Identification and modeling of behavioral traits of Advanced Persistent Threats (APTs)

Diego Staino[1] and Rocío Benigar[2]

[1] Instituto Universitario de la Policía Federal, Buenos Aires, Argentina
[2] Universidad Nacional de Río Negro, Rio Negro, Argentina
[1]diegostaino@hotmail.com
[2] rocio.benigar@gmail.com

Abstract. This research paper addresses the identification and modeling of behavioral traits in Advanced Persistent Threats (APTs), proposing an integrative approach that systematically links a series of classic criminological theories and the Big Five personality model with the analysis of these groups. It is argued that there is a lack of a formalized method for applying theoretical frameworks of crime and motivation to the reality of cybercrime, particularly regarding APT groups, making it difficult to identify behavioral patterns. This paper proposes a set of analogies derived from criminological theories combined with a practical model based on psychological traits and behavioral patterns to provide predictive insight into the behavior of APT groups, thereby facilitating decision making, implementation of countermeasures, and optimization of incident response strategies. Although limitations such as dependency on additional sources and the rapidly evolving nature of threats are acknowledged, this work aims to offer a valuable perspective for understanding and addressing these sophisticated threats.

Keywords: Cybercrime, Criminology, Cyber Intelligence, Behavior, Cyber Incident Response.

Identificación y modelado de rasgos de comportamiento sobre Amenazas Persistentes Avanzadas (APTs)

Resumen. El presente trabajo de investigación aborda la identificación y modelado de rasgos de comportamiento sobre Amenazas Persistentes Avanzadas (APTs) proponiendo un enfoque integrador que vincula de manera sistemática una serie de teorías criminológicas clásicas y un modelo psicológicos de personalidad (Big Five) con el análisis de estos grupos. Se considera que existe una carencia de un método formalizado para trasladar marcos teóricos del delito y la motivación a la realidad del ciberdelito y, en particular, sobre los grupos APTs. Esto dificulta la identificación de patrones de comportamiento. Este trabajo plantea una serie de analogías para las teorías de criminología junto con

un modelo práctico, basado en características psicológicas y patrones de conducta, que puede ofrecer una visión predictiva del comportamiento de los grupos APT, facilitando la toma de decisiones, el abordaje de contramedidas y la optimización de estrategias de respuesta a incidentes. Si bien se reconocen limitaciones como la dependencia de fuentes adicionales y la rápida evolución de las amenazas, este trabajo busca ofrecer una perspectiva valiosa para la comprensión y el abordaje de estas amenazas sofisticadas.

Palabras clave: Cibercrimen, Criminología, Ciberinteligencia, Comportamiento, Respuesta a ciber incidentes

1 Introducción

La criminología clásica ofrece un marco sólido para comprender el comportamiento delictivo que, con ciertas adaptaciones, puede emplearse para analizar el cibercrimen. Las teorías de la motivación delictiva brindan perspectivas que, al trasladarse al ámbito digital, pueden ayudar a comprender el comportamiento de grupos de ciberdelincuentes. La adaptación de estas teorías al ciberespacio implica observar la forma en que se aprenden técnicas de ataque, se crean culturas subterráneas y se satisfacen necesidades individuales o grupales a través de la ciberdelincuencia.

En concreto, se busca integrar teorías criminológicas como la Asociación Diferencial (Sutherland, 1947), la Elección Racional (Clarke D. C., 2017), la Oportunidad (Social Change and Crime Rate Trends: A Routine Activity Approach, 1979 y la Neutralización (Sykes, 1957) para comparar sus análisis con el modus operandi de Grupos de Amenazas Persistentes Avanzadas (APTs). Para esto se toma en cuenta la visión de la “organización criminal como una entidad que toma decisiones” (Guerra, 2023), y aplicando posteriormente un marco de la psicología, como el modelo de los Cinco Grandes Rasgos de la personalidad, para darles un perfil a estos grupos y finalmente obtener un marco sobre el que tomar decisiones de confrontación con estos grupos.

2 Problema de investigación

Aunque existen numerosos estudios sobre el cibercrimen y la actividad de grupos APTs, consideramos de valor aportar un enfoque integrador que vincule de manera sistemática las teorías criminológicas clásicas y los modelos psicológicos de personalidad con el análisis de estos grupos. Comprendemos que la oportunidad de mejora radica en la carencia de un método formalizado para trasladar marcos teóricos del delito y la motivación a la realidad del ciberdelito y, en particular, sobre los grupos APTs, dificultando entonces la identificación de patrones de comportamiento.

Se considera como hipótesis inicial que es posible la integración de teorías criminológicas clásicas y marcos psicológicos de personalidad que permitan obtener una visión predictiva del comportamiento de los grupos APT, facilitando la identificación de patrones conductuales y la optimización de estrategias de respuesta a incidentes.

3 Objetivo

Se propone como objetivo desarrollar un modelo teórico que permita establecer analogías entre las teorías criminológicas clásicas y las características psicológicas de los ciberdelincuentes, a fin de generar conclusiones útiles para el análisis y la comprensión de la dinámica operativa de grupos de APTs.

Como objetivos específicos se definieron:

- Analizar las principales teorías criminológicas (Asociación Diferencial, Elección Racional, Oportunidad, Ventaja Comparativa, Neutralización, Prevención Situacional) y evaluar su aplicabilidad en el contexto del cibercrimen.
- Explorar la utilidad de un modelo psicológico grupal (Cinco Grandes Rasgos de la Personalidad) para describir el comportamiento organizacional de los grupos de APTs.
- Desarrollar analogías o guías de uso que integren aspectos criminológicos y psicológicos para la prevención, detección y respuesta a incidentes de ciberseguridad.
- Aplicar el modelo resultante a un caso de estudio para validar la pertinencia de las conclusiones.

4 Metodología

Para el desarrollo de este trabajo se realizó una revisión de textos académicos junto publicaciones relevantes en ciberseguridad (incluyendo reportes de incidentes, estudios de caso, MITRE ATT&CK) para extraer patrones de conducta de grupos APTs.

A continuación, se seleccionaron y analizaron las teorías criminológicas mencionadas y se discutieron sus elementos clave, estableciendo posibles analogías con escenarios de cibercrimen. Basándonos en este análisis y considerando a las organizaciones criminales como “una entidad que toma decisiones”, se propuso aplicar el modelo psicológico de “Cinco Grandes Rasgos de la Personalidad”, explorando una aplicación práctica para la toma de decisiones.

Para finalizar, se propuso un grupo APT ficticio sobre el cual se analizó un conjunto de actividades, campañas y modus operandi para la aplicación del modelo propuesto. Evaluando así la pertinencia para la toma de decisiones en situaciones de interacción con este APT. A la luz de este caso simulado se promueve el análisis de otros grupos APTs.

5 Teorías criminológicas analizadas

A continuación, se describen las principales teorías que servirán como base para nuestro análisis:

Teoría de la Asociación Diferencial (Sutherland, 1947)**:** Se introduce la idea de que el comportamiento criminal se aprende a través de la asociación diferencial. La teoría describe una explicación genética del comportamiento delictivo, plantea que este aprendizaje ocurre mediante la interacción y comunicación con grupos personales íntimos, que actúan como fuente principal de influencia. Este aprendizaje abarca tanto técnicas como motivaciones. Por un lado, se adquieren las habilidades necesarias para cometer delitos, así como las racionalizaciones y actitudes que los justifican. Por el otro, se interiorizan actitudes favorables o desfavorables hacia las leyes, influenciadas por las definiciones culturales y sociales del entorno del individuo. El ejemplo tradicional que se le suele atribuir a esta teoría es el criminal que aprende a robar, un adolescente que crece en un vecindario donde el robo es una práctica común a la vez aprende esta conducta a través de su entorno cercano. Se considera más probable que desarrolle una actitud favorable hacia el delito. Además, aprende técnicas específicas, como qué objetos son más fáciles de sustraer o cómo evitar ser detectado. Según Sutherland, esta exposición constante a normas y valores que favorecen la delincuencia aumentaría la probabilidad de adopción de ese comportamiento delictivo.

Teoría de la Elección Racional (Clarke D. C., 2017)**:** En contraposición con la mayoría de las teorías criminológicas que describen lo que sucede con anterioridad a la comisión de un crimen, esta teoría también hace hincapié en las decisiones posteriores al evento. El principal postulado sostiene que las personas que cometen un crimen lo hacen tras un proceso de toma de decisiones. A partir de allí, incorpora la importancia de reconocer las recompensas y castigos, es decir, el costo-beneficio de realizar una acción. Al igual que las demás teorías, busca proporcionar una explicación aplicable a todos los tipos de crímenes, considerando la singularidad de cada uno y la experiencia del criminal. En este sentido, se menciona que, a mayor experiencia y conocimiento sobre el delito a cometer, menor será el tiempo que el delincuente requiere para atravesar el proceso de toma de decisiones. Parte de esta experiencia adquirida puede incluir la capacidad de gestionar miedos, escrúpulos morales y la culpa asociada con la acción delictiva. Un ejemplo de la teoría de la elección racional puede darse en un escenario hipotético donde un criminal debe elegir entre dos domicilios para cometer un robo. En términos de costo, analizará cuál de los domicilios ofrece un acceso más sencillo, carece de cámaras de seguridad o no cuenta con perros guardianes que dificulten la intrusión. En términos de beneficio podría analizar cuál tendrá una vía de escape más segura o en cuál podría encontrar más objetos de valor.

Teoría de las Actividades Cotidianas (Clarke R. V., 1993)**:** Es un marco teórico que busca comprender las condiciones que facilitan la ocurrencia de un crimen, identificando los elementos esenciales que deben coincidir para que un delito tenga lugar. Un **delincuente motivado** (persona dispuesta y con intención de cometer el delito), un **objetivo adecuado** (una víctima o un bien vulnerable a la acción del delincuente) y la **ausencia de guardianes capaces** (Personas o medidas de seguridad que podrían prevenir el delito). Un claro ejemplo de la aplicación de este marco teórico es el caso de una persona que deja su automóvil abierto bajarse, convirtiéndolo en un objetivo adecuado. Si el vehículo está estacionado en una zona poco transitada o fuera del campo visual de su dueño, se cumple con la condición de ausencia de guardianes capaces. Si a este escenario se le suma un delincuente motivado en busca de una

oportunidad para cometer un delito, es altamente probable que el automóvil sea sustraído.

Teoría de la Neutralización (Sykes, 1957)**:** Sostiene que los individuos atraviesan un proceso de aprendizaje para convertirse en criminales y en el usan mecanismos de justificación para minimizar la culpa y legitimar sus actos.

- **Negación de la responsabilidad**: en este caso se rompe el vínculo entre el individuo y sus actos. El criminal traslada la responsabilidad de sus actos hacia otra persona y/o una situación, definiéndose a sí mismo como no responsable y justificando su comportamiento, atribuyendo a factores externos y por lo general fuera de su control. Al aplicar esta técnica, el criminal elude la culpa resultante de los delitos que comete.
- **Negación del daño:** con esta técnica se rompe el vínculo entre los actos del criminal y sus consecuencias. El criminal le suele restar importancia al daño que causó a pesar de que esté incumpliendo la ley. Si fuese el caso de un daño económico, el criminal puede excusarse en que cree que para la víctima esa pérdida económica no es gran cosa, ya que podría reponerse rápidamente. Podría tratarse simplemente de "vandalismo" o "travesuras".
- **Negación de la víctima:** el criminal justifica su comportamiento al transformar a su víctima en alguien que merece sufrir un daño, pudiendo asumir un rol de vengador que ejerce justicia retributiva Puede ser que se trate de una víctima ausente o abstracta, como en el caso de delitos contra el Estado y/o empresas, donde la ausencia física imposibilita ver realmente a quién perjudica la acción.
- **Condenar a quien condena:** el criminal intenta evadir su responsabilidad sobre sus actos al desacreditar a quienes lo juzgan y al sistema normativo en el que vive. Suele verse como un desafío a cualquier figura de autoridad, pudiendo ser un efectivo policial, un docente en el aula o incluso a sus padres.
- **Apelación a lealtades superiores:** los actos del criminal se justifican al afirmar que está sirviendo a un bien mayor, sin importar si sus actos infrinjan la ley o no. Sus acciones son medios para un fin, que son necesarias para alcanzar un objetivo más importante o en nombre de grupos que considera minoría. En este caso adopta un rol de mártir o soldado dispuesto a sacrificarse por un bien común o alcanzar la justicia social.

Sykes y Matza sin embargo postulan que algunas técnicas pueden tener más afinidad con algún tipo de delito que otro, por lo que podemos hipotetizar que no en todos los casos que un criminal intenta justificarse utilizará los cinco mecanismos juntos (podría utilizar solo uno o alguno de ellos)

6 Analogía propuesta

Se propone entonces trasladar los marcos teóricos antes descritos, originalmente formulados para explicar el crimen tradicional, al entorno digital donde operan los grupos de Amenazas Persistentes Avanzadas (APTs). Específicamente se observan algunos factores de referencia como:

6.1 **Asociación Diferencial**

A continuación, se indican las posibles conexiones que puede hacer el fenómeno del cibercrimen a la teoría de la asociación diferencial. El contexto en el que operan los cibercriminales difiere de otros escenarios delictivos en los que la violencia física suele estar presente, resulta necesario aplicar enfoques teóricos distintos que permitan comprender mejor las premisas subyacentes a estas conductas (Lowry, 2019). Como toda teoría sociológica que refleja su estudio sobre una muestra delimitada en tiempo y espacio, es muy probable que existan excepciones a ella, así como también la necesidad de ajustarla y traerla al tiempo en el que se la pretenda aplicar para intentar explicar un fenómeno criminológico. Adicionalmente se considera importante resaltar la diferenciación entre "cibercriminal" y "hacker" como personas con distintas motivaciones y objetivos.

Sobre el aprendizaje del comportamiento delictivo: Los cibercriminales suelen pueden aprender sus técnicas y estrategias de hacking a través de foros en línea, comunidades, grupos de Telegram, o grupos de cibercriminales que ponen a disposición mentorías (a veces sin costo), esto facilita el aprendizaje y la transmisión de conocimientos.

Sobre las definiciones favorables a la delincuencia: A medida que los cibercriminales interactúan en comunidades digitales, pueden adoptar definiciones que justifiquen el cibercrimen, como la creencia de que las grandes empresas merecen ser hackeadas, o que el hacking es solo un juego o desafío técnico. La anonimidad en línea también facilita la creación de estas definiciones, ya que las personas pueden percibirse menos responsables de sus acciones debido a la falta de interacción cara a cara.

Sobre las técnicas de racionalización: La falta de contacto físico con las víctimas puede facilitar la justificación de las acciones, ya que no hay una visualización directa del daño humano o material. En el caso de los ataques de Ransomware, muchos grupos de cibercriminales pueden verlo como una forma de obtener dinero de forma "simple" y "anónimamente", sin enfrentar consecuencias directas.

6.2 **Elección Racional**

En un escenario hipotético, una persona descontenta con su trabajo podría tomar una decisión racional basada en un análisis detallado de los beneficios, costos y riesgos asociados con la posibilidad de realizar un ciberataque interno. Si este posee algún acceso privilegiado a información sensible o a cuentas que le permitan extraer información, podría llegar a considerar utilizarlo a su favor.

Dentro de los posibles beneficios este podría vender datos a una competencia, realizar chantaje a su propia compañía o cualquier otro tipo de acción ilícita que resulte en un beneficio económico. Por otro lado, podría llegar a considerar un beneficio personal al obtener cierto poder o control dentro de la organización, tomar represalias contra la empresa o mejorar su estatus fuera de su lugar de trabajo. Al analizar los riesgos asociados a sus acciones podría pensar en la probabilidad de que sea descubierto dentro de su compañía, ya sea por su propio entorno o alguna medida de protección.

Por último, el sujeto puede considerar las consecuencias legales y profesionales a enfrentar, despido, o incluso una causa penal.

Si dicho empleado percibe que los riesgos son bajos, por ejemplo, al observar medidas de seguridad débiles, es más probable que se sienta motivado a seguir adelante con el robo de información. En cambio, si los riesgos resultaran ser más altos que los beneficios, esto podría disuadirlo de su actitud criminal.

6.3 **Teoría de las Actividades Cotidianas**

Stuxnet es considerado uno de los ataques APT más sofisticados de la historia, ya que no solo afectó a una infraestructura crítica, sino que lo hizo de una manera que no era posible detectarla a simple vista, utilizando técnicas avanzadas y con una precisión tal que causó daño físico real. En este caso se cumplen con los tres factores necesarios para que se cumpla con la oportunidad:

Cibercriminal motivado: El ataque podría haber sido motivado por intereses estratégicos, especialmente la intención de frenar el desarrollo de armas nucleares sin recurrir a la violencia física directa.

Objetivo Adecuado: La planta de Natanz era un objetivo crucial, su actividad era esencial para el programa nuclear, la tecnología implementaba tenía vulnerabilidades específicas que fueron explotadas.

Ausencia de Guardianes Capaces: La falta de monitoreo adecuado de los distintos activos tecnológicos y la falta de protección contra accesos externos contribuyeron al éxito del ataque.

6.4 **Teoría de la Neutralización**

Consideremos un escenario hipotético: Una supuesta agencia gubernamental es víctima de un ciberataque por parte de un grupo hacktivista; un ataque de DDoS interrumpa el normal funcionamiento de los sistemas, junto con la extracción y publicación de documentos internos, demostrando una actividad de espionaje sin orden judicial a favor de la ciudadanía.

La justificación del ataque podría deducirse de la siguiente manera:

Negación de responsabilidad: "*Somos ciudadanos preocupados por nuestros derechos*", "*No tendríamos que hacer esto si el gobierno respetara nuestra privacidad*". La responsabilidad del hecho se trasladaría hacia la agencia gubernamental, se argumenta que la situación provocó la reacción del grupo hacktivista.

Negación del daño: "*No hubo daño económico ya que no se sustrajo dinero de ninguna cuenta*", "*No destruimos dependencias físicas que necesiten ser reparadas*". El impacto del ciberataque se puede ver minimizado bajo esta perspectiva asegurando que no hubo un perjuicio real, solamente se expuso la verdad.

Negación de la víctima: "*La agencia gubernamental no es una víctima, es una institución que espía a sus ciudadanos y reprime la libertad de expresión*". En este caso la víctima se sostiene como victimario y se alega un accionar basado en la justicia.

Condenar a quien condena: "*Ellos no respetan nuestra privacidad ¿Quién es el verdadero infractor?*". Se desacredita a quienes condenan el ataque, argumentando que la otra parte cometen delitos de mayor importancia bajo la protección de la ley.

Apelación a lealtades superiores: "*Alguien debe proteger la libertad y la privacidad de la gente. Si tenemos que violar una ley injusta para defender un derecho fundamental, lo haremos*." Se justifica la ilegalidad del acto apelando a una causa superior, la defensa de los derechos civiles.

7 Análisis y Aplicación sobre APTs

En la práctica, el análisis de APTs se ha centrado en aspectos técnicos (vectores de ataque, vulnerabilidades explotadas, tácticas, técnicas y procedimientos) y en atribución geopolítica o estatal de sus actividades (MITRE ATT&CK, 2025). Sin embargo, el uso de teorías criminológicas ha sido menos sistemático. Algunos informes mencionan brevemente motivaciones financieras o ideológicas, pero no suelen fundamentarse en marcos teóricos delictivos para profundizar en la comprensión del comportamiento de estos grupos.

De igual modo, las compañías de ciberseguridad elaboran perfiles de amenazas que describen el grado de sofisticación o los posibles objetivos (IBM, 2025) (Mandiant, 2025), aunque es menos frecuente encontrar análisis que los vinculen formalmente con conceptos como "oportunidad delictiva" o "racionalización del delito". Las capacidades técnicas de un grupo son reconocidas, pero su posible "cultura delictiva" o "modos de aprender y justificarse" a menudo quedan en segundo plano.

7.1 La organización del cibercrimen

El Foro Económico Mundial indica que los grupos de ciberdelincuentes se comportan como empresas transnacionales altamente rentables, adoptando y reproduciendo estrategias empresariales para aumentar el volumen y el impacto de sus actividades. En particular esta forma de operar les permite despistar a los investigadores, y el análisis de riesgo-beneficio que realizan valida sus decisiones y los impulsa a continuar con sus actividades delictivas (Umansky, 2024).

Por otro lado, se define a la ciberdelincuencia como parte del mundo del crimen organizado (Benítez, 2024). Por su estructura jerárquica, que incluye personas en posiciones de liderazgo, otras que funcionan como reclutadores de talentos, los técnicos que encabezan las campañas o ciberataques y finalmente la mano de obra quien es la encargada de llevar adelante dichos ataques bajo sus órdenes. Por su capacidad de moverse en un entorno digital que les ofrece anonimato y una baja percepción del riesgo de ser rastreados, junto a unas ganancias prometedoras, es que se puede pensar que es posible que sean vistas como empleadores para aquellos con las habilidades técnicas suficientes.

Como en toda organización cuyo objetivo es obtener ganancias, es posible teorizar que poseen una misión, una visión, una cultura de trabajo y hasta un modus operandi o dinámicas de trabajo establecidas que les permitirían llegar al "éxito" por cada campaña

realizada. Todos estos conceptos remiten a distintas teorías de las organizaciones que podrían ser aplicadas al cibercrimen organizado para entender cómo los grupos de cibercriminales operan y se estructuran.

La Teoría Clásica, desarrollada por autores como Henri Fayol, se enfoca en la estructura formal de la organización, destacando la importancia de la división del trabajo y la jerarquía. En el contexto del cibercrimen, esta teoría podría explicar cómo los cibercriminales se especializan en diferentes roles dentro de su grupo para maximizar su eficacia. La Teoría de la Administración Científica, propuesta por Frederick Winslow Taylor, busca optimizar los procesos mediante la estandarización y la selección de empleados. En el cibercrimen, esto podría aplicarse al hecho de que los grupos organizados pueden estandarizar métodos y seleccionar a sus miembros basándose en habilidades específicas, lo que lleva a un comportamiento más uniforme. Finalmente, la Teoría de la Burocracia, desarrollada por Max Weber, se centra en la creación de una estructura formal con reglas claras para asegurar la eficiencia. En grupos de cibercrimen, esta estructura podría influir en cómo los miembros siguen procedimientos establecidos para mantener la eficacia y evitar la detección. Estas teorías clásicas ofrecen una perspectiva valiosa sobre cómo los cibercriminales pueden operar de manera coordinada y eficiente, a pesar de la naturaleza ilegal de sus actividades.

7.2 **Aplicación de la teoría clásica**

Adoptar con mayor profundidad las teorías criminológicas para el estudio de los grupos APTs podría

Optimizar la prevención y la disuasión: Entender qué factores de oportunidad o motivación inciden en la selección de objetivos puede ayudar a diseñar defensas más efectivas que limiten oportunidades o aumenten riesgos.

Mejorar la identificación de patrones conductuales: Vincular comportamientos repetitivos a marcos criminológicos puede facilitar la atribución e, incluso, la predicción de ataques futuros.

Orientar estrategias de contramedidas: Medidas basadas en la Teoría de la Prevención Situacional podrían reducir las oportunidades para llevar a cabo ataques, mientras que la Teoría de la Elección Racional sugiere incrementar los costos (riesgos, dificultades técnicas) para desincentivar la actividad delictiva. (Clarke R. V., 1993)

Explicar la formación cultural de los grupos APTs: La Teoría de la Asociación Diferencial sugiere que la cultura de un grupo se fundamenta en la transmisión de conocimientos delictivos, algo observable en foros y redes clandestinas. Reconocer esta dinámica puede mejorar las acciones de contrainteligencia en dichas comunidades.

7.3 **Aplicación de los Cinco Grandes Rasgos**

El estudio de la conducta delictiva ha integrado desde hace décadas múltiples enfoques psicológicos y criminológicos que buscan identificar patrones en las características de personalidad vinculadas con el delito. En este contexto, el modelo de los Cinco Grandes Rasgos (Big Five o modelo OCEAN) emerge como un marco

integrador moderno, proporcionando dimensiones claramente definidas (apertura, responsabilidad, extraversión, amabilidad y neuroticismo) que permiten establecer conexiones directas con teorías clásicas. Por ejemplo, la dimensión de responsabilidad está estrechamente vinculada con el concepto de autocontrol en la teoría de Gottfredson y Hirschi, mientras que neuroticismo y extraversión se relacionan directamente con los postulados originales de Eysenck.

Este modelo identifica cinco dimensiones amplias que capturan la mayor parte de la variación en los rasgos de personalidad:

- **Apertura a la Experiencia (O)**: Se refiere a la curiosidad intelectual, la imaginación y la apreciación del arte. Las personas con alta apertura suelen ser creativas y disfrutan explorando nuevas ideas y experiencias.
- **Conciencia (C)**: También conocida como responsabilidad, esta dimensión se centra en la organización, la disciplina y la capacidad de planificar y cumplir objetivos. Individuos con alta conciencia tienden a ser más organizados y responsables.
- **Extraversión (E)**: Este rasgo incluye la sociabilidad, la búsqueda de emociones y la asertividad. Las personas extrovertidas suelen ser más activas socialmente y buscan interacciones con otros.
- **Amabilidad (A)**: Se relaciona con la cooperación, la empatía y la amabilidad hacia los demás. Individuos con alta amabilidad son más propensos a ser comprensivos y respetuosos.
- **Neuroticismo (N)**: Este rasgo se asocia con la propensión a experimentar emociones negativas como la ansiedad, la ira o la tristeza. Las personas con alto neuroticismo pueden ser más sensibles al estrés y las situaciones adversas.

7.4 **Modelo propuesto**

Si consideramos el comportamiento de una organización cibercriminal estructurada, como individuo único, considerando valores, misión, cultura y modus operandi propios, es posible sugerir la aplicación del modelo de Big Five. La naturaleza disciplinada, coordinada y enfocada de los grupos APT da lugar a realizar un análisis como una entidad unificada bajo esta perspectiva.

Estudios han explorado la correlación entre los cinco grandes factores de personalidad y el desempeño en entornos organizacionales (Gómez Cardona, 2024). Su análisis en una institución de salud en Colombia demuestra que este modelo es útil para evaluar la personalidad en organizaciones, facilitando la gestión del talento y la toma de decisiones estratégicas. Además, las cinco dimensiones del modelo están directamente relacionadas con el desempeño laboral, la adaptación al entorno y la efectividad organizacional. Esta aplicación ofrece una nueva perspectiva para comprender dinámicas internas, capacidad de adaptación y la manera en que su estructura psicológica colectiva influye en la ejecución de sus operaciones ilícitas.

Una propuesta de medición para aplicar el modelo al comportamiento de grupos APT podría ser la siguiente, donde 1 representa un nivel muy bajo y 5 representa un nivel muy alto:

Escala de Rasgos del Big Five

- **Apertura a la Experiencia (O)**

1: Muy baja apertura; resistencia al cambio y a nuevas ideas.
2: Baja apertura; poco interés en explorar nuevas experiencias o innovaciones.
3: Moderada apertura; alguna curiosidad, pero con limitaciones en la exploración.
4: Alta apertura; busca activamente nuevas ideas y enfoques innovadores.
5: Muy alta apertura; extremadamente curioso y creativo, siempre en busca de nuevas experiencias.

- **Conciencia (C)**

1: Muy baja conciencia; desorganizado, poco fiable y sin planificación.
2: Baja conciencia; a menudo improvisa y no sigue procedimientos.
3: Moderada conciencia; algo organizado, pero puede ser inconsistente.
4: Alta conciencia; bien organizado, planificado y responsable en sus acciones.
5: Muy alta conciencia; extremadamente meticuloso, siempre sigue procedimientos y es altamente fiable.

- **Extraversión (E)**

1: Muy baja extraversión; extremadamente reservado y evita la interacción social.
2: Baja extraversión; poco sociable, prefiere trabajar solo.
3: Moderada extraversión; interactúa ocasionalmente pero no busca atención.
4: Alta extraversión; disfruta de la interacción social y busca ser el centro de atención.
5: Muy alta extraversión; extremadamente sociable, carismático y siempre en busca de interacciones.

- **Amabilidad (A)**

1: Muy baja amabilidad; egoísta, manipulador y sin consideración por los demás.
2: Baja amabilidad; tiende a ser cínico y no muestra empatía hacia los demás.
3: Moderada amabilidad; puede ser cooperativo en ocasiones, pero no siempre.
4: Alta amabilidad; generalmente comprensivo, cooperativo y empático.
5: Muy alta amabilidad; extremadamente altruista, siempre prioriza el bienestar de los demás.

- **Neuroticismo (N)**

1: Muy bajo neuroticismo; emocionalmente estable, rara vez experimenta ansiedad o estrés.
2: Bajo neuroticismo; ocasionalmente experimenta emociones negativas, pero las maneja bien.
3: Moderado neuroticismo; experimenta emociones negativas con cierta frecuencia.
4: Alto neuroticismo; a menudo ansioso o estresado, con dificultades para manejar emociones negativas.
5: Muy alto neuroticismo; extremadamente sensible al estrés, con frecuentes emociones negativas.

7.5 Aplicación hipotética del Modelo Propuesto

El siguiente es un caso de aplicación sobre un grupo APT hipotético cuya denominación es inventada y no representa a ningún grupo en particular:

Dark Mercury es un grupo de cibercrimen organizado que opera utilizando técnicas avanzadas para infiltrarse en sistemas de seguridad altamente protegidos. El grupo es conocido por su capacidad para innovar y adaptarse rápidamente a nuevas tecnologías. Utilizan técnicas de aprendizaje automático para mejorar sus ataques y explotar vulnerabilidades desconocidas en el software más actualizado. Recientemente, desarrollaron un exploit que aprovechó una vulnerabilidad en un sistema operativo recién lanzado, antes de que los desarrolladores pudieran parchearla. A pesar de su naturaleza clandestina, Dark Mercury opera con una estructura altamente organizada y jerárquica. Cada miembro tiene un rol específico y bien definido, lo que permite una ejecución precisa de sus operaciones. Su ataque a un banco europeo fue planificado durante meses, con cada paso cuidadosamente coordinado para evitar la detección. Aunque Dark Mercury no busca la atención pública, sus ataques son lo suficientemente audaces como para generar un impacto significativo en la comunidad cibernética. No son completamente reservados, pero tampoco buscan ser el centro de atención. Aunque no reclaman responsabilidad por sus ataques, dejan pistas sutiles que sugieren su participación, lo que ha generado especulaciones en los foros de seguridad. Dark Mercury muestra una falta total de empatía hacia sus víctimas. No dudan en atacar infraestructuras críticas o robar fondos de organizaciones benéficas, siempre que se alinee con sus objetivos financieros. Recientemente, atacaron un hospital, causando interrupciones en servicios críticos y poniendo en riesgo vidas. Aunque el grupo opera bajo una gran presión, su estructura organizada y su planificación meticulosa les permiten manejar el estrés sin que afecte significativamente su desempeño. Sin embargo, pueden experimentar cierto nivel de ansiedad cuando enfrentan contramedidas efectivas. Durante un ataque reciente, cuando las defensas del objetivo se activaron inesperadamente, el grupo mostró cierta desorganización temporal antes de reajustar su estrategia.

En base al escenario propuesto, se podría proponer la siguiente puntuación:

Rasgo	Indicador	Ejemplo	Puntos
Apertura a la Experiencia	Capacidad para innovar y adaptarse rápidamente a nuevas tecnologías	Desarrollo de un zero-day para un sistema operativo nuevo.	5
Conciencia (Responsabilidad)	Posee una estructura altamente organizada y jerárquica con roles específicos.	Planificación con meses de anticipación.	5
Extraversión	Campañas audaces e innovadoras, sin buscar ser el centro de atención.	Dejan pistas sutiles que sugieren su participación	3
Amabilidad	Falta de empatía	Atacó a un hospital poniendo en riesgo cientos de vidas.	1

Neuroticismo	Pueden experimentar cierto nivel de ansiedad cuando enfrentan contramedidas efectivas.	Desorganización temporal	3

El uso de la escala resultante permitiría adoptar un enfoque integral y proactivo ante la futura interacción con este grupo de amenazas (respuesta ante incidentes, extorsión, detección y bloqueo). Esta evaluación ayudaría a anticipar su comportamiento y diseñar estrategias de defensa más efectivas.

Un grupo con “alta apertura a la experiencia” podría estar en constante innovación en sus técnicas de ataque, lo que exigiría una detección más dinámica y adaptable. Un grupo con “baja amabilidad” no dudaría en atacar infraestructuras críticas, por lo que la protección de estos sistemas debería ser prioritaria incluyendo definiciones ante un protocolo de interacción para una posible extorsión. Un grupo con “baja conciencia y baja amabilidad” combinaría una planificación meticulosa con una total falta de consideración por el impacto de sus acciones.

Aplicar este modelo a perfiles detallados permitiría detectar patrones y tendencias que podrían pasar desapercibidos en un análisis puramente técnico. Esto permitiría identificar la presencia de amenazas emergentes con mayor eficiencia, mejorando la capacidad de respuesta ante posibles ataques.

8 Limitaciones y riesgos

Este estudio presenta limitaciones que deben ser consideradas al interpretar los hallazgos. En primer lugar, al basarse en una revisión de la literatura existente y fuentes secundarias, es posible que los métodos de revisión al ser homogéneos, no sean los adecuados. Por tanto, es necesario explorar más a fondo los resultados para garantizar la calidad y el alcance del estudio propuesto. Además, es importante considerar que la rápida evolución de los grupos de amenazas podría dejar los resultados de la aplicación del modelo propuesto desactualizados. Nuestro análisis se ha limitado a interpretar las teorías junto con los escenarios propuestos sin poder verificar los resultados en un contexto práctico, consideramos que el modelo propuesto podría no ser aplicable a todos los grupos en otros contextos. Por último, debido a la complejidad multidisciplinaria del área de estudio, la integración de teorías de criminología y psicología en el ámbito tecnológico conlleva el riesgo de una simplificación excesiva que debe tenerse en cuenta a la hora de utilizar los resultados de la aplicación del modelo.

9 Trabajo futuro

Las futuras investigaciones en esta temática podrían explorar la incorporación y aplicación de otros modelos utilizados en el marco de la criminalística (como la Tetrada Oscura) para contribuir con un modelo con más variantes que permitan alinearse a

escenarios más amplios. Por otro lado, y para su validación, es crucial desarrollar la aplicabilidad del modelo en casos reales de grupos de amenazas para reconocer las dificultades de su adopción. Finalmente, es necesario poner a prueba los resultados del modelo en escenarios realistas definiendo en un mapeo claro las situaciones técnicas sobre las que toma relevancia la toma de decisiones en enfrentamientos con los grupos de amenaza evaluados.

10 Conclusiones

El estudio propuesto desarrolla un modelo teórico que establece analogías entre las teorías criminológicas y las características psicológicas de los ciberdelincuentes, con el objetivo de generar conclusiones útiles para el análisis y la comprensión de la dinámica operativa en contra de los grupos de APTs, este tiene resultados valiosos que aún puede explorarse en profundidad. Si bien el análisis técnico y la atribución geopolítica han sido enfoques predominantes en el estudio de los APTs, la aplicación sistemática de teorías criminológicas ofrece una perspectiva novedosa y valiosa. Considerar a los APTs como organizaciones con objetivos claros sobre los que aplicar marcos teóricos tanto criminológicos como psicológicos representa un avance en la comprensión y el abordaje de estas amenazas sofisticadas. Este enfoque integrador puede optimizar las estrategias de prevención, detección y respuesta ante incidentes de ciberseguridad.

11 Referencias

Benítez, L. (7 de 10 de 2024). *Delitos en la era digital: Cibercrimen & crimen organizado en un mundo interconectado*. Obtenido de Pensamiento Penal.: https://www.pensamientopenal.com.ar

Clarke, D. C. (2017). *The Reasoning Criminal: Rational Choice Perspectives on Offending.*

Clarke, R. V. (1993). Routine activity and rational choice: Advances in criminological theory.

Cressey, D. R. (1953). Other people’s money: A study in the social psychology of embezzlement. Free Press.

Gómez Cardona, N. (2024). *Correlación entre los cinco grandes factores de personalidad, neuroticismo, extraversión, apertura a la experiencia, amabilidad, conciencia y la evaluación del desempeño de los empleados de una institución prestadora de servicios*. Obtenido de Universidad de Antioquia: https://bibliotecadigital.udea.edu.co/bitstream/10495/15202/1/GomezNatalia_2014_CorrelacionCincoGrandes.pdf

IBM. (2025). *IBM X-Force Threat Intelligence Index 2024*. Obtenido de https://www.ibm.com/reports/threat-intelligence

Lowry, M. S. (2019). Breaking Bad in Cyberspace: Understanding Why and How Black Hat Hackers Manage their Nerves to Commit Their Virtual Crimes. *Information Systems Frontiers*.

Mandiant. (2025). *M-Trends 2024 Special Report*. Obtenido de https://cloud.google.com/security/resources/m-trends

MITRE ATT&CK. (2025). Obtenido de https://attack.mitre.org/

Social Change and Crime Rate Trends: A Routine Activity Approach. (1979). *American Sociological Review*.

Sutherland, E. H. (1947). *Principios de criminología (4ª ed.).*

Sykes, G. M. (1957). Techniques of neutralization: A theory of delinquency. . *American Sociological Review*.

Umansky, N. (2024). *Cómo se unen la industria y el sector público para combatir la ciberdelincuencia*. Obtenido de World Economic Forum: https://es.weforum.org/stories/2024/11/como-se-unen-la-industria-y-el-sector-publico-para-combatir-la-ciberdelincuencia/

Guerra, E. (2023). Organizaciones criminales. Apuntes desde la Teoría General de Sistemas Sociales. *Estudios Sociológicos De El Colegio De México, 41(123)*.