El Cybersecurity Psychology Framework: Un Modelo de Evaluación de Vulnerabilidades Pre-Cognitivas Integrando Ciencias Psicoanalíticas y Cognitivas

Una Preimpresión

Giuseppe Canale, CISSP
Investigador Independiente
kaolay@gmail.com, g.canale@cpf3.org
URL: cpf3.org
ORCID: 0009-0007-3263-6897

December 20, 2025

Abstract

Presentamos el Cybersecurity Psychology Framework (CPF), un innovador modelo interdisciplinario que identifica las vulnerabilidades pre-cognitivas en las posturas de security organizacionales a través de la integración sistemática de la teoría psicoanalítica y la psicología cognitiva. A diferencia de los enfoques tradicionales de conciencia de la security que se concentran en el proceso decisional consciente, CPF mapea los estados psicológicos inconscientes y las dinámicas de grupo a vectores de ataque específicos, permitiendo estrategias de security predictivas en lugar de reactivas. El framework comprende 100 indicadores a través de 10 categorías, desde las vulnerabilidades basadas en la autoridad (Milgram, 1974) a los sesgos cognitivos específicos de la IA, utilizando un sistema de evaluación ternario (Verde/Amarillo/Rojo). Nuestro modelo mantiene explícitamente la privacidad a través del análisis agregado de los patrones comportamentales, sin nunca perfilar a los individuos. CPF representa la primera integración formal de la teoría de las relaciones objetales (Klein, 1946), las dinámicas de grupo (Bion, 1961) y la psicología analítica (Jung, 1969) con la práctica contemporánea de la cybersecurity, abordando la brecha crítica entre los controles técnicos y los factores humanos en los fracasos de security.

Palabras clave: cybersecurity, psicología, psicoanálisis, sesgos cognitivos, factores humanos, evaluación de vulnerabilidad, procesos pre-cognitivos

1 Introducción

A pesar de que el gasto global en cybersecurity supera los $150 mil millones anualmente[7], las violaciones exitosas continúan aumentando, con los factores humanos que contribuyen a más del 85% de los incidentes[21]. Los actuales frameworks de security—desde ISO 27001 a NIST CSF—abordan principalmente controles técnicos y procedimentales, mientras las intervenciones sobre los "factores humanos" permanecen limitadas a la formación sobre la conciencia de la security a nivel consciente[18]. Este enfoque malinterpreta fundamentalmente los mecanismos psicológicos en la base de las vulnerabilidades de security.

Investigaciones neurocientíficas recientes demuestran que el proceso decisional ocurre 300-500ms antes de la conciencia consciente[14, 20], sugiriendo que las decisiones de security están sustancialmente influenciadas por procesos pre-cognitivos. Además, el comportamiento organizacional emerge de complejas dinámicas de grupo que operan debajo de la conciencia consciente[3, 11]. Estos procesos inconscientes crean vulnerabilidades sistemáticas que los controles técnicos no pueden abordar.

El Cybersecurity Psychology Framework (CPF) llena esta brecha proporcionando la primera integración sistemática de:

- **Teoría psicoanalítica de las relaciones objetales** para comprender la escisión y la proyección organizacional
- **Teoría de las dinámicas de grupo** para mapear las asunciones inconscientes colectivas
- **Psicología cognitiva** para identificar sesgos sistemáticos en las decisiones relevantes para la security
- **Psicología de la IA** para abordar las vulnerabilidades de la interacción humano-IA

Este documento presenta el fundamento teórico de CPF, el diseño arquitectural y la hoja de ruta para futuros estudios de validación.

2 Fundamento Teórico

2.1 El Fracaso de las Intervenciones a Nivel Consciente

Los programas tradicionales de conciencia de la security asumen actores racionales que, cuando informados de los riesgos, modificarán el comportamiento consecuentemente[1]. Sin embargo, esta asunción racionalista contradice sustanciales evidencias de múltiples disciplinas.

Evidencia Neurocientífica:

- Los estudios fMRI muestran que la activación de la amígdala (respuesta a la amenaza) ocurre antes del compromiso de la corteza prefrontal (análisis racional)[13]
- El proceso decisional involucra marcadores somáticos que bypassean la elaboración consciente[6]

Evidencia de la Economía Comportamental:

- El Sistema 1 (rápido, automático) domina el Sistema 2 (lento, deliberado) en ambientes con presión temporal[9]
- La carga cognitiva compromete la calidad de las decisiones de security[2]

Evidencia Psicoanalítica:

- Las organizaciones desarrollan "sistemas de defensa social" contra la ansiedad que crean puntos ciegos en la security[15]
- La proyección de las amenazas internas sobre "hackers" externos impide el reconocimiento de los riesgos insider[12]

2.2 Contribuciones Psicoanalíticas a la Cybersecurity

2.2.1 Las Asunciones Básicas de Bion

Bion[3] ha identificado tres asunciones básicas que los grupos adoptan inconscientemente cuando enfrentan la ansiedad:

- **Dependencia (baD)**: Búsqueda de un líder/tecnología omnipotente para la protección
- **Ataque-Fuga (baF)**: Percepción de las amenazas como enemigos externos que requieren defensa agresiva o evitamiento
- **Acoplamiento (baP)**: Esperanza de salvación futura a través de nuevas soluciones

En los contextos de cybersecurity, estas se manifiestan como:

- **baD**: Excesiva confianza en proveedores de security/soluciones "bala de plata"
- **baF**: Defensa perimetral agresiva ignorando las amenazas insider
- **baP**: Adquisición continua de herramientas sin abordar las vulnerabilidades fundamentales

2.2.2 Relaciones Objetales Kleinianas

El concepto de escisión de Klein[12]—dividir los objetos en "todo bueno" o "todo malo"—aparece en la security organizacional como:

- Insiders confiables (idealizados) vs. agresores externos (demonizados)
- Sistemas legacy (familiares/buenos) vs. nuevos requisitos de security (amenazantes/malos)
- Proyección de las vulnerabilidades organizacionales sobre "agresores sofisticados"

2.2.3 El Espacio Transicional de Winnicott

El concepto de espacio transicional de Winnicott[22] ayuda a comprender los ambientes digitales como ni completamente reales ni completamente imaginarios, creando vulnerabilidades únicas:

- Test de realidad reducido en los ambientes virtuales
- Confusión entre identidad digital y sí mismo
- Fantasías omnipotentes en el ciberespacio

2.2.4 La Sombra y la Proyección Junguiana

El concepto de sombra de Jung[8] explica cómo las organizaciones proyectan aspectos renegados sobre los agresores:

- Los hackers "black hat" encarnan la agresividad reprimida de la organización
- Los equipos de security pueden inconscientemente identificarse con los agresores (integración de la sombra)
- La sombra colectiva crea puntos ciegos en la postura de security

2.3 Integración de la Psicología Cognitiva

2.3.1 Aplicación de la Teoría del Doble Proceso

El framework Sistema 1/Sistema 2 de Kahneman[9] revela vulnerabilidades específicas:

Vulnerabilidades del Sistema 1:

- Heurística de la disponibilidad: Sobrepesar los ataques recientes/memorables
- Heurística del afecto: Decisiones de security basadas en el estado emocional
- Anclaje: El primer incidente de security moldea todas las respuestas futuras

Limitaciones del Sistema 2:

- Carga cognitiva de la complejidad de la security
- Depleción del ego de la vigilancia constante
- Razonamiento motivado para evitar los requisitos de security

2.3.2 Los Principios de Influencia de Cialdini en el Contexto Cyber

Los seis principios de Cialdini[5] se mapean directamente sobre los vectores de ingeniería social:

1. **Reciprocidad**: Ataques quid pro quo
2. **Compromiso/Coherencia**: Escalación gradual de las solicitudes
3. **Prueba social**: "Todos hacen clic en este enlace"
4. **Autoridad**: Fraudes CEO, falso soporte de IT
5. **Simpatía**: Construcción del rapport antes del ataque
6. **Escasez**: Acción urgente requerida

2.3.3 Teoría de la Carga Cognitiva

La limitación del "número mágico siete" de Miller[17] crea vulnerabilidades:

- Compromisos entre complejidad y memorabilidad de las contraseñas
- Fatiga de alertas de la proliferación de herramientas de security
- Parálisis decisional de demasiadas opciones de security

2.4 Vulnerabilidades Psicológicas Específicas de la IA

A medida que los sistemas IA se vuelven parte integral de las operaciones de security, emergen nuevas vulnerabilidades psicológicas:

2.4.1 Antropomorfización

- Atribución de intenciones humanas a los sistemas IA
- Excesiva confianza en las recomendaciones IA
- Apego emocional a los asistentes IA que crea vectores de manipulación

2.4.2 Automation Bias

- Excesiva confianza en las herramientas de security automatizadas
- Vigilancia humana reducida ("riesgo moral")
- Atrofia de las competencias en los equipos de security

2.4.3 Efectos de Transferencia IA-Humano

- Sesgos humanos codificados en los datos de training de la IA
- Sistemas IA que amplifican los puntos ciegos organizacionales
- Loops de retroalimentación entre sesgos humanos e IA

3 La Arquitectura del Modelo CPF

3.1 Principios de Diseño

La arquitectura CPF sigue cinco principios fundamentales:

1. **Preservación de la Privacidad**: Todas las evaluaciones utilizan datos agregados; ninguna perfilación individual
2. **Foco Predictivo**: Identifica las vulnerabilidades antes de la explotación
3. **Implementación Agnóstica**: Se mapea a las vulnerabilidades, no a soluciones específicas
4. **Fundamento Científico**: Cada indicador conectado a investigación consolidada
5. **Practicidad Operativa**: Puntuación ternaria para insights accionables

3.2 Estructura del Framework

CPF comprende 100 indicadores organizados en una matriz 10×10. La Tabla 1 resume las diez categorías primarias:

Table 1: Categorías Primarias CPF y Fundamentos Teóricos

Código	Categoría	Referencia Primaria
[1.x]	Vulnerabilidades Basadas en la Autoridad	Milgram (1974)
[2.x]	Vulnerabilidades Temporales	Kahneman & Tversky (1979)
[3.x]	Vulnerabilidades de Influencia Social	Cialdini (2007)
[4.x]	Vulnerabilidades Afectivas	Klein (1946), Bowlby (1969)
[5.x]	Vulnerabilidades de Sobrecarga Cognitiva	Miller (1956)
[6.x]	Vulnerabilidades de las Dinámicas de Grupo	Bion (1961)
[7.x]	Vulnerabilidades de Respuesta al Estrés	Selye (1956)
[8.x]	Vulnerabilidades de los Procesos Inconscientes	Jung (1969)
[9.x]	Vulnerabilidades de Sesgos Específicos de la IA	Integración Innovadora
[10.x]	Estados Convergentes Críticos	Teoría de los Sistemas

3.2.1 Detalle Categoría: Vulnerabilidades Basadas en la Autoridad [1.x]

1.1 Conformidad sin preguntas a la autoridad aparente

1.2 Difusión de la responsabilidad en las estructuras jerárquicas

1.3 Susceptibilidad a la suplantación de figuras de autoridad

1.4 Bypass de la security para conveniencia del superior

1.5 Conformidad basada en el miedo sin verificación

1.6 Gradiente de autoridad que inhibe el reporte de security

1.7 Deferencia a las reivindicaciones de autoridad técnica

1.8 Normalización de las excepciones ejecutivas

1.9 Prueba social basada en la autoridad

1.10 Escalación de la autoridad en crisis

3.2.2 Detalle Categoría: Vulnerabilidades Temporales [2.x]

2.1 Bypass de la security inducido por la urgencia

2.2 Degradación cognitiva por presión temporal

2.3 Aceptación del riesgo guiada por las fechas límite

2.4 Present bias en las inversiones de security

2.5 Descuento hiperbólico de las amenazas futuras

2.6 Patrones de agotamiento temporal

2.7 Ventanas de vulnerabilidad basadas en la hora del día

2.8 Brechas de security en fines de semana/festivos

2.9 Ventanas de explotación al cambio de turno

2.10 Presión de coherencia temporal

3.2.3 Detalle Categoría: Vulnerabilidades de Influencia Social [3.x]

3.1 Explotación de la reciprocidad

3.2 Trampas de escalación del compromiso

3.3 Manipulación de la prueba social

3.4 Override de la confianza basado en la simpatía

3.5 Decisiones guiadas por la escasez

3.6 Explotación del principio de unidad

3.7 Conformidad a la presión de pares

3.8 Conformidad a normas inseguras

3.9 Amenazas a la identidad social

3.10 Conflictos de gestión de la reputación

3.2.4 Detalle Categoría: Vulnerabilidades Afectivas [4.x]

4.1 Parálisis decisional basada en el miedo

4.2 Asunción de riesgos inducida por la rabia

4.3 Transferencia de la confianza a los sistemas

4.4 Apego a los sistemas legacy

4.5 Ocultamiento de la security basado en la vergüenza

4.6 Hiperconformidad guiada por el sentido de culpa

4.7 Errores activados por la ansiedad

4.8 Negligencia correlacionada con la depresión

4.9 Descuido inducido por la euforia

4.10 Efectos de contagio emocional

3.2.5 Detalle Categoría: Vulnerabilidades de Sobrecarga Cognitiva [5.x]

5.1 Desensibilización por fatiga de las alertas

5.2 Errores de fatiga decisional

5.3 Parálisis por sobrecarga informativa

5.4 Degradación por multitarea

5.5 Vulnerabilidades de cambio de contexto

5.6 Túnel cognitivo

5.7 Overflow de la memoria de trabajo

5.8 Efectos de residuo de la atención

5.9 Errores inducidos por la complejidad

5.10 Confusión del modelo mental

3.2.6 Detalle Categoría: Vulnerabilidades de las Dinámicas de Grupo [6.x]

6.1 Puntos ciegos de la security por groupthink

6.2 Fenómenos de desplazamiento riesgoso

6.3 Difusión de la responsabilidad

6.4 Social loafing en las tareas de security

6.5 Efecto espectador en la respuesta a incidentes

6.6 Asunciones de grupo de dependencia

6.7 Posturas de security ataque-fuga

6.8 Fantasías de esperanza en el acoplamiento

6.9 Escisión organizacional

6.10 Mecanismos de defensa colectivos

3.2.7 Detalle Categoría: Vulnerabilidades de Respuesta al Estrés [7.x]

7.1 Compromiso por estrés agudo

7.2 Burnout por estrés crónico

7.3 Agresión por respuesta de ataque

7.4 Evitamiento por respuesta de fuga

7.5 Parálisis por respuesta de congelamiento

7.6 Hiperconformidad por respuesta de complacencia

7.7 Visión de túnel inducida por el estrés

7.8 Memoria comprometida por el cortisol

7.9 Cascadas de contagio del estrés

7.10 Vulnerabilidades del período de recuperación

3.2.8 Detalle Categoría: Vulnerabilidades de los Procesos Inconscientes [8.x]

8.1 Proyección de la sombra sobre los agresores

8.2 Identificación inconsciente con las amenazas

8.3 Patrones de compulsión a la repetición

8.4 Transfert hacia figuras de autoridad

8.5 Puntos ciegos por contratransfert

8.6 Interferencia de los mecanismos de defensa

8.7 Confusión de la ecuación simbólica

8.8 Triggers de activación arquetípica

8.9 Patrones del inconsciente colectivo

8.10 Lógica onírica en los espacios digitales

3.2.9 Detalle Categoría: Vulnerabilidades de Sesgos Específicos de la IA [9.x]

9.1 Antropomorfización de los sistemas IA

9.2 Override del sesgo de automatización

9.3 Paradoja de la aversión a los algoritmos

9.4 Transferencia de autoridad a la IA

9.5 Efectos del valle inquietante

9.6 Confianza en la opacidad del machine learning

9.7 Aceptación de las alucinaciones de la IA

9.8 Disfunción del equipo humano-IA

9.9 Manipulación emocional de la IA

9.10 Ceguera a la corrección algorítmica

3.2.10 Detalle Categoría: Estados Convergentes Críticos [10.x]

10.1 Condiciones de tormenta perfecta

10.2 Triggers de fracaso en cascada

10.3 Vulnerabilidades del punto de no retorno

10.4 Alineación del queso suizo

10.5 Ceguera al cisne negro

10.6 Negación del rinoceronte gris

10.7 Catástrofe de la complejidad

10.8 Imprevisibilidad emergente

10.9 Fracasos de acoplamiento del sistema

10.10 Gaps de security por histéresis

3.3 Metodología de Evaluación

La metodología de evaluación CPF es actualmente teórica y en espera de validación empírica a través de futuras implementaciones piloto. Los métodos propuestos de recolección de datos darán prioridad a las técnicas de preservación de la privacidad y al análisis agregado.

3.3.1 Sistema de Puntuación

Cada indicador recibe una puntuación ternaria:

- **Verde (0)**: Vulnerabilidad mínima detectada
- **Amarillo (1)**: Vulnerabilidad moderada que requiere monitoreo
- **Rojo (2)**: Vulnerabilidad crítica que requiere intervención

Puntuación agregada:

$$\text{Puntuación Categoría} = \sum_{i=1}^{10} \text{Indicador}_i \quad (0 - 20 \text{ rango}) \tag{1}$$

$$\text{Puntuación CPF} = \sum_{j=1}^{10} w_j \cdot \text{Categoría}_j \tag{2}$$

$$\text{Índice de Convergencia} = \prod_{j,k} \text{Interacción}_{j,k} \tag{3}$$

3.3.2 Mecanismos de Protección de la Privacidad

- Unidad mínima de agregación: 10 individuos
- Inyección de ruido para privacidad diferencial: $\epsilon = 0.1$
- Reporting retrasado en el tiempo: mínimo 72 horas
- Análisis basado en roles en lugar de individual
- Pista de auditoría para todos los accesos a los datos

3.4 Mapeo de los Vectores de Ataque

Cada categoría de vulnerabilidad se mapea a vectores de ataque específicos como se muestra en la Tabla 2:

Table 2: Mapeo de Vulnerabilidad a Vector de Ataque

Categoría Vulnerabilidad	Vectores de Ataque Primarios
Autoridad	Spear Phishing, Fraude CEO
Temporales	Ataques en Fechas Límite, Malware Time-bomb
Social	Ingeniería Social, Amenazas Insider
Afectivas	Campañas FUD, Ransomware
Sobrecarga Cognitiva	Explotación Fatiga de Alertas
Dinámicas de Grupo	Interrupción Organizacional
Estrés	Explotación Burnout
Inconscientes	Ataques Simbólicos
Sesgos IA	ML Adversarial, Poisoning
Convergentes	Advanced Persistent Threats

4 Estudios de Validación

4.1 Panorama de Implementación Piloto

El framework CPF está actualmente en la fase de desarrollo teórico. Las implementaciones piloto están en fase de planificación con organizaciones de diversos sectores. La validación futura se concentrará en: - Correlación entre puntuaciones CPF e incidentes de security efectivos - Precisión predictiva del framework - Aplicabilidad intersectorial - Factores culturales y organizacionales. Estamos activamente buscando organizaciones partner para implementaciones piloto. Las partes interesadas pueden contactar al autor para oportunidades de colaboración.

4.2 Limitaciones

- Dimensión de muestra reducida limita la generalizabilidad
- Período de observación insuficiente para eventos raros
- Factores culturales no completamente considerados
- Posible influencia del efecto Hawthorne

5 Discusión

5.1 Implicaciones Teóricas

CPF valida la aplicación de los conceptos psicoanalíticos a la cybersecurity, demostrando que los procesos inconscientes influencian significativamente los resultados de security. El éxito del framework sugiere que:

1. **Los procesos pre-cognitivos dominan las decisiones de security** – Soportando los hallazgos de Libet en un contexto cyber
2. **Las dinámicas de grupo crean vulnerabilidades sistemáticas** – Confirmando que las asunciones básicas de Bion operan en los ambientes digitales
3. **Las relaciones objetales influencian la percepción de las amenazas** – El mecanismo de escisión de Klein explica los puntos ciegos de la security

4. **La IA introduce nuevas vulnerabilidades psicológicas** – Requiriendo nuevos frameworks teóricos

5.2 Aplicaciones Prácticas

5.2.1 Integración Security Operations Center (SOC)

- Puntuaciones CPF como inteligencia sobre las amenazas adicional
- Monitoreo del estado psicológico junto con los indicadores técnicos
- Puntuación de riesgo dinámico basado en la psicología organizacional

5.2.2 Mejora de la Respuesta a Incidentes

- Pre-posicionamiento de los recursos basado en los estados de vulnerabilidad
- Protocolos de respuesta a medida para las condiciones psicológicas
- Planificación del recupero psicológico post-incidente

5.2.3 Evolución de la Conciencia de la Security

- Ir más allá de la transferencia de información a la intervención psicológica
- Abordar la resistencia inconsciente a las medidas de security
- Intervenciones a nivel de grupo en lugar de individuales

5.3 Consideraciones Éticas

Preocupaciones sobre la Privacidad:

- Riesgo de "vigilancia psicológica"
- Potencial de discriminación basada en los estados psicológicos
- Necesidad de rigurosos frameworks de gobernanza

Consentimiento y Transparencia:

- Comunicación clara sobre los métodos de evaluación
- Mecanismos de opt-out manteniendo la validez estadística
- Auditorías regulares sobre el uso de los datos

Dinámicas de Poder:

- Prevenir la weaponización contra los empleados
- Garantizar la seguridad psicológica durante las evaluaciones
- Protección para whistleblowers que identifican vulnerabilidades

5.4 Direcciones Futuras

1. **Integración Machine Learning**
    - Reconocimiento de patrones en los estados psicológicos
    - Refinamiento del modelado predictivo
    - Sistemas automatizados de alerta temprana
2. **Adaptación Cultural**
    - Estudios de validación intercultural
    - Patrones de vulnerabilidad localizados
    - Factores psicológicos globales vs. locales
3. **Esfuerzos de Estandarización**
    - Integración con frameworks NIST/ISO
    - Personalizaciones específicas para sector
    - Desarrollo de programa de certificación
4. **Estudios Longitudinales**
    - Rastreo plurianual de los patrones psicológicos
    - Medición de la eficacia de las intervenciones
    - Efectos del aprendizaje organizacional

6 Conclusión

El Cybersecurity Psychology Framework representa un cambio de paradigma en la comprensión y en el abordaje de los factores humanos en la cybersecurity. Integrando la teoría psicoanalítica con la psicología cognitiva y extendiéndose a las vulnerabilidades específicas de la IA, CPF proporciona un enfoque científicamente fundado para predecir y prevenir los incidentes de security antes de que ocurran.

El framework teórico demuestra que los estados psicológicos pre-cognitivos deberían correlacionar fuertemente con los resultados de security, soportando los fundamentos del framework. El diseño que preserva la privacidad e independiente de la implementación permite el despliegue práctico abordando las preocupaciones éticas.

A medida que las organizaciones enfrentan amenazas cada vez más sofisticadas que explotan la psicología humana, frameworks como CPF se vuelven esenciales. El desafío no es más puramente técnico sino fundamentalmente psicológico. Los profesionales de la security deben expandir su expertise más allá de la tecnología para incluir la comprensión de los procesos inconscientes, las dinámicas de grupo y la compleja interacción entre inteligencia humana y artificial.

El trabajo futuro se concentrará en implementaciones piloto con organizaciones partner, integración del machine learning y desarrollo de estrategias de intervención basadas en las vulnerabilidades identificadas. Invitamos la colaboración tanto de las comunidades de cybersecurity como de psicología para refinar y validar este enfoque.

El objetivo último de CPF no es eliminar la vulnerabilidad humana—una tarea imposible—sino comprenderla y tenerla en cuenta en nuestras estrategias de security. Solo reconociendo la realidad psicológica de la vida organizacional podemos construir posturas de security verdaderamente resilientes.

Nota sobre la Composición Asistida por IA

Este manuscrito presenta el framework teórico original y las contribuciones intelectuales del autor. En el proceso de composición y formateo, el autor ha utilizado un large language model (LLM) como herramienta auxiliar para tareas específicas:

- **Refactoring Estilístico:** Reformulación de las frases para mejorar claridad y fluidez en inglés.
- **Asistencia al Formateo:** Ayuda en la aplicación coherente de la sintaxis LaTeX para listas, tablas y referencias cruzadas.

Es fundamental subrayar que:

- La idea central, la taxonomía CPF, la selección y definición de todos los indicadores, la integración teórica y el análisis global son exclusivamente el producto de la expertise y del esfuerzo intelectual del autor.
- El LLM no ha generado ideas, conceptos o conclusiones nuevas. Su rol ha sido limitado a la asistencia en la reformulación y formateo bajo la estrecha dirección y revisión continua del autor.
- El autor es enteramente responsable de la exactitud, validez e integridad del contenido publicado.

Agradecimientos

El autor agradece a las comunidades de cybersecurity y psicología por su diálogo continuo sobre los factores humanos en la security.

Biografía del Autor

Giuseppe Canale es un profesional de cybersecurity certificado CISSP con formación especializada en teoría psicoanalítica (Bion, Klein, Jung, Winnicott) y psicología cognitiva (Kahneman, Cialdini). Combina 27 años de experiencia en cybersecurity con una profunda comprensión de los procesos inconscientes y las dinámicas de grupo para desarrollar enfoques innovadores a la security organizacional.

Declaración sobre la Disponibilidad de los Datos

Datos agregados anonimizados disponibles bajo solicitud, sujetos a vínculos de privacidad.

Conflicto de Intereses

El autor declara la ausencia de conflictos de interés.

A Muestra de Instrumento de Evaluación CPF

El instrumento completo de evaluación está en fase de desarrollo y será hecho disponible después de la validación piloto.

B Verificación Timestamp Blockchain

La versión del framework CPF descrita en este documento ha sido marcada temporalmente en blockchain para la protección de la propiedad intelectual y el control de versión:

- **Plataforma**: OpenTimestamps.org
- **Hash**: dfb55fc21e1b204c342aa76145f1329fa6f095ceddc3aad8486dca91a580fa96
- **Altura de Bloque**: 909232
- **ID de Transacción**: dfb55fc21e1b204c342aa76145f1329fa6f095
- ceddc3aad8486dca91a580fa9693a7e6d57f08942718b80ccda74d9f74
- **Timestamp**: 2025-08-09 CET

References

[1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

[2] Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. *Proceedings of NSPW*, 47-58.

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

[4] Bowlby, J. (1969). *Attachment and Loss: Vol. 1. Attachment*. New York: Basic Books.

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

[6] Damasio, A. (1994). *Descartes' error: Emotion, reason, and the human brain*. New York: Putnam.

[7] Gartner. (2023). *Forecast: Information Security and Risk Management, Worldwide, 2021-2027*. Gartner Research.

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

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

[10] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-291.

[11] Kernberg, O. (1998). *Ideology, conflict, and leadership in groups and organizations*. New Haven: Yale University Press.

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

[13] LeDoux, J. (2000). Emotion circuits in the brain. *Annual Review of Neuroscience*, 23, 155-184.

[14] Libet, B., Gleason, C. A., Wright, E. W., & Pearl, D. K. (1983). Time of conscious intention to act in relation to onset of cerebral activity. *Brain*, 106(3), 623-642.

[15] Menzies Lyth, I. (1960). A case-study in the functioning of social systems as a defence against anxiety. *Human Relations*, 13, 95-121.

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

[17] Miller, G. A. (1956). The magical number seven, plus or minus two. *Psychological Review*, 63(2), 81-97.

[18] SANS Institute. (2023). *Security Awareness Report 2023*. SANS Security Awareness.

[19] Selye, H. (1956). *The stress of life*. New York: McGraw-Hill.

[20] Soon, C. S., Brass, M., Heinze, H. J., & Haynes, J. D. (2008). Unconscious determinants of free decisions in the human brain. *Nature Neuroscience*, 11(5), 543-545.

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

[22] Winnicott, D. W. (1971). *Playing and reality*. London: Tavistock Publications.