai diversi tipi di dati. S2. Applicare le migliori pratiche di archiviazione sicura dei dati, tra cui la crittografia, il controllo degli accessi e i backup regolari. S3. Creare piani di gestione delle violazioni dei dati tenendo conto della gravità delle violazioni.	Responsabilità e autonomia	RA1. Sensibilizzare alla salvaguardia dei dati e al rispetto dei diritti individuali alla privacy. RA2. Adottare un approccio etico al trattamento dei dati e alla proprietà intellettuale. RA3. Sviluppare un atteggiamento resiliente e adattivo nei confronti delle minacce e delle normative di Sicurezza Informatica in continua evoluzione.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 3: Gestione del rischio e conformità normativa

Introduzione

Questa unità fornisce le competenze essenziali per gestire i rischi correlati alla Sicurezza Informatica e garantire la conformità normativa. Integra la gestione del rischio informatico nelle pratiche di gestione del rischio a livello aziendale pur essendo consapevoli che la completa eliminazione del rischio è irraggiungibile. Si concentra invece sulla riduzione dell'impatto delle minacce attraverso programmi efficaci di gestione del rischio informatico. Il modulo introduce agli standard riconosciuti a livello internazionale, in particolare al Sistema di Gestione della Sicurezza delle Informazioni (SGSI), delineando i passaggi chiave e le azioni di controllo per la conformità. Oltre alle conoscenze e alle competenze, il modulo approfondisce lo sviluppo di atteggiamenti legati all'applicazione degli schemi di conformità SGSI e delle raccomandazioni per l'analisi, il riconoscimento e la mitigazione dei rischi, consentendo ai discenti di affrontare e gestire in modo proattivo le minacce alla Sicurezza Informatica, promuovendo un approccio sistemico alla sicurezza delle informazioni.

Obiettivo

Mettere gli studenti in condizione di acquisire le conoscenze, le competenze e le attitudini necessarie per applicare efficacemente le metodologie di gestione del rischio anche in riferimento alle norme internazionali di conformità per la Sicurezza Informatica.

LEARNING OUTCOMES

Conoscenze	K1. Definire i componenti e i requisiti del Sistema di Gestione della Sicurezza delle Informazioni. K2. Identificare la gestione del rischio informativo in funzione del Sistema di Gestione della Sicurezza delle Informazioni. K3. Descrivere l'approccio alle regole di conformità della Sicurezza Informatica.	Competenze	S1. Identificare i componenti principali del Sistema di Gestione della Sicurezza delle Informazioni S2. Progettare schemi di gestione del rischio applicati alle PMI S3. Esaminare i requisiti di conformità alle norme di Sicurezza Informatica	Responsabilità e autonomia	RA 1. Collaborare alla definizione del Sistema di Gestione della Sicurezza delle Informazioni delle PMI RA2. Rispettare il processo di gestione del rischio RA3. Affrontare l'adozione di regole di conformità alla Sicurezza Informatica

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 4: Ingegneria sociale e consapevolezza del phishing

Introduzione

Questa unità di apprendimento si concentra sull'ingegneria delle reti social (social engineering) e la consapevolezza del phishing, essenziali nel nostro mondo digitalmente connesso. Questi argomenti sono tanto critici quanto l'impatto trasformativo dei sistemi cloud sulle aziende. Al termine dell'unità, gli studenti definiranno l'ingegneria sociale, comprenderanno le sue motivazioni (come il ritorno finanziario e il furto di dati) e riconosceranno le varie tecniche di phishing e i vettori di attacco utilizzati dai criminali informatici. Questo migliorerà le loro capacità di rilevamento e risposta alle minacce. Gli studenti comprenderanno anche le implicazioni legali ed etiche degli attacchi di ingegneria sociale, promuovendo pratiche di Sicurezza Informatica responsabili. L'unità fornisce consapevolezza etica, promuove la collaborazione nella risposta agli incidenti ed enfatizza la conformità legale. È un'opportunità per professionisti IT, imprenditori, studenti VET o chiunque sia interessato, a rafforzare le conoscenze in materia di Sicurezza Informatica per un futuro digitale sicuro.

Obiettivo

Questa unità di apprendimento punta a fornire ai partecipanti le conoscenze, le competenze e gli atteggiamenti etici per definire la cosiddetta social engineering, identificare le tecniche di phishing e comprenderne efficacemente le implicazioni legali ed etiche.

LEARNING OUTCOMES

Conoscenze	K1. Definire l'ingegneria sociale (social engineering) e le sue cause nel contesto delle PMI. K2. Identificare le tecniche di phishing e i vettori di attacco che rendono vulnerabili le PMI. K3. Ricordare le implicazioni legali ed etiche dell'ingegneria delle reti social nel contesto delle PMI.	Competenze	S1. Descrivere le motivazioni principali degli attacchi a livello di social network. S2. Riconoscere metodi quali spear phishing, vishing (phishing vocale) e pretexting. S3. Comprendere le potenziali conseguenze sia per gli autori che per le vittime.	Responsabilità e autonomia	RA1. Promuovere la consapevolezza etica nel definire le motivazioni dell'ingegneria delle reti social per un uso responsabile e basato sui principi della conoscenza. RA2. Collaborare con i team per mitigare le minacce di phishing quando si identificano le tecniche e i vettori di attacco. RA3. Rispettare in modo indipendente le leggi, garantendo la legalità delle azioni e delle pratiche di “social engineering”.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 5: Sicurezza del cloud per le PMI

Introduzione

Questa unità si concentra sull'affrontare le particolari sfide di sicurezza che i sistemi cloud presentano per le PMI, che sempre più spesso si affidano a questi sistemi per la flessibilità, la scalabilità e l'efficienza dei costi. L'unità è progettata per fornire alle PMI le conoscenze e le competenze necessarie per gestire efficacemente la sicurezza del cloud. Il modulo formativo è adattato alle esigenze e ai vincoli specifici delle PMI, offrendo spunti pratici e strategie attuabili per mitigare i rischi, proteggere le informazioni sensibili e garantire la conformità alle normative di settore. I partecipanti esploreranno i principi fondamentali della sicurezza del cloud, le tecnologie all'avanguardia e acquisiranno esperienza pratica nell'implementazione delle misure di sicurezza. Che si tratti di un imprenditore, di un professionista IT, di uno studente VET o di una persona che desidera migliorare le proprie conoscenze in materia di sicurezza del cloud, questo modulo fornisce ai partecipanti gli strumenti necessari per proteggere efficacemente il futuro digitale della propria PMI.

Obiettivo

Questa unità ha lo scopo di consentire ai discenti di avere una visione dei vantaggi, dei possibili rischi e delle istruzioni per massimizzare l'impatto dell'utilizzo dei sistemi cloud per una PMI.

LEARNING OUTCOMES

Conoscenze	K1. Identificare i vantaggi dell'utilizzo di sistemi cloud per una PMI. K2. Descrivere e mitigare i possibili rischi dell'utilizzo di sistemi cloud. K3. Delineare le misure preventive che potrebbero essere prese in considerazione per la sicurezza del cloud computing delle PMI.	Competenze	S1. Analizzare gli aspetti riguardanti l'uso che le PMI possono fare del cloud computing. S2. Presentare domande e proporre soluzioni relative alla sicurezza in un contesto di gestione del rischio. S3. Illustrare i diversi tipi di requisiti legali che potrebbero avere un impatto sull'utilizzo dei sistemi cloud.	Responsabilità e autonomia	RA1. Garantire la sicurezza del cloud in conformità con le regole sui dati personali dell'UE e la legislazione nazionale in materia di protezione dati. RA2. Collaborare con i colleghi per fornire uno scenario esemplificativo di un sistema Cloud. RA3. Guidare un team per la valutazione delle opportunità di sicurezza in esecuzione di un appalto.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 6: Fondamenti di sicurezza di reti

Introduzione

La sicurezza della rete è un elemento cruciale per le PMI che vogliono difendersi dalle minacce informatiche. Comporta un approccio olistico che incorpora protezioni fisiche e software e richiede una comprensione a livello di organizzazione. I partecipanti acquisiranno una conoscenza approfondita delle precauzioni comprendendo la comprensione concettuale e le abilità interpersonali. Impareranno a conoscere le misure disponibili per le PMI per gestire la sicurezza delle reti, compresa la formazione di team dedicati in grado di eseguire azioni di protezione.

Obiettivo

Questa unità ha lo scopo di fornire una comprensione di base della sicurezza delle reti per le PMI e di come guidare la propria azienda verso la sicurezza delle PMI.

LEARNING OUTCOMES

Conoscenze	K1. Spiegare i termini e i concetti di base della sicurezza di una rete. K2. Ricordare le topologie e le strategie di base utilizzate nella comunicazione di una rete. K3. Identificare gli elementi fisici di connessione alla rete e le procedure di sicurezza fisica.	Competenze	S1. Discutere sul perché la sicurezza della rete è importante per una PMI. S2. Illustrare i possibili rischi e le possibili soluzioni per la sicurezza delle reti. S3. Illustrare le potenziali minacce alla rete e il modo in cui una PMI dovrebbe reagire e prevenirle.	Responsabilità e autonomia	RA1. Guidare un team costituito per la sicurezza della rete informatica. RA2. Fornire raccomandazioni su come un'azienda può integrare la sicurezza della rete nel suo piano aziendale. RA3. Verificare e monitorare l'implementazione delle procedure di sicurezza della rete.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 7: Sviluppo sicuro del software

Introduzione

Lo sviluppo sicuro del software è fondamentale di fronte alle crescenti minacce informatiche. È necessario incorporare pratiche di sicurezza nell'intero ciclo di sviluppo del software, dalla progettazione alla codifica, fino al collaudo, alla distribuzione e alla manutenzione. L'obiettivo è salvaguardare i dati, preservare la privacy degli utenti e garantire l'integrità e la disponibilità del sistema software. I principi chiave comprendono la difesa in profondità con più livelli di sicurezza, il privilegio minimo per l'accesso minimo e la progettazione sicura fin dalle prime fasi. È essenziale eseguire test regolari, compresi test di penetrazione e revisioni del codice. L'implementazione, la manutenzione e la risposta agli incidenti sono fondamentali per una sicurezza continua. La formazione e la consapevolezza, insieme alle risorse di supporto, migliorano ulteriormente la sicurezza dell'organizzazione. Lo sviluppo di software sicuro è indispensabile nel panorama odierno delle minacce, per mitigare i rischi e preservare la fiducia degli utenti.

Obiettivo

Imparare a implementare pratiche di sviluppo software sicure, salvaguardando i sistemi, i dati sensibili e la privacy degli utenti, riducendo al minimo i rischi di violazione e di attacco informatico e garantendo manutenzione, test e formazione.

LEARNING OUTCOMES

Conoscenze	K1. Definire le pratiche di programmazione sicura, le minacce comuni alla sicurezza e standard e schemi di sicurezza. K2. Conoscere il ciclo di vita dello sviluppo sicuro e la gestione della configurazione, la distribuzione sicura e la manutenzione. K3. Determinare la valutazione della vulnerabilità e i test di penetrazione, la crittografia e la cifratura, la sicurezza delle API e delle integrazioni.	Competenze	S1. Sperimentare la codifica sicura, la valutazione della vulnerabilità, i test di sicurezza, la crittografia e la cifratura. S2. Costruire una gestione, una distribuzione e una manutenzione sicure della configurazione e una progettazione sicura delle API. S3. Migliorare la conformità e le norme sulla privacy, l'apprendimento continuo	Responsabilità e autonomia	RA1. Gli sviluppatori hanno la responsabilità di dare priorità alla sicurezza nelle loro pratiche di programmazione. RA2. Prendere decisioni su questioni relative alla sicurezza durante il processo di sviluppo del software. RA3. Collaborare con gli esperti di sicurezza durante il processo di sviluppo per garantire che i requisiti di sicurezza siano adeguatamente soddisfatti.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 8: Protezione sicura degli endpoint

Introduzione

Nel mondo interconnesso di oggi, è essenziale proteggere gli endpoint, tra cui laptop, desktop, dispositivi mobili e server, dagli attacchi informatici. La protezione sicura degli endpoint implica la realizzazione di una strategia di difesa a più livelli per proteggere questi dispositivi da malware, ransomware, phishing e accessi non autorizzati. Ciò comporta l'implementazione di un robusto software antivirus e anti-malware, l'utilizzo di meccanismi avanzati di rilevamento e prevenzione delle minacce, l'applicazione di rigorosi controlli di accesso e misure di autenticazione e l'aggiornamento regolare di software e sistemi operativi. La protezione sicura degli endpoint è fondamentale per le organizzazioni di tutte le dimensioni e di tutti i settori in quanto consente di evitare le violazioni dei dati, di impedire l'accesso non autorizzato alle informazioni sensibili e di salvaguardare la continuità aziendale. Proteggendo gli endpoint, le organizzazioni possono ridurre il rischio di attacchi informatici, aderire alle normative di settore e proteggere la propria reputazione e la fiducia dei clienti.

Obiettivo

Imparate a proteggere gli endpoint (laptop, desktop, dispositivi mobili e server) da malware, ransomware, phishing e accessi non autorizzati, riducendo le violazioni dei dati e le interruzioni operative, garantendo al contempo la conformità e preservando la fiducia.

LEARNING OUTCOMES

Conoscenze	K1. Comprendere la sicurezza degli endpoint e la panoramica delle misure di protezione degli stessi. K2. Definire i componenti chiave della protezione sicura degli endpoint: antivirus, firewall e crittografia. K3. Determinare le *best practice* per l'implementazione della protezione sicura degli endpoint, della gestione delle patch, del rilevamento delle minacce e della formazione degli utenti.	Competenze	S1. Analizzare e rispondere alle minacce di malware, ransomware e phishing per una mitigazione efficace. S2. Gestire e configurare gli strumenti di sicurezza degli endpoint (antivirus, firewall, crittografia) per una distribuzione e un funzionamento efficaci. S3. Gestire le patch, i controlli di accesso, la crittografia dei dati e migliorare la consapevolezza degli utenti per la sicurezza degli endpoint.	Responsabilità e autonomia	RA1. Proteggere gli endpoint con antivirus, firewall, crittografia per contrastare efficacemente le minacce e le vulnerabilità. RA2. Assumere la responsabilità della sicurezza degli endpoint, identificando, riducendo i rischi, conducendo valutazioni e mantenendo la sicurezza. RA3. Rispondere rapidamente agli incidenti di sicurezza, indagare, condurre indagini forensi, implementare le misure correttive e prevenire le recidive.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 9: Gestione e risposta agli incidenti

Introduzione

La gestione e la risposta agli incidenti sono essenziali per mitigare un'ampia gamma di interruzioni di servizio e minacce. Lo scopo è identificare, analizzare e rispondere in modo efficiente agli incidenti che possono interrompere le operazioni o danneggiare i beni, la reputazione e gli stakeholder/clienti di un'organizzazione. Questi eventi accidentali comprendono attacchi informatici, violazioni di dati, disastri naturali, incidenti ed emergenze sanitarie. L'obiettivo principale è quello di ridurre al minimo l'impatto, ripristinare le operazioni e prevenire incidenti futuri, seguendo una procedura strutturata. Una gestione efficace degli incidenti richiede anche una comunicazione chiara e una collaborazione tra i team e le parti interessate. Una solida strategia consente alle organizzazioni di affrontare in modo proattivo i rischi, migliorare la resilienza, ridurre i tempi di inattività, proteggere i dati, rispettare le normative e salvaguardare la propria reputazione.

Obiettivo

Imparare a rispondere efficacemente per ridurre al minimo l'impatto di un incidente, tra cui la pronta individuazione, la mobilitazione delle risorse, la risposta coordinata e il rapido ripristino delle normali operazioni per la stabilità e la sicurezza generali.

LEARNING OUTCOMES

Conoscenze	K1. Prepararsi al rilevamento e alla segnalazione degli incidenti, la valutazione e l'analisi degli incidenti. K2. Pianificare e preparare la risposta agli incidenti, al contenimento e alla mitigazione degli incidenti. K3. Organizzare la comunicazione e il coordinamento dell'incidente, il recupero dall'incidente e le lezioni apprese.	Competenze	S1. Analizzare gli incidenti, identificare le cause e selezionare le strategie di risposta appropriate utilizzando una forte abilità di problem solving. S2. Comunicare efficacemente per la gestione e la risposta agli incidenti. S3. Applicare le conoscenze tecniche al rilevamento degli incidenti per una gestione e una risposta efficaci.	Responsabilità e autonomia	RA 1. Prepararsi a identificare e gestire tempestivamente gli incidenti che si verificano all'interno di un'organizzazione RA2. Assumersi la responsabilità del coordinamento e dell'esecuzione della risposta agli incidenti. RA3. Occuparsi della documentazione e della segnalazione degli incidenti

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

Unità 10: Business Continuity e Disaster Recovery

Introduzione

La Business Continuity e il Disaster Recovery (BCDR) sono parte integrante della strategia di gestione del rischio di un'organizzazione, in quanto garantiscono la continuità delle operazioni aziendali critiche e il recupero di sistemi e dati in caso di interruzione. La Continuità Operativa (Business Continuity) comporta una pianificazione proattiva, l'identificazione dei processi vitali, la valutazione dei rischi e lo sviluppo di strategie per mantenere le operazioni aziendali durante e dopo un'interruzione. Il Disaster Recovery si concentra sugli aspetti tecnici, coinvolgendo piani di backup e ripristino, sistemi IT resilienti e procedure per ripristinare rapidamente le normali operazioni. Entrambi gli elementi del BCDR richiedono una comprensione approfondita delle risorse, delle dipendenze e dei rischi di un'organizzazione. Sono fondamentali la collaborazione e il coordinamento tra i vari reparti, la chiarezza dei ruoli, la comunicazione, la formazione e i test. Piani BCDR efficaci riducono al minimo l'impatto delle interruzioni, mantengono la fiducia e assicurano la resilienza operativa a lungo termine.

Obiettivo

Imparare a proteggere le operazioni aziendali critiche, ridurre al minimo l'impatto delle interruzioni, identificare i rischi, sviluppare e testare piani per migliorare la resilienza dell'organizzazione e garantire la redditività a lungo termine.

LEARNING OUTCOMES

Conoscenze	K1. Definire la valutazione dei rischi e l'analisi dell'impatto sulle attività, la pianificazione della Business Continuity. K2. Identificare gli elementi IT chiave della pianificazione del Disaster Recovery e della gestione delle crisi. K3. Conoscere le strategie di backup e ripristino rilevanti per la continuità delle operazioni aziendali.	Competenze	S1. Condurre valutazioni e analisi dei rischi per identificare potenziali minacce e vulnerabilità alle operazioni aziendali critiche. S2. Creare piani completi di Business Continuity e di Disaster Recovery. S3. Elencare le procedure e le risorse necessarie per garantire la continuità delle operazioni critiche e il recupero tempestivo di sistemi e dati.	Responsabilità e autonomia	RA 1. Identificare e valutare i rischi potenziali e le vulnerabilità delle operazioni aziendali critiche e dei sistemi IT. RA2. Predisporre l'implementazione i piani completi di Business Continuity e Disaster Recovery. RA3. Monitorare e testare regolarmente i piani di Business Continuity e di Disaster Recovery per garantirne l'efficacia.

Durata

Ore di teoria	Ore di pratica	Ore di autoapprendimento	Ore di valutazione	TOTALE
0,5	2	9	0,5	12

2. OSSERVAZIONI FINALI

Nell'ambito del progetto Erasmus+ SecureFuture è stato redatto il Curriculum Europeo sulla Sicurezza Informatica con i contributi forniti dai partner a seguito dei contributi forniti da 66 professionisti del settore della Sicurezza Informatica nei loro Paesi.

Prende in considerazione le seguenti caratteristiche:

- una ripartizione modulare dei contenuti formativi in dieci aree definite come unità di competenze con relativi contenuti;
- un insieme di conoscenze, abilità, responsabilità e autonomia raccolte in una tabella per ciascuna delle dieci unità formative;
- l'assegnazione di 6 punti ECVET alle 10 unità corrispondenti a 120 ore di formazione.

Questo curriculum servirà come base per lo sviluppo dei Contenuti Formativi sulla Sicurezza Informatica Europea, come definito nel WP4 - Contenuti Formativi di SecureFuture.

Insieme, il Framework Europeo delle Qualifiche, il Curriculum Formativo e i Contenuti Formativi rappresentano una proposta innovativa con un alto potenziale per soddisfare le esigenze dei Paesi europei in materia di formazione sulla Sicurezza Informatica per i discenti della Formazione Professionale e per i dipendenti delle PMI - i principali gruppi target del progetto – e preparare professionisti della Sicurezza Informatica ben formati per difendere le PMI europee dalle minacce informatiche.