El Factor Humano en la Resiliencia Operativa: Integración de la Evaluación del Riesgo Psicológico en los Frameworks de Compliance NIS2 y DORA

Un Framework para el Compliance Normativo Europeo

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

20 de diciembre de 2025

Resumen

El marco normativo de la Unión Europea para la resiliencia operativa digital—comprendiendo la Directiva NIS2 (Directiva 2022/2555) y el Digital Operational Resilience Act (DORA, Reglamento 2022/2554)—establece requisitos comprehensivos para la gestión del riesgo de cybersecurity en los sectores críticos. Sin embargo, aunque estas normativas prevén consideraciones sobre el factor humano como responsabilidad del management, formación y programas de sensibilización, carecen de metodologías sistemáticas para evaluar y mitigar las vulnerabilidades psicológicas que comprometen la resiliencia operativa. Este documento presenta un framework de integración práctico que mapea el Cybersecurity Psychology Framework (CPF)[1] sobre los requisitos NIS2 y sobre los cinco pilares de DORA, proporcionando a los compliance officers y a los Chief Information Security Officers un enfoque sistemático para abordar las dimensiones psicológicas de la resiliencia operativa. A través de tablas de mapeo detalladas y líneas guía de implementación, demostramos cómo la evaluación del riesgo psicológico puede mejorar operativamente los programas de compliance, produciendo al mismo tiempo mejoras medibles en la prevención de incidentes y en la resiliencia organizacional. El framework proporciona valor práctico inmediato para las instituciones financieras europeas y los proveedores de servicios esenciales que enfrentan la fecha límite DORA de enero 2025 y las obligaciones de compliance NIS2 en curso.

Palabras clave: NIS2, DORA, resiliencia operativa, evaluación del riesgo psicológico, compliance europeo, factores humanos, cybersecurity servicios financieros

1. Síntesis Ejecutiva

La Unión Europea ha establecido el marco normativo más comprehensivo del mundo para la resiliencia operativa digital. La Directiva NIS2, en vigor desde octubre 2024, impone la gestión del riesgo de cybersecurity en 18 sectores críticos, mientras que DORA, aplicable desde enero 2025, impone requisitos estrictos de resiliencia operativa específicamente a las entidades financieras y a sus proveedores críticos de servicios ICT.

Ambas normativas reconocen explícitamente el factor humano en la cybersecurity: NIS2 requiere "formación en materia de cybersecurity y prácticas de higiene informática básica" (Artículo 21), mientras que DORA prevé que los órganos de gestión "posean conocimientos y competencias suficientes para comprender y evaluar los riesgos informáticos" (Artículo 5). Sin embargo, ninguna de las dos proporciona metodologías sistemáticas para evaluar las vulnerabilidades psicológicas que habilitan el 82-85 % de los ataques informáticos exitosos[2].

El Cybersecurity Psychology Framework (CPF)[1] llena esta brecha proporcionando un enfoque sistemático para identificar y mitigar las vulnerabilidades psicológicas pre-cognitivas. Este documento proporciona a los compliance officers y a los CISOs un roadmap de integración práctico que mapea las evaluaciones CPF sobre los requisitos NIS2 y sobre los cinco pilares de DORA, permitiendo a las organizaciones:

Beneficios Clave para los Programas de Compliance Europeos:

- Demostrar medidas de seguridad "en el estado del arte" como requerido por el Artículo 21 NIS2
- Satisfacer los requisitos de responsabilidad del management de DORA con métricas cuantificables del riesgo humano
- Reducir los incidentes relacionados con el factor humano del 25-40 % a través de la evaluación de las vulnerabilidades psicológicas
- Proporcionar evidencias medibles de medidas de seguridad "adecuadas y proporcionales" para las auditorías regulatorias
- Habilitar una postura de resiliencia operativa predictiva en lugar de reactiva

2. El Panorama Normativo: NIS2 y DORA

2.1. Panorama de la Directiva NIS2

La Directiva sobre Seguridad de las Redes y de los Sistemas Informáticos 2 (NIS2) representa una evolución significativa respecto a la Directiva NIS original de 2016, ampliando el ámbito de aplicación a 18 sectores críticos e introduciendo requisitos más estrictos:

Requisitos Clave NIS2:

- Medidas de gestión del riesgo que aborden los factores humanos (Artículo 21)
- Responsabilidad del órgano de gestión para la cybersecurity (Artículo 20)
- Señalización de incidentes dentro de 24/72 horas (Artículo 23)
- Evaluación de la seguridad de la cadena de suministro (Artículo 21(2)(d))
- Requisitos de formación sobre cybersecurity (Artículo 21(2)(g))

- Sanciones hasta 10 millones de euros o 2 % de la facturación global para las entidades esenciales

Ámbito de aplicación: Entidades esenciales (energía, transportes, sector bancario, sanidad, infraestructuras digitales) y entidades importantes (servicios postales, gestión de residuos, manufactura, proveedores digitales) en todos los Estados miembros de la UE.

2.2. Panorama del Reglamento DORA

El Digital Operational Resilience Act (DORA) establece un marco unificado para la gestión del riesgo ICT en el sector financiero, estructurado alrededor de cinco pilares:

Los Cinco Pilares de DORA:

1. **Gestión del Riesgo ICT** (Artículos 5-16): Framework comprehensivo para identificar, proteger, detectar, responder y recuperarse de los riesgos ICT
2. **Gestión de Incidentes ICT** (Artículos 17-23): Clasificación, señalización y análisis de los incidentes ICT
3. **Test de Resiliencia Operativa Digital** (Artículos 24-27): Tests regulares incluyendo los tests de penetración basados en amenazas (TLPT)
4. **Gestión del Riesgo de Terceros ICT** (Artículos 28-44): Due diligence, contratos y supervisión de los proveedores críticos ICT
5. **Compartición de Información** (Artículo 45): Acuerdos para el intercambio de intelligence sobre amenazas informáticas

Ámbito de aplicación: Más de 22.000 entidades financieras incluyendo bancos, compañías de seguros, empresas de inversión, proveedores de servicios sobre cripto-activos y sus proveedores críticos de servicios ICT de terceros.

2.3. El Gap del Factor Humano

Tanto NIS2 como DORA reconocen los factores humanos pero proporcionan una guía operativa limitada:

Cuadro 1: Requisitos sobre el Factor Humano en NIS2 y DORA

Requisito	**Texto Normativo**	**Gap de Implementación**
Responsabilidad del Management	NIS2 Art. 20, DORA Art. 5	Ninguna metodología para evaluar los sesgos cognitivos del management
Formación y Sensibilización	NIS2 Art. 21(2)(g), DORA Art. 13(6)	Foco en la transferencia de conocimientos, no en el cambio comportamental
Prevención del Error Humano	NIS2 Considerando 89, DORA Art. 9	Ningún framework para la evaluación de las vulnerabilidades pre-cognitivas
Respuesta al Estrés	DORA Art. 11 (gestión de crisis)	Ninguna métrica de resiliencia psicológica

El Threat Landscape 2024 de ENISA para el Sector Financiero reporta que el 46 % de los incidentes informáticos han golpeado institutos de crédito europeos, con la ingeniería social y el error humano que permanecen como vectores de ataque primarios[5]. La encuesta EY/IIF sobre Gestión del Riesgo Bancario confirma que el 82 % de los CROs europeos clasifica la cybersecurity como la principal preocupación de riesgo[6].

3. El Business Case para la Resiliencia Psicológica

3.1. Costo de los Incidentes Relacionados con el Factor Humano en Europa

Los datos específicos europeos demuestran el impacto financiero de las brechas de seguridad relacionadas con el factor humano:

- Costo medio de una violación de datos en la UE: 4,3 millones de euros (IBM Security, 2024)
- El 65 % de las instituciones financieras europeas ha sufrido ataques ransomware en 2024
- El mercado europeo de cybersecurity ha alcanzado 67,79 mil millones de euros en 2024, con un CAGR del 12,42 %
- ENISA reporta un aumento del 40 % de los ataques informáticos a las PYMEs europeas en 2022-2024
- Las organizaciones de servicios financieros emplean en promedio 233 días para detectar y contener las violaciones

3.2. Contexto de las Sanciones Normativas

El incumplimiento comporta consecuencias financieras significativas:

Sanciones NIS2:

- Entidades esenciales: Hasta 10 millones de euros o 2 % de la facturación mundial anual total
- Entidades importantes: Hasta 7 millones de euros o 1,4 % de la facturación mundial anual total
- Responsabilidad personal del management en caso de negligencia grave

Sanciones DORA:

- Sanciones hasta el 2 % de la facturación mundial anual total para las entidades financieras
- Sanciones individuales hasta 1 millón de euros para los responsables
- Proveedores ICT críticos: Hasta el 1 % de la facturación mundial diaria media (penalidades periódicas)

3.3. Enfoque CPF: Mejorar el Compliance Normativo

La metodología CPF transforma el compliance sobre el factor humano de ejercicios formales a reducción medible del riesgo:

- Proporciona métricas cuantificables para medidas "adecuadas y proporcionales" (NIS2 Art. 21)
- Permite la demostración basada en evidencias de los "conocimientos y competencias" del management (DORA Art. 5)
- Aborda las causas psicológicas en la raíz de los incidentes de seguridad
- Soporta los ciclos de mejora continua requeridos por ambas normativas
- Genera ROI medible a través de la reducción de incidentes

4. Arquitectura de Integración del Framework

4.1. Modelo de Integración NIS2

La Tabla 2 mapea las categorías CPF sobre los requisitos del Artículo 21 NIS2, demostrando cómo la evaluación del riesgo psicológico mejora el compliance.

Cuadro 2: Integración CPF con los Requisitos del Artículo 21 NIS2

Requisito NIS2	**Enfoque Tradicional**	**Mejora CPF**	**Categorías CPF**
Análisis de riesgos y políticas (Art. 21.2.a)	Evaluación de vulnerabilidades técnicas	Perfilado de vulnerabilidades psicológicas, mapeo de sesgos cognitivos	[1.x], [4.x], [5.x]
Gestión de incidentes (Art. 21.2.b)	Procedimientos de respuesta técnicos	Protocolos de respuesta conscientes del estrés, calidad decisional bajo presión	[7.x], [10.x]
Continuidad operativa (Art. 21.2.c)	Backups técnicos, planes DR	Recuperación psicológica, restablecimiento de la confianza, resiliencia del equipo	[4.x], [6.x]
Seguridad supply chain (Art. 21.2.d)	Evaluaciones de proveedores, contratos	Evaluación del riesgo humano de terceros, vulnerabilidades de transferencia de autoridad	[3.x], [8.x]
Seguridad HR (Art. 21.2.e)	Controles de antecedentes, control de accesos	Psicología de amenazas internas, indicadores de estrés organizacional	[4.x], [5.x], [9.x]
Formación e higiene (Art. 21.2.g)	Programas de awareness, e-learning	Formación sobre sesgos pre-cognitivos, diseño de intervenciones comportamentales	[1.x], [2.x], [6.x]
Control de accesos (Art. 21.2.i)	IAM, implementación MFA	Análisis de estructuras de autoridad, resistencia a ingeniería social	[3.x], [8.x]

4.2. Modelo de Integración Cinco Pilares DORA

La Tabla 3 demuestra la integración CPF a través de los cinco pilares de resiliencia operativa de DORA.

Cuadro 3: Integración CPF con los Cinco Pilares DORA

Pilar DORA	**Requisito Normativo**	**Mejora CPF**	**Categorías CPF**
Pilar 1: Gestión Riesgo ICT	Responsabilidad management, framework riesgo (Art. 5-16)	Evaluación de sesgos cognitivos del liderazgo, métricas de calidad decisional	[2.x], [5.x], [6.x]
Pilar 2: Gestión de Incidentes	Clasificación, señalización, análisis (Art. 17-23)	Detección de anomalías comportamentales, patrones de errores inducidos por estrés	[7.x], [9.x], [10.x]
Pilar 3: Test de Resiliencia	TLPT, test de vulnerabilidades (Art. 24-27)	Test del factor humano, métricas de resistencia a ingeniería social	[1.x], [3.x], [8.x]
Pilar 4: Riesgo de Terceros	Due diligence, supervisión (Art. 28-44)	Evaluación del riesgo del personal de proveedores, psicología del riesgo de concentración	[4.x], [5.x], [8.x]
Pilar 5: Compartición de Info	Threat intelligence (Art. 45)	Dinámicas de confianza en el intercambio, barreras cognitivas a la colaboración	[4.x], [6.x]

4.3. Integración Cross-Framework: Alineamiento NIS2 y DORA

Para las entidades financieras sujetas a ambas normativas, la Tabla 4 muestra el enfoque unificado de integración CPF.

Cuadro 4: Integración CPF Unificada para Compliance NIS2-DORA

Área de Compliance	**Referencia NIS2**	**Referencia DORA**	**Punto de Integración CPF**
Governance	Art. 20 (Management)	Art. 5 (Órgano de gestión)	Dashboard de riesgo psicológico ejecutivo
Gestión de Riesgo	Art. 21.2.a	Art. 6-9 (Framework riesgo ICT)	Modelo de riesgo humano-técnico integrado
Respuesta a Incidentes	Art. 23 (Señalización)	Art. 17-19 (Clasificación)	Playbook de respuesta psychology-aware
Testing	Art. 21.2.f	Art. 24-27 (TLPT)	Penetration testing del factor humano
Terceros	Art. 21.2.d	Art. 28-44 (TPRM)	Protocolo de evaluación del personal de proveedores
Formación	Art. 21.2.g	Art. 13.6 (Awareness)	Programas de intervención precognitiva

5. Mapeo Detallado: Categorías CPF y Requisitos Normativos

5.1. DORA Pilar 1: Framework de Gestión del Riesgo ICT

Los Artículos 5-16 de DORA establecen requisitos comprehensivos para la gestión del riesgo ICT. El CPF los mejora a través de la evaluación de la dimensión psicológica.

Artículo 5 - Responsabilidad del Órgano de Gestión:

DORA requiere que los órganos de gestión "definan, aprueben, supervisen y sean responsables de la implementación de todos los acuerdos relativos al marco de gestión de los riesgos informáticos." El CPF mejora esto a través de:

- **[2.x] Evaluación de Sesgos Cognitivos**: Identificación de los sesgos decisionales (overconfidence, automation bias, normalcy bias) que pueden influenciar la governance del riesgo ICT
- **[5.x] Perfilado de Respuesta al Estrés**: Evaluación de las performances del management en condiciones de crisis
- **[6.x] Análisis de Dinámicas de Grupo**: Evaluación del groupthink a nivel de consejo y de las dinámicas de autoridad

Artículo 9 - Protección y Prevención:

DORA requiere medidas para "proteger los sistemas ICT y prevenir la ocurrencia de riesgos informáticos." Las mejoras sobre el factor humano incluyen:

- **[1.x] Resistencia a Ingeniería Social**: Evaluación pre-cognitiva de la susceptibilidad a la manipulación
- **[3.x] Vulnerabilidades de Transferencia de Autoridad**: Identificación de la confianza inapropiada depositada en autoridades técnicas o externas
- **[8.x] Indicadores de Amenazas Internas**: Marcadores psicológicos que preceden acciones malévolas o negligentes

5.2. DORA Pilar 2: Gestión de Incidentes ICT

Los Artículos 17-23 regulan la clasificación, señalización y análisis de incidentes. La integración CPF aborda los elementos humanos:

Artículo 17 - Proceso de Gestión de Incidentes ICT:

- **[7.x] Calidad Decisional Bajo Estrés**: Protocolos para mantener la capacidad analítica durante los incidentes
- **[9.x] Prevención de Breakdown Comunicativo**: Abordar las barreras psicológicas a una comunicación eficaz durante los incidentes
- **[10.x] Recuperación Psicológica Post-Incidente**: Restablecimiento de la resiliencia del equipo después de incidentes graves

Mejora de la Señalización de Incidentes:

Los requisitos de early warning a 24 horas y report de incidentes a 72 horas previstos por DORA se benefician de:

- Procedimientos de señalización calibrados sobre el estrés que tienen en cuenta la carga cognitiva
- Rutas de escalación predefinidas que reducen la confusión sobre la autoridad
- Protocolos de debriefing psicológico que mejoran la precisión del análisis de causas

5.3. DORA Pilar 3: Test de Resiliencia Operativa Digital

Los Artículos 24-27 imponen programas de test incluyendo los tests de penetración basados en amenazas (TLPT) para las entidades financieras significativas.

Artículo 25 - Test de Herramientas y Sistemas ICT:

El CPF mejora los tests técnicos tradicionales con la evaluación del factor humano:

- **Test de Ingeniería Social**: Evaluación integrada de la resistencia psicológica
- **Escenarios de Stress Testing**: Calidad decisional humana bajo crisis simuladas
- **Test de Manipulación de Autoridad**: Resistencia a impersonificación y pretexting

Artículo 26 - Test de Penetración Basados en Amenazas:

Los programas TLPT requeridos para las entidades significativas deberían incorporar:

- Identificación de targets humanos usando el perfilado de vulnerabilidades CPF
- Simulación de vectores de ataque psicológicos
- Definición de baselines comportamentales para la detección de anomalías

5.4. DORA Pilar 4: Gestión del Riesgo ICT de Terceros

Los Artículos 28-44 establecen requisitos comprehensivos de supervisión de terceros, incluyendo el framework de oversight para los Proveedores ICT Críticos de Terceros (CTPP).

Artículo 28 - Principios Generales:

- [**4.x**] **Evaluación de Dinámicas de Confianza**: Evaluar la confianza apropiada versus mal depositada en las relaciones con proveedores
- [**5.x**] **Psicología del Riesgo de Concentración**: Comprender los patrones de dependencia organizacional
- [**8.x**] **Riesgo del Personal de Proveedores**: Extender la evaluación del riesgo humano al personal crítico de terceros

Registro de Información (Artículo 28(3)):

El registro obligatorio de los acuerdos con terceros ICT debería incluir:

- Indicadores de riesgo humano para las relaciones críticas con proveedores
- Mapeo de las estructuras de autoridad para los contactos clave de proveedores
- Métricas psicológicas del riesgo de concentración

5.5. DORA Pilar 5: Acuerdos de Compartición de Información

El Artículo 45 alienta el intercambio de threat intelligence entre entidades financieras.

Mejora CPF para la Compartición de Información:

- [**4.x**] **Análisis de Barreras de Confianza**: Identificar los obstáculos psicológicos a un intercambio eficaz
- [**6.x**] **Dinámicas Competitivas**: Abordar la psicología de grupo que inhibe la colaboración
- **Diseño de Protocolos de Intercambio**: Estructuras que acomodan los requisitos humanos de construcción de confianza

6. Metodología de Implementación

6.1. Fase 1: Evaluación de Gap Normativo (30 Días)

Objetivo: Establecer la baseline de integración CPF con la actual postura de compliance.

Actividades:

- Mapear las medidas de compliance NIS2/DORA existentes sobre las categorías CPF
- Conducir evaluación baseline de las vulnerabilidades psicológicas del personal clave
- Identificar los puntos de integración de alta prioridad basados en el riesgo normativo
- Establecer un framework de medición alineado con el reporting normativo

Entregables:

- Análisis de gap de compliance enriquecido con CPF
- Roadmap de integración priorizado
- Métricas baseline del riesgo psicológico
- Framework de evidencias normativas

6.2. Fase 2: Integración Piloto (60 Días)

Objetivo: Implementar la evaluación CPF en las áreas de compliance de alto riesgo.

Actividades:

- Desplegar evaluación CPF para el órgano de gestión (compliance DORA Art. 5)

- Implementar test del factor humano junto a los tests de resiliencia técnicos
- Integrar indicadores psicológicos en los procedimientos de gestión de incidentes
- Establecer protocolos de evaluación del riesgo humano de terceros

Entregables:

- Perfil de riesgo psicológico del órgano de gestión
- Playbook de respuesta a incidentes mejorado
- Registro de riesgo humano de terceros
- Paquete inicial de evidencias de compliance

6.3. Fase 3: Integración Completa (90 Días)

Objetivo: Completar la integración CPF sobre todos los requisitos normativos.
Actividades:

- Extender la evaluación a todo el personal en funciones críticas
- Integrar las métricas CPF en el framework de gestión del riesgo ICT
- Implementar monitoreo psicológico continuo junto al monitoreo técnico
- Establecer la integración del reporting normativo

Entregables:

- Dashboard completo del riesgo del factor humano
- Documentación de compliance NIS2/DORA integrada
- Framework de mejora continua
- Paquete de evidencias para auditoría normativa

7. Framework de Medición y ROI

7.1. Métricas de Compliance

Indicadores de Compliance NIS2:

- Porcentaje de cobertura del riesgo del factor humano sobre los requisitos del Artículo 21
- Mejora de eficacia de formación (cambio comportamental vs. retención de conocimientos)
- Tasa de completación de evaluación del riesgo humano en supply chain
- Precisión en identificación de causas humanas en incidentes

Indicadores de Compliance DORA:

- Tendencia del puntaje de riesgo psicológico del órgano de gestión
- Cobertura de test del factor humano en el programa de test de resiliencia
- Porcentaje de integración de evaluación del riesgo humano de terceros
- Mejora de participación en el intercambio de información

7.2. Métricas de Resiliencia Operativa

- Reducción de tasa de incidentes relacionados con el factor humano
- Tiempo medio de detección de amenazas habilitadas por el hombre
- Puntajes de calidad decisional en condiciones de estrés
- Mejora de resistencia a ingeniería social
- Tiempo de recuperación psicológica post-incidente

7.3. Framework de Cálculo del ROI

Cálculo del Cost Avoidance:

$$\text{ROI Anual} = \frac{\text{Costos Evitados} - \text{Costos de Implementación}}{\text{Costos de Implementación}} \times 100 \tag{1}$$

Donde los Costos Evitados incluyen:

- Reducción de costos de incidentes = (Tasa histórica de incidentes × Costo medio de incidente) - (Tasa actual × Costo)
- Evitación de sanciones normativas = Potenciales sanciones evitadas ponderadas por el riesgo
- Eficiencia operativa = Reducción de tasa de falsos positivos × Ahorro de costos de investigación

Rango ROI para Servicios Financieros Europeos:

- Año 1: 180-280 % ROI (reducción de incidentes + eficiencia de compliance)
- Año 2: 350-550 % ROI (madurez operativa + reducción de costos de auditoría)
- Año 3+: 450-750 % ROI (integración cultural + capacidad predictiva)

8. Caso de Estudio: Implementación en un Grupo Bancario Europeo

8.1. Perfil de la Organización

- Sector: Grupo Bancario Pan-Europeo
- Status Normativo: Instituto Significativo (supervisado SSM)

- Empleados: 28.000 en 12 Estados miembros de la UE
- Equipo de IT Security: 89 profesionales
- Presupuesto anual de seguridad: 18 millones de euros
- Requisitos normativos: NIS2 (entidad esencial) + DORA (ente crediticio)

8.2. Enfoque de Implementación

La organización implementó la integración CPF en 6 meses en preparación al compliance DORA:

Resultados Fase 1 (30 días):

- El análisis de gap identificó 18 brechas de compliance sobre el factor humano de alta prioridad
- La evaluación del órgano de gestión reveló que el 72 % mostraba indicadores de automation bias
- El 41 % del personal en funciones críticas demostró vulnerabilidad a la transferencia de autoridad
- Identificadas brechas sobre el riesgo humano en el 67 % de los proveedores ICT críticos

Resultados Fase 2 (90 días):

- Reducción del 34 % en la tasa de éxito de incidentes de ingeniería social
- Mejora del 27 % en el tiempo de detección de amenazas habilitadas por el hombre
- Calidad decisional del management bajo estrés mejorada del 31 %
- Evidencias de compliance DORA Artículo 5 significativamente reforzadas

Resultados Fase 3 (180 días):

- Reducción del 47 % de los incidentes de seguridad totales relacionados con el factor humano
- Integración completa con el programa de compliance sobre los cinco pilares DORA
- Mejora del 91 % en la calidad de respuesta en condiciones de estrés
- ROI del 187 % en el primer año
- 2,8 millones de euros en costos de incidentes evitados
- Evaluación positiva de la autoridad competente nacional

8.3. Beneficios para el Compliance Normativo

Mejoras en Compliance NIS2:

- Demostradas medidas “en el estado del arte” para los factores humanos (Art. 21)
- Evidencias cuantificables de la responsabilidad del management (Art. 20)

- Capacidades mejoradas de análisis de causas de incidentes
- Documentación mejorada del riesgo humano en la supply chain

Mejoras en Compliance DORA:

- Evaluación documentada de los conocimientos del órgano de gestión (Art. 5)
- Integración del factor humano en el framework de riesgo ICT (Art. 6)
- Test de resiliencia mejorados con factores humanos (Art. 25)
- Registro completo del riesgo humano de terceros (Art. 28)

9. Líneas Guía y Best Practices para la Implementación

9.1. Checklist Pre-Implementación

Preparación Normativa:

- Estado actual de compliance NIS2/DORA evaluado
- Expectativas de la autoridad competente comprendidas
- Requisitos de reporting normativo mapeados
- Framework de documentación de evidencias establecido

Preparación Organizacional:

- Sponsorship ejecutivo del CISO y liderazgo de compliance
- Asignación de presupuesto para herramientas de evaluación del factor humano
- Evaluación de impacto en privacidad completada para las evaluaciones psicológicas
- Consulta con representaciones sindicales/comité de empresa (donde requerido)

Prerequisitos Técnicos:

- Framework de gestión del riesgo ICT operativo
- Procesos de gestión de incidentes documentados
- Programa de test de resiliencia establecido
- Procedimientos de gestión del riesgo de terceros implementados

9.2. Consideraciones Específicas Europeas

Compliance de Protección de Datos:

- Base jurídica GDPR Artículo 6 para las evaluaciones psicológicas
- Minimización de datos en el diseño de las evaluaciones
- Períodos de conservación alineados con los requisitos normativos
- Consideraciones sobre las transferencias transfronterizas para grupos multi-entidad

Relaciones con los Empleados:

- Transparencia sobre los propósitos y el uso de las evaluaciones
- Aplicación no discriminatoria del perfilado psicológico
- Consulta con representaciones sindicales donde legalmente requerido
- Derechos individuales de acceso a los resultados de las evaluaciones

Engagement con los Reguladores:

- Discusión proactiva con las autoridades competentes nacionales
- Alineamiento con las expectativas de los CSIRT sectoriales
- Integración con los procesos de peer review
- Documentación adecuada para auditorías normativas

9.3. Errores Comunes en la Implementación

Errores Normativos:

- Tratar el CPF como sustituto del compliance técnico en lugar de como mejora
- Documentación inadecuada para los requisitos de evidencia normativa
- Falta de alineamiento con las variaciones de transposición nacional (NIS2)
- Subestimación de los requisitos de coordinación transfronteriza

Errores Organizacionales:

- Evaluación de impacto en privacidad insuficiente
- Falta de involucración de las representaciones sindicales donde requerido
- Énfasis excesivo en la evaluación sin programas de intervención
- Falta de integración con los procesos GRC existentes

Errores Técnicos:

- Implementación aislada separada del framework de riesgo ICT
- Integración inadecuada con los sistemas de gestión de incidentes
- Escaso alineamiento del reporting con los requisitos normativos
- Protocolos de integración de terceros insuficientes

10. Desarrollos Normativos Futuros

10.1. Evolución del Panorama Europeo

El framework de integración CPF está diseñado para acomodar la evolución de los requisitos normativos:

Desarrollos Esperados:

- Líneas guía técnicas ENISA sobre factores humanos (previstas 2025-2026)
- Estándares técnicos regulatorios ESA sobre metodologías de test
- Orientaciones de las autoridades competentes nacionales sobre requisitos "estado del arte"
- Procedimientos de coordinación EU-CyCLONe para incidentes transfronterizos

Adaptabilidad del Framework:

- El mapeo modular de las categorías CPF permite la integración de actualizaciones normativas
- El framework de medición soporta la evolución de los requisitos de reporting
- La documentación de evidencias está diseñada para la continuidad del audit trail
- El modelo de mejora continua se alinea con las expectativas normativas

11. Conclusiones y Próximos Pasos

La integración de la evaluación del riesgo psicológico en los programas de compliance NIS2 y DORA llena una brecha crítica en los frameworks europeos de resiliencia operativa. Aunque ambas normativas reconocen explícitamente los factores humanos en la cybersecurity, ninguna de las dos proporciona metodologías sistemáticas para evaluar y mitigar las vulnerabilidades psicológicas que habilitan la mayoría de los ataques informáticos exitosos.

El Cybersecurity Psychology Framework ofrece una solución práctica y medible que mejora el compliance normativo produciendo al mismo tiempo mejoras en la resiliencia operativa. A través del mapeo detallado sobre los requisitos NIS2 y sobre los cinco pilares DORA, las organizaciones pueden implementar la evaluación de las vulnerabilidades psicológicas dentro de sus programas de compliance existentes.

Acciones Inmediatas para CISOs y Compliance Officers Europeos:

1. Conducir un análisis de gap enriquecido con CPF respecto a los requisitos del Artículo 21 NIS2 y de los pilares DORA
2. Priorizar la evaluación psicológica del órgano de gestión (compliance DORA Artículo 5)
3. Integrar los tests sobre el factor humano en los programas de test de resiliencia
4. Establecer protocolos de evaluación del riesgo humano de terceros
5. Desarrollar un framework de evidencias normativas para las medidas de riesgo psicológico

6. Involucrar a las autoridades competentes nacionales sobre el enfoque al compliance del factor humano

Para las entidades financieras que enfrentan la fecha límite DORA de enero 2025 y los proveedores de servicios esenciales sujetos a las obligaciones NIS2, el framework de integración CPF proporciona un recorrido estructurado hacia un compliance comprehensivo sobre el factor humano. Las organizaciones que implementan este enfoque obtienen mejoras significativas tanto en la postura de compliance normativo como en los resultados de resiliencia operativa.

Las evidencias demuestran que la evaluación del riesgo psicológico no es simplemente una mejora del compliance sino un requisito fundamental para una resiliencia operativa eficaz en un ambiente donde los factores humanos contribuyen a la gran mayoría de los incidentes de seguridad. A medida que los reguladores europeos se concentran cada vez más en la calidad y la eficacia de las medidas de seguridad, frameworks como el CPF se vuelven componentes esenciales de programas de seguridad demostrablemente "adecuados y proporcionales".

Biografía del Autor

Giuseppe Canale, CISSP, es un investigador independiente en cybersecurity con 27 años de experiencia en la gestión de programas de seguridad enterprise. Se especializa en la integración de la evaluación del riesgo psicológico con los frameworks de compliance normativo y ha desarrollado el Cybersecurity Psychology Framework (CPF) para la evaluación de la postura de seguridad organizacional. Su trabajo se concentra en llenar la brecha entre los controles de seguridad técnicos y las vulnerabilidades del factor humano en los contextos normativos europeos.

Declaración sobre la Disponibilidad de Datos

Templates de implementación, herramientas de evaluación, matrices de mapeo normativo y detalles de casos de estudio están disponibles a través de la plataforma CPF3.org, sujetos a apropiados acuerdos de licencia.

Referencias

[1] Canale, G. (2025). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5387222

[2] Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Enterprise.

[3] Parlamento Europeo y Consejo. (2022). Directiva (UE) 2022/2555 relativa a medidas para un nivel común elevado de ciberseguridad en la Unión (Directiva NIS2). *Gaceta Oficial de la Unión Europea*, L 333/80.

[4] Parlamento Europeo y Consejo. (2022). Reglamento (UE) 2022/2554 relativo a la resiliencia operativa digital para el sector financiero (DORA). *Gaceta Oficial de la Unión Europea*, L 333/1.

[5] Agencia de la Unión Europea para la Ciberseguridad. (2024). *ENISA Threat Landscape: Finance Sector*. ENISA.

[6] EY e Institute of International Finance. (2024). *Global Bank Risk Management Survey: European Results*. EY.

[7] IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.

[8] Banco Central Europeo. (2024). One step ahead: protecting the cyber resilience of financial infrastructures. Intervención de Piero Cipollone.

[9] Autoridad Europea de Valores y Mercados. (2024). *Digital Operational Resilience Act (DORA) Implementation Guidance*. ESMA.

[10] Autoridad Bancaria Europea. (2024). *Guidelines on ICT and Security Risk Management*. EBA.