CPF-101 Piano di Formazione

Progettazione del Corso di Fondamenti del Framework
40 Ore — 80 Slide

Sviluppo Formazione CPF3
Giuseppe Canale, CISSP
g.canale@cpf3.org

Gennaio 2025

Abstract

Questo piano di formazione definisce la progettazione didattica per CPF-101: Fondamenti del Framework, il corso fondazionale di 40 ore richiesto per tutte le certificazioni professionali CPF. Il documento fornisce schemi a livello di modulo che consentono la generazione sistematica di slide, lo sviluppo di esercizi e la creazione di valutazioni. Ogni modulo include obiettivi di apprendimento, struttura dei contenuti, metodi di insegnamento, ripartizione delle slide, materiali richiesti e elementi di valutazione. Questo piano serve come documento di riferimento per creare presentazioni guidate da istruttore, materiali di apprendimento autonomo e elementi per l'esame di certificazione.

Contents

1 Panoramica del Corso

1.1 Identificazione del Corso

Codice: CPF-101 — **Titolo:** Fondamenti del Framework — **Durata:** 40 ore (5 giorni intensivi o 10 mezze giornate) — **Slide:** 80 totali — **Formato:** Guidato da istruttore o autonomo

1.2 Target Audience

Professionisti della cybersecurity, professionisti della sicurezza delle informazioni, auditor della sicurezza e professionisti della gestione del rischio che perseguono la certificazione CPF Assessor, Practitioner o Auditor. Prerequisiti includono laurea triennale (o equivalente) e 2+ anni di esperienza in cybersecurity o psicologia.

1.3 Obiettivi di Apprendimento

Al completamento, i partecipanti saranno in grado di: (1) Spiegare i meccanismi psicologici pre-cognitivi alla base dell'82-85% degli incidenti di sicurezza, (2) Identificare i fondamenti teorici della psicoanalisi e della psicologia cognitiva, (3) Descrivere tutti i 10 domini CPF e 100 indicatori, (4) Articolare i requisiti di protezione della privacy, (5) Applicare la metodologia di punteggio ternario a scenari, (6) Mappare CPF a ISO 27001 e NIST CSF 2.0.

1.4 Struttura del Corso

Parte I - Fondamenti (12h, Moduli 1-3): Introduzione alla Psicologia della Cybersecurity (4h), Fondamenti Psicoanalitici (4h), Fondamenti di Psicologia Cognitiva (4h).

Parte II - Domini CPF (20h, Moduli 4-13): Dieci moduli di 2 ore che coprono Autorità [1.x], Temporale [2.x], Influenza Sociale [3.x], Affettivo [4.x], Sovraccarico Cognitivo [5.x], Dinamiche di Gruppo [6.x], Risposta allo Stress [7.x], Processi Inconsci [8.x], Bias Specifici dell'IA [9.x], Stati Critici Convergenti [10.x].

Parte III - Applicazione (8h, Moduli 14-15): Privacy ed Etica (4h), Integrazione e Applicazione (4h).

1.5 Metodo di Valutazione

Formativa: Quiz di modulo (3-5 domande ciascuno), 15 esercizi pratici, 5 case study. Sommativa: Esame scritto di 100 domande (60 a scelta multipla, 30 basate su scenari, 10 di analisi caso), 3 ore, punteggio di superamento 70%. La certificazione richiede il 90% di presenza e un accordo etico firmato.

1.6 Materiali Forniti

Workbook Partecipante CPF-101 (80 pagine), Scheda di Riferimento Rapido Tassonomia CPF, Esempio Field Kit (Indicatore 1.1 completo), Pacchetto Case Study (5 scenari), Template di Valutazione, Documenti del framework CPF (tassonomia, requisiti CPF-27001, schema di certificazione).

2 Strutture dei Moduli

2.1 Modulo 1: Introduzione alla Psicologia della Cybersecurity

2.1.1 Panoramica

Durata: 4 ore — **Slide:** 6

Obiettivi di Apprendimento: Articolare perché la consapevolezza tradizionale sulla sicurezza non riesce a prevenire l'82-85% degli incidenti; spiegare le evidenze neuroscientifiche per il processo decisionale pre-cognitivo; descrivere l'architettura CPF (10 domini, 100 indicatori, punteggio ternario); mappare l'integrazione CPF con ISO 27001 e NIST CSF; analizzare una violazione maggiore attraverso la lente CPF.

Concetti Chiave: Elaborazione pre-cognitiva, Sistema 1 vs Sistema 2, divario del fattore umano, architettura del framework, strategia di integrazione.

2.1.2 Schema dei Contenuti

1. Divario del Fattore Umano (45 min): Spesa globale vs violazioni in aumento, statistiche Verizon DBIR, fallimento del modello dell'attore razionale, perché la formazione sulla consapevolezza fornisce falsa sicurezza, esempi del mondo reale (Target, Anthem, SolarWinds).

2. Elaborazione Pre-Cognitiva (60 min): Evidenze neuroscientifiche (Libet 1983, Soon 2008), attivazione amigdala 300-500ms prima della consapevolezza cosciente, studi decisionali fMRI, marcatori somatici Damasio, hardwiring evolutivo crea vulnerabilità, implicazioni per la formazione sulla sicurezza, dimostrazione video.

3. Architettura CPF (60 min): Panoramica struttura 10x10, breve introduzione a tutti i 10 domini, punteggio ternario (Verde/Giallo/Rosso), design privacy-first (aggregazione, privacy differenziale, ritardi temporali), panoramica metodologia di valutazione.

4. Integrazione con Framework (45 min): Mappatura ISO 27001:2022 (Clausola 7.2 Competenza, 7.3 Consapevolezza, potenziamento Allegato A), integrazione NIST CSF 2.0 (Identifica/Proteggi/Rileva/Rispondi/Recupera), CPF come livello di intelligence psicologica, relazione complementare.

5. Case Study: Violazione Target (30 min): Narrativa tecnica, analisi psicologica CPF (vulnerabilità autorità, fatica da allerta, dinamiche di gruppo, pressione temporale), come la valutazione potrebbe prevedere la convergenza, interventi preventivi, discussione.

2.1.3 Metodi di Insegnamento

Lezione: Statistiche/grafici per il divario del fattore umano, video neuroscienze con immagini fMRI, diagramma framework animato, tabelle di confronto ISO/NIST.

Esercizi: (1) Analisi Fallimento Consapevolezza - condividere esempi di formazione falliti (15 min), (2) Esperimento Decisionale Pre-Cognitivo - dimostrazione live autorità/urgenza (10 min), (3) Navigazione Framework - esercitazione veloce con Scheda di Riferimento Rapido (20 min).

Discussione: "Pensa a un incidente - la formazione sulla consapevolezza avrebbe potuto prevenirlo?", "Cosa significa una decisione pre-conscia di 300-500ms per il tuo programma?", "Spiega CPF al CISO in 60 secondi."

Case Study: Violazione Target presentata cronologicamente, gruppi identificano vulnerabilità, collegano ai domini CPF, sintetizzano la previsione dello stato convergente.

2.1.4 Ripartizione Slide

Slide 1.1: "La Crisi del Fattore Umano" - Grafico trend di spesa vs violazioni, statistiche Verizon, visuale silhouette umana vs fortezza.

Slide 1.2: "Processo Decisionale Pre-Cognitivo" - Diagramma timeline (0ms→300ms→500ms→800ms), risultati Libet/Soon, diagramma cervello (amigdala vs corteccia prefrontale).

Slide 1.3: "Architettura Framework CPF" - Griglia 10x10 con nomi/icone domini, 100 indicatori, callout punteggio ternario, design privacy-first.

Slide 1.4: "Sistema di Punteggio Ternario" - Confronto a tre colonne (Verde/Giallo/Rosso), esempio indicatore 1.1, formule categoria/punteggio CPF.

Slide 1.5: "Integrazione con ISO 27001 e NIST CSF" - Diagramma diviso che mostra punti di potenziamento, messaggio "CPF complementa non sostituisce".

Slide 1.6: "Violazione Target Attraverso la Lente CPF" - Timeline, storia tecnica, sovrapposizione analisi CPF (4 domini identificati), prompt esercizio.

2.1.5 Materiali Necessari

Workbook Modulo 1 (pagine 1-15), Scheda di Riferimento Rapido Tassonomia, video neuroscienze (5 min), handout case study Target (2 pagine), Fogli di Lavoro Esercizi 1.1 e 1.3, lavagna/strumento collaborazione digitale.

2.1.6 Elementi di Valutazione

Quiz (5 domande): Q1: Verizon DBIR

Rubrica Esercizio (Navigazione Framework): Velocità 5 indicatori ¡2 min (2 pts), accuratezza dominio/numero (3 pts), spiegazione comprensione (3 pts), applicazione scenario (2 pts). Totale 10 pts (7+ superamento).

2.2 Modulo 2: Fondamenti Psicoanalitici

2.2.1 Panoramica

Durata: 4 ore — **Slide:** 7

Obiettivi di Apprendimento: Spiegare le assunzioni di base di Bion (baD/baF/baP) in contesti di sicurezza; applicare le relazioni oggettuali di Klein (scissione, proiezione) ai punti ciechi organizzativi; identificare l'ombra e l'inconscio collettivo di Jung nella percezione della minaccia; descrivere la rilevanza dello spazio transizionale di Winnicott per la sicurezza digitale; analizzare le posture di sicurezza attraverso la lente psicoanalitica.

Concetti Chiave: Assunzioni di base, relazioni oggettuali, scissione, proiezione, ombra, inconscio collettivo, spazio transizionale, sistemi di difesa sociale.

2.2.2 Schema dei Contenuti

1. Assunzioni di Base di Bion (75 min): Bion "Esperienze nei Gruppi" (1961), tre posture difensive sotto ansia. baD (Dipendenza): Ricerca leader/tecnologia onnipotente, pensiero magico strumenti sicurezza, indicatore [6.6]. baF (Attacco-Fuga): Focus nemico esterno, mentalità fortezza, cecità minaccia interna, indicatore [6.7]. baP (Accoppiamento): Speranza

salvezza futura, shopping continuo di strumenti, indicatore [6.8]. Riconoscimento nei team di sicurezza, creazione vulnerabilità.

2. Relazioni Oggettuali Kleiniane (60 min): Contributi Klein, Meccanismo Scissione (divisione tutto buono/tutto cattivo, insider idealizzati vs attaccanti demonizzati, invisibilità minaccia interna, [6.9] scissione organizzativa), Meccanismo Proiezione (vulnerabilità organizzative attribuite esternamente, apprendimento bloccato, [8.1] proiezione ombra), Sistemi di difesa sociale Menzies Lyth (conformità ritualistica checklist, [6.10] difese collettive), identificazione pattern.

3. Psicologia Junghiana (60 min): Concetto Ombra (aspetti disconosciuti proiettati, hacker black hat incarnano aggressività organizzativa, identificazione attaccante team sicurezza, red team come espressione ombra, indicatori [8.1][8.2]), Archetipi (CISO Eroe, Trickster hacker, Consulente Saggio, Minaccia Interna Ombra, [8.8] attivazione archetipica), Inconscio collettivo (dinieghi condivisi del settore, mito "troppo piccolo per essere preso di mira", pattern [8.9]), lavoro sull'ombra per riduzione vulnerabilità.

4. Spazio Transizionale Winnicott (30 min): Concetto oggetti/spazi transizionali, ambienti digitali come transizionali (né reali né immaginari, ridotta verifica della realtà, fantasie online onnipotenti, confusione identità digitale, abbassamento guardia social media, [8.10] logica del sogno, [8.7] equazione simbolica), meccanismi di sfruttamento, implicazioni di design.

5. Esercizio: Analisi Caso Psicoanalitico (15 min): Caso ransomware sanitario, gruppi identificano assunzione di base, evidenze scissione, proiezioni, elementi ombra. Presentazioni, facilitatore mappa su indicatori CPF [6.x] e [8.x].

2.2.3 Metodi di Insegnamento

Lezione: Diagrammi organizzativi Bion, visuali scissione/proiezione Klein, immagini archetipiche Jung, confronto spazio fisico vs digitale Winnicott.

Esercizi: (1) Identificazione Assunzione Base - 3 vignette, identificare baD/baF/baP (20 min), (2) Scissione nella Cultura della Sicurezza - elencare entità fidate/minacciose, discutere punti ciechi (15 min), (3) Riconoscimento Ombra - riflessione anonima "cosa l'org rifiuta di riconoscere" (15 min).

Discussione: "Visto pensiero proiettile d'argento?", "Come descrive l'org gli attaccanti?", "Quali rituali di sicurezza forniscono falsa comfort?"

Media: Clip video dinamiche di gruppo (5 min), animazione ombra Jung, diagramma scissione.

2.2.4 Ripartizione Slide

Slide 2.1: "Panoramica Assunzioni di Base di Bion" - Tre posture con icone (corona, spada/scudo, speranza), citazione Bion, inconscio non deliberato.

Slide 2.2: "Assunzioni di Base nella Sicurezza" - Tabella a tre colonne (baD/baF/baP con comportamenti, esempi, vulnerabilità, indicatori CPF).

Slide 2.3: "Scissione e Proiezione Kleiniana" - Diagramma scissione buono/cattivo, meccanismo scissione (insider fidati, minacce interne invisibili), meccanismo proiezione (colpa esterna, nessun apprendimento), citazione Klein, indicatori [6.9][8.1].

Slide 2.4: "L'Ombra di Jung nella Sicurezza" - Silhouette luce/buio, concetto ombra, manifestazioni sicurezza (black hat, red team, identificazione), ombra collettiva (dinieghi del settore), citazione Jung, indicatori [8.1][8.2][8.9].

Slide 2.5: "Archetipi nella Sicurezza" - Quattro immagini archetipiche (CISO Eroe, Trickster hacker, Consulente Saggio, Minaccia Interna Ombra), descrizioni con vulnerabilità, nota pattern inconsci, indicatore [8.8].

Slide 2.6: "Spazio Transizionale di Winnicott" - Tabella confronto fisico vs digitale, implicazioni sicurezza (onnipotenza, confusione identità, logica del sogno, equazioni simboliche), citazione Winnicott, indicatori [8.10][8.7], esempio social media.

Slide 2.7: "Esercizio Analisi Caso Psicoanalitico" - Breve caso ransomware sanitario, framework analisi (assunzione base, scissione, proiezione, ombra, difese), istruzioni compito gruppo, risultati attesi, domanda debrief.

2.2.5 Materiali Necessari

Workbook Modulo 2 (pagine 16-30), Esercizio 2.1 foglio lavoro tre vignette, Esercizio 2.2 template scissione, Esercizio 2.3 carte ombra anonime, handout caso sanitario (2 pagine), immagini archetipiche, video dinamiche gruppo (5 min), lavagna.

2.2.6 Elementi di Valutazione

Quiz (5 domande): Q1: Caratteristica baD → ricerca protettore onnipotente corretto. Q2: Definizione scissione → divisione inconscia tutto buono/cattivo corretto. Q3: Indicatore proiezione ombra → [8.1] corretto. Q4: Rilevanza spazio transizionale → né reale né immaginario, ridotta verifica della realtà corretto. Q5: Assunzione base shopping continuo strumenti → baP corretto.

Rubrica Esercizio (Scissione): Elencare 3+ entità fidate e minacciose (2 pts), riconoscere idealizzazione/demonizzazione (3 pts), identificare 2+ punti ciechi (3 pts), suggerire come affrontare la scissione (2 pts). Totale 10 pts (7+ superamento).

2.3 Modulo 3: Fondamenti di Psicologia Cognitiva

2.3.1 Panoramica

Durata: 4 ore — **Slide:** 7

Obiettivi di Apprendimento: Spiegare le implicazioni della teoria del doppio processo di Kahneman (Sistema 1/2) per la sicurezza; applicare i sei principi di influenza di Cialdini al social engineering; analizzare l'impatto del carico cognitivo di Miller sui compiti di sicurezza; identificare euristiche/bias che abilitano lo sfruttamento; valutare le strutture organizzative attraverso la lente cognitiva.

Concetti Chiave: Sistema 1/2, euristiche, bias cognitivi, principi di influenza (reciprocità, impegno, prova sociale, autorità, simpatia, scarsità), carico cognitivo, memoria di lavoro.

2.3.2 Schema dei Contenuti

1. Doppio Processo Kahneman (75 min): "Pensieri Lenti e Veloci" (2011), Sistema 1 (veloce, automatico, inconscio, riconoscimento pattern, emotivo, euristiche, sempre attivo), Sistema 2 (lento, deliberato, conscio, faticoso, analitico, capacità limitata, si esaurisce). Problema decisioni sicurezza (la maggior parte decisioni ¡1 sec Sistema 1, verifica richiede 10-30 sec Sistema 2, pressione temporale = predominanza Sistema 1, attaccanti sfruttano Sistema 1). Euristiche chiave (disponibilità, rappresentatività, ancoraggio, conferma, bias ottimismo). Indicatori CPF sfruttano vulnerabilità Sistema 1.

2. Sei Principi Cialdini (75 min): "Influenza" (2007), ogni principio = vettore di attacco. (1) Reciprocità: Obbligo di ricambiare favori, attacchi quid pro quo, sfruttamento [3.1]. (2) Impegno/Coerenza: Allinearsi a impegni precedenti, escalation graduale piede nella porta, trappole [3.2]. (3) Prova Sociale: Guardare agli altri, manipolazione "tutti hanno cliccato", manipolazione [3.3], conformità [3.8]. (4) Autorità: Deferenza all'autorità, frode CEO, IT falso, Dominio [1.x] intero. (5) Simpatia: Accondiscendere a persone simpatiche, costruzione rapporto, override fiducia [3.4]. (6) Scarsità: Valore cose limitate, attacchi urgenza, decisioni scarsità [3.5]. Riconoscimento principi combinati in attacchi (BEC = Autorità + Scarsità + Impegno).

3. Carico Cognitivo Miller (45 min): "Numero Magico 7±2" (1956), limiti memoria di lavoro (7±2 item ora 4±1, durata 15-30 sec, facilmente sopraffatta). Carico compito sicurezza (complessità intrinseca, complessità estranea non necessaria, apprendimento germinale, totale = somma dei tre, sovraccarico = errori/euristiche/Sistema 1). Manifestazioni sovraccarico (fatica allerta, fatica decisionale, degrado multitasking, errori complessità). Dominio [5.x] tutti i 10 indicatori relativi a limiti capacità. Principio di design: ridurre carico estraneo.

4. Decisione sotto Incertezza (30 min): Teoria del Prospetto (Kahneman/Tversky 1979), Aversione alla perdita (perdite più grandi di guadagni, efficacia ransomware, [4.1] paralisi paura, [2.3] rischio scadenza), Effetti di inquadramento (presentazione cambia decisioni, inquadramento protezione vs restrizione), Fallacità costo irrecuperabile (continuare basandosi su investimento passato, persistenza strumento inefficace, [4.4] attaccamento legacy).

5. Esercizio: Analisi Sfruttamento Cognitivo (15 min): Tre email di social engineering, compiti (identificare principi Cialdini, target Sistema 1 o 2, manipolazione carico cognitivo, contromisure basate su psicologia cognitiva), discussione gruppo come ciascuna inganna Sistema 1, facilitatore collega a indicatori CPF.

2.3.3 Metodi di Insegnamento

Lezione: Doppio processo con illusioni ottiche e decisioni rapide, Cialdini con esempi pubblicitari poi sicurezza, Carico cognitivo con test span di cifre, Decision-making con esercizio di inquadramento.

Esercizi: (1) Test Velocità Sistema 1 vs 2 - 20 email 3 sec ciascuna poi tempo illimitato, confrontare accuratezza (15 min), (2) Mappatura Cialdini - 6 scenari mappare principi, discutere combinazioni (20 min), (3) Simulazione Carico Cognitivo - compito sicurezza con distrazioni, sperimentare sovraccarico (15 min).

Discussione: "Cliccato qualcosa che non avresti dovuto - Sistema 1 o 2?", "Principio Cialdini più pericoloso?", "Quante decisioni di sicurezza giornaliere? Costo cognitivo?"

Media: Estratto TED Kahneman (5 min), dimostrazioni Candid Camera Cialdini (10 min), animazione carico cognitivo (3 min).

2.3.4 Ripartizione Slide

Slide 3.1: "Pensieri Lenti e Veloci" - Schermo diviso tabella Sistema 1 vs 2 (velocità, modalità, energia, metodo, ruolo sicurezza, vulnerabilità/limitazione), intuizione chiave la maggior parte decisioni in tempo Sistema 1, citazione Kahneman, diagramma cervello.

Slide 3.2: "Euristiche e Bias" - Cinque euristiche con definizioni, esempi sicurezza, vulnerabilità (disponibilità, rappresentatività, ancoraggio, conferma, ottimismo).

Slide 3.3: "Panoramica Sei Principi di Cialdini" - Griglia sei box con icone, nomi principi, descrizioni one-line, messaggio "Ciascuno = vettore di attacco".

Slide 3.4: "Sei Principi nel Social Engineering" - Tabella dettagliata (principio, meccanismo, esempio sicurezza, indicatore CPF) per tutti e sei, nota su principi combinati, esempio BEC.

Slide 3.5: "Teoria del Carico Cognitivo" - Visuale capacità memoria di lavoro (7±2 ora 4±1), diagramma tre tipi di carico (intrinseco, estraneo, germinale), manifestazioni sovraccarico sicurezza (fatica allerta, fatica decisionale, multitasking, complessità), citazione Miller, nota Dominio [5.x].

Slide 3.6: "Decision-Making sotto Incertezza" - Spiegazione avversione alla perdita con esempio ransomware, dimostrazione effetti inquadramento, fallacia costo irrecuperabile con persistenza strumento, indicatori [4.1][2.3][4.4].

Slide 3.7: "Esercizio Sfruttamento Cognitivo" - Tre esempi email visualizzati, framework analisi (principi Cialdini, target Sistema, manipolazione carico, contromisure), istruzioni compito gruppo, prompt discussione.

2.3.5 Materiali Necessari

Workbook Modulo 3 (pagine 31-45), Esercizio 3.1 set test 20 email, Esercizio 3.2 carte sei scenari, Esercizio 3.3 setup simulazione distrazione, tre email di phishing per analisi, video Kahneman (5 min), clip Cialdini (10 min), animazione carico cognitivo (3 min), lavagna.

2.3.6 Elementi di Valutazione

Quiz (5 domande): Q1: Caratteristiche Sistema 1 → veloce, automatico, inconscio corretto. Q2: Principio Cialdini reciprocità → obbligo di ricambiare favori corretto. Q3: Capacità memoria di lavoro Miller → 7±2 (o 4±1) corretto. Q4: Quale Dominio affronta sovraccarico cognitivo → [5.x] corretto. Q5: Aversione alla perdita spiega → efficacia ransomware corretto.

Rubrica Esercizio (Analisi Email): Identificare 2+ principi Cialdini (3 pts), determinare correttamente target Sistema 1/2 (2 pts), spiegare manipolazione carico cognitivo (3 pts), suggerire contromisura efficace (2 pts). Totale 10 pts (7+ superamento).

2.4 Modulo 4: Dominio [1.x] Vulnerabilità Basate su Autorità

2.4.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Comprendere la ricerca sull'obbedienza di Milgram e le implicazioni per la cybersecurity; identificare i 10 indicatori di autorità; applicare il punteggio ternario a scenari di conformità all'autorità; raccomandare le prime 3 strategie di rimedio.

Concetti Chiave: Deferenza all'autorità, diffusione di responsabilità, frode CEO, BEC, protocolli di verifica.

2.4.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Esperimenti Milgram 65% obbedienza, dirottamento amigdala neuroscienze, meccanismo di sopravvivenza deferenza all'autorità evolutivo, Sistema 1 vs 2 in contesti di autorità.

2. Dieci Indicatori Autorità (30 min): Tabella panoramica 1.1-1.10, Approfondimento 1.1 (conformità incondizionata, osservabili, domande di valutazione, punteggio G/V/R), Appro-

fondimento 1.3 (suscettibilità impersonificazione, lacune autenticazione email, fallimenti verifica, multi-canale), pattern tra indicatori rimanenti.

3. Vettori di Attacco e Incidenti (30 min): Perdite BEC $43B FBI, caso violazione Target via autorità fornitore, spear phishing con pretese di autorità, social engineering supporto IT, punti di fallimento tecnico (bypass MFA, escalation privilegi).

4. Valutazione e Soluzioni (30 min): Indicatori osservabili nelle organizzazioni, albero decisionale punteggio ternario, Prime 3 soluzioni (protocollo verifica duale, formazione sfida autorità, programma test simulazione), priorità di implementazione (alto/medio/lungo termine).

5. Esercizio (10 min): Scenario caso email bonifico CFO, studenti valutano punteggio/ragionamento/soluzion discussione gruppo e feedback.

2.4.3 Metodi di Insegnamento

Lezione: Milgram con filmati storici, diagrammi neuroscienze, visuali flusso attacco.

Esercizio: Scenario frode CFO, valutazione individuale poi confronto gruppo.

Discussione: "Visto bypass autorità nella tua org?", "Come verificare richieste executive insolite?"

2.4.4 Ripartizione Slide

Slide 4.1: "Perché Obbediamo: Vulnerabilità Autorità" - Visuale Milgram, diagramma neuroscienze, contesto evolutivo, statistica 65%, attivazione 300-500ms, transizione a frode CEO.

Slide 4.2: "10 Indicatori Autorità" - Tabella 1.1-1.10 con brevi descrizioni, evidenzia 1.1 e 1.3 per approfondimento, icone indicatori.

Slide 4.3: "Vettori di Attacco in Azione" - Statistica BEC $43B, timeline violazione Target, esempi spear phishing, diagramma flusso attacco, frammento email reale (redatto).

Slide 4.4: "Valutazione e Soluzioni" - Checklist osservabili, albero decisionale punteggio G/V/R, prime 3 soluzioni con icone/timeline, prompt esercizio scenario CFO.

2.4.5 Materiali Necessari

Field Kit 1.1 e 1.3 (riferimento), Sezione Tassonomia [1.x], Case study Target, Handout esercizio CFO.

2.4.6 Elementi di Valutazione

Quiz: Q1:

Rubrica Esercizio: ID Vulnerabilità (2 pts), punteggio ternario con giustificazione (3 pts), soluzione rilevante (3 pts), comprensione priorità implementazione (2 pts). Totale 10 pts (7+ superamento).

2.5 Modulo 5: Dominio [2.x] Vulnerabilità Temporali

2.5.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Spiegare gli effetti della pressione temporale sulle decisioni di sicurezza; identificare i 10 indicatori temporali; riconoscere i pattern di attacco guidati da scadenze; applicare la valutazione della vulnerabilità temporale.

Concetti Chiave: Sfruttamento urgenza, degrado pressione temporale, attacchi scadenza, bias presente, sconto iperbolico.

2.5.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Degrado cognitivo pressione temporale (Kahneman/Tversky), bias presente (ricompense immediate sovrappesate), sconto iperbolico (minacce future scontate), spegnimento Sistema 2 sotto pressione temporale.

2. Dieci Indicatori Temporali (30 min): Tabella panoramica 2.1-2.10, Approfondimento 2.1 (bypass indotto urgenza, attacchi "agisci ora", punteggio), Approfondimento 2.3 (accettazione rischio guidata scadenza, pressione fine trimestre, punteggio), pattern temporali.

3. Vettori di Attacco e Incidenti (30 min): Attacchi scadenza (stagione fiscale, fine trimestre), sfruttamento ora del giorno (cambi turno, ore tarde), vulnerabilità weekend/festività, esempi caso social engineering temporale.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità temporale, criteri di punteggio, Prime 3 soluzioni (periodi di riflessione per richieste urgenti, protocolli sicurezza cambi turno, rilevamento anomalie temporali), implementazione.

5. Esercizio (10 min): Scenario pagamento fattura urgente con pressione temporale, valutare vulnerabilità temporali, raccomandare controlli.

2.5.3 Metodi di Insegnamento

Lezione: Esperimenti pressione temporale, dimostrazioni bias presente, timeline attacchi temporali.

Esercizio: Scenario pagamento urgente sotto pressione temporale simulata.

Discussione: "Quando sono peggiori le decisioni di sicurezza?", "Compromessi sicurezza fine trimestre?"

2.5.4 Ripartizione Slide

Slide 5.1: "Pressione Temporale e Sicurezza" - Degrado cognitivo sotto vincoli temporali, spiegazione bias presente, sconto iperbolico, spegnimento Sistema 2.

Slide 5.2: "10 Indicatori Temporali" - Tabella 2.1-2.10, evidenzia 2.1 e 2.3, pattern vulnerabilità temporale.

Slide 5.3: "Vettori di Attacco Temporali" - Attacchi scadenza (fiscale, fine trimestre), finestre ora del giorno, sfruttamento weekend/festività, esempi caso con timeline.

Slide 5.4: "Valutazione e Soluzioni" - Osservabili temporali, albero decisionale punteggio, prime 3 soluzioni (periodi riflessione, protocolli turno, rilevamento anomalie), prompt esercizio.

2.5.5 Materiali Necessari

Field Kit 2.1 e 2.3, Tassonomia [2.x], Handout esercizio pagamento urgente.

2.5.6 Elementi di Valutazione

Quiz: Q1: Definizione bias presente → ricompense immediate sovrappesate corretto. Q2: Indicatore per bypass urgenza → 2.1 corretto. Q3: Amplificatore vulnerabilità temporale → pressione temporale, scadenze corretto.

Rubrica Esercizio: ID Vulnerabilità temporale (3 pts), analisi pressione urgenza (2 pts), punteggio con giustificazione (3 pts), raccomandazione controlli temporali (2 pts). Totale 10 pts (7+ superamento).

2.6 Modulo 6: Dominio [3.x] Vulnerabilità di Influenza Sociale

2.6.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Applicare i principi di Cialdini a contesti di sicurezza; identificare i 10 indicatori di influenza sociale; analizzare i pattern di attacco di social engineering; progettare contromisure all'influenza sociale.

Concetti Chiave: Reciprocità, impegno/coerenza, prova sociale, simpatia, scarsità, principio unità, pressione dei pari, conformità.

2.6.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Revisione sei principi Cialdini (da Modulo 3), influenza sociale come meccanismo evolutivo, psicologia della conformità, effetti di combinazione negli attacchi.

2. Dieci Indicatori Sociali (30 min): Tabella panoramica 3.1-3.10, Approfondimento 3.1 (sfruttamento reciprocità, quid pro quo, punteggio), Approfondimento 3.3 (manipolazione prova sociale, attacchi "tutti hanno cliccato", punteggio), pattern influenza sociale tra indicatori.

3. Vettori di Attacco e Incidenti (30 min): Campagne social engineering (costruzione pretesto, stabilimento rapporto), attacchi pressione pari (trasmissioni IT false), sfruttamento conformità (tutti aggiornano password), principio unità (richieste false team), casi reali social engineering.

4. Valutazione e Soluzioni (30 min): Osservabili influenza sociale, criteri di punteggio, Prime 3 soluzioni (protocolli verifica prova sociale, sistemi validazione pari, formazione consapevolezza influenza), priorità di implementazione.

5. Esercizio (10 min): Email di social engineering che combina multiple principi Cialdini, identificare quali principi usati, valutare punteggio vulnerabilità, raccomandare difese.

2.6.3 Metodi di Insegnamento

Lezione: Dimostrazioni principi Cialdini, esempi video social engineering, analisi combinazione influenza.

Esercizio: Analisi email phishing multi-principio, identificazione gruppo delle tecniche.

Discussione: "Principio Cialdini più efficace nella tua esperienza?", "Come resistere alla prova sociale nella sicurezza?"

2.6.4 Ripartizione Slide

Slide 6.1: "Meccanismi di Influenza Sociale" - Revisione visiva sei principi Cialdini, base evolutiva, psicologia della conformità, effetti attacchi combinati.

Slide 6.2: "10 Indicatori Influenza Sociale" - Tabella 3.1-3.10, evidenzia 3.1 e 3.3, pattern vulnerabilità influenza sociale.

Slide 6.3: "Pattern di Attacco Social Engineering" - Esempi campagne (pretesto, rapporto, pressione), scenari sfruttamento conformità, richieste false principio unità, casi reali.

Slide 6.4: "Valutazione e Soluzioni" - Checklist osservabili sociali, albero decisionale punteggio, prime 3 soluzioni (protocolli verifica, validazione pari, formazione consapevolezza), prompt esercizio email multi-principio.

2.6.5 Materiali Necessari

Field Kit 3.1 e 3.3, Tassonomia [3.x], clip video social engineering (5 min), Handout esercizio multi-principio.

2.6.6 Elementi di Valutazione

Quiz: Q1: Definizione principio reciprocità → obbligo di ricambiare favori corretto. Q2: Indicatore prova sociale → 3.3 corretto. Q3: Combinazione più pericolosa → multiple risposte accettabili (Autorità + Scarsità, Prova Sociale + Simpatia).

Rubrica Esercizio: Identificare 3+ principi Cialdini (3 pts), spiegare meccanismo influenza (2 pts), punteggio vulnerabilità con giustificazione (3 pts), raccomandazioni difesa (2 pts). Totale 10 pts (7+ superamento).

2.7 Modulo 7: Dominio [4.x] Vulnerabilità Affettive

2.7.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Spiegare le decisioni di sicurezza guidate dall'emozione; identificare i 10 indicatori affettivi; riconoscere gli attacchi di manipolazione emotiva; applicare la valutazione della vulnerabilità affettiva.

Concetti Chiave: Sfruttamento paura, rischio indotto rabbia, trasferimento fiducia, attaccamento, nascondimento vergogna, contagio emotivo.

2.7.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Primato emozione su cognizione (LeDoux), euristica affettiva (Slovic), contagio emotivo (Hatfield), dirottamento amigdala in contesti sicurezza, stati emotivi alterano percezione rischio.

2. Dieci Indicatori Affettivi (30 min): Tabella panoramica 4.1-4.10, Approfondimento 4.1 (paralisi basata paura, FUD ransomware, punteggio), Approfondimento 4.5 (nascondimento sicurezza basato vergogna, mancata segnalazione incidente, punteggio), pattern affettivi.

3. Vettori di Attacco e Incidenti (30 min): Attacchi basati paura (ransomware, tattiche spavento), manipolazione rabbia (contenuto provocatorio), sfruttamento fiducia (supporto falso),

prevenzione vergogna segnalazione, contagio emotivo nelle violazioni, esempi caso.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità affettiva, criteri di punteggio, Prime 3 soluzioni (sicurezza psicologica per segnalazione, formazione regolazione emotiva, protocolli resistenza FUD), implementazione.

5. Esercizio (10 min): Scenario ransomware con manipolazione paura, valutare vulnerabilità emotive, progettare interventi sicurezza psicologica.

2.7.3 Metodi di Insegnamento

Lezione: Neuroscienze emozione, dimostrazioni euristica affettiva, esempi attacco emotivo.

Esercizio: Scenario paura ransomware, analisi individuale poi gruppo di manipolazione emotiva.

Discussione: "Decisioni sicurezza basate paura prese?", "Come creare sicurezza psicologica per segnalazione incidenti?"

2.7.4 Ripartizione Slide

Slide 7.1: "Emozione e Decisioni di Sicurezza" - Primato emozione (LeDoux), spiegazione euristica affettiva, diagramma dirottamento amigdala, alterazione percezione rischio emotiva.

Slide 7.2: "10 Indicatori Affettivi" - Tabella 4.1-4.10, evidenzia 4.1 e 4.5, pattern vulnerabilità emotiva.

Slide 7.3: "Attacchi di Manipolazione Emotiva" - Basati paura (FUD ransomware), manipolazione rabbia, sfruttamento fiducia, prevenzione segnalazione vergogna, effetti contagio emotivo, esempi caso.

Slide 7.4: "Valutazione e Soluzioni" - Osservabili affettivi, albero decisionale punteggio, prime 3 soluzioni (sicurezza psicologica, regolazione emotiva, resistenza FUD), prompt esercizio scenario ransomware.

2.7.5 Materiali Necessari

Field Kit 4.1 e 4.5, Tassonomia [4.x], Handout esercizio ransomware, video contagio emotivo (3 min).

2.7.6 Elementi di Valutazione

Quiz: Q1: Definizione euristica affettiva → decisioni basate su stato emotivo corretto. Q2: Indicatore paralisi paura → 4.1 corretto. Q3: Indicatore nascondimento basato vergogna → 4.5 corretto.

Rubrica Esercizio: Identificazione manipolazione paura (3 pts), valutazione vulnerabilità emotiva (2 pts), punteggio con giustificazione (3 pts), progettazione intervento sicurezza psicologica (2 pts). Totale 10 pts (7+ superamento).

2.8 Modulo 8: Dominio [5.x] Vulnerabilità da Sovraccarico Cognitivo

2.8.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Applicare la teoria del carico cognitivo di Miller alla sicurezza; identificare i 10 indicatori di sovraccarico; riconoscere gli attacchi di sfruttamento della capacità; progettare interventi di riduzione del carico cognitivo.

Concetti Chiave: Limiti memoria di lavoro, fatica allerta, fatica decisionale, degrado multitasking, tunneling cognitivo.

2.8.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Miller 7±2 memoria di lavoro (ora 4±1), tipi carico cognitivo (intrinseco, estraneo, germinale), conseguenze sovraccarico capacità, esaurimento Sistema 2, complessità compito sicurezza.

2. Dieci Indicatori Sovraccarico (30 min): Tabella panoramica 5.1-5.10, Approfondimento 5.1 (desensibilizzazione fatica allerta, sovraccarico SOC, punteggio), Approfondimento 5.2 (errori fatica decisionale, scelte sicurezza ripetute, punteggio), pattern sovraccarico.

3. Vettori di Attacco e Incidenti (30 min): Sfruttamento fatica allerta (rumore prima attacco), tempistica fatica decisionale (attacchi fine giornata), finestre vulnerabilità multitasking, errori indotti complessità, caso fatica allerta SOC Target.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità sovraccarico, criteri di punteggio, Prime 3 soluzioni (consolidamento e ottimizzazione allerta, semplificazione decisionale, budget carico cognitivo), implementazione.

5. Esercizio (10 min): Scenario analista SOC sovraccarico con 50+ allerta, valutare vulnerabilità cognitive, progettare strategia riduzione allerta.

2.8.3 Metodi di Insegnamento

Lezione: Dimostrazioni memoria di lavoro (span cifre), visualizzazione fatica allerta, esperimenti fatica decisionale.

Esercizio: Simulazione sovraccarico SOC, sperimentare limiti capacità cognitiva.

Discussione: "Quante decisioni di sicurezza giornaliere?", "Fatica allerta nel tuo SOC?"

2.8.4 Ripartizione Slide

Slide 8.1: "Carico Cognitivo e Limiti di Capacità" - Visuale Miller 7±2 (4±1), diagramma tre tipi carico, conseguenze sovraccarico, esaurimento Sistema 2, impatto complessità sicurezza.

Slide 8.2: "10 Indicatori Sovraccarico Cognitivo" - Tabella 5.1-5.10, evidenzia 5.1 e 5.2, pattern vulnerabilità sovraccarico.

Slide 8.3: "Attacchi di Sfruttamento Cognitivo" - Esempi sfruttamento fatica allerta, attacchi tempistica fatica decisionale, finestre multitasking, errori complessità, caso SOC Target con 40+ allerta ignorate.

Slide 8.4: "Valutazione e Soluzioni" - Osservabili sovraccarico (conteggi allerta, frequenza decisioni), albero decisionale punteggio, prime 3 soluzioni (consolidamento, semplificazione, budget

carico), prompt esercizio scenario SOC.

2.8.5 Materiali Necessari

Field Kit 5.1 e 5.2, Tassonomia [5.x], Esercizio sovraccarico SOC con scenario 50-allerta, materiali test span cifre.

2.8.6 Elementi di Valutazione

Quiz: Q1: Capacità memoria di lavoro Miller → 7±2 o 4±1 corretto. Q2: Indicatore fatica allerta → 5.1 corretto. Q3: Indicatore fatica decisionale → 5.2 corretto.

Rubrica Esercizio: Identificazione sovraccarico cognitivo (3 pts), analisi limiti capacità (2 pts), punteggio vulnerabilità con giustificazione (3 pts), strategia riduzione allerta (2 pts). Totale 10 pts (7+ superamento).

2.9 Modulo 9: Dominio [6.x] Vulnerabilità Dinamiche di Gruppo

2.9.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Applicare le assunzioni di base di Bion ai team di sicurezza; identificare i 10 indicatori di dinamica di gruppo; riconoscere i pattern di vulnerabilità collettiva; progettare interventi a livello di gruppo.

Concetti Chiave: Groupthink, spostamento al rischio, diffusione di responsabilità, ozio sociale, effetto spettatore, assunzioni di base (baD/baF/baP).

2.9.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Revisione assunzioni di base Bion (da Modulo 2), groupthink (Janis), fenomeno spostamento al rischio, diffusione di responsabilità (Latané), inconscio collettivo nei team sicurezza.

2. Dieci Indicatori Gruppo (30 min): Tabella panoramica 6.1-6.10, Approfondimento 6.1 (punti ciechi sicurezza groupthink, pressione consenso, punteggio), Approfondimento 6.3 (diffusione di responsabilità, "qualcun altro controllerà", punteggio), pattern gruppo.

3. Vettori di Attacco e Incidenti (30 min): Attacchi dirompimento organizzativo (sfruttando dinamiche gruppo), fallimenti decisionali collettivi, effetto spettatore nella risposta incidenti, social engineering a livello gruppo, NASA Challenger come parallelo groupthink.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità gruppo, criteri di punteggio, Prime 3 soluzioni (ruoli dissenso red team, assegnazione responsabilità, protocolli decisione gruppo), implementazione.

5. Esercizio (10 min): Scenario decisione comitato sicurezza con pressione groupthink, identificare vulnerabilità gruppo, progettare meccanismi dissenso.

2.9.3 Metodi di Insegnamento

Lezione: Esempi video groupthink, dimostrazioni spostamento al rischio, assunzioni di base nei team.

Esercizio: Decisione comitato con groupthink, sperimentare pressione consenso.

Discussione: "Groupthink nel tuo team sicurezza?", "Come incoraggiare dissenso in sicurezza?"

2.9.4 Ripartizione Slide

Slide 9.1: "Psicologia di Gruppo nella Sicurezza" - Breve revisione assunzioni base Bion, concetto groupthink (Janis), spostamento al rischio, diffusione di responsabilità, vulnerabilità collettive.

Slide 9.2: "10 Indicatori Dinamiche di Gruppo" - Tabella 6.1-6.10, evidenzia 6.1 e 6.3, pattern vulnerabilità gruppo.

Slide 9.3: "Vettori di Attacco a Livello Gruppo" - Tecniche dirompimento organizzativo, fallimenti decisionali collettivi, effetto spettatore in IR, social engineering gruppo, parallelo groupthink Challenger.

Slide 9.4: "Valutazione e Soluzioni" - Osservabili gruppo (dinamiche riunione, pattern decisione), albero decisionale punteggio, prime 3 soluzioni (ruoli dissenso, assegnazione responsabilità, protocolli decisione), prompt esercizio scenario comitato.

2.9.5 Materiali Necessari

Field Kit 6.1 e 6.3, Tassonomia [6.x], video groupthink (5 min), Handout esercizio comitato.

2.9.6 Elementi di Valutazione

Quiz: Q1: Definizione groupthink → pressione consenso previene valutazione critica corretto. Q2: Indicatore groupthink → 6.1 corretto. Q3: Indicatore diffusione di responsabilità → 6.3 corretto.

Rubrica Esercizio: Identificazione groupthink (3 pts), analisi pressione consenso (2 pts), punteggio vulnerabilità con giustificazione (3 pts), progettazione meccanismo dissenso (2 pts). Totale 10 pts (7+ superamento).

2.10 Modulo 10: Dominio [7.x] Vulnerabilità da Risposta allo Stress

2.10.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Spiegare l'impatto della fisiologia dello stress sulla sicurezza; identificare i 10 indicatori di risposta allo stress; riconoscere gli attacchi di sfruttamento dello stress; progettare interventi di resilienza allo stress.

Concetti Chiave: Stress acuto vs cronico, risposte attacco/fuga/immobilizzazione/accudimento, compromissione cortisolo, contagio da stress, burnout.

2.10.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Fisiologia stress Selye, attivazione asse HPA, effetti cortisolo su cognizione/memoria, stress acuto vs cronico, quattro risposte F (attacco/fuga/immobilizzazione/acc meccanismi contagio stress.

2. Dieci Indicatori Stress (30 min): Tabella panoramica 7.1-7.10, Approfondimento 7.1 (compromissione stress acuto, degrado risposta incidente, punteggio), Approfondimento 7.2 (burnout stress cronico, esaurimento analista SOC, punteggio), pattern stress.

3. Vettori di Attacco e Incidenti (30 min): Attacchi induzione stress (creare caos poi sfruttare), finestre sfruttamento burnout, risposta incidente sotto stress acuto, contagio stress durante violazioni, casi stress ransomware sanitario.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità stress, criteri di punteggio, Prime 3 soluzioni (formazione inoculazione stress, programmi prevenzione burnout, gestione stress incidente), implementazione.

5. Esercizio (10 min): Scenario risposta incidente sotto stress simulato, valutare vulnerabilità stress, progettare protocolli resilienza.

2.10.3 Metodi di Insegnamento

Lezione: Diagrammi fisiologia stress, effetti cortisolo, spiegazioni quattro risposte F.

Esercizio: Risposta incidente con pressione temporale e informazioni incomplete, sperimentare compromissione stress.

Discussione: "Livello stress durante ultimo incidente?", "Burnout nel tuo team sicurezza?"

2.10.4 Ripartizione Slide

Slide 10.1: "Stress e Prestazione di Sicurezza" - Fisiologia stress Selye, diagramma asse HPA, effetti cognitivi cortisolo, confronto acuto vs cronico, quattro risposte F.

Slide 10.2: "10 Indicatori Risposta allo Stress" - Tabella 7.1-7.10, evidenzia 7.1 e 7.2, pattern vulnerabilità stress.

Slide 10.3: "Attacchi di Sfruttamento dello Stress" - Tecniche induzione stress, tempistica sfruttamento burnout, IR sotto stress acuto, effetti contagio stress, casi ransomware sanitario.

Slide 10.4: "Valutazione e Soluzioni" - Osservabili stress (prestazione incidente, esaurimento team), albero decisionale punteggio, prime 3 soluzioni (formazione inoculazione, prevenzione burnout, gestione stress), prompt esercizio scenario IR.

2.10.5 Materiali Necessari

Field Kit 7.1 e 7.2, Tassonomia [7.x], Scenario esercizio stressante IR, diagrammi fisiologia stress.

2.10.6 Elementi di Valutazione

Quiz: Q1: Quattro risposte F $\rightarrow$ attacco/fuga/immobilizzazione/accudimento corretto. Q2: Indicatore stress acuto $\rightarrow$ 7.1 corretto. Q3: Indicatore stress cronico/burnout $\rightarrow$ 7.2 corretto.

Rubrica Esercizio: Identificazione vulnerabilità stress (3 pts), analisi compromissione stress (2 pts), punteggio vulnerabilità con giustificazione (3 pts), progettazione protocollo resilienza (2 pts). Totale 10 pts (7+ superamento).

2.11 Modulo 11: Dominio [8.x] Vulnerabilità da Processi Inconsci

2.11.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Applicare concetti psicoanalitici alla sicurezza; identificare i 10 indicatori inconsci; riconoscere lo sfruttamento inconscio; progettare interventi consapevoli dell'ombra.

Concetti Chiave: Proiezione ombra, identificazione inconscia, transfert, controtransfert, meccanismi di difesa, archetipi.

2.11.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Revisione inconscio psicoanalitico (da Modulo 2), ombra Jung, proiezione Klein, transfert/controtransfert, meccanismi di difesa nella sicurezza, pattern archetipici.

2. Dieci Indicatori Inconsci (30 min): Tabella panoramica 8.1-8.10, Approfondimento 8.1 (proiezione ombra sugli attaccanti, attribuzione esterna, punteggio), Approfondimento 8.4 (transfert a figure autorità, idealizzazione leader sicurezza, punteggio), pattern inconsci.

3. Vettori di Attacco e Incidenti (30 min): Attacchi simbolici che sfruttano inconscio, manipolazione transfert, attivazione archetipica (eroe/trickster), sfruttamento meccanismi di difesa, identificazione inconscia con attaccanti.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità inconscia, criteri di punteggio, Prime 3 soluzioni (facilitazione lavoro ombra, formazione consapevolezza transfert, riconoscimento meccanismi di difesa), implementazione.

5. Esercizio (10 min): Post-mortem violazione organizzativa con colpa esterna, identificare difese inconsce, progettare integrazione ombra.

2.11.3 Metodi di Insegnamento

Lezione: Revisione meccanismi inconsci, esempi ombra, transfert nelle organizzazioni.

Esercizio: Analisi post-mortem violazione per proiezione e ombra.

Discussione: "Cosa l'org rifiuta di riconoscere?", "Idealizzazione dei leader sicurezza?"

2.11.4 Ripartizione Slide

Slide 11.1: "L'Inconscio nella Sicurezza" - Concetto inconscio psicoanalitico, meccanismo proiezione ombra, transfert/controtransfert, meccanismi di difesa, archetipi.

Slide 11.2: "10 Indicatori Processi Inconsci" - Tabella 8.1-8.10, evidenzia 8.1 e 8.4, pattern vulnerabilità inconscia.

Slide 11.3: "Sfruttamento Inconscio" - Esempi attacco simbolico, manipolazione transfert, attivazione archetipica (sfruttamento eroe/trickster), uso meccanismi di difesa, identificazione con attaccanti.

Slide 11.4: "Valutazione e Soluzioni" - Osservabili inconsci (pattern colpa esterna, idealizzazione), albero decisionale punteggio, prime 3 soluzioni (lavoro ombra, consapevolezza transfert, riconoscimento difese), prompt esercizio post-mortem violazione.

2.11.5 Materiali Necessari

Field Kit 8.1 e 8.4, Tassonomia [8.x], Esercizio post-mortem violazione con narrativa colpa esterna.

2.11.6 Elementi di Valutazione

Quiz: Q1: Definizione proiezione ombra → aspetti disconosciuti proiettati su altri corretto. Q2: Indicatore proiezione ombra → 8.1 corretto. Q3: Indicatore transfert → 8.4 corretto.

Rubrica Esercizio: Identificazione difesa inconscia (3 pts), analisi proiezione/ombra (2 pts), punteggio vulnerabilità con giustificazione (3 pts), progettazione integrazione ombra (2 pts). Totale 10 pts (7+ superamento).

2.12 Modulo 12: Dominio [9.x] Vulnerabilità da Bias Specifici dell'IA

2.12.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Spiegare la psicologia dell'interazione IA-umano; identificare i 10 indicatori di bias IA; riconoscere lo sfruttamento della vulnerabilità IA; progettare controlli di sicurezza consapevoli dell'IA.

Concetti Chiave: Antropomorfizzazione, bias automazione, avversione algoritmo, trasferimento autorità IA, valle inquietante, accettazione allucinazione.

2.12.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Psicologia interazione umano-IA, tendenza antropomorfizzazione, bias automazione (sovra-affidamento), avversione algoritmo (sotto-fiducia), trasferimento autorità IA, effetti valle inquietante, ricerca emergente psicologia IA.

2. Dieci Indicatori IA (30 min): Tabella panoramica 9.1-9.10, Approfondimento 9.1 (antropomorfizzazione sistemi IA, attaccamento emotivo, punteggio), Approfondimento 9.2 (override bias automazione, accettazione IA non critica, punteggio), pattern vulnerabilità IA.

3. Vettori di Attacco e Incidenti (30 min): Social engineering IA (manipolazione chatbot), sfruttamento deepfake (voce/video), avvelenamento raccomandazione IA, attacchi bias automazione (ML malevolo), sfruttamento allucinazione, casi ML avversariale.

4. Valutazione e Soluzioni (30 min): Osservabili vulnerabilità IA, criteri di punteggio, Prime 3 soluzioni (formazione alfabetizzazione IA, requisiti umano-in-loop, protocolli verifica output IA), implementazione.

5. Esercizio (10 min): Scenario phishing generato IA con pretesto chatbot, valutare vulnerabilità specifiche IA, progettare controlli di verifica.

2.12.3 Metodi di Insegnamento

Lezione: Ricerca psicologia IA, dimostrazioni antropomorfizzazione, esempi bias automazione.

Esercizio: Scenario phishing chatbot IA, sperimentare pressione antropomorfizzazione.

Discussione: "Fiducia negli strumenti sicurezza IA quanto?", "Sperimentato allucinazioni IA?"

2.12.4 Ripartizione Slide

Slide 12.1: "Psicologia Interazione IA-Umano" - Tendenza antropomorfizzazione, bias automazione vs avversione algoritmo, trasferimento autorità IA, valle inquietante, ricerca emergente.

Slide 12.2: "10 Indicatori Bias Specifici IA" - Tabella 9.1-9.10, evidenzia 9.1 e 9.2, pattern vulnerabilità IA.

Slide 12.3: "Attacchi di Sfruttamento IA" - Social engineering IA (chatbot), deepfake (esempi voce/video), avvelenamento raccomandazione, attacchi bias automazione, sfruttamento allucinazione, casi ML avversariale.

Slide 12.4: "Valutazione e Soluzioni" - Osservabili IA (livelli fiducia strumenti IA, pratiche verifica), albero decisionale punteggio, prime 3 soluzioni (alfabetizzazione IA, umano-in-loop, protocolli verifica), prompt esercizio phishing chatbot.

2.12.5 Materiali Necessari

Field Kit 9.1 e 9.2, Tassonomia [9.x], Esercizio phishing chatbot IA, esempi video deepfake (3 min).

2.12.6 Elementi di Valutazione

Quiz: Q1: Definizione antropomorfizzazione → attribuire intenzioni umane all'IA corretto. Q2: Indicatore bias automazione → 9.2 corretto. Q3: Indicatore trasferimento autorità IA → 9.4 corretto.

Rubrica Esercizio: Identificazione vulnerabilità IA (3 pts), analisi antropomorfizzazione (2 pts), punteggio vulnerabilità con giustificazione (3 pts), progettazione controllo verifica (2 pts). Totale 10 pts (7+ superamento).

2.13 Modulo 13: Dominio [10.x] Stati Critici Convergenti

2.13.1 Panoramica

Durata: 2 ore — **Slide:** 4

Obiettivi di Apprendimento: Spiegare il concetto di convergenza vulnerabilità; identificare i 10 indicatori di stato convergente; riconoscere le condizioni di tempesta perfetta; progettare sistemi di monitoraggio convergenza.

Concetti Chiave: Tempesta perfetta, guasti a cascata, punti di non ritorno, allineamento formaggio svizzero, cigni neri, rinoceronti grigi, catastrofe complessità.

2.13.2 Schema dei Contenuti

1. Fondamento Psicologico (20 min): Emergenza teoria dei sistemi, modello formaggio svizzero Reason, incidenti normali Perrow, matematica convergenza (moltiplicazione non addizione), dinamiche punto di non ritorno, teoria della complessità nella sicurezza.

2. Dieci Indicatori Convergenti (30 min): Tabella panoramica 10.1-10.10, Approfondimento 10.1 (condizioni tempesta perfetta, allineamento multiple vulnerabilità, punteggio), Ap-

profondimento 10.4 (allineamento formaggio svizzero, allineamento buchi critico, punteggio), pattern convergenza.

3. Vettori di Attacco e Incidenti (30 min): Tempeste perfette APT (multiple vulnerabilità sfruttate), attacchi guasto a cascata, violazioni punto di non ritorno, sfruttamento formaggio svizzero, SolarWinds come caso convergenza, eventi cigno nero vs rinoceronte grigio.

4. Valutazione e Soluzioni (30 min): Osservabili stato convergente, criteri di punteggio (esponenziale non lineare), Prime 3 soluzioni (dashboard monitoraggio convergenza, analisi correlazione vulnerabilità, sistemi allerta precoce), implementazione.

5. Esercizio (10 min): Scenario vulnerabilità multi-dominio, calcolare rischio convergenza, progettare monitoraggio per rilevamento tempesta perfetta.

2.13.3 Metodi di Insegnamento

Lezione: Visuale modello formaggio svizzero, dimostrazione matematica convergenza, timeline SolarWinds.

Esercizio: Scenario multi-vulnerabilità, calcolare rischio esponenziale.

Discussione: "Sperimentato violazione tempesta perfetta?", "Come monitorare convergenza nella tua org?"

2.13.4 Ripartizione Slide

Slide 13.1: "Convergenza Vulnerabilità" - Concetto emergenza sistema, visuale formaggio svizzero Reason, matematica convergenza (moltiplicazione), dinamiche punto di non ritorno, catastrofe complessità.

Slide 13.2: "10 Indicatori Critici Convergenti" - Tabella 10.1-10.10, evidenzia 10.1 e 10.4, pattern vulnerabilità convergenza.

Slide 13.3: "Attacchi di Stato Convergente" - Tempeste perfette APT, guasti a cascata, violazioni punto di non ritorno, allineamento buchi formaggio svizzero, timeline convergenza SolarWinds, cigno nero vs rinoceronte grigio.

Slide 13.4: "Valutazione e Soluzioni" - Osservabili convergenti (multiple vulnerabilità simultanee), approccio punteggio esponenziale, prime 3 soluzioni (dashboard monitoraggio, analisi correlazione, allerta precoce), prompt esercizio scenario multi-dominio.

2.13.5 Materiali Necessari

Field Kit 10.1 e 10.4, Tassonomia [10.x], Visuale modello formaggio svizzero, Esercizio multi-vulnerabilità, Case study SolarWinds.

2.13.6 Elementi di Valutazione

Quiz: Q1: Calcolo rischio convergenza → moltiplicazione non addizione corretto. Q2: Indicatore tempesta perfetta → 10.1 corretto. Q3: Indicatore allineamento formaggio svizzero → 10.4 corretto.

Rubrica Esercizio: Identificazione multi-vulnerabilità (3 pts), calcolo convergenza (2 pts), punteggio rischio esponenziale (3 pts), progettazione sistema monitoraggio (2 pts). Totale 10 pts (7+ superamento).

2.14 Modulo 14: Privacy ed Etica

2.14.1 Panoramica

Durata: 4 ore — **Slide:** 8

Obiettivi di Apprendimento: Articolare i principi di valutazione che preservano la privacy; applicare la matematica della privacy differenziale; implementare i requisiti di aggregazione minima; progettare meccanismi di ritardo temporale; spiegare i confini etici nella valutazione psicologica.

Concetti Chiave: Privacy differenziale, unità di aggregazione, ritardi temporali, divieto di profilazione individuale, valutazione etica, gestione dati.

2.14.2 Schema dei Contenuti

1. Principi che Preservano la Privacy (60 min): Perché la privacy conta nella valutazione psicologica, principio solo aggregazione (mai individuale), unità di aggregazione minima (10 individui), concetto privacy differenziale (epsilon = 0.1), requisito ritardo temporale (72 ore minimo), analisi basata su ruolo non individuale, divieto di uso per valutazione performance.

2. Matematica Privacy Differenziale (45 min): Concetto budget privacy epsilon, meccanismi iniezione rumore, tradeoff privacy-utilità, razionale CPF epsilon = 0.1, esempi implementazione pratica, metodi verifica.

3. Requisiti Gestione Dati (45 min): Crittografia a riposo (AES-256) e in transito (TLS 1.3), controlli accesso e tracce di audit, limiti conservazione (5 anni massimo), procedure distruzione sicura, considerazioni trasferimento dati transfrontaliero, mappatura conformità GDPR/CCPA.

4. Confini Etici (45 min): CPF è valutazione organizzativa non clinica, nessuna diagnosi o terapia individuale, le vulnerabilità psicologiche sono caratteristiche umane normali non fallimenti, divieto di stigmatizzazione o colpa, requisiti consenso informato, meccanismi opt-out mantenendo validità statistica, protezioni whistleblower.

5. Case Studies: Violazioni Privacy (30 min): Abusi storici profilazione psicologica, lezioni Cambridge Analytica, preoccupazioni sorveglianza dipendenti, analisi tre scenari violazione, discussione confini etici.

6. Esercizio: Valutazione Impatto Privacy (15 min): Progettare valutazione per reparto 50 persone, garantire unità di aggregazione, calcolare parametri privacy differenziale, implementare ritardi temporali, verificare nessuna profilazione individuale possibile.

2.14.3 Metodi di Insegnamento

Lezione: Principi privacy con esempi violazione, matematica privacy differenziale con visualizzazioni, framework etico con confronti caso.

Esercizi: (1) Calcolo unità aggregazione per varie dimensioni org (15 min), (2) Selezione parametri privacy differenziale (15 min), (3) Progettazione valutazione impatto privacy (15 min).

Discussione: "Tensione tra valutazione e privacy?", "Come garantire nessuna profilazione individuale?", "Preoccupazioni etiche con valutazione psicologica?"

Case Studies: Tre scenari violazione privacy, analisi gruppo di cosa è andato storto, progettazione salvaguardie.

2.14.4 Ripartizione Slide

Slide 14.1: "Principi di Valutazione Privacy-First" - Perché la privacy conta, principio solo aggregazione, minimo 10 individui, privacy differenziale epsilon, ritardo temporale 72 ore, analisi basata su ruolo, nessun uso valutazione performance.

Slide 14.2: "Privacy Differenziale Spiegata" - Concetto budget privacy epsilon, visuale iniezione rumore, grafico tradeoff privacy-utilità, razionale CPF epsilon = 0.1, esempio implementazione.

Slide 14.3: "Unità di Aggregazione Minima" - Requisito 10 individui, calcolo per diverse dimensioni org, sfide piccole organizzazioni, esempi unità aggregazione (reparti, ruoli, sedi).

Slide 14.4: "Meccanismi Ritardo Temporale" - Razionale 72 ore minimo, diagramma flusso di lavoro reporting ritardato, previene sorveglianza in tempo reale, bilancia tempestività con privacy.

Slide 14.5: "Requisiti Gestione Dati" - Crittografia (AES-256, TLS 1.3), controlli accesso e audit, limiti conservazione 5 anni, distruzione sicura, considerazioni transfrontaliero, mappatura GDPR/CCPA.

Slide 14.6: "Confini Etici" - Valutazione organizzativa non clinica, nessuna diagnosi individuale, vulnerabilità sono normali, divieto stigma/colpa, consenso informato, meccanismi opt-out, protezioni whistleblower.

Slide 14.7: "Case Studies Violazione Privacy" - Lezioni Cambridge Analytica, preoccupazioni sorveglianza dipendenti, tre esempi scenario (cosa è andato storto, salvaguardie necessarie), prompt discussione.

Slide 14.8: "Esercizio Valutazione Impatto Privacy" - Scenario reparto 50 persone, calcolo unità aggregazione, parametri privacy differenziale, implementazione ritardo temporale, verifica nessuna profilazione individuale possibile, istruzioni esercizio gruppo.

2.14.5 Materiali Necessari

Workbook Modulo 14 (pagine 61-75), Calcolatore privacy differenziale, Foglio lavoro unità aggregazione, Tre case studies violazione privacy (2 pagine ciascuno), Template valutazione impatto privacy, Checklist conformità GDPR/CCPA.

2.14.6 Elementi di Valutazione

Quiz (5 domande): Q1: Unità aggregazione minima → 10 individui corretto. Q2: Privacy differenziale CPF epsilon → 0.1 corretto. Q3: Ritardo temporale minimo → 72 ore corretto. Q4: Conservazione dati massima → 5 anni corretto. Q5: Tipo valutazione CPF → organizzativa non clinica corretto.

Rubrica Esercizio (Valutazione Impatto Privacy): Calcolo corretto unità aggregazione (2 pts), parametri privacy differenziale appropriati (2 pts), implementazione ritardo temporale (2 pts), verifica nessuna profilazione possibile (2 pts), piano gestione dati completo (2 pts). Totale 10 pts (7+ superamento).

2.15 Modulo 15: Integrazione e Applicazione

2.15.1 Panoramica

Durata: 4 ore — **Slide:** 7

Obiettivi di Apprendimento: Mappare CPF a clausole ISO 27001:2022; integrare CPF con funzioni NIST CSF 2.0; progettare strategie di implementazione organizzativa; superare le sfide comuni; applicare il framework alla valutazione finale.

Concetti Chiave: Integrazione ISO 27001, mappatura NIST CSF, strategia di implementazione, change management, sfide comuni, progressione maturità.

2.15.2 Schema dei Contenuti

1. Integrazione CPF e ISO 27001:2022 (60 min): Panoramica standard CPF-27001:2025, mappatura a clausole ISO (4.1 contesto, 6.1 valutazione rischio, 7.2 competenza, 7.3 consapevolezza, 8.2 pianificazione operativa, 9.1 monitoraggio, 10.1 miglioramento), potenziamento Allegato A, PVMS come parallelo a ISMS, requisiti documentazione, considerazioni audit.

2. Integrazione CPF e NIST CSF 2.0 (45 min): Mappatura funzioni NIST (Identifica: valutazione CPF identifica rischi umani, Proteggi: controlli psicologici complementano tecnici, Rileva: indicatori comportamentali abilitano rilevamento, Rispondi: primo soccorso psicologico durante incidenti, Recupera: affrontare trauma psicologico post-violazione), esempi potenziamento sottocategorie, CPF come livello di intelligence fattore umano.

3. Strategie di Implementazione (60 min): Approccio a fasi (valutazione, pilota, rollout, continuo), coinvolgimento stakeholder (buy-in esecutivo, middle management, partecipazione staff), considerazioni change management, pianificazione risorse (personale, tecnologia, budget), requisiti formazione, pianificazione comunicazione, identificazione quick win.

4. Sfide Comuni e Soluzioni (30 min): Sfida: "Sembra invasivo" - Soluzione: Enfatizzare protezioni privacy e aggregazione, Sfida: "Troppo psicologico per team sicurezza" - Soluzione: Concentrarsi su osservabili non terapia, Sfida: "Non abbiamo psicologi" - Soluzione: Formazione CPF crea competenza, Sfida: "ROI non chiaro" - Soluzione: Metriche riduzione incidenti, Sfida: "Complessità integrazione" - Soluzione: Iniziare piccolo pilota, Sfida: "Resistenza al cambiamento" - Soluzione: Dimostrare valore attraverso pilota.

5. Progressione Maturità (30 min): Livello 1 Fondazione (Punteggio CPF 100-149), Livello 2 Intermedio (70-99), Livello 3 Avanzato (40-69), Livello 4 Esemplare (0-39), percorsi di progressione, costruzione capacità nel tempo.

6. Esercizio Finale: Mini-Valutazione Completa (45 min): Scenario organizzativo realistico con multiple indicatori attraverso domini, studenti conducono valutazione abbreviata usando Scheda di Riferimento Rapido, applicano punteggio ternario, calcolano punteggi categoria e CPF, identificano stati convergenti, raccomandano primi 5 interventi, presentano risultati al gruppo.

2.15.3 Metodi di Insegnamento

Lezione: Framework ISO/NIST con diagrammi sovrapposizione CPF, visualizzazione roadmap implementazione, grafici progressione livello maturità.

Esercizi: (1) Esercizio mappatura clausola ISO - assegnare domini CPF a clausole ISO (20 min), (2) Potenziamento funzione NIST - progettare integrazione CPF per una funzione (20 min), (3) Pianificazione implementazione - creare piano pilota 90 giorni con stakeholder/risorse (20 min), (4) Mini-valutazione finale (45 min).

Discussione: "Sfida di implementazione più grande anticipata?", "Come ottenere buy-in esecutivo?", "Integrazione con programma sicurezza esistente?"

Case Study: Percorso implementazione CPF organizzazione sanitaria (pilota a Livello 2 in 18

mesi), lezioni apprese, fattori di successo.

2.15.4 Ripartizione Slide

Slide 15.1: "CPF e ISO 27001:2022" - Panoramica CPF-27001:2025, tabella mappatura clausole (4.1, 6.1, 7.2, 7.3, 8.2, 9.1, 10.1), esempi potenziamento Allegato A, PVMS parallelo a ISMS.

Slide 15.2: "CPF e NIST CSF 2.0" - Cinque funzioni con punti di integrazione CPF (Identifica rischi umani, Proteggi con controlli psicologici, Rileva via indicatori comportamentali, Rispondi con primo soccorso psicologico, Recupera affrontando trauma), esempi potenziamento sottocategoria, visuale livello di intelligence fattore umano.

Slide 15.3: "Strategia di Implementazione" - Diagramma approccio a fasi (valutazione, pilota, rollout, continuo), piramide coinvolgimento stakeholder, considerazioni change management, checklist pianificazione risorse, identificazione quick win.

Slide 15.4: "Sfide Comuni e Soluzioni" - Tabella sei coppie sfida-soluzione (sembra invasivo/protezioni privacy, troppo psicologico/focus osservabili, nessuno psicologo/formazione crea competenza, ROI non chiaro/metriche incidenti, integrazione complessa/iniziare piccolo, resistenza/dimostrare valore).

Slide 15.5: "Progressione Maturità" - Visuale quattro livelli (Fondazione 100-149, Intermedio 70-99, Avanzato 40-69, Esemplare 0-39), caratteristiche di ogni livello, percorsi di progressione, timeline costruzione capacità.

Slide 15.6: "Case Study: Implementazione Sanitaria" - Background organizzazione, timeline implementazione (pilota a Livello 2 in 18 mesi), sfide incontrate e soluzioni, fattori di successo chiave, lezioni apprese, outcomes misurabili.

Slide 15.7: "Esercizio Finale: Mini-Valutazione" - Descrizione scenario organizzativo (vulnerabilità multi-dominio), istruzioni compito valutazione (identificare indicatori, applicare punteggio, calcolare punteggi, trovare convergenza, raccomandare interventi), formato presentazione, criteri di valutazione.

2.15.5 Materiali Necessari

Workbook Modulo 15 (pagine 76-90), Standard ISO 27001:2022 (riferimento), Documento NIST CSF 2.0 (riferimento), Documento requisiti CPF-27001:2025, Scheda di Riferimento Rapido per esercizio finale, Pacchetto scenario finale (5 pagine), Template pianificazione implementazione, Handout case study sanitario (3 pagine).

2.15.6 Elementi di Valutazione

Quiz (5 domande): Q1: Clausola ISO che CPF affronta primariamente → 7.2 Competenza e 7.3 Consapevolezza corretto. Q2: Contributo CPF funzione NIST Identifica → identificazione rischio umano corretto. Q3: Intervallo punteggio Livello 2 CPF → 70-99 corretto. Q4: Prima fase implementazione → valutazione corretto. Q5: Tipo standard CPF-27001 → requisiti PVMS organizzativo corretto.

Rubrica Esercizio Finale: Identificazione indicatori attraverso domini (3 pts), punteggio ternario accurato con giustificazione (3 pts), calcolo corretto punteggio categoria e CPF (2 pts), riconoscimento stato convergente (1 pt), raccomandazioni intervento appropriate (1 pt). Totale 10 pts (7+ superamento).

Rubrica Completamento Corso: Tutti i 15 quiz di modulo superati (15 pts), partecipazione

attiva negli esercizi (10 pts), mini-valutazione finale superata (10 pts), accordo etico firmato (5 pts). Totale 40 pts (28+ superamento per completamento corso, esame scritto separato richiesto per certificazione).

3 Appendici

3.1 Appendice A: Inventario Completo Slide

Modulo	Slide	Titolo	Tipo	Durata
Modulo 1	1.1	La Crisi del Fattore Umano	Lezione	10 min
Modulo 1	1.2	Processo Decisionale Pre-Cognitivo	Lezione	15 min
Modulo 1	1.3	Architettura Framework CPF	Lezione	15 min
Modulo 1	1.4	Sistema di Punteggio Ternario	Lezione	15 min
Modulo 1	1.5	Integrazione con ISO 27001 e NIST CSF	Lezione	15 min
Modulo 1	1.6	Violazione Target Attraverso la Lente CPF	Case Study	30 min
Modulo 2	2.1	Panoramica Assunzioni di Base di Bion	Lezione	15 min
Modulo 2	2.2	Assunzioni di Base nella Sicurezza	Lezione	20 min
Modulo 2	2.3	Scissione e Proiezione Kleiniana	Lezione	20 min
Modulo 2	2.4	L'Ombra di Jung nella Sicurezza	Lezione	15 min
Modulo 2	2.5	Archetipi nella Sicurezza	Lezione	15 min
Modulo 2	2.6	Spazio Transizionale di Winnicott	Lezione	10 min
Modulo 2	2.7	Esercizio Analisi Caso Psicoanalitico	Esercizio	15 min
Modulo 3	3.1	Pensieri Lenti e Veloci	Lezione	20 min
Modulo 3	3.2	Euristiche e Bias	Lezione	15 min
Modulo 3	3.3	Panoramica Sei Principi di Cialdini	Lezione	15 min
Modulo 3	3.4	Sei Principi nel Social Engineering	Lezione	20 min
Modulo 3	3.5	Teoria del Carico Cognitivo	Lezione	15 min
Modulo 3	3.6	Decision-Making sotto Incertezza	Lezione	10 min
Modulo 3	3.7	Esercizio Sfruttamento Cognitivo	Esercizio	15 min
Modulo 4	4.1	Perché Obbediamo: Vulnerabilità Autorità	Lezione	20 min
Modulo 4	4.2	10 Indicatori Autorità	Lezione	30 min
Modulo 4	4.3	Vettori di Attacco in Azione	Lezione	30 min
Modulo 4	4.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 5	5.1	Pressione Temporale e Sicurezza	Lezione	20 min
Modulo 5	5.2	10 Indicatori Temporali	Lezione	30 min
Modulo 5	5.3	Vettori di Attacco Temporali	Lezione	30 min
Modulo 5	5.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 6	6.1	Meccanismi di Influenza Sociale	Lezione	20 min
Modulo 6	6.2	10 Indicatori Influenza Sociale	Lezione	30 min
Modulo 6	6.3	Pattern di Attacco Social Engineering	Lezione	30 min
Modulo 6	6.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 7	7.1	Emozione e Decisioni di Sicurezza	Lezione	20 min
Modulo 7	7.2	10 Indicatori Affettivi	Lezione	30 min
Modulo 7	7.3	Attacchi di Manipolazione Emotiva	Lezione	30 min
Modulo 7	7.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 8	8.1	Carico Cognitivo e Limiti di Capacità	Lezione	20 min
Modulo 8	8.2	10 Indicatori Sovraccarico Cognitivo	Lezione	30 min
Modulo 8	8.3	Attacchi di Sfruttamento Cognitivo	Lezione	30 min
Modulo 8	8.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 9	9.1	Psicologia di Gruppo nella Sicurezza	Lezione	20 min
Modulo 9	9.2	10 Indicatori Dinamiche di Gruppo	Lezione	30 min
Modulo 9	9.3	Vettori di Attacco a Livello Gruppo	Lezione	30 min

Modulo	Slide	Titolo	Tipo	Durata
Modulo 9	9.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 10	10.1	Stress e Prestazione di Sicurezza	Lezione	20 min
Modulo 10	10.2	10 Indicatori Risposta allo Stress	Lezione	30 min
Modulo 10	10.3	Attacchi di Sfruttamento dello Stress	Lezione	30 min
Modulo 10	10.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 11	11.1	L'Inconscio nella Sicurezza	Lezione	20 min
Modulo 11	11.2	10 Indicatori Processi Inconsci	Lezione	30 min
Modulo 11	11.3	Sfruttamento Inconscio	Lezione	30 min
Modulo 11	11.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 12	12.1	Psicologia Interazione IA-Umano	Lezione	20 min
Modulo 12	12.2	10 Indicatori Bias Specifici IA	Lezione	30 min
Modulo 12	12.3	Attacchi di Sfruttamento IA	Lezione	30 min
Modulo 12	12.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 13	13.1	Convergenza Vulnerabilità	Lezione	20 min
Modulo 13	13.2	10 Indicatori Critici Convergenti	Lezione	30 min
Modulo 13	13.3	Attacchi di Stato Convergente	Lezione	30 min
Modulo 13	13.4	Valutazione e Soluzioni	Lezione/Esercizio	40 min
Modulo 14	14.1	Principi di Valutazione Privacy-First	Lezione	20 min
Modulo 14	14.2	Privacy Differenziale Spiegata	Lezione	15 min
Modulo 14	14.3	Unità di Aggregazione Minima	Lezione	15 min
Modulo 14	14.4	Meccanismi Ritardo Temporale	Lezione	10 min
Modulo 14	14.5	Requisiti Gestione Dati	Lezione	15 min
Modulo 14	14.6	Confini Etici	Lezione	15 min
Modulo 14	14.7	Case Studies Violazione Privacy	Case Study	20 min
Modulo 14	14.8	Esercizio Valutazione Impatto Privacy	Esercizio	30 min
Modulo 15	15.1	CPF e ISO 27001:2022	Lezione	30 min
Modulo 15	15.2	CPF e NIST CSF 2.0	Lezione	30 min
Modulo 15	15.3	Strategia di Implementazione	Lezione	30 min
Modulo 15	15.4	Sfide Comuni e Soluzioni	Lezione	15 min
Modulo 15	15.5	Progressione Maturità	Lezione	15 min
Modulo 15	15.6	Case Study: Implementazione Sanitaria	Case Study	20 min
Modulo 15	15.7	Esercizio Finale: Mini-Valutazione	Esercizio	45 min
Totale: 80 slide, 40 ore				

3.2 Appendice B: Riepilogo Banca Esercizi

Esercizi Modulo 1:

- 1.1 Analisi Fallimento Consapevolezza (15 min): Condividere esempi formazione falliti, identificare perché interventi coscienti non hanno funzionato
- 1.2 Esperimento Decisionale Pre-Cognitivo (10 min): Dimostrazione live scenari autorità/urgenza, riflettere su decisioni rapide
- 1.3 Navigazione Framework (20 min): Esercitazione veloce con Scheda di Riferimento Rapido, localizzare indicatori attraverso domini

Esercizi Modulo 2:

- 2.1 Identificazione Assunzione Base (20 min): Tre vignette, identificare baD/baF/baP e vulnerabilità

- 2.2 Scissione nella Cultura della Sicurezza (15 min): Elencare entità fidate/minacciose, discutere punti ciechi da idealizzazione/demonizzazione
- 2.3 Riconoscimento Ombra (15 min): Riflessione anonima "cosa l'org rifiuta di riconoscere"
- 2.4 Analisi Caso Psicoanalitico (15 min): Ransomware sanitario, identificare assunzione base, scissione, proiezioni

Esercizi Modulo 3:

- 3.1 Test Velocità Sistema 1 vs 2 (15 min): 20 email 3 sec ciascuna poi tempo illimitato, confrontare tassi accuratezza
- 3.2 Mappatura Principio Cialdini (20 min): Sei scenari, mappare principi influenza, discutere combinazioni
- 3.3 Simulazione Carico Cognitivo (15 min): Compito sicurezza con distrazioni, sperimentare degrado sovraccarico
- 3.4 Analisi Sfruttamento Cognitivo (15 min): Tre email phishing, identificare principi/Sistema/manipolazi carico

Esercizi Moduli 4-13 Dominio (10 min ciascuno): Ogni dominio include esercizio basato su scenario che applica punteggio ternario a caso realistico con discussione.

Esercizi Modulo 14:

- 14.1 Calcolo Unità Aggregazione (15 min): Calcolare per varie dimensioni org, garantire requisiti privacy
- 14.2 Parametri Privacy Differenziale (15 min): Selezionare epsilon appropriato, comprendere tradeoff privacy-utilità
- 14.3 Valutazione Impatto Privacy (30 min): Progettare valutazione per reparto 50 persone, verificare nessuna profilazione

Esercizi Modulo 15:

- 15.1 Mappatura Clausola ISO (20 min): Assegnare domini CPF a clausole ISO 27001
- 15.2 Potenziamento Funzione NIST (20 min): Progettare integrazione CPF per una funzione NIST
- 15.3 Pianificazione Implementazione (20 min): Creare piano pilota 90 giorni con stakeholder/risorse
- 15.4 Mini-Valutazione Finale (45 min): Completare valutazione abbreviata con punteggio e raccomandazioni

Totale: 25 esercizi attraverso 40 ore

3.3 Appendice C: Progettazione Esame

Struttura Esame Scritto CPF-101:

Formato: 100 domande, 3 ore, libro chiuso, computer-based

Tipi Domanda:

- 60 Scelta Multipla: Singola risposta corretta da 4 opzioni
- 30 Basate su Scenario: Scenario breve con domanda che richiede analisi
- 10 Analisi Caso: Case study esteso con domande complesse multi-step

Distribuzione Contenuti per Modulo:

Modulo	Domande	Aree di Focus
Modulo 1	8	Processi pre-cognitivi, architettura framework, integrazione
Modulo 2	8	Concetti Bion, Klein, Jung, Winnicott in sicurezza
Modulo 3	8	Kahneman, Cialdini, Miller, bias cognitivi
Moduli 4-13	50	5 domande per dominio, punteggio ternario, vettori di attacco, soluzioni
Modulo 14	12	Requisiti privacy, privacy differenziale, etica
Modulo 15	14	Integrazione ISO/NIST, implementazione, scenari finali
Totale	**100**	

Distribuzione Livello Cognitivo (Tassonomia di Bloom):

- Conoscenza/Ricordo: 20% (20 domande) - Fatti, definizioni, terminologia
- Comprensione/Applicazione: 40% (40 domande) - Spiegare concetti, applicare a scenari
- Analisi/Sintesi: 40% (40 domande) - Analizzare situazioni complesse, integrare multiple concetti

Standard Superamento: 70% (70 risposte corrette)

Processo Sviluppo Domande:

- Validazione psicometrica con gruppi pilota
- Distribuzione difficoltà item: 30% facile, 50% moderato, 20% difficile
- Analisi statistica regolare (indice discriminazione, indice difficoltà)
- Miglioramento continuo basato su dati performance

Politica Ripetizione:

- Prima ripetizione: periodo attesa 30 giorni, 50% tariffa
- Seconda ripetizione: periodo attesa 30 giorni, 50% tariffa
- Dopo tre fallimenti: Formazione aggiuntiva richiesta, periodo attesa 6 mesi

3.4 Appendice D: Materiali di Riferimento

Documenti Framework CPF:

- The Cybersecurity Psychology Framework: Documento tassonomia completo con tutti i 100 indicatori
- CPF-27001:2025 Requisiti: Standard PVMS organizzativo
- Schema Certificazione CPF: Percorsi e requisiti certificazione professionale
- Esempio Field Kit: Indicatore 1.1 completo (fondazione, operativo, field kit)

Papers di Ricerca Fondazionali:

- Milgram, S. (1974). Obedience to Authority
- Bion, W. R. (1961). Experiences in Groups
- Klein, M. (1946). Notes on some schizoid mechanisms
- Jung, C. G. (1969). The Archetypes and the Collective Unconscious
- Winnicott, D. W. (1971). Playing and Reality
- Kahneman, D. (2011). Thinking, Fast and Slow
- Kahneman, D. & Tversky, A. (1979). Prospect Theory
- Cialdini, R. B. (2007). Influence: The Psychology of Persuasion
- Miller, G. A. (1956). The Magical Number Seven, Plus or Minus Two

Standard Framework Sicurezza:

- ISO/IEC 27001:2022 Information Security Management Systems
- ISO/IEC 27002:2022 Code of Practice for Information Security Controls
- NIST Cybersecurity Framework 2.0
- ISO 19011:2018 Guidelines for Auditing Management Systems (per percorso Auditor)

Riferimenti Privacy ed Etica:

- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- Differential Privacy: A Survey of Results (Dwork, 2008)
- APA Ethical Principles of Psychologists and Code of Conduct

Field Kit Referenziati (per modulo):

- Modulo 4: Field Kit 1.1 (Conformità incondizionata), 1.3 (Suscettibilità impersonificazione)

- Modulo 5: Field Kit 2.1 (Bypass urgenza), 2.3 (Accettazione rischio scadenza)
- Modulo 6: Field Kit 3.1 (Sfruttamento reciprocità), 3.3 (Manipolazione prova sociale)
- Modulo 7: Field Kit 4.1 (Paralisi paura), 4.5 (Nascondimento vergogna)
- Modulo 8: Field Kit 5.1 (Fatica allerta), 5.2 (Fatica decisionale)
- Modulo 9: Field Kit 6.1 (Groupthink), 6.3 (Diffusione di responsabilità)
- Modulo 10: Field Kit 7.1 (Stress acuto), 7.2 (Burnout cronico)
- Modulo 11: Field Kit 8.1 (Proiezione ombra), 8.4 (Transfert)
- Modulo 12: Field Kit 9.1 (Antropomorfizzazione), 9.2 (Bias automazione)
- Modulo 13: Field Kit 10.1 (Tempesta perfetta), 10.4 (Allineamento formaggio svizzero)

Nota: Tutti i 100 Field Kit disponibili come libreria di riferimento separata per valutatori certificati.

Controllo Documento

Cronologia Versioni:

Versione	Data	Cambiamenti
1.0	Gennaio 2025	Rilascio iniziale

Piano di Revisione: Revisione annuale dopo ogni erogazione corso, revisione maggiore basata su statistiche esame, feedback partecipanti, e aggiornamenti framework.

Approvazione:

Proprietario Documento: Sviluppo Formazione CPF3

Approvato da: Giuseppe Canale, CISSP

Data: Gennaio 2025

Istruzioni d'Uso:

Questo piano abilita la generazione modulare di slide usando il seguente workflow:

1. Selezionare modulo da Sezione 2 (Strutture Moduli)
2. Rivedere panoramica modulo, schema contenuti, metodi insegnamento, e ripartizione slide
3. Generare contenuto slide usando assistenza AI con struttura prompt: "Generare contenuto slide per [Modulo X, Slide Y] basato su CPF-101-Piano-di-Formazione.tex Sezione 2.X. Includere [materiali specificati]. Formato output: [titolo, bullet, note, suggerimenti visivi]."
4. Riferirsi agli appropriati Field Kit e Sezioni Tassonomia come specificato in Materiali Necessari
5. Implementare esercizi da Appendice B con rubriche fornite
6. Sviluppare elementi di valutazione seguendo la progettazione Appendice C

Informazioni di Contatto:

Sviluppo Formazione CPF3

Sito web: https://cpf3.org

Email: training@cpf3.org

Fine del CPF-101 Piano di Formazione