La_SEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid
2026
Volumen 7, nº 2, pp., 13-26
ISSN 2659-9791
UAM
- DRAFTS OF ECONOMIC INTELLIGENCE -

# PROPUESTA DE INVESTIGACIÓN: PERSONALIDAD Y CONDUCTAS CONTRAPRODUCENTES EN EL ENTORNO LABORAL

Pereyra López, Nereida*

## Resumen

Durante años, en psicología de la personalidad se ha buscado consensuar modelos explicativos que permitan comprender y predecir los fundamentos e indicadores del comportamiento humano. Paralelamente, en el ámbito empresarial se ha reconocido a las personas como un elemento clave en las organizaciones, concretamente en lo referente a conductas problemáticas, dado que estas pueden suponer importantes obstáculos, pérdidas económicas y consecuencias legales. Sin embargo, no ha sido hasta hace relativamente poco cuando se ha puesto una atención específica en las conductas maliciosas relacionadas con la difusión de información privada de una empresa. En este contexto, el presente trabajo recoge la teoría de la personalidad como fundamento relativamente estable del comportamiento humano y la estudia como posible predictor de conductas maliciosas, específicamente aquellas relacionadas con la filtración deliberada de información sensible de la organización. Para ello, se ha realizado una revisión de los principales modelos teóricos de la psicología de la personalidad, de entre los cuales se ha seleccionado como marco de referencia el modelo PEN de Eysenck por su robustez y aplicabilidad al entorno empresarial. Posteriormente, se ha relacionado este modelo con los indicadores y terminología presentes en la literatura empresarial sobre conductas maliciosas y se ha diseñado una investigación mixta para analizar, en una muestra representativa, la posible correlación entre dichos rasgos de personalidad y la propensión a cometer conductas maliciosas en el entorno laboral.

**Palabras clave:** PEN, personalidad, Eysenck, ciberseguridad, conductas contraproducentes, *insiders* maliciosos, amenaza interna.

## Abstract

*For years, personality psychology has sought to agree on explanatory models that allow us to understand and predict the foundations and indicators of human behaviour. At the same time, in the business world, people have been recognised as a key element in organisations, specifically in relation to problematic behaviour, given that this can pose significant obstacles, economic losses and legal consequences. However, it is only relatively recently that specific attention has been paid to malicious behaviour related to the dissemination of a company's private information. In this context, this paper takes personality theory as a relatively stable foundation of human behaviour and studies it as a possible predictor of malicious behaviour, specifically that related to the deliberate leaking of sensitive information from the organisation. To this end, a review of the main theoretical models of personality psychology was conducted, from which Eysenck's PEN model was selected as a reference framework due to its robustness and applicability to the business environment. Subsequently, this model was linked to the indicators and terminology found in the business literature on malicious behaviour, and a mixed research design was developed to analyse, in a representative sample, the possible correlation between these personality traits and the propensity to engage in malicious behaviour in the workplace.*

***Key words:*** *PEN, personality, Eysenck, cybersecurity, counterproductive behaviour, malicious insiders, internal threat.*

* *Escuela de Inteligencia Económica (La_SEI). Universidad Autónoma de Madrid (Spain)* Correo de contacto: nereida.npl@gmail.com

# 1. Introducción

En los últimos años el incremento de la dependencia tecnológica en el entorno empresarial ha hecho que la ciberseguridad se haya convertido en un punto clave para la protección ante amenazas (Eftimie, S. et al., 2020). Ante este escenario, el concepto de fuga de información ha adquirido relevancia como un riesgo de alto impacto, especialmente al ser relacionado con el factor humano como vector para que se produzca (Alzaabi, F.R. y Mehmood, A., 2024).

El factor humano se conceptualiza como el conjunto de características y conductas individuales de los empleados que pueden provocar una vulnerabilidad o perjuicio en la ciberseguridad de una organización. Cada vez son más las normativas que imponen la necesidad de gestionar el riesgo cibernético que pueden suponer las personas dentro de las organizaciones, como NIS2 o DORA, y también las instituciones como ENISA que se dedican a investigarlo (Douligeris et al., 2020).

Ahora bien, desde la psicología se establece que las conductas de las personas se producen en base a elementos como la personalidad, motivaciones, percepciones, atribuciones, atención o emociones, que intervienen en el procesamiento cognitivo que realizan cuando interaccionan con el mundo; y es en las diferencias individuales de estos elementos donde radican las diferencias de las conductas (Horstmann, K. T., 2021). Del mismo modo afectan a las conductas que tiene las personas en entornos digitales y laborales (Martinko, M. J., 2002; Parasuraman, R., y Jiang, Y., 2012).

En el presente trabajo se propone una línea de investigación basada en las relaciones observadas en la literatura entre los factores de personalidad y las conductas que comprometen la seguridad de la información de una empresa. Para ello, se propone el estudio de una muestra conformada por trabajadores que hayan cometido o no este tipo de conductas. Los datos recogidos incluirán sus intencionalidades y motivaciones ante diversos escenarios (como la posibilidad de una ganancia económica o de actuar por venganza) y el perfil de personalidad, evaluado mediante la herramienta de EPQ-R de Eysenck.

Los resultados esperados son que la dimensión de psicoticismo, según el modelo PEN de Eysenck, sea el factor más predisponente, dado que la evidencia la vincula con una alta tolerancia al riesgo, baja responsabilidad y tendencias egocéntricas; características asociadas a conductas maliciosas.

## 1.1. Fuga de información

La ciberseguridad puede estar comprometida por el factor humano y en la literatura se ha identificado que uno de los riesgos relacionados es la fuga de información. Esta se concibe como la exposición intencional (robo, espionaje, sabotaje y fraude) o no (errores humanos, fallos del sistema) de datos privados de una organización que sólo deben ser conocidos para un grupo de personas determinado y terminan siendo visibles o accesibles para terceras personas (Cheng, L., et al., 2017; Instituto Nacional de Ciberseguridad [INCIBE], 2017). Es un tema crucial pues como se recoge en el informe "Cost of a Data Breach" de IBM (2025), la vulneración de los datos ha supuesto un coste medio mundial de unos 4,4 millones de dólares, aunque sólo el 49% de las empresas que han sufrido este tipo de accidentes planean invertir en seguridad de datos.

### 1.1.1. Causas

Entre las causas de la fuga de información se encuentran diversas clasificaciones. Desde el Instituto Nacional de Ciberseguridad (INCIBE) se identifican dos tipos principales de causas que pueden originar fugas de información: las organizativas y las técnicas. Entre las organizativas se encuentran la falta de clasificación de la información en función del nivel de confidencialidad, la falta de conocimiento y formación de los trabajadores en materia de ciberseguridad, la ausencia de procedimientos, pautas y obligaciones claras de ciberseguridad o la ausencia de acuerdos de confidencialidad. En cuanto a las causas técnicas, se incluyen la presencia de códigos maliciosos o *malware*, accesos no autorizados a sistemas e infraestructuras, el acceso generalizado a la información almacenada en la nube y el uso de tecnologías móviles que pueden almacenar información sensible y confidencial de la organización (Instituto Nacional de Ciberseguridad [INCIBE], 2016).

No obstante, desde la perspectiva del factor humano, se identifican como causas la acción de agentes externos con la intención de robar datos (como ataques cibernéticos, suplantación de identidad y accesos no autorizados en la nube) (Alqahtani, N., 2025) y la intervención de agentes internos. Entre los últimos, se distinguen dos tipos: los no intencionales y los intencionales.

La fuga no intencional de información se define como la divulgación accidental por parte de un empleado de datos de la organización que no están destinados a ser compartidos con personas externas a esta (Ritala, P., et al., 2015).

Esta puede producirse principalmente por una falta de conciencia, capacitación en ciberseguridad, el uso inadecuado de herramientas tecnológicas y errores (como, por ejemplo, publicaciones o envíos accidentales de información sensible, cifrado inadecuado o errores de configuración) (Cheng, L., et al., 2017).

La fuga intencional es la exposición deliberada de información de la organización a personas que no tenían acceso (Ritala, P., et al., 2015). Esta se produce por motivaciones del trabajador (como una ganancia económica y provocar un perjuicio).

Ya en 2023 Kaspersky, en su "Kaspersky Human Factor 360º report 2023" expuso que en los dos años anteriores un 85 % de las empresas de todo el mundo había sufrido algún incidente cibernético, "el 17 % de los cuales fueron causados por un comportamiento malicioso deliberado por parte de los empleados." O, dicho de otra manera, producidos por amenazas internas o *insiders* maliciosos. Además, en su investigación, concluyeron que, de las empresas entrevistadas, el 20% de los empleados que "cometieron conductas maliciosas tenía como intención el beneficio personal", datos que venían a indicar el mantenimiento de una tendencia preocupante que se venía plasmando años atrás (Saxena, N. et al., 2020). Además, en el Verizon Data Breach Investigations Report (2025) se identificó que en el 60% de los incidentes estaba involucrado el factor humano.

Entre las causas más descritas y consensuadas en la literatura es el beneficio económico (Verizon, 2025; Saxena, N. et al., 2020) y la venganza. Por ello, no es de extrañar que entre un tercio y la mitad de las empresas a nivel mundial consideren en los próximos años invertir en softwares de detección de este tipo de amenazas (Kaspersky, 2023) pues "comprender las razones detrás de los ataques es necesario para desarrollar estrategias efectivas que reduzcan los riesgos asociados." (Eftimie, S. et al., 2020).

La distinción entre ambos tipos es clave para diseñar estrategias de prevención y mitigación efectivas, dado que las medidas destinadas al control de las fugas accidentales difieren de las que están orientadas a las intencionales. Comprender dicha diferencia permitirá a las organizaciones implementar y desarrollar políticas de seguridad más adecuadas.

### 1.1.2. Relevancia

Este fenómeno resulta de gran importancia para las organizaciones porque supone unas implicaciones de alto impacto para estas (INCIBE, 2016; Idensohn, C.J., et al., 2025). Como consecuencias se identifican principalmente cinco tipos: Operativas, económicas, legales, reputacionales y de seguridad.

Las operativas contemplan la pérdida de la ventaja competitiva (por ejemplo, cuando un competidor obtiene información sobre estrategias comerciales o propiedad intelectual), la pérdida de relaciones con socios y proveedores (al perder la confianza en la organización) y la interrupción de la actividad comercial (pudiéndose producir errores en la producción o provocar accidentes) (Wong, W., et al., 2019; Vafaei-Zadeh, A. et al., 2020).

Las legales implican hacer frente a la normativa, especialmente estricta para países europeos (con normativas como la RGPD) (Agencia Española de Protección de Datos [AEPD], 2021). Y las económicas han sido identificadas como la más costosas, con un promedio de unos 4,99 millones de dólares (IBM, 2025b).

Las reputacionales involucran daños a la imagen de la empresa y la generación de una opinión pública negativa (Wong, W., 2019). Y las de seguridad provocan que, al difundirse información sensible, pueda comprometer a la propia organización y a los individuos (por ejemplo, en caso de la difusión de datos personales) a fraudes, amenazas o ataques cibernéticos (Ahmadian, M., y Marinescu, D., 2020).

Además, se ha registrado en años anteriores una tendencia al alza. En 2019 se registró a nivel global un incremento de 4 mil millones a más de 22 mil millones de filtraciones respecto a 2018 (Neto, N. et al., 2021). Especialmente, se reporta que este incremento significativo general se debe a la incorporación extendida de trabajo remoto y al uso de la nube (Lubenets, S., et al., 2024); y por ello las indicaciones y las tendencias de las empresas es de orientar esfuerzos y recursos hacia la prevención y mitigación de este tipo de amenazas (Eftimie, S. et al., 2020; AEPD, 2021); Lavanya, P., y Shankar Sriram, V. S., 2022).

Así pues, el punto de partida es considerar que la fuga de información puede darse por la acción humana (amenaza o *insider*) y desde esta perspectiva en la literatura se plantea un camino para la detección de amenazas internas (Georgiadou, A., et al., 2022) con variables diferenciales individuales. Por tanto, el presente trabajo se centra en la fuga de información intencional.

## 1.2. Insider

### 1.2.1. Concepto

Tal y como se acaba de comentar, una fuga de información puede estar producida por una amenaza interna o *insider*. Este se define como una persona que dispone de acceso legítimo a los sistemas y a la información de la organización y que la utiliza de manera indebida, comprometiendo la seguridad de esta (INCIBE, 2023).

### 1.2.2. Tipos

En la literatura científica se describe una categorización dentro del concepto *insiders* según su intencionalidad: Los no intencionales y los intencionales.

Los no intencionales (o negligentes) son trabajadores que, sin ser conscientes del perjuicio que provocan, realizan acciones (como errores, despistes o desinformación) que constituyen "actos imprudentes (INCIBE, 2023) o conductas de "curiosidad o descuido" (Marbut, A. y Harms, P., 2023). Dichas acciones pueden conducir a situaciones de riesgo que un atacante o estafador puede aprovechar al conseguir de estos usuarios legítimos su información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta (INCIBE, 2017; Alhathally, L.,2020).

Los intencionales son empleados descontentos que, ya sea de forma individual o en colaboración con amenazas externas, utilizan deliberadamente su acceso legítimo para provocar un perjuicio a la organización o a los compañeros por venganza, ganancias financieras o ambos, (Saxena, N., et al, 2020; IBM, 2025b). En contraste con el grupo anterior, en estos casos existe una plena conciencia de sus actos (Eftimie, S. et al., 2020), así como una influencia significativa de factores psicológicos que acompañan a las conductas maliciosas (de daño intencional) (Idensohn, C. J., 2025). Es decir, los no intencionales carecen de esa conciencia y actúan sin una planificación deliberada de las conductas perjudiciales, pero cometen errores o descuidos que provocan fuga de información e incluso son objeto de ingeniería social (Zamorano, A., 2018)., y los *insiders* intencionales actúan con reflexión, planificación y racionalización de conductas no éticas (Marbut, A. y Harms, P., 2023).

### 1.2.3. Relevancia

Las amenazas internas constituyen uno de los mayores desafíos en materia de ciberseguridad para las organizaciones, especialmente debido a la disposición de accesos legítimos que disponen estas personas en los sistemas y su conocimiento sobre los procesos y datos sensibles. Pues son estos privilegios legítimos lo que usan para poder incurrir en los comportamientos perjudiciales, comprometiendo la confidencialidad, integridad o disponibilidad de la información corporativa (Chai, K., y Zolkipli, M., 2021) al tener la capacidad de eludir los controles internos, tener conocimiento o por disponer de accesos legítimos, como en el caso de robo de propiedad intelectual, el fraude o la filtración de datos (Liang, N., et al., 2023).

Si bien los datos muestran que este tipo de fenómenos es una minoría en el total de los incidentes registrados, las "pérdidas que provocan son las más costosas" y complicadas de detectar (Sowa, T., 2024). No obstante, los datos reportados en 2021 en el IBM X-Force Threat Intelligence Index recogían que "hasta un 60% de los ciberataques han sido cometidos por *insiders*" y que el tipo de información que han difundido era altamente confidencial (como "documentos clasificados del FBI, el ejército de Estados Unidos y fraudes bancarios con pérdidas de hasta 7 mil millones de dólares") (Al-Shehari, T. y Alsowali, R., 2021).

Y más recientemente, desde el Ponemon Institute y DTEX Systems (2025) anuncian que se está produciendo un incremento significativo de casos pasando de 3.269 en su estudio de 2018 a 7.868 en la investigación de este año, con una elevación del coste de 15,4 millones de dólares en 2022 a 17,4 millones de dólares en 2025.

Es decir, los *insiders* maliciosos pueden provocar un daño potencial mayor con un impacto especialmente elevado en la reputación de la empresa y en la confianza de los clientes y socios. Además, son difíciles de detectar, a menudo son subestimados o no reportados y pueden combinar diversas técnicas, lo que implica la necesidad de desarrollar continuamente métodos de detección. Asimismo, estos actores maliciosos pueden evolucionar con el tiempo.

De modo que las empresas dado que tienen responsabilidad de proteger su información sensible (Alzaabi, F. y Mehmood, a., 2024; Anju, A., et al., 2023) deben implementar estrategias para salvaguardar la seguridad de su información confidencial; para lo que requiere el monitoreo y control de los accesos de los trabajadores, evaluaciones del comportamiento del personal, firma de acuerdos de confidencialidad y secretos comerciales y la promoción de una cultura organizacional orientada a fomentar la responsabilidad y confianza (Shelke, P. y Hamalainen, T., 2024) y comprender el riesgo es relevante para poder reducir la probabilidad de ocurrencia (Ponemon Institute & DTEX Systems, 2025); pero en la actualidad existe una falta de investigación que aporte marcos teóricos y datos precisos al respecto.

## 1.3. Conductas contraproducentes o *counterproductive behaviors* (CWB)

### 1.3.1. Concepto

Teniendo presente que el factor humano en la fuga de información está relacionado con las conductas de los individuos, en el ámbito empresarial y de la ciberseguridad se describen comportamientos que suponen un riesgo para las organizaciones por su potencial para facilitar fugas de información crítica o confidencial. Estas conductas se engloban bajo el concepto "comportamiento laboral contraproducente" (CWB, por sus siglas en inglés), definido como el conjunto de comportamientos indeseables de un empleado destinados intencional y voluntariamente a producir un daño o a socavar los planes y objetivos de la organización o

de sus miembros (Zhou, Z., 2018; Zappalà, S. et al., 2022; American Psychological Association, 2023).

Este concepto contempla, entre otras, las conductas propias de *insider* malicioso. De entre las más reconocidas se encuentran la destrucción de la propiedad privada de la empresa, el uso de mentiras para el absentismo, los insultos a los compañeros, el hurto de objetos de la empresa o al empleador, el sabotaje, el fraude, el robo, el espionaje, el acoso (incluido el acoso sexual), la discriminación, la violencia en el lugar de trabajo, el consumo de drogas y alcohol y la violación de los acuerdos de confidencialidad (American Psychological Association, 2023). Algunas de estas conductas pueden comprometer directamente la seguridad de la información de la organización.

La literatura pone en relieve que estas conductas se producen con frecuencia y generan pérdidas económicas significativas para las organizaciones. Principalmente se ha identificado que elementos individuales (como una percepción de insatisfacción o injusticia en el puesto de trabajo) produce un estado de malestar en el trabajador que, con el tiempo, puede provocar que este opte por realizar conductas contraproducentes, incluso de carácter malicioso (si se presentan ira, venganza o búsqueda de ganancia individual). Por tanto, la comisión de estas conductas se ha relacionado con una reducción de la productividad y una pérdida de ganancias (por sabotaje, daño a la propiedad, robo, …) (Carpenter, N.et al., 2020). Además, las conductas contraproducentes maliciosas suponen un coste de miles de millones a las empresas (Carpenter, N.et al., 2020). De modo que, en las últimas dos décadas se ha intensificado el esfuerzo en investigación sobre las causas y motivaciones que expliquen que se produzcan. Zhou, Z. (2018).

### 1.3.2. Tipos y relación con los *insiders* maliciosos

Con respecto a la tipología, se distinguen principalmente tres tipos derivados de las razones que motivan conductas contraproducentes maliciosas: las organizativas, que resultan en comportamientos negativos dirigidos a la organización como "un salario injusto, aburrimiento en el trabajo o insatisfacción laboral"; las interpersonales, que resultan en comportamientos "dirigidos a otras personas" como "discusiones o una baja calidad de las relaciones en el trabajo"; y las individuales, que pueden ser "sociales, económicas, tecnológicas, legales, ambientales, psicosomáticas, demográficas, …" y que "deben analizarse en un contexto específico". No obstante, dentro de las organizativas se ha identificado una subclasificación que comprende el sabotaje, el fraude, el espionaje y robo de información o propiedad intelectual.

- El sabotaje. Se trata de una conducta que provoca graves perjuicios tanto a personas como organizaciones y se observa frecuentemente en trabajadores descontentos o insatisfechos pero que tienen conocimientos técnicos y accesos autorizados; un ejemplo descrito es la manipulación no autorizada de un sitio web. (Lavanya, P. y Shankar Sriram, V.S., 2022).
- El robo de propiedad intelectual. Se describe como la obtención indebida de información a la que se tiene acceso y que puede ser transferido posteriormente a otras empresas. (Lavanya, P. y Shankar Sriram, V.S., 2022).
- El fraude. Se trata de un acceso ilegal a datos financieros de la empresa para los que son requeridos accesos privilegiados autorizados, más característico de trabajadores con cierto rango (Lavanya, P. y Shankar Sriram, V.S., 2022).
- El espionaje. Consiste en la extracción sistemática de la información de la empresa frecuentemente para provocar un perjuicio a esta o un beneficio a otra organización. (Lavanya, P. y Shankar Sriram, V.S., 2022. No obstante, cuando es alguien externo quien trata de extraer esta información a este sujeto, es importante tener presente la forma de elicitar la información, puesto que, de lo contrario, el relato fácilmente puede estar sesgado.

Estas conductas maliciosas son las que se han identificado como resultado de los factores de personalidad en ciberseguridad (Georgiadou, A., et al., 2022) (Lavanya, P. y Shankar Sriram, V.S., 2022) (Saxena, N. et al., 2020) y su posible difusión (IBM., 2025b). Y esta perspectiva plantea una relación relevante entre ciertos rasgos de personalidad, que podrían ser suficientes para explicar la aparición este tipo de comportamientos (Szostek, D., et al., 2020).

### 1.3.3. Diferencias individuales en los comportamientos de *insiders* maliciosos

En la investigación sobre conductas maliciosas en el entorno laboral, se ha observado que los rasgos de conciencia y la amabilidad (pertenecientes al modelo de los Cinco Grandes) correlacionan significativamente con la tendencia a evitar este tipo de conductas. Así, una "puntuación más alta en la conciencia" se asocia a la evitación de comportamientos contraproducentes y "una puntuación más alta en amabilidad" se relaciona con mayores niveles de empatía y una tendencia a evitar los conflictos. (Szostek, D., et al., 2020).

Ambos rasgos han sido incluidos en herramientas de medición en psicología, como el BF-Q, que mide las dimensiones de afabilidad y tesón (o responsabilidad) dentro de la teoría de los Cinco Grandes o en la dimensión de psicoticismo del EPQ-R del modelo de los tres rasgos (PEN) de

Eysenck (1985,1991). Por tanto, es posible evaluar y detectar estas características individuales diferenciales, que pueden indicar más probabilidades de que un trabajador cometa una conducta de *insider* malicioso, provocando un perjuicio a la empresa.

Y en la literatura de ciberseguridad, se ha podido observar que la búsqueda de sensaciones propia de este rasgo resulta un predictor de amenazas internas, explicado por la curiosidad y la exploración característica de esta "curiosidad", así como un bajo autocontrol seleccionado como predictor de "comportamientos desadaptativos" y "participación actividades delictivas" como el robo (Tharshini, N. K., 2021); es más, se han descrito como uno de los motivos de ciberdelitos; aunque otras facetas como la amabilidad y la disposición a ayudar a los demás correlacionarían negativamente "con la probabilidad de cometer delitos internos" (Ruohonen, J., y Saddiqa, M., 2025).

Esta realidad refleja un creciente reconocimiento de relación entre amenazas internas, los comportamientos maliciosos y la psicología de la personalidad, aunque esta conexión todavía no resulta del todo clara o evidente (Ruohonen, J., y Saddiqa, M., 2025) (Zappalà, S. et al., 2022). Por ello, el presente trabajo pretende aportar claridad mediante una propuesta de investigación que ahonde en las diferencias individuales relacionadas con conductas maliciosas. Como señala Basu, S., et al. (2018) "comprender y aprovechar estas diferencias puede ser valioso en la prevención e intervención de amenazas internas", lo que facilita la creación de herramientas para anticiparse (K. Renaud et al., 2024), planteamiento que merece especial atención.

## 1.4. Actualidad

Las líneas de trabajo actuales se centran especialmente en la detección de comportamientos disruptivos o problemáticos, su monitorización y la implantación de estrategias de mitigación para parar esta posible amenaza interna o sus efectos. Algunas de las propuestas son el modelo DeepMIT propuesto por D. Sun, M. et al. (2021), que tiene capacidad de entrenamiento y detecta las amenazas prácticamente en tiempo real; o el que proponen Kim, J. et al. (2019). Ambos son métodos de detección de amenazas internas basados en el "modelado del comportamiento del usuario y los algoritmos de detección de anomalías". No obstante, se centran en trabajadores que ya realizan una actividad laboral.

## 1.5. Marco teórico de referencia

### 1.5.1. Psicología de la personalidad

Desde los inicios de la psicología de la personalidad se ha intentado buscar cuáles son aquellas características individuales que diferencia a un individuo de otro. Para ello, se han ido proponiendo diversos modelos partiendo de una concepción tipológica con autores como James, Freud o Jung, a la que siguieron teorías más biológicas como la de Allport, en la que proponía un sistema neuropsicológico: una "disposición interna que se manifiesta en la experiencia interior y en el comportamiento manifiesto" (Musek, J., 2024).

Posteriormente se abrieron paso los enfoques que abandonaban del todo la idea de las tipologías para introducir el enfoque de las dimensiones, que fue cobrando importancia hasta ser el predominante en la disciplina, desde el cual se han desarrollado las teorías más actuales y las que se han instaurado como más relevantes. Entre estas encontramos teorías estructurales como la de Eysenck con su modelo de los 3 grandes o PEN (siglas de Psicoticismo, Extraversión y Neuroticismo) con el cuestionario EPQ-R adaptado por Tea-Ediciones (H. J. Eysenck y S. B. G. Eysenck, 1985, 1991) para medirlas, o Catell (Musek, J., 2024) con el 16-PF (Cattell, Cattell y Cattell, 1993/TEA Ediciones) que evalúa los 16 factores de la personalidad que consideró esenciales (Afabilidad, Razonamiento, Estabilidad, Dominancia, Animación, Atención a las normas, Atrevimiento, Sensibilidad, Vigilancia, Abstracción, Privacidad, Aprensión, Apertura al cambio, Autosuficiencia, Perfeccionismo y Tensión) y que en la actualidad se han englobado en 5 dimensiones generales que lo hace de fácil paralelismo con otro de los modelos relevantes en la disciplina: los Cinco Grandes (Barbaranelli, Caprara, Rabasca y Pastorelli, 2003).

El modelo de los Cinco Grandes, propuesto por Goldberg y desarrollado también por McCrae y Costa, es uno de los más extendidos y que aún en la actualidad es ampliamente usado. A otros modelos más recientes, si bien son propuestas más detalladas, se les ha criticado cuestiones como tener excesivas subdivisiones de las dimensiones, centrarse en elementos que son más motivacionales y emocionales o que están basados en el léxico. Por ello, para la elección del modelo de personalidad en el que fundamentar la propuesta de investigación se consideraron sólo los dos modelos más extendidos y utilizados: el modelo de los Cinco Grandes (*Big Five*, en inglés*)* y el modelo PEN de Eysenck por su robustez teórica.

En la revisión de la literatura la mayoría optaban por utilizar como marco teórico el modelo de los 5 grandes, pero no se ha utilizado de una manera homogénea que permita la comparación directa de los resultados; así como que incluso en algunas ocasiones se han suprimido algunos rasgos sin fundamentación teórica para ello. De esta manera, resulta más idóneo recurrir al modelo propuesto por Eysenck: un modelo sencillo con tres dimensiones que engloban los factores descritos en la literatura, basado en una robusta teoría biológica y de fácil comprensión (Ruohonen, J. y Saddiqa, M., 2025),

El enfoque de los tres rasgos de Eysenck (PEN) es un modelo teórico que se ha desarrollado a partir de numerosos estudios psicométricos experimentales y se ha situado como uno de los más conocidos para "la evaluación de la personalidad". Además, es de aplicación breve y con corrección online disponible (H. J. Eysenck y S. B. G. Eysenck, 1985, 1991).

Sin embargo, ha sido criticado por su simplicidad y ambigüedad en el rasgo psicoticismo como predictor de psicosis, que era la idea de origen. Concretamente, se cuestiona que este modelo esté vinculado a la psicopatía o conductas desviadas. Sin embargo, esta es precisamente la razón por la que resulta ventajoso utilizarlo y adoptarlo como marco teórico para la propuesta de investigación. El objetivo es detectar conductas contraproducentes asociadas a insensibilidad, impulsividad y egocentrismo, las cuales se han relacionado con prácticas maliciosas realizadas por trabajadores contra una organización (van kampen, D., 2009).

Además, es un modelo que permite hacer "deducciones comprobables basadas en hallazgos genéticos, fisiológicos, de aprendizaje, etc." y es por ello que Eysenck consideró que las dimensiones de Psicoticismo, Extraversión y Neuroticismo eran las fundamentales para describir la personalidad (van Kampen, D., 2009).

En el modelo se describen tres dimensiones en un continuo con un espectro completo que comprende tanto estados "anormales" situados en extremos como comportamientos "normales" (van Kampen, D., 2009). El primer rasgo es el psicoticismo, con un fuerte componente genético (Tharshini, N. et al., 2021) que "parece estar relacionado con ciertas secreciones hormonales y bioquímicas, como la serotonina y los metabolitos de dopamina, y con las hormonas sexuales" (Eysenck, H. J., 1983). Se caracteriza por insensibilidad, escasa vinculación emocional con los demás, impulsividad y egocentrismo (van, Kampen, D., 2009). También está relacionado con conductas antisociales involucradas en la comisión de delitos y, de manera más específica, unido a "la falta de empatía y el sentido de derecho" con relación al riesgo de amenaza interna (Maasberg, M. et al., 2015), además del factor de la percepción del riesgo, la conciencia, el historial de violaciones de reglas legales (Georgiadou, A. et al., 2022) y la manipulación (Maasberg, M., et al., 2015). Además, se ha encontrado que el extremo superior de la dimensión, la psicopatía, "está más presente en población que comente delitos que en la población general", haciéndolo un "predictor sólido del comportamiento criminal" (Tharshini, N. K., 2021).

No obstante, cabe desgranar la escala Psicoticismo del modelo para comprender las relaciones con el modelo de los Cinco Grandes, entendiéndola como un paraguas que engloba una serie de conductas relacionadas con la "frialdad, egocentrismo, hostilidad, suspicacia, impersonalidad y agresividad" (Eysenck, H. J., 1983) y, de manera aproximada a categorías de otros modelos, se le atribuye una relación con el factor amabilidad y conciencia (van Kampen, D., 2009), dos aspectos que frecuentemente mencionados en la literatura relacionada con las "conductas contraproducentes" en entorno laboral.

El segundo elemento es la extraversión y parece estar relacionada con la "excitación cortical, mediad por la formación reticular"; haciendo que bajos niveles (introversión) partan de una mayor excitación cortical en reposo y, en contraposición, altos nivele de extraversión parten de una menor activación cortical (Eysenck, H. J., 1983), por lo que se define como una forma de interaccionar caracterizada por impulsividad, sociabilidad, hablador, enérgico, activo, optimista (Eysenck, H. J., 1983), búsqueda de estimulación y dominio social o amabilidad (Revelle, W., 2016) y apertura (Georgiadou, A. et al., 2022). Por tanto, esta dimensión es un continuo que va desde la introversión hasta la extraversión (Revelle, W., 2016).

En último término, el neuroticismo "parece estar relacionada con las diferencias en el funcionamiento del sistema límbico, mediado por el sistema autónomo". Esto hace que las personas inestables se caractericen por una actividad excesiva de estos elementos (Eysenck, H. J., 1983). Por tanto, se conceptualiza como un continuo que va de una mayor estabilidad emocional (bajo neuroticismo) a menor (alto neuroticismo) acompañado de una emocionalidad negativa predominante (Revelle, W., 2016). En el polo de la estabilidad la persona se caracterizaría por una actitud de calma y temperamento tranquilo mientras que en el polo de la inestabilidad la persona se caracterizaría por comportamiento ansioso, cambios notorios en los estados emocionales o excitabilidad, entre otros (Eysenck, H. J., 1983). Y en investigaciones posteriores se ha descrito como una mayor tendencia a estados de tensión, el comportamiento hipersensible (van Kampen, D., 2009) y la reactividad emocional". Así, personas con alto neuroticismo tienden a mostrar "impulsos emocionales elevados" y una dificultad para gestionar el estrés. Algunos estudios, como el de Cale (2006), recogen que un elevado neuroticismo puede predecir la delincuencia; sin embargo, esta relación es menor que la que guarda el rasgo de psicoticismo, y se incrementa cuando ambos rasgos están presentes de manera conjunta.

### 1.5.2. Relación entre CWB con personalidad

Hershcovis, M. S., et al. (2007) registraron la agresión (también entendida como desviación o comportamiento antisocial) como un problema persistente y significativo en el entorno laboral. En su revisión, concluyeron que la personalidad representaba un componente crucial en la aparición

de este tipo de conductas, tanto por las diferencias individuales como por las predisposiciones estables a involucrarse en ciertos comportamientos. Además, determinaron que estas conductas se asocian con la presencia de ira (entendida como "predisposición a responder a situaciones con hostilidad") y la "afectividad negativa" (entendida como la "mediad en la que los individuos experimentan emociones angustiantes, como la hostilidad, el miedo y la ansiedad") (Hershcovis, M. S., 2007). Asimismo, enfatizaron que la personalidad influye en la manera en la que una persona interpreta una misma situación. Y es este carácter estable el que se utiliza como justificación en este trabajo para usar la personalidad como variable explicativa y predictiva de estas conductas en el entorno laboral.

También mencionar que hay un número considerable de investigadores que exploran estas relaciones desde la tríada oscura, con el maquiavelismo, la psicopatía, el narcisismo y el rencor como "predisposición a desarrollar conductas problemáticas"(Kircaburun, K. y Griffiths, M. D., 2018), siendo especialmente destacable, el comportamiento antisocial un factor clave para describir a las amenazas internas (*insiders* maliciosos) con relación a conductas contraproducentes o "desviadas" en el lugar de trabajo (Maasberg, M., et al., 2015). Por tanto, hay una clara relación entre niveles altos de neuroticismo, psicoticismo y la extraversión, especialmente unido a un sistema motivacional predominante con sensibilidad a la recompensa (BAS) congruente con la búsqueda de sensaciones, que está asociado con conductas criminales (Hernández-Flórez, N. et al., 2022).

# 2. Hipótesis y metodología propuestas

A partir del planteamiento para detectar *insiders* maliciosos basado en la personalidad se plantean las siguientes hipótesis:

H1: El modelo PEN de Eysenck es adecuado para predecir conductas maliciosas que deriven en una fuga de información.

H2: Existen correlaciones significativas entre los niveles altos de Psicoticismo y la comisión de conductas contraproducentes maliciosas.

H3: Las dimensiones de Extraversión y Neuroticismo tienen menos relación con incurrir en conductas contraproducentes maliciosas, pero pueden actuar modulando la tipología.

A partir de estas, la propuesta de investigación que se plantea en el presente trabajo es la de explorar en una muestra real si se cumplen las relaciones esperadas entre ciertos rasgos de personalidad (Psicoticismo, Extraversión y Neuroticismo) y las conductas de *insider* malicioso recogido en la literatura (sabotaje, fraude, robo y espionaje) a través de un diseño experimental.

## 2.1. Metodología y procedimiento

A partir de la revisión bibliográfica y las relaciones propuestas entre la personalidad y las conductas de *insider* malicioso se propone un estudio mixto con diseño descriptivo correlacional en el que se evaluarán de manera estandarizada los rasgos de personalidad del modelo PEN (Psicoticismo, Extraversión y Neuroticismo) y en el que se aplicará un cuestionario de escenarios para evaluar motivaciones y tendencias comportamentales ante escenarios que las eliciten.

Un diseño mixto permite abordar de manera más integrada la cuestión sobre amenazas internas, comprendiendo tanto el factor cuantitativo de la personalidad como cualitativo de las conductas maliciosas y sus motivaciones, pudiendo entonces combinar el análisis estadístico con unas variables cualitativas (Jogulu, U., y Pansiri, J., 2011). Además, este enfoque facilita la interpretación de los resultados en contextos complejos como la personalidad en el entorno laboral, permitiendo contextualizarlos con la información cualitativa (Ryu, S. (2020).

Se recogerán tanto datos sociodemográficos como los rasgos de personalidad de manera cuantitativa, y las tendencias comportamentales de manera cualitativa. Las variables categóricas (edad, sexo, nivel educativo, cargo, departamento, tipo de contrato, tipo de jornada laboral y antigüedad) se analizarán mediante los estadísticos descriptivos de frecuencias y porcentajes; mientras que para la variable continua edad se utilizará la media, la desviación estándar y el mínimo y máximo. Y se estudiarán las relaciones entre las variables mediante el análisis de la correlación (Coeficiente de Pearson, si las variables cumplen los supuestos de normalidad, o Spearman, si no se cumplen). Además, sobre la información cualitativa obtenida del cuestionario de escenarios, se identificarán patrones comunes. Con la combinación de ambos tipos de datos, se podrá obtener una visión más completa.

Finalmente, se propone que se automatice y digitalice el máximo posible la administración de ambas herramientas para un mejor manejo de la muestra y de los datos para poder tratarlos posteriormente.

## 2.2. Materiales

Para los datos sociodemográficos (edad, sexo, nivel educativo, cargo, departamento, tipo de contrato, tipo de jornada laboral y antigüedad) se precisará solicitarlos mediante un formulario de participación. Para garantizar la anonimidad en ningún momento se solicitará el nombre y apellidos, sino que se identificará a cada participante con un código numérico al que se asociarán los resultados de las herramientas evaluativas. Asimismo, tampoco estará presente en el proceso de la investigación ningún otro miembro de la empresa que no sea la persona evaluada, siendo, por tanto, exclusivamente acompañada por un miembro de la investigación para poder asistir en caso de dudas en la realización de esta. También se entregará un consentimiento informado.

Para la recogida de datos cuantitativos sobre los rasgos de personalidad, se administrará el cuestionario EPQ-R adaptado digitalizado que proporciona la editorial TEA-ediciones (H. J. Eysenck y S. B. G. Eysenck (1985, 1991), identificando a cada sujeto con el código asignado inicialmente, y, mediante el sistema de corrección en línea, se obtendrán los resultados, pasado el tiempo preciso en el mismo formato; esto facilitará el manejo de este grupo de datos. El resultado de cada participante será introducido en una base de datos para poder ser comparable con el resto de los participantes. La duración de esta fase se estima de unos 70', en función de la demora del participante en responder a cada ítem.

En el caso de la recogida de datos cualitativos sobre las tendencias comportamentales, se administrará un cuestionario de escenarios digitalizado con *Google Forms* con un listado de preguntas que tienen el objetivo de explorar las decisiones que toma el participante ante diversos escenarios relacionados con conductas maliciosas (sabotaje, fraude, robo de información y espionaje). El uso de este tipo de herramienta permite recoger información como opiniones, percepciones, emociones o cualquier aspecto que el evaluador no hubiera contemplado, proporcionando así información más detallada sobre la variable de estudio (Tombs, M., y Strange, H., 2024). La duración de esta fase se estima de unos 20'.

En último término, se determina que para el análisis de los datos se utilice un *software* de análisis, como SPSS o el *software* de libre acceso R, que son programas estadísticos que proporcionan una amplia variedad de técnicas estadísticas (agrupaciones, regresiones lineales, correlaciones, …) y técnicas gráficas que soportan y manejan eficazmente datos y sus cálculos (R Core Team, 2025) e incluso permiten "obtener conclusiones más precisas en el análisis de relaciones complejas" (IBM, 2025a).

## 2.3. Participantes

Los participantes serán empleados/as de las distintas áreas de varias organizaciones seleccionados con un muestreo por conveniencia (voluntariedad) que se inscribirán mediante un formulario de participación. El tamaño de la muestra idealmente será de entre 300 y 500 participantes que deberán pasar los criterios de inclusión (ser mayor de edad, estar en posesión de un contrato laboral vigente y tener capacidad para comprender y completar ambos cuestionarios autoadministrados) y de exclusión (rellenado indebido o incompleto de los cuestionarios).

En la muestra se pretende incluir a todos los trabajadores, no obstante, aquellos que sí han incurrido en conductas *insider* malicioso no se encontrarán formando parte de la empresa.

## 2.4. Procedimiento

Para poder llevar a cabo la investigación se prevé contar con la colaboración del departamento de RRHH para realizar la difusión del estudio mediante el correo corporativo. En el folleto informativo se especificarán los objetivos del estudio (explorar las relaciones entre conductas maliciosas y los rasgos de personalidad) y qué implica participar en el estudio: completar un cuestionario de personalidad y un cuestionario de escenarios con el objetivo de explorar las tendencias de comportamiento ante escenarios propuestos, relacionados con el sabotaje, el fraude, el robo de información y el espionaje. Y la duración de la evaluación está estimada para unas 1,5-2h.

Para participar deberán rellenan un formulario online creado para este estudio. Se les informará del rango horario (dentro del horario laboral) y la zona habilitada de la empresa para realizar la administración de los cuestionarios, y se les asignará un código identificativo que deberán presentar cuando se personen. Este código permitirá saber qué resultados corresponden a un único participante a la par que se mantiene el anonimato.

Tras una o dos semanas para garantizar la difusión del anuncio de la investigación, una responsable se personará en el rango horario y localización establecidos para atender a los voluntarios que se personen. En caso de dudas asistirá a los participantes, pero se recomienda limitar la interacción con ellos para no sesgar o alterar los resultados. El tiempo total previsto para la realización de los cuestionarios es de 1,5-2h a realizar dentro del horario laboral y se llevará a cabo mediante un ordenador, administrando en primer lugar el cuestionario de personalidad y, en segundo lugar, un cuestionario de preguntas sobre escenarios.

Al principio de la prueba se recodará el carácter anónimo de la misma y la posibilidad de abandonar y eliminar sus respuestas de la base de datos. También se recalcará que el tratamiento de los datos será confidencial y exclusivo para fines de la propia investigación.

# 3. Resultados esperados

Una vez recogidos y analizados los datos, se esperan obtener relaciones de mayor o menor peso entre las cuatro conductas maliciosas descritas anteriormente con los tres rasgos de personalidad del modelo PEN de Eysenck.

Para el sabotaje, dado que a nivel teórico se ha podido relacionar más con aspectos como la venganza, la ira, el bajo rendimiento y comportamientos de adicción (Maasberg, M., et al., 2015), se espera que aparezca con una relación significativa a un nivel alto de psicoticismo (por una baja responsabilidad y conciencia de las consecuencias de la conducta y una baja percepción del riesgo a ser detectado), un alto neuroticismo (reacciones de alta emocionalidad) y un nivel medio a alto de extraversión (por la búsqueda de sensaciones).

Para el robo, puesto que se ha identificado que la motivación predominante es de ganancia financiera (Maasberg, M., et al., 2015), se esperan altos niveles de psicoticismo que se traducen en egoísmo, búsqueda de sensaciones y baja tolerancia al riesgo a ser descubierto.

En el caso del fraude, al haber sido relacionada a nivel teórico también con la búsqueda de una ganancia financiera (Maasberg, M., et al., 2015), también se esperan altos niveles de psicoticismo.

Y en el caso del espionaje, al relacionarse con una baja percepción del riesgo, bajos niveles de tensión o ansiedad, manipulación (Lavanya, P. y Shankar Sriram, V.S., 2022) se esperan altos niveles de psicoticismo y de extraversión y bajos niveles de neuroticismo.

Por tanto, se espera que como condición esencial para cada una de las cuatro conductas maliciosas la persona presente unos niveles altos en psicoticismo, resultados que serían congruentes con la literatura sobre delincuencia al encontrarse también relacionado con la comisión de delitos (Tharshini, N. K., 2021).

# 4. Discusión

Los distintos modelos teóricos de personalidad, habiendo sido comparados y discutidos en revisiones sistemáticas y, tal y como menciona van Kampen D. (2009), podríamos considerar que están diseñados para responder a diferentes propósitos, por lo que no son excluyentes ni se pone a uno como mejor opción que otro de manera absoluta. No obstante, no hay consenso en el uso de los modelos teóricos de personalidad y aun siendo el modelo de los 5 grandes el más extendido no se usa de manera consensuada, habiendo algunos autores que no utilizan todos los rasgos del modelo.

Sin embargo, dado que el propósito de este estudio es aportar un fundamento teórico claro y sencillo de comprender y manejar lo suficientemente robusto, el modelo PEN de Eysenck encaja perfectamente como marco teórico.

En segundo término, dependiendo del ámbito al que pertenezca la investigación, los constructos que se utilizan son a nivel comportamental como el más extendido de "comportamiento contraproducente en el trabajo" o "CWB" que tienen de trasfondo unos patrones de personalidad que no se exponen en el mismo. Además, se habla de rasgos de personalidad, pero no se plasman relaciones directas con conductas del entorno de la ciberseguridad y empresa. En este punto, el presente trabajo propone unas relaciones iniciales para acercar ambos lados de la investigación y que sirva para la aplicación práctica, que viene siendo una demanda urgente para el sector de la ciberseguridad.

Además, en la literatura se ha identificado que las conductas vienen determinadas por motivaciones (principalmente de ganancia económica y venganza) acompañadas de características personales como el egoísmo, la búsqueda de sensaciones, la alta tolerancia al riesgo (a ser descubiertos), la baja amabilidad y la baja consciencia o responsabilidad (Maasberg, M., et al., 2015) (Zhou, Z., 2018). Estos aspectos son los que también caracterizan especialmente a un nivel alto de psicoticismo y en cierta medida de la dimensión extraversión, quedando el neuroticismo con menos peso. Esto, sirve de evidencia de que, de las tres, la que es condición necesaria en un nivel elevado para la comisión de delitos es el Psicoticismo; resultados ya obtenidos en delitos de otro tipo (Tharshini, N. K., 2021). No obstante, dado que el patrón conductual cambia cuando se combina la dimensión del Psicoticismo con la Extraversión y /o con el Neuroticismo, es necesario prestar también atención a las correlaciones que puedan aparecer; evitando cualquier enfoque sesgado que se centre exclusivamente en la primera dimensión.

Por otro lado, tras la evaluación de la literatura se ha observado que el foco de atención mayoritariamente está

puesto sobre personas que ya realizan o han realizado actividad laboral en la empresa (Sun, D., et al., 2021) y, por tanto, resulta evidente que, y así se recoge, se deban contemplar en las herramientas evaluativas para ello varios factores y no solo el individual. Sin embargo, dado que el presente trabajo propone una investigación para explorar las relaciones estables entre personalidad y conductas contraproducentes maliciosas, los hallazgos podrían ser incorporados en un proceso de selección como factores predisponentes; siempre y cuando se conciba que en todo caso debe darse el motivo, la capacidad y oportunidad" para incurrir en conductas contraproducentes maliciosas (Maasberg, M. et al., 2025).

## 4.1. Limitaciones

Entre las limitaciones que podrían encontrase en la aplicación de esta propuesta de investigación se encuentran.

- El problema ético que surge cuando los trabajadores no quieren que se les realice un perfilado de la personalidad cuyo resultado pueda correlacionarse con probabilidades de comisión de delitos, ya que esto podría ser percibido como una manifestación de desconfianza por parte de la organización. En este trabajo se propone anonimizar los datos como medida principal para mitigar esta preocupación.
- La dificultad para poder acceder a sujetos requeridos como parte de la muestra representativa, bien porque fueron despedidos bien porque no quieran participar. Son aquellos que ya cometieron este tipo de delitos.
- La complejidad metodológica que supone aplicar un diseño mixto en el que se deben integrar variables cuantitativas y cualitativas, para lo cual deben estar bien definidas, así como ser preciso un mayor tiempo para la recolección y análisis de los resultados.

## 4.2. Futuras líneas de investigación

En referencia al modelo de personalidad sería interesante realizar la misma investigación con teorías como la que proponen Dirk Van Kampen con el modelo 5DPT, por sus siglas en inglés; considerado una propuesta de actualización del modelo PEN de Eysenck; por tanto, evaluar si con este modelo se obtienen los mismos o diferentes resultados.

En cuanto a la aplicabilidad de la investigación sería interesante llevar a cabo la propuesta con una muestra real y posteriormente elaborar un modelo predictivo entrenado con dichos resultados para que, mediante un software permita al evaluador, por ejemplo, en un proceso de selección, añadir esta herramienta para poder tomar decisiones informadas.

Finalmente, aportaría un gran valor al desarrollo de una teoría robusta poder incorporar en la muestra participantes que hayan incurrido en delitos de *insider* malicioso.

# 5. Referencias bibliográficas


Agencia Española de Protección de Datos (AEPD). (2021). *Guía para la notificación de brechas de datos personales* (junio 2021). https://www.aepd.es/guias/guia-brechas-seguridad.pdf

Ahmadian, M., y Marinescu, D. (2020). Information Leakage in Cloud Data Warehouses. *IEEE Transactions on Sustainable Computing, 5*, 192-203. https://doi.org/10.1109/TSUSC.2018.2838520

Al-Shehari, T., y Alsowail, R. (2021). An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques. *Entropy, 23*. https://doi.org/10.3390/e23101258.

Alhathally, L., AlZain, M. A., Al-Amri, J., Baz, M., y Masud, M. (2020). Cyber security Attacks: Exploiting weaknesses. *International Journal of Recent Technology and Engineering, 8*(5), 906–913. https://doi.org/10.35940/ijrte.e4876.018520

Alqahtani, N. (2025). Security Threats to Databases in E-Commerce Systems: A Systematic Literature Review. *Journal of Computer Science.* https://doi.org/10.3844/jcssp.2025.25.33

Alzaabi, F. R., y Mehmood, A. (2024). Classifying malicious insider threats based on user activity and behavioral profile using machine learning. *2024 International Conference on Engineering and Emerging Technologies (ICEET)*, 1–6.

Alzaabi, F., y Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. *IEEE Access*, 12, 30907-30927. https://doi.org/10.1109/ACCESS.2024.3369906

American Psychological Association. (2023). *Counterproductive work behavior*. En APA Dictionary of Psychology. Recuperado el 14 de agosto de 2025, de https://dictionary.apa.org/counterproductive-work-behavior

Anju, A., M, N., K, S., Ravikumar, H., P, S., y Krishnamurthy, M. (2023). Detection of Insider Threats Using Deep Learning. 2023 *3rd International Conference on*

*Pervasive Computing and Social Networking (ICPCSN)*, 264-269. https://doi.org/10.1109/ICPCSN58827.2023.00050

Barbaranelli, C., Caprara, G. V., Rabasca, A., y Pastorelli, C. (2003).

Basu, S., Victoria Chua, Y. H., Wah Lee, M., Lim, W. G., Maszczyk, T., Guo, Z., y Dauwels, J. (2018). Towards a data-driven behavioral approach to prediction of insider-threat. *2018 IEEE International Conference on Big Data (Big Data)*, 4994–5001.

*Big Five Questionnaire (BFQ)* (adaptación española, TEA Ediciones). TEA Ediciones.

Board International announces results from its Global Planning Survey on Enterprise Planning. (2023). Board.com. https://www.board.com/news/board-international-announces-results-its-global-planning-survey-enterprise-planning

Cale, E. M. (2006). A quantitative review of the relations between the "Big 3" higher order personality dimensions and antisocial behavior. *Journal of Research in Personality, 40*(3), 250–284. https://doi.org/10.1016/j.jrp.2005.01.001

Carpenter, N., Whitman, D., y Amrhein, R. (2020). Unit-Level Counterproductive Work Behavior (CWB): A Conceptual Review and Quantitative Summary. *Journal of Management, 47*, 1498 - 1527. https://doi.org/10.1177/0149206320978812

Cattell, R. B., Cattell, A. K. S., y Cattell, H. E. P. (1993). *16 PF-5. Cuestionario factorial de personalidad* (5.ª ed., adaptado por TEA Ediciones). TEA Ediciones. https://www.hogrefe-tea.com/public/catalogo/producto/16-PF-5--CUESTIONARIO-FACTORIAL-DE-PERSONALIDAD--5-EDICION

Chai, K., y Zolkipli, M. (2021). Revisión sobre Confidencialidad, Integridad y Disponibilidad en Seguridad de la Información. *Revista de TIC en Educación*. https://doi.org/10.37134/jictie.vol8.2.4.2021

Cheng, L., Liu, F., y Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach. *Wiley Interdisciplinary Reviews. Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

*Cost of a Data Breach*. (2025). https://www.ibm.com/downloads/documents/es-es/137a3e32273ed1f5

Douligeris, C., Raghimi, O., Lourenço, M. B., Marinos, L., Sfakianakis, A., Doerr, C., Armin, J., Riccardi, M., Wim, M., Thaker, N., Stirparo, P., Samwel, P., Paganini, P., Adachi, S., Lingris,, S., y Hemke, T. (2020). *Insider threat. ENISA Threat Landscape*. https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Insider%20Threat%20A4.pdf

Eftimie, S., Moinescu, R., y Racuciu, C. (2020). Insider threat detection using natural language processing and personality profiles. *2020 13th International Conference on Communications (COMM)*, 325–330.

Eysenck, H. J. (1983). Psychophysiology and Personality: Extraversion, Neuroticism and Psychoticism. En *Individual Differences and Psychopathology* (pp. 13–30). Elsevier.

Georgiadou, A., Mouzakitis, S., y Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems, 62*(4), 706–716. https://doi.org/10.1080/08874417.2021.1903367

H. J. Eysenck y S. B. G. Eysenck (1985, 1991). *EPQ-R. Cuestionario de Personalidad de Eysenck - Revisado*. Adaptado por: Ortet, G., Ibáñez, M. I., Ipola, M. M. y Silva, F. TEA ediciones.

Hernández-Flórez, N., Lhoeste-Charris, Á., Acosta-Acuña, L., Ballestas-Zabaleta, C., Bravo-Baldovino, Y., Chanchila-Martinez, L., y Hernández-Andrade, G. (2022). Rasgos de la personalidad asociados a la conducta criminal: perspectiva de los modelos de Eysenck y Gray. *Búsqueda, 9*(2), 616. https://doi.org/10.21892/01239813.616

Hershcovis, M. S., Turner, N., Barling, J., Arnold, K. A., Dupré, K. E., Inness, M., LeBlanc, M. M., y Sivanathan, N. (2007). Predicting workplace aggression: a meta-analysis. *The Journal of Applied Psychology, 92*(1), 228–238. https://doi.org/10.1037/0021-9010.92.1.228

*Hogrefe TEA Ediciones*. (n.d.). Hogrefe-tea.com. Retrieved August 13, 2025, from https://www.hogrefe-tea.com/public/catalogo/producto/BFQ--CUESTIONARIO-BIG-FIVE

Horstmann, K. T., Rauthmann, J. F., Sherman, R. A., y Ziegler, M. (2021). Unveiling an exclusive link: Predicting behavior with personality, situation perception, and affect in a preregistered experience sampling study. *Journal of Personality and Social Psychology, 120*(5), 1317–1343. https://doi.org/10.1037/pspp0000357

https://www.hogrefe-tea.com/public/catalogo/producto/BFQ--CUESTIONARIO-BIG-FIVE

IBM. (2025a). *IBM SPSS Statistics – Funciones*. IBM. https://www.ibm.com/es-es/products/spss-statistics/features

IBM. (2025b). *What are Insider Threats?* https://www.ibm.com/think/topics/insider-threats

Idensohn, C. J., Flowerday, S. V., van der Schyff, K., y Chua, Y. T. (2025). *Malicious insider threats in cybersecurity: A fraud triangle and Machiavellian perspective.* https://doi.org/10.2139/ssrn.5314919

Instituto Nacional de Ciberseguridad (INCIBE). (2016). *Cómo gestionar una fuga de información: Una guía de aproximación para el empresario* (Versión PDF). INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

Instituto Nacional de Ciberseguridad (INCIBE). (2017). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario* (PDF). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Instituto Nacional de Ciberseguridad (INCIBE). (2023). *Insiders: cómo atacan desde dentro*. INCIBE. https://www.incibe.es/empresas/blog/insiders-como-atacan-desde-dentro

Jogulu, U., y Pansiri, J. (2011). Mixed methods: a research design for management doctoral dissertations. *Management Research Review, 34*, 687-701. https://doi.org/10.1108/01409171111136211

Kaspersky Lab. (2023). *Kaspersky Human Factor 360° report 2023.* https://media.kasperskydaily.com/wp-content/uploads/sites/92/2023/11/22070742/KasperskyHumanFactor360Report2023.pdf

Kim, J., Park, M., Kim, H., Cho, S., y Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences (Basel, Switzerland), 9*(19), 4018. https://doi.org/10.3390/app9194018

Kircaburun, K., y Griffiths, M. D. (2018). The dark side of internet: Preliminary evidence for the associations of dark personality traits with specific online activities and problematic internet use. *Journal of Behavioral Addictions, 7*(4), 993–1003. https://doi.org/10.1556/2006.7.2018.109

Lavanya, P., y Shankar Sriram, V. S. (2022). Detection of insider threats using deep learning: A review. In *Smart Innovation, Systems and Technologies* (pp. 41–57). Springer Nature Singapore.

Liang, N., Biros, D., y Luse, A. (2023). An Empirical Comparison of Malicious Insiders and Benign Insiders. *Journal of Computer Information Systems, 64*, 762 - 774. https://doi.org/10.1080/08874417.2023.2251427

Lubenets, S., Harchenko, I., y Shediakova, T. (2024). Trends, challenges and solutions of digital information security in Central and Eastern Europe. *Journal of Economics and International Relations*. https://doi.org/10.26565/2310-9513-2024-19-02

Maasberg, M., Warren, J., y Beebe, N. L. (2015). *The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits*. https://doi.org/10.1109/HICSS.2015.423

Marbut, A., y Harms, P. (2023). Fiends and Fools: A Narrative Review and Neo-socioanalytic Perspective on Personality and Insider Threats. *Journal of Business and Psychology*. https://doi.org/10.1007/s10869-023-09885-9

Martinko, M. J., Gundlach, M. J., y Douglas, S. C. (2002). Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment, 10*(1–2), 36–50. https://doi.org/10.1111/1468-2389.00192

Musek, J. (2024). *Personality Psychology. A new perspective*. Springer International Publishing.

Neto, N., Madnick, S., Paula, A., y Borges, N. (2021). Developing a Global Data Breach Database and the Challenges Encountered. *Journal of Data and Information Quality (JDIQ), 13*, 1 - 33. https://doi.org/10.1145/3439873

Parasuraman, R., y Jiang, Y. (2012). Diferencias individuales en cognición, afecto y rendimiento: Enfoques conductuales, de neuroimagen y genética molecular. *NeuroImage, 59*, 70-82. https://doi.org/10.1016/j.neuroimage.2011.04.040

Ponemon Institute, & DTEX Systems. (2025). *2025 cost of insider risks global report*. Ponemon Institute & DTEX Systems. https://www2.dtexsystems.com/l/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf

R Core Team. (2025). *About R*. The R Project for Statistical Computing. https://www.r-project.org/about.html

Renaud, K., Warkentin, M., Pogrebna, G., y van der Schyff, K. (2023). VISTA: An inclusive insider threat taxonomy, with mitigation strategies. *Information & Management, 103877*. https://doi.org/10.1016/j.im.2023.103877

Ritala, P., Olander, H., Michailova, S., y Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation, 35*, 22–31. https://doi.org/10.1016/j.technovation.2014.07.011

Ruohonen, J., y Saddiqa, M. (2025). What do we know about the psychology of insider threats? In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 186–211). Springer Nature Switzerland.

Ryu, S. (2020). The role of mixed methods in conducting design-based research. *Educational Psychologist, 55*, 232 - 243. https://doi.org/10.1080/00461520.2020.1794871

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., y Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics, 9*(9), 1460. https://doi.org/10.3390/electronics9091460

Shelke, P. y Hamalainen, T. (2024). Análisis de estrategias multidimensionales para la detección de amenazas cibernéticas en el monitoreo de seguridad. *Conferencia europea sobre guerra cibernética y seguridad*. https://doi.org/10.34190/eccws.23.1.2123

Sowa, T. (2024). Malicious Insiders' Threats to the Personal Data Security. The Hard to Comply Rules of the GDPR. *Global Privacy Law Review*. https://doi.org/10.54648/gplr2025001

Sun, D., Liu, M., Li, M., Shi, Z., Liu, P., y Wang, X. (2021). DeepMIT: A novel malicious insider threat detection framework based on recurrent neural network. *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*.

Sun, D., Liu, M., Li, M., Shi, Z., Liu, P., y Wang, X. (2021). DeepMIT: A novel malicious insider threat detection framework based on recurrent neural network. *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*.

Szostek, D., Balcerzak, A., P., and Rogalska, E. (2020). The relationship between personality, organizational and interpersonal counterproductive work challenges in industry 4.0. *Acta Montanistica Slovaca, 25*(4),577-592. https://doi.org/10.46544/ams.v25i4.11

Tharshini, N. K., Ibrahim, F., Kamaluddin, M. R., Rathakrishnan, B., y Che Mohd Nasir, N. (2021). The link between individual personality traits and criminality: A systematic review. *International Journal of Environmental Research and Public Health, 18*(16), 8663. https://doi.org/10.3390/ijerph18168663

Tombs, M., y Strange, H. (2024). Using Qualitative Questionnaires in Medical Education Research. *Perspectives on Medical Education, 13*, 280 - 287. https://doi.org/10.5334/pme.1102

Vafaei-Zadeh, A., Ramayah, T., Hanifah, H., Kurnia, S., y Mahmud, I. (2020). Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia. *Information & Management, 57*(8), 103386. https://doi.org/10.1016/j.im.2020.103386

van Kampen, D. (2009). Personality and psychopathology: A theory-based revision of Eysenck's PEN model. *Clinical Practice and Epidemiology in Mental Health: CP & EMH, 5*(1), 9–21. https://doi.org/10.2174/1745017900905010009

Verizon. (2025). *2025 Data Breach Investigations Report Small- and Medium-Sized Business Snapshot* (Informe en PDF). https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf

Wong, W., Tan, H., Tan, K. y Tseng, M. (2019) Factores humanos en la fuga de información: estrategias de mitigación para la integridad del intercambio de información. *Ind. Maneg. Sistema de datos, 119*, 1242-1267. https://doi.org/10.1108/IMDS-12-2018-0546

Zamorano Salardón, Andrea (2018) El factor humano en la fuga de información privilegiada y su relación con la personalidad. *Drafts of Economic Intelligence* (ISSN 2659-9791), Vol. 1 nº 2; pp. 11 – 22

Zappalà, S., Sbaa, M. Y., Kamneva, E. V., Zhigun, L. A., Korobanova, Z. V., y Chub, A. A. (2022). Current approaches, typologies and predictors of deviant work behaviors: A scoping review of reviews. *Frontiers in Psychology, 12*, 674066. https://doi.org/10.3389/fpsyg.2021.674066

Zhou, Z. (2018). *Counterproductive Work Behavior (CWB)*. Oxfordbibliographies. https://doi.org/10.1093/OBO/9780199846740-0143