# CPF-27001:2025

Sistema di Gestione delle Vulnerabilità Psicologiche
Requisiti

Giuseppe Canale, CISSP
Ricercatore Indipendente
g.canale@cpf3.org

Gennaio 2025

**Sommario**

Questo documento specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un Sistema di Gestione delle Vulnerabilità Psicologiche (PVMS) all'interno delle organizzazioni. CPF-27001:2025 affronta il gap critico nei framework di cybersecurity fornendo requisiti sistematici per identificare e mitigare le vulnerabilità psicologiche pre-cognitive che contribuiscono all'82-85% degli incidenti di sicurezza. A differenza degli standard tradizionali di security awareness che si concentrano sul processo decisionale conscio, CPF-27001 stabilisce requisiti per valutare i processi inconsci, le dinamiche di gruppo e gli stati affettivi che abilitano il social engineering e le violazioni legate al fattore umano. Lo standard è applicabile a tutte le organizzazioni indipendentemente dal tipo, dimensione o natura, ed è progettato per integrarsi perfettamente con ISO/IEC 27001:2022 e NIST Cybersecurity Framework 2.0.

**Parole chiave:** vulnerabilità psicologica, cybersecurity, fattori umani, ISO 27001, gestione della sicurezza, assessment pre-cognitivo

## Indice

# 1 Introduzione

## 1.1 Contesto e Background

Nonostante la crescita esponenziale degli investimenti in cybersecurity che superano i $150 miliardi annualmente, le violazioni di successo continuano ad aumentare, con i fattori umani che contribuiscono all'82-85% degli incidenti secondo il Verizon Data Breach Investigations Report. Questo fallimento persistente rivela un gap fondamentale negli attuali framework di sicurezza: mentre le vulnerabilità tecniche ricevono attenzione sistematica attraverso standard come ISO/IEC 27001:2022 e NIST Cybersecurity Framework 2.0, le vulnerabilità psicologiche rimangono non affrontate.

La ricerca neuroscientifica dimostra che le decisioni rilevanti per la sicurezza avvengono 300-500 millisecondi prima della consapevolezza cosciente, con il sistema di rilevamento delle minacce dell'amigdala che inizia le risposte prima che la corteccia prefrontale ingaggi il pensiero razionale. Questo processing pre-cognitivo, combinato con le dinamiche di gruppo inconsce identificate da Bion, Klein e Jung, crea vulnerabilità sistematiche che nessuna quantità di formazione sulla security awareness a livello conscio può affrontare.

I framework di sicurezza tradizionali assumono implicitamente modelli di attore razionale dove gli individui, quando informati dei rischi, modificano il comportamento di conseguenza. Questa assunzione non tiene conto di:

- **Processi pre-cognitivi** che determinano le decisioni prima della consapevolezza cosciente
- **Dinamiche di gruppo inconsce** che sovrastano il giudizio individuale sotto stress
- **Stati affettivi** che bypassano la valutazione razionale della sicurezza
- **Sovraccarico cognitivo** che forza la dipendenza da euristiche sfruttabili
- **Compliance basata sull'autorità** che innesca risposte automatiche alla gerarchia percepita

CPF-27001:2025 affronta questi gap stabilendo requisiti per l'assessment sistematico e la mitigazione delle vulnerabilità psicologiche, permettendo alle organizzazioni di raggiungere posture di sicurezza predittive che prevengono gli incidenti legati al fattore umano prima che si verifichino.

## 1.2 Relazione con Altri Standard

CPF-27001:2025 è progettato per complementare e migliorare i framework di sicurezza esistenti piuttosto che sostituirli. Lo standard si integra con:

**ISO/IEC 27001:2022**: CPF-27001 affronta la Clausola 7.2 (Competenza) e la Clausola 7.3 (Consapevolezza) fornendo metodi sistematici per valutare i fattori psicologici che influenzano il comportamento di sicurezza.

**ISO/IEC 27002:2022**: Mentre ISO/IEC 27002 fornisce guida all'implementazione dei controlli di sicurezza, non affronta i fattori psicologici che determinano l'efficacia dei controlli.

**NIST Cybersecurity Framework 2.0**: CPF-27001 si mappa direttamente alle funzioni NIST CSF 2.0 fornendo il livello di intelligenza psicologica che migliora l'efficacia di ciascuna funzione.

### 1.3 Struttura di Questo Documento

Questo documento segue la struttura delle Direttive ISO/IEC con clausole numerate che specificano i requisiti. I requisiti sono espressi usando linguaggio normativo: “shall” indica requisiti obbligatori, “should” indica raccomandazioni e “may” indica permessi.

## 2 Ambito

### 2.1 Generale

Questo documento specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un Sistema di Gestione delle Vulnerabilità Psicologiche (PVMS) nel contesto dell’organizzazione. I requisiti specificati in CPF-27001:2025 sono generici e applicabili a tutte le organizzazioni, indipendentemente dal tipo, dimensione o natura.

### 2.2 Applicazione

CPF-27001:2025 deve essere applicato dalle organizzazioni che richiedono gestione sistematica dei rischi di sicurezza legati al fattore umano e cercano di integrare l’assessment delle vulnerabilità psicologiche con i framework di sicurezza esistenti.

### 2.3 Esclusioni

CPF-27001:2025 non affronta l’assessment delle vulnerabilità tecniche, l’architettura di sicurezza di rete, i controlli crittografici, le misure di sicurezza fisica, l’assessment psicologico clinico individuale o la gestione delle performance dei dipendenti.

## 3 Riferimenti Normativi

**ISO/IEC 27001:2022**, Sistemi di gestione della sicurezza delle informazioni — Requisiti

**ISO/IEC 27002:2022**, Codice di pratica per i controlli della sicurezza delle informazioni

**NIST Cybersecurity Framework 2.0**

**Milgram, S. (1974)**, Obedience to Authority

**Bion, W. R. (1961)**, Experiences in Groups

**Klein, M. (1946)**, Notes on some schizoid mechanisms

**Kahneman, D. (2011)**, Thinking, Fast and Slow

## 4 Termini e Definizioni

### 4.1 Termini Specifici CPF

**vulnerabilità pre-cognitiva**: Debolezza psicologica che opera al di sotto della consapevolezza cosciente e abilita lo sfruttamento della sicurezza prima che avvenga la valutazione razionale.

**sistema di gestione delle vulnerabilità psicologiche (PVMS)**: Parte del sistema di gestione per stabilire, implementare, operare, monitorare, revisionare, mantenere e migliorare la sicurezza psicologica.

**schema OFTLISRV**: Metodologia di implementazione sistematica che comprende Osservabili, Fonti Dati, Temporalità, Logica di Rilevamento, Interdipendenze, Soglie, Risposte e Validazione.

**stato convergente**: Condizione dove multiple vulnerabilità psicologiche si allineano simultaneamente, creando probabilità di violazione esponenzialmente aumentata.

**Authority Resilience Quotient (ARQ)**: Capacità misurata di mantenere scetticismo appropriato verso le rivendicazioni di autorità durante il processo decisionale rilevante per la sicurezza.

**basic assumption dependency (baD)**: Stato di gruppo inconscio caratterizzato dalla ricerca di protezione onnipotente e abdicazione della responsabilità personale per la sicurezza.

**basic assumption fight-flight (baF)**: Stato di gruppo inconscio caratterizzato dalla percezione delle minacce come nemici esterni che richiedono difesa aggressiva o evitamento completo.

**basic assumption pairing (baP)**: Stato di gruppo inconscio caratterizzato dalla speranza in una futura soluzione messianica piuttosto che affrontare le vulnerabilità attuali.

**behavioral risk indicator (BRI)**: Metrica quantificabile derivata dal comportamento osservabile che indica il livello di vulnerabilità psicologica.

**sistema di scoring ternario**: Metodologia di assessment che utilizza classificazione a tre stati (Green/Yellow/Red) corrispondenti a livelli di vulnerabilità minima, moderata e critica.

**differential privacy**: Framework matematico che assicura che la presenza o assenza dei dati di qualsiasi individuo cambi le probabilità di output al massimo di $e^{\varepsilon}$ dove $\varepsilon$ rappresenta il budget privacy.

**unità di aggregazione minima**: Dimensione del gruppo più piccola per cui i dati di assessment psicologico possono essere riportati, stabilita a dieci individui per prevenire la profilazione individuale.

**ritardo temporale**: Intervallo di tempo minimo tra la raccolta dati e la reportistica, stabilito a 72 ore per prevenire la sorveglianza in tempo reale.

### 4.2 Termini Psicologici

**processing Sistema 1**: Processing cognitivo veloce, automatico, inconscio che opera attraverso riconoscimento di pattern e risposta emotiva.

**processing Sistema 2**: Processing cognitivo lento, deliberato, conscio che richiede risorse e tempo significativi.

**amygdala hijack**: Stato neurologico dove il sistema di rilevamento delle minacce dell'amigdala sovrasta il processing razionale della corteccia prefrontale.

**carico cognitivo**: Quantità totale di sforzo mentale utilizzato nella memoria di lavoro.

**splitting**: Meccanismo di difesa primitivo dove il panorama della sicurezza è inconsciamente diviso in oggetti tutto-buono e tutto-cattivo.

**proiezione**: Attribuzione inconscia delle proprie caratteristiche negate su oggetti esterni.

**transfert**: Redirezione inconscia di sentimenti e attitudini da relazioni passate su autorità o sistemi di sicurezza presenti.

**groupthink**: Fenomeno psicologico dove il desiderio di armonia previene la valutazione critica.

**social proof**: Tendenza a conformarsi al comportamento altrui, specialmente sotto incertezza.

**reciprocità**: Obbligo di restituire favori che gli attaccanti sfruttano.

### 4.3 Acronimi

**CPF**: Cybersecurity Psychology Framework

**PVMS**: Psychological Vulnerability Management System

**ARQ**: Authority Resilience Quotient

**baD/baF/baP**: Basic Assumptions (Dependency, Fight-Flight, Pairing)

**BRI**: Behavioral Risk Indicator

**ISMS**: Information Security Management System

## 5 Contesto dell'Organizzazione

### 5.1 Comprensione dell'Organizzazione e del Suo Contesto

L'organizzazione deve determinare le questioni esterne e interne rilevanti al suo scopo e che influenzano la sua capacità di raggiungere i risultati previsti del suo sistema di gestione delle vulnerabilità psicologiche.

L'organizzazione deve determinare i fattori psicologici specifici della cultura organizzativa che influenzano il comportamento di sicurezza, le minacce di social engineering specifiche del settore, i requisiti normativi e i pattern storici di incidenti di sicurezza legati al fattore umano.

### 5.2 Comprensione dei Bisogni e delle Aspettative delle Parti Interessate

L'organizzazione deve determinare le parti interessate rilevanti per il PVMS e i loro requisiti, inclusi dipendenti, direzione, clienti, regolatori, fornitori di assicurazione, partner e auditor.

### 5.3 Determinazione dell'Ambito del PVMS

L'organizzazione deve determinare i confini e l'applicabilità del PVMS per stabilire il suo ambito, considerando le questioni esterne e interne, i requisiti delle parti interessate e le unità organizzative coperte.

### 5.4 Sistema di Gestione delle Vulnerabilità Psicologiche

L'organizzazione deve stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione delle vulnerabilità psicologiche in conformità con i requisiti di questo documento.

## 6 Leadership

### 6.1 Leadership e Impegno

L'alta direzione deve dimostrare leadership e impegno rispetto al PVMS assicurando che policy e obiettivi siano stabiliti, le risorse siano disponibili e l'importanza della gestione efficace delle

vulnerabilità psicologiche sia comunicata.

### 6.2 Policy

L'alta direzione deve stabilire una policy CPF che sia appropriata allo scopo dell'organizzazione, includa l'impegno per l'assessment sistematico delle vulnerabilità psicologiche e la protezione della privacy, e fornisca il framework per stabilire gli obiettivi.

### 6.3 Ruoli, Responsabilità e Autorità Organizzative

L'alta direzione deve assicurare che le responsabilità e le autorità per i ruoli rilevanti siano assegnate e comunicate, inclusi Coordinatore CPF, Responsabile Privacy, Specialisti di Assessment e Coordinatori di Risposta.

## 7 Pianificazione

### 7.1 Azioni per Affrontare Rischi e Opportunità

#### 7.1.1 Generale

L'organizzazione deve determinare i rischi e le opportunità necessari per assicurare che il PVMS raggiunga i risultati previsti, prevenga effetti indesiderati e raggiunga il miglioramento continuo.

#### 7.1.2 Assessment delle Vulnerabilità Psicologiche

L'organizzazione deve stabilire processi per l'assessment delle vulnerabilità psicologiche che valutino le vulnerabilità attraverso tutti i dieci domini CPF, utilizzino 100 indicatori, impieghino metodologie che preservano la privacy, operino su unità di aggregazione minime di dieci individui, implementino differential privacy con $\varepsilon = 0.1$ e mantengano ritardi temporali di minimo 72 ore.

#### 7.1.3 Trattamento del Rischio Psicologico

L'organizzazione deve definire e applicare processi per il trattamento del rischio psicologico, selezionando opzioni appropriate per modificare, ritenere, evitare o condividere i rischi.

### 7.2 Obiettivi CPF e Pianificazione

L'organizzazione deve stabilire obiettivi CPF misurabili a funzioni e livelli rilevanti, come ridurre il conteggio degli indicatori Yellow/Red, diminuire l'indice di convergenza e ridurre gli incidenti di sicurezza legati al fattore umano.

### 7.3 Pianificazione dei Cambiamenti

Quando l'organizzazione determina la necessità di cambiamenti al PVMS, i cambiamenti devono essere effettuati in modo pianificato considerando lo scopo, l'integrità, le risorse e le protezioni della privacy.

# 8 Supporto

## 8.1 Risorse

L'organizzazione deve determinare e fornire le risorse necessarie per l'istituzione, implementazione, mantenimento e miglioramento continuo del PVMS, inclusi personale, infrastruttura tecnologica, strumenti di assessment e risorse finanziarie.

## 8.2 Competenza

L'organizzazione deve determinare la competenza necessaria delle persone che influenzano le performance del PVMS e assicurare che le persone siano competenti basandosi su educazione, formazione o esperienza appropriate.

Le competenze del Coordinatore CPF includono comprensione dei principi di cybersecurity, conoscenza della teoria psicologica, familiarità con i processi pre-cognitivi e comprensione delle metodologie che preservano la privacy.

Le competenze dello Specialista di Assessment includono formazione formale in psicologia o scienze comportamentali, comprensione dei concetti psicoanalitici, conoscenza dei bias cognitivi e familiarità con i metodi di data science.

## 8.3 Consapevolezza

L'organizzazione deve assicurare che le persone siano consapevoli della policy CPF, del loro contributo all'efficacia del PVMS, delle protezioni della privacy e che le vulnerabilità psicologiche sono caratteristiche umane normali, non fallimenti individuali.

## 8.4 Comunicazione

L'organizzazione deve determinare la necessità di comunicazioni interne ed esterne rilevanti per il PVMS, incluso cosa comunicare, quando, con chi e come.

## 8.5 Informazioni Documentate

Il PVMS dell'organizzazione deve includere informazioni documentate richieste da CPF-27001 e determinate necessarie per l'efficacia, incluse policy CPF, ambito, metodologia di assessment, procedure di privacy, piani di trattamento dei rischi e risultati di audit.

# 9 Operazione

## 9.1 Pianificazione e Controllo Operativo

L'organizzazione deve pianificare, implementare e controllare i processi necessari per soddisfare i requisiti del PVMS, inclusi cicli di assessment regolari, monitoraggio continuo, raccolta dati che preserva la privacy, implementazione del trattamento dei rischi e integrazione con le operazioni di sicurezza.

## 9.2 Assessment delle Vulnerabilità Psicologiche

### 9.2.1 Generale

L'organizzazione deve definire e applicare il processo di assessment delle vulnerabilità psicologiche per l'identificazione sistematica delle vulnerabilità attraverso i domini CPF, che avviene a intervalli pianificati con metodologie validate che mantengono le protezioni della privacy.

### 9.2.2 Processo di Assessment

L'assessment delle vulnerabilità psicologiche deve valutare 100 indicatori attraverso 10 domini:

**Dominio 1: Vulnerabilità Basate sull'Autorità** - Compliance incondizionata, diffusione di responsabilità, suscettibilità all'impersonificazione dell'autorità, bypass della sicurezza per i superiori, compliance basata sulla paura, effetti del gradiente di autorità, deferenza verso l'autorità tecnica, normalizzazione delle eccezioni esecutive, social proof basato sull'autorità, escalation dell'autorità in crisi.

**Dominio 2: Vulnerabilità Temporali** - Bypass indotto dall'urgenza, degradazione cognitiva da pressione temporale, accettazione del rischio guidata dalle scadenze, present bias, sconto iperbolico, pattern di esaurimento temporale, finestre di vulnerabilità legate all'ora del giorno, cali nei weekend/festività, sfruttamento del cambio turno, pressione di coerenza temporale.

**Dominio 3: Vulnerabilità dell'Influenza Sociale** - Sfruttamento della reciprocità, trappole di escalation dell'impegno, manipolazione del social proof, override della fiducia basato sul liking, decisioni guidate dalla scarsità, sfruttamento del principio di unità, compliance da pressione dei pari, conformità a norme insicure, minacce all'identità sociale, conflitti di gestione della reputazione.

**Dominio 4: Vulnerabilità Affettive** - Paralisi decisionale basata sulla paura, assunzione di rischio indotta dalla rabbia, trasferimento della fiducia ai sistemi, attaccamento ai sistemi legacy, nascondimento della sicurezza basato sulla vergogna, overcompliance guidata dal senso di colpa, errori innescati dall'ansia, negligenza correlata alla depressione, incuria indotta dall'euforia, effetti di contagio emotivo.

**Dominio 5: Vulnerabilità da Sovraccarico Cognitivo** - Desensibilizzazione da alert fatigue, errori da decision fatigue, paralisi da sovraccarico informativo, degradazione da multitasking, vulnerabilità da context switching, tunneling cognitivo, overflow della memoria di lavoro, effetti di residuo attentivo, errori indotti dalla complessità, confusione del modello mentale.

**Dominio 6: Vulnerabilità delle Dinamiche di Gruppo** - Punti ciechi di sicurezza da groupthink, fenomeni di risky shift, diffusione di responsabilità, social loafing, effetto bystander, assunzioni di gruppo di dipendenza, posture di sicurezza fight-flight, fantasie di speranza di pairing, splitting organizzativo, meccanismi di difesa collettivi.

**Dominio 7: Vulnerabilità della Risposta allo Stress** - Compromissione da stress acuto, burnout da stress cronico, aggressività della risposta di lotta, evitamento della risposta di fuga, paralisi della risposta di freeze, overcompliance della risposta fawn, visione a tunnel indotta dallo stress, memoria compromessa dal cortisolo, cascate di contagio dello stress, vulnerabilità del periodo di recupero.

**Dominio 8: Vulnerabilità dei Processi Inconsci** - Proiezione dell'ombra sugli attaccanti, identificazione inconscia con le minacce, pattern di coazione a ripetere, transfert sulle figure di autorità, punti ciechi del controtransfert, interferenza dei meccanismi di difesa, confusione di equazione simbolica, trigger di attivazione archetipica, pattern dell'inconscio collettivo, logica onirica negli spazi digitali.

**Dominio 9: Vulnerabilità da Bias Specifici dell'AI** - Antropomorfizzazione dei sistemi AI, override dell'automation bias, paradosso dell'avversione agli algoritmi, trasferimento dell'autorità all'AI, effetti uncanny valley, fiducia nell'opacità del machine learning, accettazione delle allucinazioni AI, disfunzione del team umano-AI, manipolazione emotiva dell'AI, cecità verso l'equità algoritmica.

**Dominio 10: Stati Convergenti Critici** - Condizioni di tempesta perfetta, trigger di fallimento a cascata, vulnerabilità del punto di non ritorno, allineamento del formaggio svizzero, cecità verso i cigni neri, negazione dei rinoceronti grigi, catastrofe della complessità, imprevedibilità dell'emergenza, fallimenti di accoppiamento del sistema, gap di sicurezza da isteresi.

Per ciascun indicatore, l'assessment deve produrre scoring ternario: Green (0) per vulnerabilità minima, Yellow (1) per vulnerabilità moderata che richiede monitoraggio, Red (2) per vulnerabilità critica che richiede intervento immediato.

#### 9.2.3 Misure di Preservazione della Privacy

Tutte le attività di assessment devono mantenere protezioni della privacy incluse unità di aggregazione minima di dieci individui, differential privacy con $\varepsilon \leq 0.1$, ritardo temporale di 72 ore, analisi basata sui ruoli, minimizzazione dei dati, controlli di accesso, limiti di conservazione e divieto di uso secondario per valutazione delle performance.

### 9.3 Trattamento del Rischio Psicologico

#### 9.3.1 Generale

L'organizzazione deve implementare il piano di trattamento dei rischi che affronta le vulnerabilità psicologiche identificate attraverso l'assessment, riconoscendo che le vulnerabilità sono questioni sistemiche organizzative, non fallimenti individuali.

#### 9.3.2 Protocolli di Risposta

L'organizzazione deve stabilire protocolli di risposta graduati: lo status Green continua il monitoraggio standard, lo status Yellow aumenta il monitoraggio e implementa interventi preventivi, lo status Red innesca escalation immediata e trattamento d'emergenza, la convergenza critica attiva le procedure di risposta d'emergenza.

#### 9.3.3 Monitoraggio Continuo

L'organizzazione deve implementare il monitoraggio continuo degli indicatori critici di vulnerabilità psicologica integrato con le operazioni di sicurezza, incluso monitoraggio in tempo reale, integrazione SIEM, alerting automatizzato e correlazione con il monitoraggio tecnico.

## 10 Valutazione delle Performance

### 10.1 Monitoraggio, Misurazione, Analisi e Valutazione

L'organizzazione deve valutare le performance e l'efficacia del PVMS determinando cosa deve essere monitorato (indicatori, efficacia del trattamento dei rischi, performance dei processi), metodi per risultati validi, tempistiche e parti responsabili.

Gli indicatori chiave di performance includono numero di indicatori in ciascuno status, analisi delle tendenze, valori dell'indice di convergenza, tassi di incidenti legati al fattore umano, tassi di compliance alle policy, tempi di risposta e efficacia del trattamento dei rischi.

### 10.2 Audit Interno

L'organizzazione deve condurre audit interni a intervalli pianificati per fornire informazioni su se il PVMS è conforme ai requisiti ed è efficacemente implementato e mantenuto.

L'ambito dell'audit deve valutare la conformità della metodologia di assessment, l'efficacia delle protezioni della privacy, l'adeguatezza della competenza, l'implementazione del trattamento dei rischi, l'integrazione con l'ISMS e l'evidenza del miglioramento continuo.

### 10.3 Riesame della Direzione

L'alta direzione deve revisionare il PVMS a intervalli pianificati per assicurare la continua idoneità, adeguatezza ed efficacia. Gli input del riesame includono lo status delle azioni precedenti, i cambiamenti nelle questioni, il feedback sulle performance, i risultati degli audit, i risultati dell'assessment dei rischi e le opportunità di miglioramento. Gli output del riesame includono decisioni sui miglioramenti, modifiche al PVMS e necessità di risorse.

## 11 Miglioramento

### 11.1 Non Conformità e Azione Correttiva

Quando si verifica una non conformità, l'organizzazione deve reagire per controllarla e correggerla, valutare la necessità di azione per eliminare le cause, implementare qualsiasi azione necessaria, revisionare l'efficacia e apportare modifiche al PVMS se necessario.

Le non conformità comuni includono mancato mantenimento dell'unità di aggregazione minima, dati di assessment usati per valutazione delle performance, protezioni della privacy inadeguate, assessment che non copre i domini applicabili, competenza insufficiente e mancanza di integrazione con l'ISMS.

### 11.2 Miglioramento Continuo

L'organizzazione deve migliorare continuamente l'idoneità, adeguatezza ed efficacia del PVMS attraverso il raffinamento regolare delle metodologie, il miglioramento delle protezioni della privacy, il miglioramento dell'integrazione con la sicurezza tecnica, lo sviluppo di interventi efficaci e l'espansione dell'ambito di assessment.

### 11.3 Aggiornamenti del Framework

L'organizzazione deve stabilire un processo per aggiornare gli indicatori CPF e la metodologia di assessment per affrontare nuove vulnerabilità, cambiamenti nelle tecniche di attacco, progressi nella ricerca psicologica e evoluzione tecnologica.

Gli aggiornamenti del framework devono essere revisionati attraverso la gestione del cambiamento, mantenere la compatibilità retroattiva dove fattibile, essere validati prima dell'implementazione, essere documentati con motivazione e essere comunicati agli stakeholder.

## Bibliografia

**CPF-27002:2025**, Gestione delle Vulnerabilità Psicologiche — Codice di Pratica

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

**Verizon (2024)**, Data Breach Investigations Report

**IBM Security (2023)**, Cost of a Data Breach Report