Modello di Scoring e Maturità CPF

Versione 1.0

Cybersecurity Psychology Framework

Valutazione Quantitativa e Maturità Organizzativa

Giuseppe Canale, CISSP
Ricercatore Indipendente
g.canale@cpf3.org
ORCID: 0009-0007-3263-6897

Gennaio 2025

Sommario

Questo documento presenta un framework unificato per la valutazione quantitativa e la progressione della maturità nella psicologia della cybersecurity. Il Sistema di Scoring CPF fornisce formule matematiche per il calcolo del Punteggio CPF complessivo, dieci Quozienti Specifici di Dominio e l'Indice di Convergenza da 100 indicatori comportamentali. Il Modello di Maturità CPF definisce sei livelli di maturità organizzativa (0-5) con requisiti specifici di progressione, metriche e calcoli del ROI. La guida all'integrazione mappa i punteggi quantitativi ai livelli di maturità, consentendo alle organizzazioni di valutare la resilienza psicologica attuale, confrontarsi con i peer e pianificare miglioramenti strategici. Il framework si applica a tutte le organizzazioni indipendentemente dalle dimensioni o dal settore, con pesi empiricamente validati e fattori di calibrazione specifici per settore.

Indice

Parte I

Sistema di Scoring CPF

1 Introduzione

1.1 Scopo della Valutazione Quantitativa

Il Cybersecurity Psychology Framework trasforma i fattori umani nella sicurezza da valutazione soggettiva a misurazione quantitativa rigorosa. Le organizzazioni affrontano l'85% delle violazioni originate dallo sfruttamento delle vulnerabilità umane, ma mancano di metodi sistematici per misurare, monitorare e migliorare la resilienza psicologica.

Il Sistema di Scoring CPF affronta questa lacuna fornendo:

- **Misurazione Oggettiva**: Formule matematiche che convertono le osservazioni comportamentali in punteggi standardizzati
- **Capacità Predittiva**: Correlazione validata tra punteggi CPF e incidenti di sicurezza reali
- **Benchmarking**: Confronto con organizzazioni simili e standard di settore
- **Analisi delle Tendenze**: Monitoraggio longitudinale dei cambiamenti nelle vulnerabilità psicologiche
- **Quantificazione del ROI**: Analisi costi-benefici degli interventi di sicurezza psicologica

1.2 Relazione con i Requisiti CPF-27001

CPF-27001:2025 stabilisce i Sistemi di Gestione delle Vulnerabilità Psicologiche (PVMS) come controlli formali di cybersecurity paralleli ai tradizionali Sistemi di Gestione della Sicurezza delle Informazioni (ISMS). La metodologia di scoring supporta direttamente i requisiti CPF-27001:

- **Clausola 6.1 (Valutazione del Rischio)**: Il Punteggio CPF quantifica l'esposizione al rischio psicologico
- **Clausola 8.1 (Pianificazione Operativa)**: I Quozienti di Dominio identificano le priorità di intervento
- **Clausola 9.1 (Monitoraggio)**: Il punteggio continuo monitora l'efficacia dei controlli
- **Clausola 9.2 (Audit Interno)**: Le metriche standardizzate consentono una valutazione oggettiva
- **Clausola 10.1 (Miglioramento)**: L'analisi delle tendenze guida il miglioramento sistematico

1.3 Integrazione con la Valutazione della Maturità

Il punteggio quantitativo fornisce le basi per la determinazione del livello di maturità. Le organizzazioni progrediscono attraverso i livelli di maturità raggiungendo soglie di punteggio specifiche e mantenendole per periodi definiti.

1.4 Come Utilizzare Questo Documento

Professionisti della Sicurezza: La Sezione 2 fornisce la metodologia di scoring degli indicatori. La Sezione 3 dettaglia l'aggregazione a livello di dominio. La Sezione 4 spiega il calcolo del Punteggio CPF complessivo.

Responsabili del Rischio: La Sezione 5 presenta i Quozienti di Dominio per una valutazione granulare del rischio. La Sezione 6 copre l'Indice di Convergenza per la valutazione del rischio composto.

Dirigenti: La Sezione 7 fornisce la calibrazione specifica per settore. La Parte II presenta la roadmap di progressione della maturità con calcoli del ROI.

Auditor: La Parte III dettaglia l'integrazione scoring-maturità con criteri di certificazione e requisiti di evidenza.

2 Scoring degli Indicatori Individuali

2.1 Sistema di Scoring Ternario

Ciascuno dei 100 indicatori CPF riceve un punteggio ternario che rappresenta la gravità della vulnerabilità:

Verde (0): Vulnerabilità Minima Rilevata

- Comportamenti osservabili entro parametri accettabili
- Controlli funzionanti efficacemente con tasso di eccezione $< 5\%$
- Nessun intervento immediato richiesto
- Gli indicatori rimangono stabili nella finestra di osservazione di 90 giorni

Giallo (1): Vulnerabilità Moderata che Richiede Monitoraggio

- I comportamenti osservabili mostrano pattern preoccupanti
- Controlli parzialmente efficaci con tasso di eccezione 5-15%
- Intervento preventivo raccomandato entro 30-60 giorni
- L'analisi delle tendenze indica potenziale escalation senza azione

Rosso (2): Vulnerabilità Critica che Richiede Intervento Immediato

- I comportamenti osservabili indicano alto rischio di sfruttamento (>15% tasso di fallimento)
- Controlli inefficaci o assenti; bypass sistematico osservato
- Remediation urgente richiesta entro 7-14 giorni
- Correlazione diretta con pattern storici di incidenti di sicurezza

2.2 Scoring Basato su Evidenze

Lo scoring valido degli indicatori richiede molteplici fonti di dati indipendenti:

Requisiti Minimi:

- Almeno 3 fonti di dati indipendenti per indicatore
- Triangolazione delle evidenze attraverso metodi di raccolta
- Validazione statistica dove applicabile ($n \geq 30$)
- Aggregazione che preserva la privacy (minimo 10 individui per metrica)

Categorie di Fonti di Dati:

1. Log di Sistema (autenticazione, pattern di accesso)
2. Osservazioni Comportamentali (performance nei test di sicurezza)
3. Analisi delle Comunicazioni (metadati email, pattern dei messaggi)
4. Dati di Sondaggio (valutazioni auto-riportate anonime)
5. Metriche di Performance (tempi di task, tassi di errore, eccezioni)

Metodologia di Triangolazione:

Per il punteggio dell'indicatore S_i, il livello di confidenza C_i è:

$$C_i = \frac{\sum_{j=1}^{n} w_j \cdot \mathbb{1}[\text{fonte}_j \text{ concorda}]}{n} \tag{1}$$

dove $n \geq 3$ fonti e w_j = peso di affidabilità della fonte. I punteggi richiedono $C_i \geq 0.67$ (accordo maggioritario).

2.3 Esempi di Scoring

Esempio 1: Indicatore di Autorità 1.1 (Conformità Acritica)

Fonte di Dati 1 - Log del Gateway Email: L'analisi di 500 email da domini apparentemente dirigenziali su 30 giorni mostra il 23% di azione immediata senza verifica (timestamp azione $<$ 5 minuti dopo la ricezione).

Fonte di Dati 2 - Osservazioni dell'Audit di Sicurezza: Durante l'audit trimestrale, 8 su 15 dipendenti campionati (53%) hanno rispettato le richieste dell'auditor senza verifica dell'ID nonostante i requisiti di policy.

Fonte di Dati 3 - Sondaggio Anonimo: Il sondaggio dei dipendenti ($n = 127$) mostra che il 67% riporta disagio nel mettere in discussione figure di autorità apparenti, con il 45% che afferma di verificare "raramente o mai" le richieste di autorità.

Logica di Scoring:

- Analisi email: 23% conformità non verificata → soglia ROSSO (>15%)
- Osservazione audit: 53% non conformità → soglia ROSSO

- Dati sondaggio: 45% non verifica mai → soglia ROSSO
- Evidenza convergente: 3/3 fonti indicano ROSSO
- **Punteggio Finale: 2 (Rosso)**

Esempio 2: Indicatore Temporale 2.7 (Vulnerabilità per Ora del Giorno)

Fonte di Dati 1 - Simulazione di Phishing: Tassi di click per orario: 0800-1200: 8%, 1200-1600: 12%, 1600-2000: 19%. Pomeriggio mostra aumento del 137% rispetto alla mattina.

Fonte di Dati 2 - Eccezioni nei Controlli di Accesso: Tasso di concessione eccezioni per ora: Mattina 2.3%, Pomeriggio 7.1% (aumento del 309%).

Fonte di Dati 3 - Risposta agli Allarmi di Sicurezza: Tempo medio di risposta: Mattina 12 min, Pomeriggio 28 min (aumento del 133%).

Logica di Scoring:

- Pattern circadiano confermato in tutte le fonti
- Picco di vulnerabilità 1600-2000 mostra >100% di degradazione
- Rientra nella soglia GIALLO (equivalente al tasso di eccezione 5-15%)
- **Punteggio Finale: 1 (Giallo)**

Esempio 3: Indicatore Cognitivo 5.1 (Alert Fatigue)

Fonte di Dati 1 - Dati SIEM degli Allarmi: Allarmi giornalieri: media 847. Tasso di investigazione: 96% (settimana 1) → 23% (settimana 12).

Fonte di Dati 2 - Dati delle Interviste: Auto-riportato dagli analisti: "Ignoro automaticamente la maggior parte degli allarmi bassi/medi senza leggerli."

Fonte di Dati 3 - Analisi degli Incidenti: 3 violazioni confermate originate da allarmi ignorati negli ultimi 90 giorni.

Logica di Scoring:

- Il tasso di investigazione è sceso del 76% indicando grave affaticamento
- Impatto di sicurezza confermato da allarmi ignorati
- Desensibilizzazione auto-riportata conferma problema sistematico
- **Punteggio Finale: 2 (Rosso)**

3 Scoring a Livello di Dominio

3.1 Calcolo del Punteggio di Dominio

Il framework CPF organizza 100 indicatori in 10 domini di 10 indicatori ciascuno. Lo scoring a livello di dominio aggrega i punteggi dei singoli indicatori.

Per il dominio d contenente gli indicatori i_1 fino a i_{10}:

$$\text{Punteggio\_Dominio}_d = \sum_{i=1}^{10} \text{Indicatore}_i \tag{2}$$

dove ogni Indicatore$_i \in \{0, 1, 2\}$

Intervallo di Punteggio: 0-20 per dominio

Soglie di Interpretazione:

- **0-6 (Verde)**: Bassa vulnerabilità, monitoraggio standard
- **7-13 (Giallo)**: Vulnerabilità moderata, monitoraggio rafforzato
- **14-20 (Rosso)**: Alta vulnerabilità, remediation immediata

3.2 Esempi di Punteggio di Dominio

Tabella 1: Esempio di Punteggi di Dominio

Dominio	**Codice**	**Punteggio**	**Stato**
Basato sull'Autorità	[1.x]	8/20	Giallo
Temporale	[2.x]	14/20	Rosso
Influenza Sociale	[3.x]	5/20	Verde
Affettivo	[4.x]	11/20	Giallo
Sovraccarico Cognitivo	[5.x]	16/20	Rosso
Dinamiche di Gruppo	[6.x]	7/20	Giallo
Risposta allo Stress	[7.x]	12/20	Giallo
Processo Inconscio	[8.x]	4/20	Verde
Bias Specifici dell'IA	[9.x]	9/20	Giallo
Stati Convergenti	[10.x]	6/20	Verde

4 Punteggio CPF Complessivo

4.1 Formula di Aggregazione Pesata

Il Punteggio CPF complessivo aggrega tutti i punteggi di dominio utilizzando pesi empiricamente validati.

$$\text{Punteggio\_CPF} = 100 - \left(\sum_{d=1}^{10} w_d \times \text{Punteggio\_Dominio}_d \right) \times 2.5 \tag{3}$$

dove:

- w_d = peso empiricamente validato per il dominio d
- $\sum_{d=1}^{10} w_d = 1.0$ (i pesi sommano all'unità)
- Il fattore di moltiplicazione 2.5 scala all'intervallo 0-100

Punteggi CPF più alti indicano migliore resilienza psicologica.

4.2 Pesi dei Domini (Empiricamente Validati)

Basati sulla correlazione con incidenti di sicurezza reali in 127 organizzazioni:

Tabella 2: Pesi dei Domini CPF

Dominio	**Peso**	**Razionale**
Autorità [1.x]	0.15	Massima correlazione con social engineering (r=0.847)
Temporale [2.x]	0.12	Forte predittore di bypass da scadenze (r=0.823)
Influenza Sociale [3.x]	0.11	Abilitatore chiave delle minacce interne (r=0.791)
Affettivo [4.x]	0.10	Correlazione moderata con errori decisionali (r=0.712)
Sovraccarico Cognitivo [5.x]	0.11	Forte predittore di sfruttamento dell'alert fatigue (r=0.834)
Dinamiche di Gruppo [6.x]	0.09	Fattore di rischio organizzativo moderato (r=0.678)
Risposta allo Stress [7.x]	0.10	Correlazione moderata con fallimenti nella risposta agli incidenti (r=0.756)
Processo Inconscio [8.x]	0.08	Vulnerabilità più bassa ma persistente (r=0.623)
Specifico IA [9.x]	0.07	Vettore di minaccia emergente
Stati Convergenti [10.x]	0.07	Moltiplicatore di rischio

4.3 Interpretazione del Punteggio CPF

Tabella 3: Intervalli del Punteggio CPF

Punteggio	**Valutazione**	**Livello di Rischio**
80-100	Eccellente	Minimo
60-79	Buono	Basso-Moderato
40-59	Discreto	Moderato-Alto
20-39	Scarso	Alto
0-19	Critico	Grave

4.4 Esempio di Calcolo

Utilizzando i punteggi di dominio dalla Tabella 1:

$$\begin{aligned}\text{Somma Pesata} &= (8 \times 0.15) + (14 \times 0.12) + (5 \times 0.11) + (11 \times 0.10) \\ &\quad + (16 \times 0.11) + (7 \times 0.09) + (12 \times 0.10) \\ &\quad + (4 \times 0.08) + (9 \times 0.07) + (6 \times 0.07) \\ &= 9.49\end{aligned}$$

$$\text{Punteggio\_CPF} = 100 - (9.49 \times 2.5) = 76.28 \tag{4}$$

Risultato: Punteggio 76.28 = valutazione "Buono" (intervallo 60-79). Rischio basso-moderato con lacune nei domini Temporale e Sovraccarico Cognitivo.

5 Quozienti Specifici di Dominio

5.1 Concetto e Scopo

I Quozienti di Dominio forniscono una valutazione granulare che consente la pianificazione di interventi mirati. Ogni quoziente incorpora la pesatura specifica dell'indicatore basata sulla correlazione empirica con lo sfruttamento.

Formula generale:

$$\text{QD}_d = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{5}$$

5.2 Quoziente di Resilienza all'Autorità (QRA)

Misura la resistenza organizzativa allo sfruttamento basato sull'autorità.

$$\text{QRA}_{\text{base}} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{6}$$

Pesi degli Indicatori (Dominio Autorità):

Tabella 4: Pesi QRA

Indicatore	**Codice**	**Peso**
Conformità Acritica	1.1	0.18
Diffusione della Responsabilità	1.2	0.12
Impersonificazione dell'Autorità	1.3	0.15
Bypass per Superiori	1.4	0.10
Conformità Basata sulla Paura	1.5	0.11
Gradiente di Autorità	1.6	0.09
Autorità Tecnica	1.7	0.08
Eccezioni Dirigenziali	1.8	0.07
Riprova Sociale dell'Autorità	1.9	0.06
Escalation di Crisi	1.10	0.04

Aggiustamento Culturale:

$$\text{QRA}_{\text{aggiustato}} = \text{QRA}_{\text{base}} \times C_{\text{fattore}} \tag{7}$$

$$C_{\text{fattore}} = 1 + 0.3 \times \left(\frac{\text{PDI} - 50}{50}\right) + 0.2 \times \left(\frac{\text{UAI} - 50}{50}\right) \tag{8}$$

dove PDI = Indice di Distanza dal Potere, UAI = Indice di Evitamento dell'Incertezza (Hofstede).

5.3 Quoziente di Vulnerabilità Temporale (QVT)

$$\text{QVT} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{9}$$

Pesi: 2.1 (0.16), 2.2 (0.14), 2.3 (0.13), 2.4 (0.11), 2.5 (0.10), 2.6 (0.12), 2.7 (0.09), 2.8 (0.08), 2.9 (0.04), 2.10 (0.03)

5.4 Quoziente di Influenza Sociale (QIS)

$$\text{QIS} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{10}$$

Pesi: 3.1 (0.15), 3.2 (0.13), 3.3 (0.14), 3.4 (0.12), 3.5 (0.11), 3.6 (0.10), 3.7 (0.09), 3.8 (0.08), 3.9 (0.05), 3.10 (0.03)

5.5 Quoziente di Vulnerabilità Affettiva (QVA)

$$\text{QVA} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{11}$$

Pesi: 4.1 (0.14), 4.2 (0.12), 4.3 (0.13), 4.4 (0.11), 4.5 (0.10), 4.6 (0.09), 4.7 (0.11), 4.8 (0.08), 4.9 (0.07), 4.10 (0.05)

5.6 Quoziente di Sovraccarico Cognitivo (QSC)

$$\text{QSC} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{12}$$

Pesi: 5.1 (0.16), 5.2 (0.14), 5.3 (0.12), 5.4 (0.11), 5.5 (0.10), 5.6 (0.09), 5.7 (0.11), 5.8 (0.08), 5.9 (0.06), 5.10 (0.03)

5.7 Quoziente di Dinamiche di Gruppo (QDG)

$$\text{QDG} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{13}$$

Pesi: 6.1 (0.15), 6.2 (0.13), 6.3 (0.12), 6.4 (0.10), 6.5 (0.11), 6.6 (0.12), 6.7 (0.09), 6.8 (0.08), 6.9 (0.06), 6.10 (0.04)

5.8 Quoziente di Risposta allo Stress (QRS)

$$\text{QRS} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{14}$$

Pesi: 7.1 (0.15), 7.2 (0.14), 7.3 (0.12), 7.4 (0.11), 7.5 (0.13), 7.6 (0.10), 7.7 (0.09), 7.8 (0.08), 7.9 (0.05), 7.10 (0.03)

5.9 Quoziente di Processo Inconscio (QPI)

$$\text{QPI} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{15}$$

Pesi: 8.1 (0.14), 8.2 (0.13), 8.3 (0.12), 8.4 (0.11), 8.5 (0.10), 8.6 (0.12), 8.7 (0.09), 8.8 (0.08), 8.9 (0.07), 8.10 (0.04)

5.10 Quoziente di Bias Specifico IA (QIA)

$$\text{QIA} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{16}$$

Pesi: 9.1 (0.16), 9.2 (0.15), 9.3 (0.12), 9.4 (0.11), 9.5 (0.10), 9.6 (0.11), 9.7 (0.09), 9.8 (0.08), 9.9 (0.05), 9.10 (0.03)

5.11 Quoziente di Stato Convergente (QSC)

$$\text{QSC} = 20 - \sum_{i=1}^{10} w_i \times I_i \tag{17}$$

Pesi: 10.1 (0.18), 10.2 (0.15), 10.3 (0.13), 10.4 (0.12), 10.5 (0.10), 10.6 (0.09), 10.7 (0.08), 10.8 (0.07), 10.9 (0.05), 10.10 (0.03)

6 Indice di Convergenza

6.1 Definizione Matematica

L'Indice di Convergenza (IC) misura il rischio moltiplicativo quando più vulnerabilità si allineano:

$$\text{IC} = \prod_{i=1}^{n} (1 + v_i) \tag{18}$$

dove:

- v_i = punteggio di vulnerabilità normalizzato solo per indicatori vulnerabili
- n = numero di indicatori in stato Giallo o Rosso
- Normalizzazione: v_i = Punteggio_Indicatore/2 (Rosso=1.0, Giallo=0.5)

6.2 Interpretazione delle Soglie

6.3 Rilevamento della Tempesta Perfetta

Stato convergente critico identificato quando:

- 3 o più domini in stato Rosso simultaneamente

Tabella 5: Soglie dell'Indice di Convergenza

Intervallo IC	**Rischio**	**Azione Richiesta**
$IC < 2$	Basso	Monitoraggio standard
$2 \leq IC < 5$	Moderato	Monitoraggio rafforzato
$5 \leq IC < 10$	Alto	Intervento immediato
$IC \geq 10$	Critico	Risposta di emergenza

- Indice di Convergenza > 8
- Alti punteggi di interdipendenza tra domini vulnerabili

Esempio di Tempesta Perfetta:

- Autorità [1.x]: Rosso (punteggio 16/20)
- Temporale [2.x]: Rosso (punteggio 15/20)
- Risposta allo Stress [7.x]: Rosso (punteggio 14/20)
- $IC = (1 + 0.8) \times (1 + 0.75) \times (1 + 0.7) = 5.35$

6.4 Esempi di Calcolo

Scenario 1 - Bassa Convergenza:

L'organizzazione ha 5 indicatori Gialli distribuiti su 5 domini.

$$IC = (1 + 0.5)^5 = 7.59$$

Rientra nell'intervallo Moderato. Monitorare ma nessuna crisi immediata.

Scenario 2 - Alta Convergenza:

L'organizzazione ha 3 domini Rossi più 2 Gialli.

$$IC = (1 + 1.0) \times (1 + 1.0) \times (1 + 1.0) \times (1 + 0.5) \times (1 + 0.5) = 18.0$$

Convergenza critica che richiede risposta di emergenza.

Scenario 3 - Tempesta Perfetta:

4 indicatori Rossi nello stesso dominio più 2 Rossi in un altro.

$$IC = (1 + 1.0)^6 = 64$$

Convergenza catastrofica - violazione imminente probabile.

7 Calibrazione Specifica per Settore

7.1 Razionale della Calibrazione

Diversi settori mostrano differenze di base nelle vulnerabilità dovute all'ambiente normativo, cultura organizzativa, caratteristiche della superficie di attacco, disponibilità di risorse e tolleranza al rischio.

7.2 Fattori di Calibrazione

Tabella 6: Fattori di Calibrazione per Settore

Settore	**Fattore**	**Giustificazione**
Servizi Finanziari	1.15	Alta pressione normativa, gerarchie complesse
Sanità	1.20	Gerarchie mediche, stress critico per la vita
Governo	1.25	Strutture burocratiche, avversione al rischio
Tecnologia	0.85	Strutture più piatte, consapevolezza della sicurezza
Vendita al Dettaglio	1.00	Baseline (settore di riferimento)
Manifatturiero	1.05	Gerarchie tradizionali, focus operativo
Energia/Utilities	1.10	Infrastrutture critiche, cultura della sicurezza
Istruzione	0.95	Libertà accademica, gerarchia limitata

7.3 Applicazione

$$\text{Punteggio\_Aggiustato} = \text{Punteggio\_Base} \times \text{Fattore\_Settore} \tag{19}$$

Esempio:

- Punteggio CPF Base: 65 (Buono)
- Settore: Servizi Finanziari (fattore 1.15)
- Punteggio Aggiustato: $65 \times 1.15 = 74.75 \rightarrow$ Ancora Buono, intervallo superiore

La calibrazione riconosce che un punteggio di 65 nei Servizi Finanziari rappresenta una resilienza effettiva più alta di 65 nella Tecnologia a causa del baseline di vulnerabilità intrinsecamente più alto.

Parte II

Modello di Maturità CPF

8 Panoramica del Modello

8.1 Scopo

Il Modello di Maturità CPF fornisce alle organizzazioni un percorso strutturato per valutare e migliorare la resilienza psicologica contro le minacce cyber. Basato sui 100 indicatori del framework, questo modello definisce sei livelli di maturità attraverso i quali le organizzazioni progrediscono mentre sviluppano sofisticate capacità di gestione delle vulnerabilità pre-cognitive.

8.2 Principi Fondamentali

- **Miglioramento Progressivo**: Ogni livello si costruisce sulle capacità precedenti
- **Basato su Evidenze**: La maturità è dimostrata attraverso risultati misurabili
- **Copertura Olistica**: Affronta tutte le 10 categorie di vulnerabilità CPF
- **Implementazione Pratica**: Requisiti attuabili a ogni livello
- **Miglioramento Continuo**: Rivalutazione regolare e avanzamento

9 Livelli di Maturità

9.1 Livello 0: Inconsapevole

"Punto Cieco Psicologico"

Caratteristiche:

- Nessun riconoscimento dei fattori psicologici nella cybersecurity
- Sicurezza focalizzata interamente sui controlli tecnici
- Fattori umani incolpati post-incidente senza analisi sistematica
- Nessuna raccolta dati sulle vulnerabilità psicologiche

Profilo di Rischio: CRITICO

- Probabilità di Incidente: 85% annuo
- Moltiplicatore del Costo Medio di Violazione: 3.5x media di settore
- Tempo di Recupero: 2-3x più lungo delle organizzazioni mature

9.2 Livello 1: Iniziale

"Risveglio"

Caratteristiche:

- Consapevolezza di base che la psicologia impatta la sicurezza
- Formazione sulla consapevolezza della sicurezza ad-hoc
- Risposta reattiva allo sfruttamento psicologico
- Comprensione limitata delle vulnerabilità pre-cognitive

Capacità Richieste:

- Briefing di consapevolezza dirigenziale sul CPF completato
- Valutazione CPF iniziale condotta (minimo 20 indicatori)
- Fattori psicologici inclusi nei report degli incidenti
- Programma di consapevolezza della sicurezza include concetti base di psicologia

Metriche:

- Punteggio CPF: >20/100 (Indicatori Rossi <40%)
- Copertura: Minimo 3/10 categorie valutate
- Frequenza: Valutazione annuale
- Formazione: 50% del personale con consapevolezza di base

Organizzazioni Tipiche:

- PMI che iniziano il percorso di sicurezza
- Aziende dopo il primo grande incidente

Investimento Richiesto: €25-50k valutazione iniziale

9.3 Livello 2: In Sviluppo

"Costruire le Fondamenta"

Caratteristiche:

- Valutazione sistematica delle vulnerabilità psicologiche
- Interventi mirati per indicatori ad alto rischio
- Integrazione con framework di sicurezza esistenti
- Monitoraggio regolare delle metriche psicologiche chiave

Capacità Richieste:

- Valutazione CPF completa (100 indicatori) completata
- Mappa di calore delle vulnerabilità psicologiche mantenuta
- Playbook di risposta includono fattori psicologici
- Team di sicurezza formato in psicologia di base

Metriche:

- Punteggio CPF: >40/100 (Indicatori Rossi <25%)
- Copertura: 7/10 categorie attivamente monitorate
- Frequenza: Valutazione trimestrale
- Formazione: 75% del personale, inclusi moduli specializzati

Criteri di Avanzamento:

- 6 mesi al Livello 1
- Sponsorizzazione dirigenziale assicurata
- Budget allocato per interventi psicologici
- Riduzione misurabile nel successo del social engineering (>30%)

Organizzazioni Tipiche:

- Imprese di medie dimensioni
- Settori regolamentati (conformità iniziale)

Investimento Richiesto: €100-250k annualmente

9.4 Livello 3: Definito

"Approccio Sistematico"

Caratteristiche:

- Gestione proattiva delle vulnerabilità psicologiche
- Analisi predittive per periodi ad alto rischio
- Integrazione interfunzionale (HR, IT, Risk)
- Interventi personalizzati per ruolo/dipartimento

Capacità Richieste:

- Dashboard di monitoraggio CPF in tempo reale
- Modelli predittivi per stati di vulnerabilità
- Fattori psicologici nella valutazione del rischio dei fornitori

- Simulazione di incidenti include scenari psicologici
- Valutazione culturale integrata con CPF

Metriche:

- Punteggio CPF: >60/100 (Nessun indicatore rosso >30 giorni)
- Copertura: 10/10 categorie con KPI
- Frequenza: Valutazione mensile, monitoraggio giornaliero
- Formazione: 90% del personale + certificazioni specializzate
- Tempo di Risposta: <4 ore per indicatori psicologici

Capacità Avanzate:

- Riconoscimento di pattern basato su IA
- Integrazione di analisi comportamentali
- Stress testing per la resilienza psicologica
- Reporting CPF a livello di consiglio

Organizzazioni Tipiche:

- Grandi imprese
- Servizi finanziari
- Infrastrutture critiche

Investimento Richiesto: €500k-1M annualmente

9.5 Livello 4: Gestito

"Controllato Quantitativamente"

Caratteristiche:

- Gestione quantitativa dei rischi psicologici
- Ottimizzazione continua basata sui dati
- Leadership nel benchmark di settore
- Resilienza psicologica come vantaggio competitivo

Capacità Richieste:

- Previsione delle vulnerabilità basata su ML (>80% accuratezza)
- Trigger di intervento automatizzati
- Metriche di sicurezza psicologica a livello organizzativo

- Valutazione del rischio psicologico di terze parti
- CPF integrato con i prezzi delle assicurazioni cyber

Metriche:

- Punteggio CPF: >80/100 (Intervento proattivo prima del giallo)
- Accuratezza Predittiva: >80% per gli incidenti
- Copertura: Monitoraggio in tempo reale di tutti gli indicatori
- Formazione: 100% del personale + 25% professionisti certificati
- ROI: Dimostrabile 5:1 sugli interventi psicologici

Leadership di Settore:

- Casi di studio pubblicati
- Partecipazione al benchmarking tra peer
- Riconoscimento normativo
- Riduzioni dei premi assicurativi (>20%)

Organizzazioni Tipiche:

- Leader Fortune 500
- Contractor della difesa
- Istituzioni finanziarie globali

Investimento Richiesto: €1-2.5M annualmente

9.6 Livello 5: Ottimizzazione

"Eccellenza Adattiva"

Caratteristiche:

- Sistema di difesa psicologica auto-migliorante
- Innovazione nei metodi di sicurezza psicologica
- Thought leadership di settore
- Resilienza ad attacchi psicologici sconosciuti/zero-day

Capacità Richieste:

- Sistemi di difesa psicologica autonomi
- Contributo alla ricerca per l'evoluzione del CPF
- Condivisione di intelligence sulle minacce cross-industry

- Laboratorio di innovazione sulla sicurezza psicologica
- Chief Psychology Officer (CPO) certificato a livello di consiglio

Metriche:

- Punteggio CPF: >90/100 (Stato verde continuo)
- Innovazione: 2+ nuovi metodi pubblicati annualmente
- Previsione: >95% accuratezza, inclusi attacchi nuovi
- Certificazione: 50%+ del personale certificato CPF
- Influenza: Contributo agli standard di settore

Indicatori di Eccellenza:

- Zero exploit psicologici riusciti (12+ mesi)
- Le compagnie assicurative lo usano come benchmark
- I framework normativi fanno riferimento alle pratiche
- Partnership di ricerca accademica
- Depositi di brevetti per metodi di sicurezza psicologica

Organizzazioni Tipiche:

- Giganti tecnologici
- Agenzie di sicurezza nazionale
- Banche di importanza sistemica globale (G-SIB)

Investimento Richiesto: €2.5M+ annualmente

10 Percorsi di Progressione

10.1 Timeline Tipica

10.2 Acceleratori

- **Campione Dirigenziale**: Sponsor C-level riduce la timeline del 30%
- **Incidente Maggiore**: Urgenza post-violazione accelera del 40%
- **Requisito Normativo**: Mandato di conformità guida adozione più veloce
- **Attività M&A**: Requisiti di due diligence accelerano la maturità
- **Assicurazione Cyber**: Incentivi sui premi guidano la progressione

Tabella 7: Timeline di Transizione dei Livelli di Maturità

Transizione	Durata	Sfide Principali
$0 \rightarrow 1$	3-6 mesi	Buy-in dirigenziale, valutazione iniziale
$1 \rightarrow 2$	6-12 mesi	Allocazione risorse, sviluppo competenze
$2 \rightarrow 3$	12-18 mesi	Integrazione processi, cambiamento culturale
$3 \rightarrow 4$	18-24 mesi	Quantificazione, automazione
$4 \rightarrow 5$	24+ mesi	Innovazione, thought leadership

10.3 Bloccanti Comuni

- Mancanza di competenze psicologiche nel team di sicurezza
- Resistenza organizzativa ai fattori "soft"
- Vincoli di budget per controlli non tecnici
- Preoccupazioni sulla privacy riguardo la valutazione psicologica
- Complessità di integrazione con framework esistenti

11 Metodologia di Valutazione

11.1 Framework di Scoring

Pesi delle Dimensioni:

- Copertura (25%): Quante categorie CPF valutate
- Profondità (25%): Completezza della valutazione per categoria
- Integrazione (20%): Incorporazione nelle operazioni di sicurezza
- Efficacia (20%): Riduzione del rischio misurabile
- Innovazione (10%): Approcci nuovi e contributi

11.2 Requisiti di Evidenza

Evidenza Documentale:

- Report di valutazione con timestamp
- Piani di intervento e risultati
- Registri di formazione e certificazioni
- Report di incidenti con fattori psicologici
- Presentazioni al consiglio/dirigenza

Evidenza Tecnica:

- Screenshot delle dashboard
- Configurazioni degli allarmi
- API di integrazione
- Report di accuratezza dei modelli predittivi
- Log di risposta automatizzata

Evidenza dei Risultati:

- Metriche di riduzione degli incidenti
- Documentazione dei risparmi sui costi
- Aggiustamenti dei premi assicurativi
- Punteggi di feedback dei dipendenti
- Confronti benchmark

12 Benchmark di Settore

12.1 Distribuzione per Settore (Baseline 2025)

Tabella 8: Distribuzione dei Livelli di Maturità per Settore

Settore	L0	L1	L2	L3	L4	L5
Servizi Finanziari	5%	15%	35%	30%	12%	3%
Sanità	25%	35%	25%	12%	3%	0%
Tecnologia	10%	20%	30%	25%	12%	3%
Governo	15%	30%	30%	20%	5%	0%
Vendita al Dettaglio	40%	30%	20%	8%	2%	0%
Manifatturiero	45%	30%	15%	8%	2%	0%
Energia/Utilities	10%	25%	35%	25%	5%	0%

12.2 Correlazione della Maturità con i Risultati di Sicurezza

Tabella 9: Risultati di Sicurezza per Livello di Maturità

Livello	Probabilità Violazione	Perdita Media	Recupero
Livello 0	85% annuo	€8.5M	287 giorni
Livello 1	65% annuo	€5.2M	198 giorni
Livello 2	40% annuo	€3.1M	123 giorni
Livello 3	20% annuo	€1.8M	67 giorni
Livello 4	8% annuo	€0.9M	23 giorni
Livello 5	<2% annuo	€0.3M	<24 ore

13 Roadmap di Implementazione

13.1 Guida Rapida all'Avvio (Primi 90 Giorni)

Giorni 1-30: Valutazione

- Briefing dirigenziale sul Modello di Maturità CPF
- Valutazione rapida (20 indicatori critici)
- Analisi delle lacune rispetto al livello target
- Sviluppo del business case

Giorni 31-60: Pianificazione

- Allocazione delle risorse
- Formazione del team (sicurezza + psicologia)
- Selezione dei fornitori per strumenti/formazione
- Creazione della roadmap con milestone

Giorni 61-90: Lancio

- Interventi iniziali per le lacune critiche
- Campagna di comunicazione
- Avvio del programma di formazione
- Metriche baseline stabilite

13.2 Percorso di Certificazione

CPF-F (Foundation) - Livello 1

- Formazione di 2 giorni
- Esame di 60 domande
- Investimento €500
- Rinnovo annuale

CPF-P (Practitioner) - Livello 2-3

- Formazione di 5 giorni + practicum
- Esame di 100 domande + caso di studio
- Investimento €1,500
- 40 ore CPE richieste

CPF-E (Expert) - Livello 4

- Formazione avanzata di 10 giorni
- Presentazione di tesi
- Investimento €3,500
- Contributo al framework richiesto

CPF-M (Master) - Livello 5

- Solo su invito
- Ricerca pubblicata richiesta
- Riconoscimento di settore
- Plasma l'evoluzione del framework

14 Modello di Calcolo del ROI

14.1 Costi-Benefici per Livello

Tabella 10: Analisi ROI per Transizione di Maturità

Transizione	Investimento	Beneficio Annuo	Payback	VAN 5 Anni
$0 \rightarrow 1$	€50k	€200k	3 mesi	€850k
$1 \rightarrow 2$	€250k	€600k	5 mesi	€2.5M
$2 \rightarrow 3$	€750k	€1.5M	6 mesi	€5.8M
$3 \rightarrow 4$	€1.5M	€3M	6 mesi	€12M
$4 \rightarrow 5$	€2.5M	€5M	6 mesi	€20M

14.2 Componenti del Calcolo

Riduzione dei Costi:

- Prevenzione incidenti (frequenza $\times$ costo medio)
- Recupero più veloce (downtime ridotto)
- Premi assicurativi più bassi
- Riduzione delle sanzioni di conformità

Protezione dei Ricavi:

- Retention dei clienti (fattore fiducia)
- Vantaggio competitivo
- Premio di valutazione M&A
- Punteggio di preferenza dei fornitori

Guadagni di Efficienza:

- Risposta automatizzata alle minacce
- Riduzione dei falsi positivi
- Spesa di sicurezza ottimizzata
- Costi di audit ridotti

15 Allineamento Normativo

15.1 Mappatura della Conformità

Tabella 11: Requisiti di Conformità Normativa

Regolamento	Livello Min.	Raccomandato	Premium
GDPR Articolo 32	Livello 1	Livello 2	Livello 3
Direttiva NIS2	Livello 2	Livello 3	Livello 4
DORA (Finanziario)	Livello 2	Livello 3	Livello 4
CCPA	Livello 1	Livello 2	Livello 3
ISO 27001:2022	Livello 1	Livello 2	Livello 3
SOC 2 Tipo II	Livello 2	Livello 3	Livello 4
PCI DSS v4.0	Livello 1	Livello 2	Livello 3

15.2 Vantaggi di Audit

Benefici Livello 3+:

- Evidenza di controllo pre-approvata
- Durata dell'audit ridotta (30-40%)
- Meno findings e osservazioni
- Scoring di fiducia normativa
- Rinnovo certificazione fast-track

Parte III

Integrazione Scoring-Maturità

16 Soglie di Punteggio per Livello di Maturità

Tabella 12: Requisiti di Scoring per Livello di Maturità

Livello	Punteggio CPF Min	Domini Rossi Max	IC Max	Certificazione
Livello 0	0-19	Nessun limite	>10	Nessuna
Livello 1	20-39	≤8	<10	CPF-F idoneo
Livello 2	40-59	≤5	<8	CPF-P idoneo
Livello 3	60-79	≤2	<5	CPF-P richiesto
Livello 4	80-89	0	<3	CPF-E idoneo
Livello 5	90-100	0	<2	CPF-M idoneo

17 Requisiti di Progressione

Per avanzare dal Livello N al Livello N+1:

- Raggiungere la soglia minima del Punteggio CPF
- Mantenere il punteggio per la durata minima (3-6 mesi)
- Ridurre gli indicatori Rossi sotto il massimo
- Dimostrare riduzione misurabile degli incidenti
- Completare la formazione/certificazione richiesta
- Superare audit indipendente

18 Ciclo di Miglioramento Continuo

1. **Valutare**: Calcolo trimestrale del Punteggio CPF
2. **Analizzare**: Identificare i domini con performance bassa
3. **Intervenire**: Implementare remediation mirata
4. **Monitorare**: Tracciare i miglioramenti degli indicatori
5. **Validare**: Verificare il miglioramento del punteggio
6. **Certificare**: Ottenere il riconoscimento del livello di maturità

Tabella 13: Template di Scoring del Dominio

Indicatore	Punteggio (0/1/2)	Peso	Punteggio Pesato
X.1	___	w_1	___
X.2	___	w_2	___
X.3	___	w_3	___
...	...	...	...
X.10	___	w_{10}	___
Totale			___/20

A Schede di Lavoro per lo Scoring

A.1 Scheda di Calcolo del Punteggio di Dominio

A.2 Scheda di Calcolo del Punteggio CPF

$$\begin{aligned}\text{Somma Pesata} &= \sum_{d=1}^{10} w_d \times \text{Punteggio\_Dominio}_d \\ &= (\_\_\_ \times 0.15) + (\_\_\_ \times 0.12) + ... \\ &= \_\_\_\end{aligned}$$

$$\text{Punteggio\_CPF} = 100 - (\text{Somma Pesata} \times 2.5) = \_\_\_$$

B Checklist di Valutazione della Maturità

B.1 Checklist Livello 1

- ☐ Briefing di consapevolezza dirigenziale completato
- ☐ Valutazione CPF iniziale (20+ indicatori)
- ☐ Fattori psicologici nei report degli incidenti
- ☐ Psicologia di base nel programma di awareness
- ☐ Punteggio CPF > 20
- ☐ 3+ categorie valutate

B.2 Checklist Livello 2

- ☐ Valutazione completa di 100 indicatori completata
- ☐ Mappa di calore delle vulnerabilità mantenuta
- ☐ Fattori psicologici nei playbook di risposta
- ☐ Formazione in psicologia per il team di sicurezza
- ☐ Punteggio CPF > 40

☐ 7+ categorie monitorate

☐ Valutazione trimestrale stabilita

B.3 Checklist Livello 3

☐ Dashboard CPF in tempo reale operativa

☐ Modelli predittivi implementati

☐ Integrazione interfunzionale (HR/IT/Risk)

☐ Interventi specifici per ruolo implementati

☐ Punteggio CPF > 60

☐ Tutte le 10 categorie con KPI

☐ Valutazione mensile + monitoraggio giornaliero

C Tabelle Dati di Benchmark

C.1 Distribuzione del Punteggio CPF per Settore

Tabella 14: Benchmark del Punteggio CPF (Media ± DS)

Settore	**Punteggio Medio**	**75° Percentile**
Servizi Finanziari	68 ± 12	76
Sanità	52 ± 15	63
Tecnologia	71 ± 11	78
Governo	58 ± 14	67
Vendita al Dettaglio	48 ± 13	56
Manifatturiero	54 ± 12	62
Energia/Utilities	63 ± 13	72

D Glossario

QRA (Quoziente di Resilienza all'Autorità): Quoziente specifico di dominio che misura la resistenza allo sfruttamento basato sull'autorità.

Indice di Convergenza (IC): Metrica di rischio moltiplicativo che misura l'allineamento di vulnerabilità multiple.

Punteggio CPF: Punteggio complessivo di vulnerabilità psicologica organizzativa (scala 0-100, più alto = migliore resilienza).

Quoziente di Dominio (QD): Metrica di resilienza specifica per categoria (scala 0-20).

Livello di Maturità: Livello di capacità organizzativa (0-5) nella gestione delle vulnerabilità psicologiche.

Vulnerabilità Pre-Cognitiva: Debolezza psicologica che opera sotto la consapevolezza cosciente.

Scoring Ternario: Valutazione della vulnerabilità a tre livelli (Verde/Giallo/Rosso o 0/1/2).

Riferimenti bibliografici

[1] Canale, G. (2025). CPF-27001:2025 Sistema di Gestione delle Vulnerabilità Psicologiche – Requisiti.

[2] Canale, G. (2025). The Cybersecurity Psychology Framework. *SSRN Electronic Journal*.

[3] Milgram, S. (1974). *Obedience to authority*. New York: Harper & Row.

[4] Bion, W. R. (1961). *Experiences in groups*. London: Tavistock Publications.

[5] Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

[6] Klein, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psychoanalysis*, 27, 99-110.

[7] Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.

[8] Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon Enterprise Solutions.

[9] Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Thousand Oaks, CA: Sage Publications.

[10] Jung, C. G. (1969). *The Archetypes and the Collective Unconscious*. Princeton: Princeton University Press.