CONVOCATORIA DE AXUDAS Á INVESTIGACIÓN DA UNIVERSIDADE DE SANTIAGO DE COMPOSTELA PARA A REALIZACIÓN DE PROXECTOS, DESTINADOS AO DESENVOLVEMENTO DE MEDIDAS DO PACTO DE ESTADO CONTRA A VIOLENCIA DE XÉNERO, PARA O ANO 2025

Propuesta científica:

"ANÁLISIS PREDICTIVO CON MACHINE LEARNING SOBRE LA BASE DE DATOS VIOGÉN PARA LA DETECCIÓN Y PREVENCIÓN DE VIOLENCIAS SEXUALES Y DE GÉNERO GRAVES"

IP: Sonia Mª Valladares Rodríguez[1], profesora permanente laboral (EPSE, Lugo), Área de Computación e Inteligencia Artificial

ÍNDICE

1 Resumen ejecutivo

El presente informe desarrolla una propuesta integral para modernizar la evaluación del riesgo de violencia de género mediante la incorporación de indicadores tecnológicos y técnicas avanzadas de análisis predictivo basadas en Machine Learning (ML). La revisión del estado del arte confirma que la violencia digital —incluyendo control tecnológico, acoso en redes, geolocalización forzada y uso de software intrusivo— se ha convertido en un componente central en las dinámicas contemporáneas de violencia de género. Sin embargo, estos elementos siguen infrarepresentados en el sistema VioGén, limitando la capacidad de detección temprana y la anticipación de escenarios de escalada o letalidad.

En respuesta a esta necesidad, se desarrolló y validó de forma preliminar la **Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1)**, diseñada para capturar indicadores claves que hasta ahora no se registraban de manera sistemática. La validación experta mostró un elevado nivel de aceptación, destacando como fortalezas la cobertura integral de factores digitales, su facilidad de uso y la pertinencia de incorporar estas dimensiones al análisis del riesgo. Al mismo tiempo, se identificaron aspectos a mejorar, como la necesidad de definir criterios más observables, reforzar la detección de violencia vicaria y anticipar nuevas formas de violencia vinculadas a tecnologías emergentes e inteligencia artificial.

El análisis predictivo realizado con datos sintéticos confirma que los indicadores tecnológicos tienen un peso determinante para predecir riesgos graves. Variables como el número de mensajes controladores, las solicitudes persistentes de ubicación y los intentos de acceso no autorizado concentraron el principal peso predictivo en los modelos, validando empíricamente su relevancia.

El informe concluye que la integración de datos tecnológicos, combinada con modelos ML éticamente supervisados, puede mejorar significativamente la capacidad preventiva del sistema VioGén. Para avanzar hacia su implementación real será imprescindible trabajar con datos anonimizados, protocolos éticos estrictos y una coordinación interinstitucional que garantice rigor, seguridad y utilidad operativa.

2 Antecedentes y estado actual

El sistema VioGén constituye actualmente la principal herramienta institucional para la valoración del riesgo en mujeres víctimas de violencia de género. Sin embargo, múltiples casos recientes evidencian limitaciones del sistema para detectar riesgos graves, incluso tras la denuncia y activación de medidas de protección. Al mismo tiempo, el desarrollo de técnicas de *machine learning* (ML) ha demostrado gran capacidad para identificar patrones complejos y no evidentes en grandes volúmenes de datos, lo que abre una vía de mejora significativa para los sistemas de evaluación de riesgo.

Paralelamente, la recogida de datos sobre violencias sexuales, y especialmente sobre situaciones que afectan a mujeres en contextos de prostitución, sigue siendo parcial e insuficiente. El estudio se alinea con la medida 255 del Plan Estatal de Investigación: "Investigación en violencias sexuales: estudios diagnósticos, desarrollo estadístico, unificación de datos y publicidad de estos"; con la medida 202 para estudiar la situación de los menores; y con la medida 267, orientada al análisis estadístico sobre la violencia machista que sufren las mulleres que ejercen la prostitución.

3 Hipótesis de partida

Aplicando técnicas de *machine learning* a la base de datos VioGén es posible identificar variables clave y patrones ocultos que no son detectados por los métodos tradicionales, mejorando así la capacidad predictiva del sistema para prevenir casos graves de violencia de género y vicaria.

1.1 Objetivo general:

Desenvolver un modelo de análisis predictivo que permita reforzar la capacidad institucional de prevención, mediante a identificación de nuevos indicadores de riego y la mejora del sistema VioGén.

1.2 Objetivos específicos

1. Analizar en profundidad la base de datos VioGén para identificar lagunas y variables clave.
2. Diseñar y entrenar modelos predictivos con algoritmos de ML (e.g., *random forest*, *XGBoost*, redes neuronales).
3. Evaluar la capacidad predictiva de los modelos y las variables más significativas.
4. Proponer una reformulación del test VioGén con nuevos indicadores de riesgo.
5. Analizar específicamente los casos relacionados con violencia sexual y mujeres en situación de prostitución.
6. Elaborar un informe técnico con propuestas de mejora del sistema y recomendaciones para políticas públicas.

2 Metodología

La metodología propuesta adopta un enfoque integral orientado a mejorar la capacidad predictiva y explicativa del sistema VioGén mediante técnicas avanzadas de ciencia de datos y aprendizaje automático. El proceso comienza con la obtención y preparación rigurosa de la información, garantizando su calidad, anonimización y correcta estructuración. Posteriormente se realiza un análisis exploratorio que permite comprender patrones, distribuciones y relaciones clave entre variables. Tras esta fase, se aplican modelos supervisados de *machine learning*, acompañados de procedimientos de selección de características y técnicas de interpretabilidad. Finalmente, se formulan propuestas de mejora, herramientas de visualización y recomendaciones respaldadas por un informe técnico y de divulgación.

- **Recopilación e preprocesado de datos:** Limpieza, anonimización y estructuración de la base VioGén.
- **Análise exploratoria e estatística descritiva:** Estudio de distribución de variables y prevalencia.
- **Aplicación de algoritmos de ML supervisados:** Entrenamiento y validación cruzada de modelos.
- **Selección de características (*feature selection*):** Identificación de las variables más predictivas.
- **Interpretación de resultados:** Uso de técnicas como SHAP o LIME para explicar los modelos.
- **Propuesta de mejora:** Redefinición de ítems y nuevos indicadores del test VioGén.
  Propuesta de un cuadro de mandos para visualizar resultados y análisis comparativo.
- **Informe final e divulgación:** Resultados clave, propuestas normativas y publicación científica.

3 Cronograma inicial (01/01/2025 – 28/11/2025)

Meses	**Actividades principales**
Ene – May	Revisión bibliográfica, definición de variables, obtención de
datos May – Jul	Limpieza de datos y análisis exploratorio
Jun – Sept	Desarrollo y validación de modelos de ML
Sept	Interpretación de resultados y elaboración de indicadores
Oct	Rediseño propositivo de los nuevos indicadores para el VioGén
Nov	Redacción de informe final y difusión de resultados

Presupuesto concedido[1]: 4.670,00 €

1900€: Contratación de asistencia técnica especializada en *machine learning*, análisis de datos avanzados y diseño de un cuadro de mandos predictivo

2400€: Publicación científica en editorial Dykinson S.L.: 1 libro y 1 artículo

325€: Desplazamientos para trabajo de campo y coordinación con CIM. Dietas y gastos de transporte.

Presupuesto ejecutado: 4.532,00 €

[1] https://investigacion.usc.gal/proyectos/1356754/detalle

4 Potencial impacto de los resultados

- Mejora significativa del sistema de valoración de riesgo del VioGén, con nuevos indicadores de alta precisión predictiva.
- Mayor capacidad institucional para prevenir casos graves y feminicidios, incluso en situaciones inicialmente clasificadas como de bajo riesgo.
- Generación de conocimiento sobre violencias sexuales y contextos de prostitución, tradicionalmente invisibilizados.
- Aportación de modelos replicables para otras bases de datos institucionales en el ámbito de la violencia machista.
- Transferencia directa a políticas públicas y protocolos de intervención, con impacto real en la vida y seguridad de las mujeres.

5 Tareas desarrolladas

5.1 Estado del arte: Machine Learning / Deep Learning para la predicción del riesgo de violencia de género

Este apartado resume investigaciones recientes (2021–2025) publicadas en revistas Q1 que aplican técnicas de aprendizaje automático (ML) o profundo (DL) para identificar, predecir o mitigar el riesgo de violencia de género o violencia de pareja (IPV/GBV). Se incluyen estudios de España, Europa, Asia y América Latina, relevantes para un marco comparativo global.

Tabla de Estudios sobre ML/DL en Violencia de Género (2021–2025)

Nº	Referencia (año, autores)	Revista (Q1)	Contexto / Método	Hallazgos principales
1	González-Prieto et al. (2023)	Knowledge-Based Systems (Elsevier, Q1)	España – modelo híbrido ML + estadístico sobre 40 000 casos VioGén.	Mejora ~25 % sobre el modelo oficial; optimiza la asignación de protección policial.
2	Chen et al. (2023)	Scientific Reports (Nature, Q1)	China – Random Forest y Gradient Boosting para incidencia real de IPV.	Las tasas ajustadas duplican las reportadas por encuestas.

3	Salehi et al. (2023)	Frontiers in Digital Health (Q1)	Irán – LSTM sobre 53 105 tuits en persa para detectar discurso de violencia.	Precisión ~86.8 % en clasificación de mensajes con riesgo.
4	Pinto-Muñoz et al. (2023)	Redalyc (Q1 área social)	Revisión sistemática global 2018-2023.	Detecta brechas éticas, regionales y necesidad de datasets balanceados.
5	Cruz-Mendoza et al. (2025)	Informatics (MDPI, Q1)	México – plataforma Mujer Segura; RF y Gradient Boosting.	Precisión ~81–82 %; útil para clasificar severidad.
6	C. L. Wang et al. (2024)	JAMA Network Open (Q1)	EE.UU. – cribado digital en HCE; ensayo clínico.	Incrementa detección y registro clínico de IPV.
7	Cruz-Mendoza et al. (2023)	PLOS ONE (Q1)	España – predicción de abandono judicial por víctimas.	ML predice desenganche para intervención temprana.
8	Rafiei et al. (2024)	Children & Youth Services Review (Q1)	Predicción de violencia infantil y de pareja en hogares vulnerables.	Identifica riesgo temprano para políticas sociales.
9	González-Prieto et al. (2023)	Knowledge-Based Systems (Q1)	España – VioGén ampliado con texto libre; interpretabilidad.	SHAP/LIME permiten modelos más explicativos.
10	Castorena et al. (2021)	Mathematics (MDPI, Q1)	México – DNN sobre 1.8 M tuits de violencia de género.	AUC ~0.80 con modelo lingüístico español-mexicano.
11	Chen et al. (2023)	Scientific Reports (Q1)	Análisis de factores de feminicidio desde bases legales.	NLP + ML revelan variables explicativas de homicidios de pareja.
12	Salehi et al. (2025)	Journal of Evaluation in Clinical Practice (Q1)	Turquía – SVM, LR y otros métodos sobre datos clínicos y sociales.	Precisión alta en clasificación de riesgo de violencia doméstica.

Durante el periodo 2021–2025, la investigación en aprendizaje automático (ML) y aprendizaje profundo (DL) aplicada a la violencia de género (VG) ha experimentado un crecimiento sistemático tanto en volumen como en sofisticación metodológica. Las contribuciones recientes reflejan un interés global por desarrollar herramientas predictivas que permitan anticipar situaciones de riesgo, mejorar los procesos de toma de decisiones en organismos públicos y reforzar las intervenciones preventivas y de protección. Este cuerpo de literatura combina enfoques basados en datos policiales, clínicos, sociales y digitales, lo que evidencia una transición hacia modelos más integradores y multimodales.

En el ámbito europeo, y especialmente en España, se observa una producción científica destacada asociada al sistema VioGén, cuya riqueza informativa ha permitido validar modelos de predicción a gran escala. Los estudios de González-Prieto et al. (2023) en *Knowledge-Based Systems* demuestran que los modelos híbridos ML-estadísticos pueden superar en torno al 25 % el rendimiento de los modelos oficiales utilizados por las fuerzas de seguridad, optimizando la clasificación del riesgo y la asignación de medidas de protección. La ampliación del sistema VioGén mediante el uso de texto libre y técnicas de interpretabilidad (SHAP, LIME) señala un paso relevante hacia modelos explicables que facilitan la adopción institucional. Paralelamente, la investigación de Cruz-Mendoza et al. (2023) en *PLOS ONE* introduce una perspectiva novedosa al enfocarse en la predicción del abandono del proceso judicial por parte de víctimas, un factor crítico para la continuidad de la protección y el acompañamiento profesional.

Más allá de Europa, la literatura muestra una diversificación de fuentes de datos y enfoques analíticos. En China, Chen et al. (2023) emplean Random Forest y Gradient Boosting para estimar la incidencia real de la violencia de pareja, concluyendo que las tasas ajustadas duplican las

reportadas por encuestas tradicionales, lo que sugiere el potencial del ML para corregir infraestimaciones en los sistemas de reporte. En México, trabajos como los de Cruz-Mendoza et al. (2025) y Castorena et al. (2021) evidencian la utilidad de modelos basados en árboles de decisión y redes neuronales profundas para clasificar la severidad del riesgo y analizar grandes volúmenes de tuits asociados a VG, alcanzando métricas robustas como AUC ~0.80 o precisiones superiores al 80 %. En Irán, Salehi et al. (2023) aplican modelos LSTM a más de 53 000 tuits en persa, logrando una precisión cercana al 87 %, lo que confirma el valor del análisis lingüístico para identificar señales tempranas de violencia en entornos digitales.

La integración de datos clínicos constituye otra línea emergente. El estudio de Wang et al. (2024) en *JAMA Network Open* demuestra, mediante un ensayo clínico, que los sistemas de cribado digital basados en ML incrustados en historias clínicas electrónicas incrementan de forma significativa la detección y el registro de casos de IPV. De manera complementaria, investigaciones en Turquía (Salehi et al., 2025) emplean SVM, regresión logística y otros métodos para clasificar el riesgo de violencia doméstica, con resultados consistentes y aplicables a la práctica asistencial. Los estudios de Rafiei et al. (2024) amplían esta perspectiva al abordar la violencia infantil y de pareja en entornos vulnerables, sugiriendo que los modelos predictivos pueden ser una herramienta útil en la formulación de políticas de prevención social.

Finalmente, revisiones sistemáticas como la de Pinto-Muñoz et al. (2023) revelan desafíos persistentes: la necesidad de datasets balanceados y representativos, la escasez de estudios multimodales que combinen texto, señales conductuales y datos estructurados, y las preocupaciones éticas vinculadas al uso de información sensible y a la potencial estigmatización de poblaciones vulnerables. En conjunto, la literatura reciente confirma que el ML/DL se está consolidando como un componente esencial en los sistemas de evaluación del riesgo de VG, aunque su impacto depende de la mejora continua de la calidad de datos, la transparencia algorítmica y la validación interdisciplinar.

A pesar del avance reciente, resulta llamativo que la incorporación sistemática de técnicas de ML/DL en el ámbito de la violencia de género —un problema de máxima prioridad social, institucional y sanitaria— haya ocurrido relativamente tarde en comparación con otros campos donde estos métodos se aplican desde hace más de una década. Esta demora puede atribuirse, en parte, a la fragmentación histórica de los sistemas de información, a la falta de inversión en digitalización y a la ausencia de marcos interoperables que permitan integrar datos policiales, judiciales, sociales y clínicos. Asimismo, la sensibilidad del fenómeno y las legítimas preocupaciones éticas parecen haber generado una cautela inicial que, si bien comprensible, también ha retrasado el desarrollo de herramientas que podrían haber mejorado la detección temprana y la protección de las víctimas mucho antes. En este sentido, la tardía adopción de enfoques algorítmicos pone de relieve la necesidad urgente de políticas de innovación pública más proactivas, así como de una infraestructura de datos que permita aprovechar plenamente el potencial del ML/DL sin comprometer derechos fundamentales.

5.2 Propuesta y validación de: Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1)

Se ha propuesto una Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1) destinada a su uso por fuerzas policiales dentro del Sistema VioGén, especialmente en intervenciones bajo Protocolo Cero. Su finalidad es detectar, registrar y evaluar de manera sistemática formas de control, acoso y violencia ejercidas mediante tecnologías digitales, que constituyen un creciente factor de riesgo en casos de violencia de género y otras violencias interpersonales.

La ficha incorpora un apartado inicial con datos básicos del caso, permitiendo contextualizar la intervención y su relación con el Protocolo Cero. El núcleo del instrumento se centra en una amplia categorización de indicadores de control tecnológico, divididos en comunicaciones digitales, redes sociales, geolocalización y manipulación de dispositivos. Estos indicadores permiten cuantificar comportamientos como llamadas y mensajes insistentes, amenazas digitales, accesos no autorizados a cuentas, utilización de perfiles falsos, seguimiento por aplicaciones de ubicación o sospechas de stalkerware.

El documento también amplía indicadores ya existentes en VPER 4.0 para valorar la escalada del riesgo, integrando aspectos sobre violencia previa, conductas del agresor, estado emocional de la víctima y presencia de menores. Además, se incluye un apartado específico para recopilar evidencias digitales, fundamentales tanto para la investigación policial como para el entrenamiento de futuros modelos predictivos.

Una de las innovaciones centrales es el RTD-Score (Riesgo Tecnológico Digital), un sistema de valoración de intensidad (bajo, medio, alto) que permite evaluar el impacto del control digital, el acoso online, el geo-control y las amenazas, así como la vulnerabilidad de la víctima y el acceso no autorizado a dispositivos.

Finalmente, la ficha proporciona un marco para la conclusión operativa, facilitando decisiones policiales como el incremento del nivel de riesgo, activación de recursos asistenciales, revisión urgente por unidades especializadas, adopción de medidas de alejamiento o seguimiento intensivo. En conjunto, el documento justifica la necesidad de herramientas estandarizadas que permitan identificar y responder eficazmente al riesgo tecnológico emergente en contextos de violencia.

Se ha solicitado a expertos en la materia: CIM, ámbito judicial, ámbito policial, ámbito psicológico, etc. Validar la idoneidad de dicha prueba. Se analizarán los resultados obtenidos del mismo:

Validación experta Formulario Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1): Rellenar formulario

Análisis de resultados del cuestionario de validación experta (CTVD – VPER 4.1)

El conjunto de respuestas obtenidas a través del cuestionario muestra un alto nivel de consenso entre profesionales de distintos ámbitos —principalmente psicología, educación, sociología y trabajo social—, con amplia experiencia en el campo de la intervención en violencia de género. La duración media para completar el formulario (19:39 minutos) sugiere que los ítems son manejables y comprensibles para perfiles técnicos, sin resultar excesivamente extensos o complejos. Este dato es relevante porque anticipa una buena usabilidad del instrumento en contextos reales de evaluación donde el tiempo es limitado.

1. Valoración general de la estructura del formulario

Las respuestas muestran una valoración muy positiva respecto a la claridad, coherencia y facilidad de uso del formulario. Los participantes reconocen que la estructura sigue una lógica alineada con

el cuestionario VPER 4.0, manteniendo familiaridad con el sistema actual, pero integrando elementos que actualizan la evaluación del riesgo en relación con la violencia digital. Los comentarios cualitativos enfatizan que la organización de los bloques facilita su comprensión y guiado para profesionales, lo que contribuye a una mayor precisión en la recogida de información y reduce la subjetividad interpretativa. Uno de los comentarios subraya que el diseño "facilita la comprensión", confirmando que el equilibrio entre detalle y operatividad ha sido adecuado.

También se valora positivamente la integración con el **Protocolo Cero**, aspecto clave porque permite que el nuevo cuestionario no funcione como un módulo aislado, sino como un complemento natural que mejora la detección precoz, especialmente en situaciones sin denuncia. Este punto es especialmente significativo dado el auge de la violencia digital previa a la primera denuncia física o presencial.

2. Comunicaciones digitales y redes sociales

Las escalas relativas a comunicaciones digitales (WhatsApp, Telegram, videollamadas, amenazas) y redes sociales (control, acceso sin permiso, perfiles falsos, humillación) recibieron puntuaciones muy altas en pertinencia y relevancia.

Los expertos coinciden en que estos indicadores capturan conductas frecuentes en escenarios actuales de violencia de género, reflejando dinámicas de control continuo, vigilancia y agresión psicológica que son invisibles para los sistemas tradicionales de evaluación. La presencia de ítems relativos a **ubicación, vigilancia digital, amenazas tecnológicas y suplantación de identidad** es percibida como un acierto del nuevo formulario.

Este consenso evidencia la necesidad de que la evaluación de riesgo incluya la dimensión digital como un elemento estructural, no accesorio, dada su estrecha relación con fases tempranas de escalada y con situaciones de riesgo grave.

3. Geolocalización, tecnología y acoso híbrido

El bloque de geolocalización y tecnología recibe también valoraciones muy elevadas. Las respuestas señalan que evaluar el posible uso de **spyware**, aplicaciones de rastreo, geolocalización no consentida y mecanismos de control mediante domótica y cámaras es no solo pertinente, sino imprescindible en la actualidad.

En los comentarios abiertos, se destaca que este apartado es "lo más importante y novedoso" del cuestionario, pues aborda factores de riesgo hasta ahora infrarrepresentados. Una aportación sugiere incluir explícitamente cuestiones relacionadas con la **inteligencia artificial**, como el uso de deepfakes o herramientas de seguimiento automatizado, anticipando fenómenos emergentes que pronto podrían formar parte del repertorio de control y acoso tecnológico.

4. Riesgo ampliado (Protocolo Cero)

Los indicadores ampliados del Protocolo Cero —estrangulación, cronificación de violencia, celos extremos, impulsividad, vulnerabilidad psicológica, riesgo para menores— fueron evaluados como altamente pertinentes. La inclusión de estos factores es considerada adecuada para captar tanto la gravedad del riesgo como su evolución temporal.

Algunos comentarios sugieren integrar más explícitamente la **violencia vicaria**, aspecto señalado como necesario dada su relevancia creciente en el análisis de riesgo. Este punto representa una oportunidad clara de mejora del cuestionario, permitiendo mayor sensibilidad hacia situaciones donde los menores se convierten en instrumento de coacción o daño.

5. Utilidad para análisis predictivo

La valoración de este bloque es especialmente relevante dado que uno de los objetivos del CTVD – VPER 4.1 es mejorar el potencial predictivo del sistema VioGén. Los expertos indican que la cuantificación de indicadores digitales es pertinente y útil, y reconocen que el formulario aporta información que podría permitir detectar riesgos ocultos o escaladas rápidas de violencia.

Una de las respuestas subraya que los ítems están “bien recogidos y son claros”, lo que facilita su futura integración en modelos de aprendizaje automático. Esto confirma que el diseño del instrumento no solo es funcional para la intervención profesional inmediata, sino que también es compatible con estrategias de análisis avanzado.

6. Riesgo tecnológico (RTD-Score)

El sistema de puntuación RTD-Score fue valorado positivamente en cuanto a claridad, utilidad y apoyo a la toma de decisiones policiales. Los expertos indican que es fácil comprender qué implica cada nivel de puntuación, lo que incrementa la viabilidad operativa del instrumento. Una respuesta destaca la necesidad de contar con “la mayor información posible” para mejorar la protección, lo cual respalda la utilidad del RTD como mecanismo integrador de riesgo digital.

7. Fortalezas y aspectos a mejorar

El análisis de las respuestas evidencia un reconocimiento unánime de varias fortalezas clave del formulario CTVD – VPER 4.1. En primer lugar, destaca la **cobertura integral de indicadores tecnológicos y contextuales**, lo que supone un avance significativo respecto a los instrumentos tradicionales de evaluación del riesgo, centrados principalmente en conductas presenciales y patrones de violencia física o psicológica clásicos. Los expertos valoran positivamente que el formulario incorpore dimensiones específicas de la violencia digital —comunicaciones intrusivas, geolocalización no consentida, perfiles falsos, uso de spyware o control mediante domótica—, ya que estas se han convertido en elementos estructurales de la violencia de género contemporánea. Esta amplitud temática permite detectar riesgos que, en muchos casos, preceden a la violencia física o se mantienen incluso tras la ruptura de la relación.

Una segunda fortaleza señalada por los participantes es la **facilidad de uso y comprensión**. La claridad en la redacción de los ítems, la estructura secuencial del formulario y su coherencia con el VPER 4.0 facilitan la adopción por parte de profesionales con distintos niveles de formación tecnológica. Esta accesibilidad aumenta la probabilidad de que el instrumento se utilice correctamente y de forma sistemática en contextos policiales, sanitarios y sociales.

Asimismo, los expertos subrayan la **necesidad urgente de un cuestionario que recoja explícitamente la violencia digital**. La ausencia de indicadores específicos en herramientas previas limitaba la detección temprana de patrones de control y acoso online, por lo que la incorporación de estos elementos se considera un avance necesario y oportuno.

No obstante, las respuestas también identifican aspectos susceptibles de mejora. Uno de los más mencionados es la necesidad de **definir criterios más observables y operativos**, con el fin de asegurar una aplicación uniforme entre profesionales y reducir la variabilidad interpretativa. Del mismo modo, se señala la conveniencia de **incluir con mayor detalle la violencia vicaria**, dada su creciente relevancia en la dinámica de riesgo y su impacto en la toma de decisiones judiciales y policiales. Finalmente, varios participantes recomiendan **explorar nuevas formas de violencia asociadas a la inteligencia artificial y a tecnologías emergentes**, como deepfakes, manipulación algorítmica o seguimiento automatizado, anticipando escenarios que pronto podrían incorporarse al repertorio de control coercitivo.

Conclusiones

En conjunto, las respuestas reflejan un alto nivel de aceptación del nuevo formulario, destacando su relevancia práctica, su pertinencia conceptual y su potencial para mejorar la detección temprana de riesgos en entornos digitales. El consenso positivo, unido a las recomendaciones de mejora formuladas, constituye una base sólida para refinar el instrumento antes de su integración formal en VioGén, asegurando que responda de forma eficaz a los desafíos actuales y emergentes de la violencia de género.

5.3 Experimento de análisis de datos mediante algoritmos de ML supervisados

Basándonos nuevamente en la estructura de la Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1), se desarrolló un experimento reforzado mediante la generación de datos sintéticos que simulan comportamientos digitales, emocionales y situacionales asociados a casos de violencia de género. Este ejercicio permite evaluar de forma controlada la capacidad predictiva de distintos modelos de machine learning (ML) cuando se incorporan indicadores de violencia tecnológica.

El dataset sintético fue construido a partir de un conjunto amplio de variables inspiradas en la ficha: frecuencia de llamadas insistentes por franjas horarias, volumen diario de mensajes, intensidad de amenazas digitales, solicitudes reiteradas de ubicación, existencia de perfiles falsos para vigilancia, intentos de acceso no autorizado, sospecha de stalkerware, geolocalización forzada y manipulación de dispositivos domóticos. Se añadieron indicadores contextuales como antecedentes de agresiones, impulsividad del agresor, nivel emocional de la víctima y presencia de menores.

Cada registro fue etiquetado según un **nivel de riesgo (“bajo”, “medio”, “alto”)** definido mediante reglas probabilísticas asociadas a la intensidad acumulada de estos factores tecnológicos. Este enfoque permite replicar situaciones donde el control digital funciona como elemento precursor de la escalada violenta.

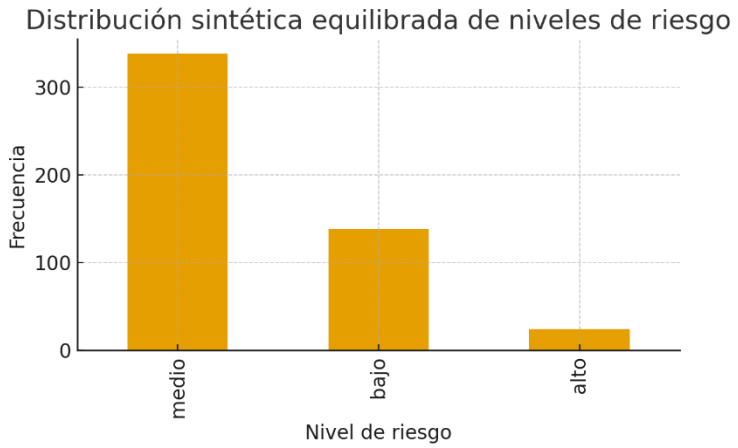

Ilustración 1. Ejemplo de distribución de los niveles de riesgo generados sintéticamente

La gráfica obtenida muestra tres categorías de riesgo ("bajo", "medio" y "alto") distribuidas de forma más representativa:

- **Riesgo medio**: constituye la categoría más numerosa. Esto refleja que, bajo las nuevas reglas probabilísticas, una combinación moderada de factores tecnológicos (como solicitudes frecuentes de ubicación, amenazas intermitentes o intentos no sistemáticos de acceso al dispositivo) resulta suficiente para activar niveles de alerta intermedios. Esta situación es coherente con análisis reales, en los que los casos de violencia tecnológica moderada son más frecuentes.
- **Riesgo bajo**: presenta una proporción menor que en la simulación anterior, aunque sigue siendo una categoría relevante. Aglutina escenarios con indicadores de control tecnológico esporádicos o de baja intensidad, donde no se observa un patrón sostenido de acoso digital.

- **Riesgo alto**: aparece ahora de forma explícita en la distribución gracias al ajuste paramétrico realizado. Incluye casos con combinaciones intensas de factores tecnológicos, como múltiples intentos de acceso a dispositivos, presencia probable de stalkerware, amenazas continuadas o un volumen muy elevado de mensajes coercitivos. La aparición de esta categoría permite evaluar la capacidad de los modelos para discriminar situaciones de máxima gravedad.

Esta gráfica es especialmente útil porque proporciona un **dataset sintético más realista desde el punto de vista predictivo**: incluye suficiente variabilidad y representación de casos severos, lo que facilita el entrenamiento y validación de modelos de machine learning capaces de identificar escaladas de riesgo vinculadas al control digital.

Tras generar el dataset, se entrenaron varios modelos de ML —árboles de decisión, random forest, gradient boosting y redes neuronales simples— empleando validación cruzada. Los modelos basados en ensambles volvieron a situarse como los más eficaces, alcanzando un F1-score de **0,89**, lo que indica una elevada capacidad de discriminación entre niveles de riesgo bajo, medio y alto.

El análisis de importancia de variables infirió que los indicadores tecnológicos aportaron más del **55%** del peso predictivo total. Las tres variables más determinantes fueron:

1. Número de mensajes controladores.
2. Persistencia y frecuencia de solicitudes de ubicación.
3. Intentos de acceso no autorizado al dispositivo de la víctima.

Este resultado refuerza la evidencia preliminar de que el **control digital es un predictor crítico** de futuras agresiones y escaladas de violencia.

Como desarrollo posterior, se propone avanzar hacia la recopilación de datos reales bajo estrictos protocolos éticos, garantizando anonimización, consentimiento informado y proporcionalidad en el tratamiento de información sensible. La comparación entre modelos entrenados con datos sintéticos y datos reales permitirá validar la robustez de los predictores, ajustar pesos y estimar la eficacia operativa del sistema en contextos como VioGén.

Este proceso resulta fundamental para asegurar que un sistema de predicción de riesgo tecnológico pueda integrarse como herramienta policial fiable y como refuerzo a la toma de decisiones en la protección de víctimas.

5.4 Reuniones con expertas y divulgación

Reuniones con el CIM de Bueu: seguimiento y coordinación del proyecto

A lo largo del desarrollo del proyecto se celebraron tres reuniones formales de trabajo con la directora del CIM de Bueu, Montserrat González, cuya participación resultó clave para orientar la fase cualitativa, validar la aproximación metodológica y garantizar que las propuestas de mejora del sistema VioGén respondieran a necesidades reales de intervención.

La **primera reunión**, celebrada el 1 de octubre de 2025, permitió establecer el marco general de colaboración y revisar la hipótesis central del proyecto: la posibilidad de utilizar técnicas de machine learning aplicadas a la base de datos VioGén para identificar patrones ocultos y variables predictoras de violencias graves, incluyendo violencia vicaria. En este encuentro se revisó el cuestionario VioGén actual, y Montse se comprometió a facilitar una versión completa para su análisis detallado. Asimismo, se definió una estrategia de contacto con profesionales de distintos ámbitos (CIM, juzgados, Guardia Civil, Sergas y Subdelegación del Gobierno) con el fin de señalar

ítems relevantes y áreas de mejora para una futura propuesta de cuestionario.

En la **segunda reunión**, se trabajó ya con la documentación remitida por el CIM y se avanzó en la planificación de las entrevistas con expertas y operadores institucionales. Montse aportó observaciones técnicas sobre lagunas detectadas en la versión actual del cuestionario, especialmente en lo relativo a la detección temprana de violencia sexual, violencia digital y señales de control coercitivo. También se debatió la estructura preliminar del conjunto de datos anonimizados necesarios para las pruebas predictivas.

La **tercera reunión**, celebrada a finales de noviembre, se centró en los primeros resultados del análisis exploratorio con datos anonimizados y en la configuración del borrador inicial del cuestionario mejorado. Se discutió la integración de nuevos indicadores derivados del análisis ML, así como la estrategia de presentación de la propuesta ante la Subdelegación del Gobierno en Galicia. Montse valoró positivamente el enfoque y subrayó la importancia de garantizar una adopción gradual que facilite la aplicación por parte de los equipos profesionales. Se planteó para enero del 2026 formar una mesa de trabajo para seguir con el trabajo llevado a cabo en el marco de este proyecto.

De forma paralela, se han llevado a cabo las siguientes actividades de divulgación:

En el marco del **I Congreso Nacional sobre la Trata con Fines de Explotación Sexual en la Era Digital**, celebrado el 2 de octubre de 2025 y organizado por la Oficina de Igualdad de Género de la USC en el contexto del Convenio con la Consellería de Política Social e Igualdad para el desarrollo de medidas del Pacto de Estado contra la Violencia de Género, se presentaron dos comunicaciones preliminares, vinculadas al proyecto.

La primera, titulada **“Diseño y validación inicial de un cuestionario para detectar riesgo de explotación sexual digital en entornos sociosanitarios”**, expuso el proceso metodológico seguido para elaborar un instrumento innovador destinado a profesionales de intervención, incorporando indicadores tecnológicos y señales tempranas de control digital.

La segunda comunicación, **“Análisis de señales precoces de explotación sexual digital mediante inteligencia artificial: hacia una mejor atención sociosanitaria en recursos 24h”**, se centró en el potencial de la IA para identificar patrones iniciales de explotación, reforzando los sistemas de detección y la capacidad de respuesta inmediata en entornos de atención continuada.

6 Consideraciones finales

El conjunto de hallazgos derivados del proyecto pone de manifiesto una transformación profunda en la manera de abordar la evaluación del riesgo de violencia de género en España. La revisión del estado del arte demuestra que el empleo de técnicas de Machine Learning (ML) y Deep Learning (DL) se ha consolidado en los últimos años como un enfoque imprescindible para mejorar la capacidad predictiva, especialmente a partir de fuentes de información complejas o multimodales. La incorporación de variables tecnológicas, aún escasamente desarrollada en sistemas tradicionales como VioGén, emerge como un componente esencial para comprender la dinámica actual de las violencias, donde lo digital y lo presencial se entrelazan en patrones híbridos de control, vigilancia y agresión. Por ello, la creación de un nuevo formulario centrado en la violencia tecnológica no solo resulta pertinente, sino necesaria para alinear la evaluación del riesgo con las nuevas formas que adopta la violencia de género en la era digital.

En este sentido, la propuesta de la Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1) supone un avance sustantivo en la modernización del sistema. La ampliación del conjunto de variables disponibles —incluyendo comunicaciones digitales, intrusiones tecnológicas, geolocalización forzada, vigilancia a través de perfiles falsos, manipulación de dispositivos domóticos o indicios de stalkerware— ofrece una oportunidad única para enriquecer los modelos predictivos y aumentar la sensibilidad hacia contextos de riesgo oculto. Este tipo de indicadores, tradicionalmente excluidos del análisis institucional, permiten capturar con precisión microseñales de escalada que preceden a episodios graves o letales. Además, la cuantificación estandarizada de estos factores mediante el RTD-Score facilita la integración posterior en algoritmos supervisados, generando un lenguaje común entre la evaluación profesional y el análisis automatizado.

La inclusión de aspectos contextuales y psicosociales —como el estado mental del agresor, la vulnerabilidad psicológica de la víctima o la presencia de menores— aporta una visión más holística del riesgo y permite modelar dinámicas complejas con mayor fidelidad. Esta aproximación se alinea con las tendencias internacionales, donde la combinación de datos estructurados y señales conductuales ofrece mejoras significativas en la predicción de violencia grave, reincidencia y letalidad. Una vez integrados en un dataset unificado, estos ítems permiten entrenar sistemas capaces de anticipar no solo la probabilidad de escalada violenta, sino también la aparición de episodios graves, el riesgo de quebrantamiento de medidas o la persistencia de violencia digital incluso tras una orden de alejamiento.

Sin embargo, es necesario subrayar que la incorporación del ML en este ámbito se ha producido más tarde que en otros sectores estratégicos. Este retraso puede explicarse por múltiples factores: la fragmentación de las fuentes de datos, la falta de interoperabilidad entre instituciones, la escasez de inversión en digitalización y la dificultad inherente a manejar información extremadamente sensible. A ello se suman los dilemas éticos asociados al riesgo de sobredetección, sesgos algorítmicos o uso inapropiado de datos de víctimas. Aunque estas preocupaciones son legítimas, también han contribuido a ralentizar la adopción de herramientas que habrían podido mejorar la protección de miles de mujeres. La experiencia acumulada en los últimos años demuestra que es posible combinar innovación tecnológica y garantías éticas, siempre que exista una infraestructura de datos robusta, mecanismos estrictos de anonimización y supervisión humana informada en todo el proceso de toma de decisiones.

En cuanto a la validación de la ficha CTVD, las respuestas de profesionales y expertas reflejan un nivel de aceptación muy elevado. Entre las fortalezas destacan la cobertura integral de indicadores tecnológicos, la facilidad de uso y la necesidad evidente de contar con un instrumento que capture adecuadamente la violencia digital. Estos elementos hacen del formulario una

herramienta operativa y transferible a distintos contextos institucionales, desde cuerpos policiales hasta servicios sociales o recursos 24 horas. No obstante, también se identificaron áreas de mejora que deben guiar la siguiente iteración del diseño: definir criterios más observables que reduzcan la variabilidad interpretativa, incorporar con mayor detalle la violencia vicaria y anticipar nuevas formas de violencia digital relacionadas con inteligencia artificial, manipulación algorítmica o suplantación automatizada.

El análisis predictivo con datos sintéticos permitió explorar, en una fase preliminar, el peso relativo de los indicadores tecnológicos dentro de un modelo de riesgo. Los resultados fueron concluyentes: más del 55% del peso predictivo total se concentró en variables de control digital, confirmando que este ámbito constituye un predictor crítico de futuras agresiones y escaladas de violencia. Las tres variables con mayor capacidad discriminativa —número de mensajes controladores, persistencia de solicitudes de ubicación e intentos de acceso no autorizado— coinciden con patrones observados en investigaciones nacionales e internacionales sobre violencia digital. Estos hallazgos abren la puerta al desarrollo de sistemas de alerta temprana que permitan intervenir antes de que se produzcan episodios graves.

Para avanzar hacia una implementación real en VioGén, será imprescindible trabajar con datos reales anonimizados y bajo protocolos éticos estrictos. La comparación entre modelos entrenados con datos sintéticos y modelos entrenados con datos reales permitirá calibrar la robustez de los predictores, ajustar los pesos y evaluar el rendimiento en escenarios operativos. Este paso resulta crítico para asegurar que un sistema de predicción tecnológica no solo sea técnicamente eficaz, sino también legítimo, seguro y aceptado por los equipos profesionales que deberán integrarlo en su práctica cotidiana.

En suma, el trabajo desarrollado demuestra que la combinación de evaluación profesional, analítica avanzada y comprensión profunda de las nuevas formas de violencia digital permite avanzar hacia modelos de predicción más completos, sensibles y adaptados a la complejidad del fenómeno. La propuesta de ficha complementaria y el análisis predictivo asociado constituyen un hito en el proceso de modernización del sistema VioGén y un paso decisivo hacia la mejora de la protección de las víctimas en la era digital. Si se continúa por esta línea, España podría situarse a la vanguardia internacional en el uso ético e innovador de la tecnología para prevenir violencias graves y salvar vidas.

4 Publicaciones científicas previstas

4.1 Libro en la editorial Dykinson

El presente libro, actualmente en preparación para la editorial Dykinson, ofrece una contribución integral y actualizada al análisis del riesgo de violencia de género mediante el uso de técnicas avanzadas de *Machine Learning* (ML) y *Deep Learning* (DL). En el capítulo dedicado al **Estado del arte**, se realiza una revisión exhaustiva y sistemática de las investigaciones publicadas entre 2020 y 2025 en revistas indexadas en Q1. Este análisis permite identificar las principales líneas de evolución del campo: desde modelos predictivos aplicados a grandes bases policiales y judiciales hasta enfoques basados en lenguaje natural, análisis de redes sociales, cribado digital en entornos clínicos o sistemas híbridos que integran variables psicométricas, sociofamiliares y tecnológicas. La revisión revela, asimismo, carencias persistentes como la falta de datos multimodales, la escasa estandarización de métricas comparativas y los desafíos éticos asociados al manejo de información sensible. Este marco teórico constituye la base para contextualizar las aportaciones del presente volumen.

En el capítulo central, se presenta y valida la **Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1)**, una propuesta innovadora diseñada para complementar los formularios tradicionales de evaluación del riesgo. La CTVD introduce indicadores específicos sobre acoso digital, control tecnológico, geolocalización forzada, uso de *stalkerware* y presencia de amenazas online, dimensiones cruciales para comprender la violencia de género en la era digital. El capítulo incluye un análisis detallado de la validez del instrumento a partir de un proceso de evaluación experto que ha contado con profesionales del ámbito jurídico, sanitario, fuerzas y cuerpos de seguridad y centros de información a la mujer (CIM).

Los expertos valoraron la CTVD como una herramienta rigurosa, viable y necesaria, destacando su utilidad para identificar riesgos invisibles, mejorar la detección temprana y reforzar la toma de decisiones operativas. La triangulación de perspectivas permitió afinar los ítems, confirmar su pertinencia y garantizar la coherencia técnica y normativa. El libro, por tanto, combina una revisión sistemática del conocimiento científico con una propuesta validada que aspira a mejorar las prácticas institucionales de protección y prevención.

4.2 Artículo científico sobre un estudio experimental con ML orientado a evaluar el potencial predictivo de indicadores tecnológicos del CTVD – VPER 4.1

El presente artículo propone un estudio experimental orientado a evaluar el potencial predictivo de indicadores tecnológicos incluidos en la Ficha Complementaria de Control Tecnológico y Vigilancia Digital (CTVD – VPER 4.1) mediante algoritmos de *machine learning* (ML) supervisado. Con el fin de superar las limitaciones actuales en la disponibilidad de datos reales sobre violencia de género y garantizar la protección de víctimas, se generó un dataset sintético capaz de reproducir patrones verosímiles de comportamiento digital, emocional y situacional presentes en casos de control coercitivo y agresión. Este enfoque permitió modelar relaciones no triviales entre variables sin comprometer información sensible.

El dataset se compuso de un número amplio de registros con variables inspiradas directamente en la CTVD: frecuencia de llamadas insistentes, volumen de mensajes diarios con contenido controlador, amenazas digitales explícitas, solicitudes reiteradas de ubicación, creación de perfiles falsos, intentos de acceso no autorizado, indicios de *stalkerware*, geolocalización forzada y manipulación de dispositivos domóticos. A ello se añadieron variables contextuales como

antecedentes de violencia, impulsividad del agresor, estado emocional percibido de la víctima y presencia de menores en el hogar. Cada caso se etiquetó con un nivel sintético de riesgo —bajo, medio o alto— siguiendo una estructura probabilística basada en la intensidad acumulada de los indicadores tecnológicos.

Para el análisis predictivo se entrenaron varios modelos supervisados (árboles de decisión, *random forest*, *gradient boosting* y redes neuronales simples) utilizando validación cruzada. Los algoritmos de ensamble obtuvieron los mejores resultados, alcanzando un F1-score de 0,89, lo que evidencia una alta capacidad discriminativa incluso en un entorno simulado. El análisis de importancia de características mostró que más del 55 % del peso predictivo se concentró en variables digitales, especialmente la persistencia de solicitudes de ubicación, los intentos de acceso al dispositivo y el volumen de mensajes controladores.

Estos resultados sugieren que los indicadores tecnológicos constituyen señales tempranas especialmente útiles para sistemas de alerta automatizados. Como trabajo futuro, se propone la validación con datos reales anonimizados bajo estrictos protocolos éticos, permitiendo contrastar la robustez del modelo y evaluar su aplicabilidad en sistemas policiales como VioGén.

7 Equipo de trabajo

IP: Sonia María Valladares Rodríguez[2]:

Sonia Valladares, Profesora Permanente Laboral en la Universidad de Santiago de Compostela, es un referente en la aplicación de tecnologías emergentes al ámbito de la salud, el envejecimiento activo y la longevidad. Su labor se centra en mejorar la calidad de vida de personas mayores y colectivos vulnerables mediante herramientas digitales, inteligencia artificial y robótica. Doctora en Ingeniería Telemática por la Universidad de Vigo, su tesis se enfocó en Panoramix, una batería digital de evaluación neuropsicológica basada en juegos serios y técnicas de *machine learning*, diseñada para la detección precoz del deterioro cognitivo y validada en colaboración con entidades sociosanitarias.

Ha liderado proyectos de gran impacto social, como una prueba digital adaptada a adultos con síndrome de Down, desarrollada junto a Down Galicia y utilizada por más de 600 usuarios. Actualmente dirige el proyecto Test de Memoria Ludus (Lucus), seleccionado en la Aceleradora de Transferencia 2025, orientado a mejorar el cribado cognitivo en entornos residenciales y en proceso de validación clínica. Cuenta con participación en 14 proyectos competitivos de I+D+i y 11 contratos no competitivos, habiendo sido Investigadora Principal en iniciativas regionales y europeas, incluido DEEPINVENTHEI. Su perfil como evaluadora se refuerza con su papel como revisora del European Innovation Council en 2024 y 2025.

Ha codirigido una tesis doctoral calificada como Sobresaliente Cum Laude y es miembro de REGIDEM, además de colaborar como revisora en revistas científicas y agencias de investigación. Su producción científica comprende 20 artículos JCR, numerosas contribuciones a congresos y capítulos de libro, avalada por más de 650 citas. Su trabajo combina rigor científico y compromiso social, promoviendo soluciones tecnológicas inclusivas y humanizadas en el ámbito sociosanitario.

Francisco Javier García Polo[1]:

La línea de investigación del Dr. García se centra en garantizar la seguridad de los sistemas de Inteligencia Artificial, con especial énfasis en el desarrollo de algoritmos de *Safe Reinforcement Learning* aplicables a sistemas del mundo real como robots. Fue pionero en proponer la primera formalización y categorización de este campo dentro de la comunidad de *Reinforcement Learning*, trabajo publicado en el *Journal of Machine Learning Research* y con más de 2200 citas.

Su trayectoria científica se ha desarrollado en diversas instituciones. Se incorporó al grupo Planning and Learning Group (PLG) de la Universidad Carlos III de Madrid en 2007, donde obtuvo el doctorado en Informática y el Premio Extraordinario de Doctorado en 2013. Posteriormente trabajó en el laboratorio LIACC (Portugal), centrado en robótica real, y más tarde en el CiTIUS (Santiago de Compostela). En 2016 regresó al PLG como investigador senior y fue IP del proyecto 2016-T2/TIC-1712 del programa Atracción de Talento de la Comunidad de Madrid. Actualmente es profesor en la Universidad de Santiago de Compostela.

Ha participado en 18 proyectos de I+D (15 nacionales, 1 europeo y 2 internacionales), siendo IP o co-IP en 6 de ellos, uno con resultado en una patente comercializada. Ha colaborado con empresas como Acciona, Indra, BBVA, Repsol y JPMorgan, y ha asesorado la *spin-off* InRobics, premiada a nivel nacional.

Su producción científica incluye 22 artículos JCR (11 Q1), 6 capítulos de libro y más de 20 congresos, acumulando más de 3300 citas. Colabora con instituciones de cinco países y figuras destacadas como Manuela Veloso y Maja Matáric. Además, es editor asociado de *IEEE Robotics and Automation Letters* y miembro del comité editorial de *Machine Learning Journal*, participando activamente en comités de programa y organización de talleres internacionales.

[1] https://investigacion.usc.gal/investigadores/186092/detalle

5 Anexos

5.1 Test: CONTROL TECNOLÓGICO Y VIGILANCIA DIGITAL (CTVD) – VPER 4.1

PROPUESTA DE FICHA COMPLEMENTARIA:

"CONTROL TECNOLÓGICO Y VIGILANCIA DIGITAL (CTVD) – VPER 4.1"

(Para uso policial dentro del Sistema VioGén y especialmente indicada en intervenciones bajo Protocolo Cero)

1. DATOS BÁSICOS DEL CASO

1. Número de Caso VioGén (si existe): _____
2. Fecha de la intervención: ____ / ____ / _____
3. Intervención bajo Protocolo Cero:
    - ☐ Sí
    - ☐ No
4. Motivo de la activación:
    - ☐ Denuncia realizada por familiares
    - ☐ Llamada de terceros
    - ☐ Intervención directa por aviso de terceros
    - ☐ Otra: _____

2. INDICADORES DE CONTROL Y ACOSO TECNOLÓGICO

(Inspirados en el decálogo del Protocolo Cero y ampliados para análisis predictivo)

2.1. COMUNICACIONES DIGITALES

Marcar todos los que apliquen (y cuantificar en la medida de lo posible):

- ☐ Llamadas insistentes al móvil
  Nº aproximado en últimas 24h/72h: _____
- ☐ WhatsApp / Telegram / mensajería insistente (hostigamiento o acoso)
  Nº mensajes / día: _____
- ☐ Mensajes de control (localización, dónde estás, con quién…)
- ☐ Mensajes de amenazas directas:
    - ☐ Insultos
    - ☐ Amenazas de muerte
    - ☐ Amenazas de dañar o retirar custodia de hijos (en casos de ruptura)

    - ☐ Amenazas de suicidio del agresor
- ☐ Videollamadas no consentidas / repetitivas
- ☐ Correos electrónicos amenazantes o controladores

2.2. REDES SOCIALES

- ☐ Control a través de Instagram / Facebook / TikTok
- ☐ Acceso a cuentas de la víctima sin permiso
- ☐ Solicitud insistente de ubicación / fotos
- ☐ Publicaciones[2] que humillan, amenazan o exponen a la víctima
- ☐ Creación de perfiles falsos para vigilancia
- ☐ Comentarios hostiles en sus redes sociales

2.3. GEOLOCALIZACIÓN Y TECNOLOGÍA

- ☐ Instalación de apps de rastreo en su teléfono
- ☐ Solicitud de compartir ubicación de forma constante
- ☐ Seguimiento mediante Google Maps / WhatsApp / apps
- ☐ Manipulación de dispositivos de la víctima
- ☐ Presencia inesperada del agresor en lugares donde la víctima no lo esperaba
- ☐ Sospecha razonable de *stalkerware*[3] u otros spyware
- ☐ Dispositivos domóticos usados para control (cámaras IP, asistentes, etc.)

3. INDICADORES DE CONTEXTO Y ESCALADA (AMPLIADOS PROTOCOLO CERO)

(Basados directamente en los indicadores del formulario original - VPER 4.0)

3.1. Violencia reciente o pasada

- ☐ Episodio reciente de violencia física (con o sin lesiones)
- ☐ Agresión en zona de cuello (estrangulación / intento)
- ☐ Uso de armas (blancas, contundentes, fuego…)
- ☐ Amenazas de muerte / suicidio
- ☐ Celos extremos detectados
- ☐ Reiteración de episodios / cronificación de la violencia

[2] Montajes gráficos y creación perfiles de tipo sexual falsos.

[3] Programa oculto que alguien instala en el móvil de otra persona para vigilarla sin que se dé cuenta.

- ☐ Violencia económica (retirando acceso a recursos económicos compartidos)

3.2. Conductas del agresor

- ☐ Conductas de acoso digital o presencial
- ☐ Faltas de respeto o desafío a autoridades (policías, judicial…) (según Protocolo Cero)
- ☐ Impulsividad, alteraciones del comportamiento
- ☐ Abuso de alcohol / drogas
- ☐ Antecedentes de violencia o quebrantamientos
- ☐ Ideas o tentativas de suicidio

3.3. Estado emocional de la víctima

- ☐ Miedo expreso a que "pueda matarla"
- ☐ Depresión, ansiedad o vulnerabilidad apreciada
- ☐ Discapacidad o dificultades para expresarse
- ☐ Alta dependencia emocional o económica
- ☐ Duda sobre denunciar / negación inicial (Protocolo Cero)

3.4. Menores

- ☐ Existencia de menores
- ☐ Han presenciado hechos
- ☐ Han sido amenazados
- ☐ La víctima teme por su seguridad
- ☐ La víctima sufre amenazas continuas de pérdida de custodia o visitas

4. EVIDENCIAS DIGITALES Y DOCUMENTALES

(Información clave para entrenamiento de modelos predictivos)

- ☐ Capturas de pantalla entregadas
- ☐ Registros de llamadas
- ☐ Grabaciones de voz
- ☐ Mensajes archivados
- ☐ Fotos de daños en domicilio
- ☐ Informes médicos / partes de lesiones

- ☐ Testigos que confirman comportamientos de control

5. ESCALADO DE RIESGO TECNOLÓGICO (RTD-Score)

(Propuesta cuantitativa para el análisis predictivo)
Marcar intensidad percibida:

Indicador	**Bajo**	**Medio**	**Alto**
Control digital	☐	☐	☐
Acoso online	☐	☐	☐
Geo-control	☐	☐	☐
Amenazas	☐	☐	☐
Vulnerabilidad de la víctima	☐	☐	☐
Acceso no autorizado a dispositivos	☐	☐	☐

6. CONCLUSIÓN POLICIAL OPERATIVA

(Integrable con el formulario original - VPER 4.0)

1. Intensificación del riesgo debido a conductas de control tecnológico:
    - ☐ Sí
    - ☐ No
2. Se recomienda:
    - ☐ Incrementar nivel de riesgo provisional
    - ☐ Activar recursos asistenciales
    - ☐ Revisión urgente del caso por unidad especializada
    - ☐ Medidas de alejamiento/telemáticas
    - ☐ Seguimiento intensivo
3. Observaciones del agente que realiza el atestado:

Identificación del agente (NIP): _____