A. PROPUESTA PROYECTO DE INVESTIGACIÓN

1. TIPO DE PROYECTO:

Interno	**X**	**Grupal**	
Semilla		**Multidisciplinario**	

2. TIPO DE INVESTIGACIÓN:

Básica		**Aplicada**	**X**

3. UNIDAD EJECUTORA *(Departamento, Instituto o Estructura de Investigación):*

3.1. Departamento de Electrónica, Telecomunicaciones y Redes de Información
3.2. Departamento de Informática y Ciencias de la Computación

4. LINEA(S) DE INVESTIGACIÓN:

4.1. Seguridad y privacidad

5. TÍTULO DEL PROYECTO *(mínimo 10 palabras):*

Detección de fraude mediante análisis de tópicos y métodos de clasificación

6. RESUMEN *(máximo 200 palabras)*

El fraude involucra comúnmente prácticas ilegales realizadas principalmente en entidades corporativas, y que pueden ejecutarlas desde sus más altos directivos hasta empleados de nómina. Es además un delito penado por la ley. Existen muchas técnicas desarrolladas para detectar, analizar, y prevenir este comportamiento, siendo de las más importantes el triángulo del fraude, asociado con el modelo clásico de auditoria bancaria. El factor humano está ampliamente integrado en la auditoría de este tipo de actividades como un componente principal, además del análisis cuantitativo clásico de transacciones comerciales, que ya se están aplicando como parte de la auditoría de fraude. Este componente proporciona un valor añadido interesante porque las transacciones examinadas por el auditor pueden ser mejor diferenciadas y priorizadas.

Sin embargo, el análisis manual o tradicional de un conjunto de transacciones es limitado. El uso de tecnología de punta como el aprendizaje automático o el procesamiento de lenguaje natural podría ayudar a tomar en cuenta el comportamiento humano en el análisis y a descubrir patrones de fraude que no son evidentes.

Este proyecto de investigación propone apoyar en los conocimientos sobre la prevención y detección de fraude en estudiantes y profesionales, mediante el análisis del triángulo del fraude por lo cual se plantea las siguientes propuestas:

- Revisar el estado de arte con relación a fraude en un ámbito general.
- Plantear un modelo basado en la teoría del del triángulo del fraude orientado en su detección.

7. PALABRAS CLAVE *(4-6)*

Fraude, triangulo del fraude, comportamiento humano sospechoso, detección

8. OBJETIVOS

8.1. OBJETIVO GENERAL

Analizar los aspectos relacionados con el fraude y alternativas para detectarlo, revisando detalles como la intencionalidad, tomando en cuenta el comportamiento humano sospechoso y no sospechoso.

8.2. OBJETIVOS ESPECÍFICOS

a. Realizar la revisión de literatura sobre la detección de fraude a través del análisis del comportamiento humano aplicando técnicas de minería de datos.
b. Detectar patrones inusuales de comportamiento en un conjunto de datos mediante la teoría del triángulo del fraude.

9. HIPÓTESIS (opcional)

La teoría del triángulo del fraude puede apoyar en la toma de decisiones para contribuir en la planificación de estrategias en defensa de la seguridad de la información.

10. DETALLE DE LOS RESULTADOS ESPERADOS *(con relación a los objetivos)*

a. Elaboración de estado del arte enfocado en el análisis y detección temprana de fraude.
b. Propuesta sobre la aplicación de técnicas y análisis general para detección de fraude.

11. IMPACTO DE LA INVESTIGACIÓN (*científico, social, económico u otros)*

11.1. Impacto Social

La tecnología se ha convertido en un elemento esencial en las relaciones sociales producto de la interacción entre personas (Ciudadano-Ciudadano, C2C), personas con organizaciones (ciudadanos- negocios, C2B) y entre organizaciones (negocios-negocios (B2B). La seguridad de la información bajo este contexto es un elemento clave no solo enfocado en especialistas de seguridad sino también a la sociedad en general, por lo cual este proyecto de investigación contribuye en aportar conocimientos para que los diferentes actores, específicamente los especialistas de seguridad de las organizaciones puedan mejorar sus habilidades en el análisis y establecimiento de estrategias contra actos ilícitos como el fraude en defensa de la seguridad de la información. El proyecto también tiene la finalidad de aportar a la sociedad en la cultura de ética y moral que se debe fortalecerse a nivel de país frente a esta problemática.

11.2. Impacto Económico

Debido al crecimiento de actividades ilícitas en el entorno empresarial, más del 70% de estas ignoran el impacto del fraude en su economía. En la región, el 39% de casos implicaron pérdidas por más 170 millones de dólares debido a este problema [1]. En el ámbito empresarial y corporativo, la corrupción y los fraudes generan cada año graves afectaciones económicas en las organizaciones, lo cual revela un déficit de atención a este flagelo y que preocupa aún más ya que un alto porcentaje de ejecutivos ignoran el impacto para las organizaciones en las que trabajan. En este sentido, el proyecto pretende mitigar en gran medida estos actos delictivos, detectando conductas sospechosas en las organizaciones públicas y privadas, que, según la teoría, puedan desembocar en la materialización de un fraude corporativo. En esa línea, este proyecto podría traducirse en un beneficio económico significativo a las diferentes organizaciones en el país.

11.3. Impacto Político

En la actualidad, el desarrollo de las tecnologías de información y comunicaciones (TIC) transforman la forma en que llevamos las relaciones humanas y las estructuras sociales y políticas nacionales e internacionales, incluyendo las consideraciones de seguridad y defensa tanto en el espacio físico y virtual. En este contexto el Estado Ecuatoriano debe promover, en esta era tecnológica, la consolidación de un gobierno eficaz y transparente a través de plataformas tecnológicas, y, por el otro, desarrollar las capacidades para proteger a los ciudadanos y organizaciones público-privadas frente ataques virtuales [2].

En Ecuador se promulgaron políticas sustentables en el ámbito de la ciberseguridad, como el Acuerdo Ministerial No. 166, emitido por la Secretaría Nacional de la Administración Pública, que obliga a las instituciones públicas la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI). El Ministerio de Información y Telecomunicaciones continúa con el fortalecimiento de los aspectos de ciberseguridad a través de las políticas de manejo de incidentes y vulnerabilidades en proveedores de servicios de telecomunicaciones [3].

El proyecto pretende fortalecer las habilidades de los especialistas de seguridad de la información en la generación de estrategias en el campo de la ciberseguridad, específicamente en la lucha contra el fraude, apoyando el cumplimiento de las políticas públicas establecidas.

11.4. Impacto Científico

En el ámbito científico en los últimos años se han establecido investigaciones y conferencias referentes al combate contra el fraude, donde se ha potenciado el análisis de propuestas para fortalecer los procedimientos y respuesta frente amenazas informáticas bajo el nuevo entorno tecnológico. El presente proyecto de investigación busca promover la generación de conocimiento científico al considerar el aporte de la teoría del triángulo del fraude, para la creación de estrategias de defensa contra el fraude para protección a los intereses de las organizaciones en general.

12. ESTADO DEL ARTE, E INVESTIGACIONES PREVIAS DEL EQUIPO *(máximo tres carillas)*

Existen pocos trabajos de investigación que integren técnicas de minería de datos asociadas con la teoría del triángulo del fraude y que lo hagan mediante el análisis del comportamiento humano para identificar posibles casos de fraude. En este contexto, se encontraron los siguientes estudios en la literatura que contribuyen a este tema.

En [4] se plantea un artefacto (prototipo) en la forma de un modelo arquitectónico genérico que intenta considerar los factores del triángulo de fraude. De esta manera, además del análisis aplicado como parte de la auditoría de fraude tradicional, se toma en cuenta el factor humano, el que proporciona un valor agregado ya que las transacciones examinadas por un auditor pueden diferenciarse y priorizarse mejor. Al distinguir entre tipos de comportamiento (sospechoso y no sospechoso), es posible descubrir transacciones que son parte de un patrón difícilmente reconocible usando medios tradicionales. Al igual que el trabajo anterior, Carolyn Holton[5] propone diseñar un artefacto para detectar comunicaciones asociadas con descontento, principalmente en mensajes de correo electrónico a través de técnicas de minería de datos y el triángulo de la teoría del fraude.

Por otro lado, Mieke Jans [6] se enfoca en el fraude interno pues representa la mayoría de los casos identificados por PwC y ACFE, concentrándose principalmente en la reducción del riesgo de fraude interno mediante la combinación de la detección y prevención del fraude. Utiliza técnicas de minería de datos predictivas o técnicas de clasificación predictivas más precisas con el propósito de identificar si una observación es fraudulenta o no. En esta investigación se aplica la metodología IFR² [7] para reducir el riesgo de fraude interno, marco que utiliza la teoría del triángulo del fraude para evaluar y minimizar las oportunidades de fraude.

Vimal Kumar [8] en su trabajo analiza detalladamente acerca del fraude en el sector bancario, clasificando los tipos y definiciones de fraudes existentes. También enumera y explica las diferentes técnicas de minería de datos utilizadas por investigadores para el estudio del fraude tomando en cuenta los factores que lo causan mediante el modelo del triángulo del fraude, relacionando la presión, oportunidad y racionalización con este comportamiento. Concluye además manifestando que la prevención es un requisito indispensable en el sector bancario y las técnicas de minería de datos son fundamentales para reducir los casos de fraude.

Ravisankar [9] utiliza la teoría del triángulo del fraude para identificar las razones del incremento de actividades fraudulentas en empresas. Se apoya en técnicas inteligentes como la red neuronal de alimentación directa multicapa (MLFF), máquinas de vectores de soporte (SVM), el método grupal de manejo de datos (GMDH), programación genética (GP), regresión logística (LR) y red neuronal probabilística (PNN). Propone predecir el fraude en estados financieros sobre un conjunto de datos de 202 empresas chinas.

También se han propuesto marcos para la detección de fraude; uno de estos sugiere [10] la integración de una base de conocimientos de auditores y de una técnica en procesos de auditoria, que tiene el objetivo de ayudar a los auditores a descubrir fraudes financieros internos de manera más eficiente, aplicando técnicas de minería de datos. En [11] se propone un sistema basado en un marco de detección de fraude automatizado, utilizando agentes inteligentes, técnicas de fusión de datos y varias técnicas de minería de datos. Por otro lado, [6] plantea la ausencia de un marco metodológico para mitigar el fraude interno, y presenta un marco denominado IFR2 para la reducción del riesgo de fraude interno.

También se identificaron revisiones de técnicas de minería de datos y aprendizaje automático para la detección de fraude; entre ellas, [12] es una revisión de trabajos de investigación relacionados con los métodos de minería de datos aplicados para detección de fraude financiero (FFD). En [13] se clasifica, compara y resume métodos y técnicas de detección de fraude, [14] propone una investigación para ayudar a los contadores públicos certificados a seleccionar datos y tecnologías de minería de datos adecuadas para detectar el fraude.

Dhiya Al-Jumeily [15] investiga sistemas existentes para la detección de fraude y propone el desarrollo de un nuevo sistema que permita detectar aplicaciones potencialmente fraudulentas, garantizando que las organizaciones dispongan de una imagen clara de los solicitantes y de las aplicaciones en línea que utilizan, e intentando identificar si las personas que presentan solicitudes en línea son realmente quienes dicen ser.

Finalmente, en [16] se analiza el problema de la falta de acceso a datos financieros para la investigación del fraude, debido principalmente a políticas legales que protegen la privacidad de registro financieros de clientes. Mediante la utilización de técnicas de simulación se logra evitar las preocupaciones de privacidad en los datos reales. Esta simulación pretende recrear el comportamiento por parte de clientes ficticios simulados de una manera que no haya fuga de registros financieros privados.

13. DESCRIPCIÓN DETALLADA DEL PROYECTO, INCLUIDO METODOLOGÍA *(máximo tres carillas)*

Ante la proliferación de actos ilícitos relacionados con fraude, que suele involucrar interacciones complejas entre los defraudadores, se requieren estrategias de detección anticipada y defensa. Nuestra propuesta plantea analizar estos escenarios con la teoría del triángulo del fraude.

Usando esta teoría, el objetivo es encontrar patrones ocultos a raíz de la observación del factor humano, y caracterizar un comportamiento (“sospechoso y no sospechoso”) relacionado con cualquier actividad; esto implica identificar patrones conocidos y desconocidos. Esto requiere

analizar toda la información relacionada con el fraude, priorizando los eventos más relevantes a partir de la experiencia de un auditor.

La ocurrencia de fraude se explica mejor con la ayuda del *triángulo del fraude* de Donald R. Cressey, un destacado experto en sociología del crimen que escribió una serie de investigaciones sobre la prevención del delito, introduciendo esta idea, ilustrada en la Figura 1. Cressey investiga las razones detrás de la pregunta '¿por qué la gente comete fraude?', y determina la respuesta en los siguientes tres elementos críticos: presión, oportunidad y racionalización. La teoría de Cressey implica que los tres elementos deben estar consecutivamente presentes para provocar la intención de cometer fraude. La primera condición necesaria en el triángulo del fraude es la idea de presión percibida, relacionada con la motivación y el impulso detrás de las acciones fraudulentas de un individuo. Esta motivación suele presentarse frecuentemente en personas bajo algún tipo de tensión, principalmente financiera [17]. El segundo elemento es la oportunidad percibida, incluyendo las acciones detrás del crimen y la capacidad de cometer fraude. Finalmente, el tercer componente se relaciona con la idea de que el individuo puede racionalizar sus acciones deshonestas, haciendo que sus elecciones ilegales parezcan justificadas y aceptables [18].

Este proyecto de investigación plantea la detección de eventos de fraude en una colección de frases sobre la que se construye una herramienta de clasificación de dichas frases o conjuntos de palabras en un entorno de presión, oportunidad y justificación.

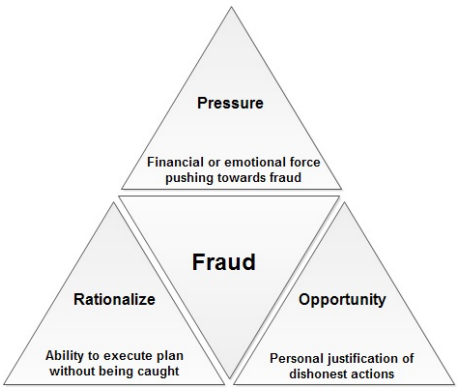

Fig. 1 Triángulo del fraude propuesto por Donald R. Cressey.

Más concretamente, el presente proyecto plantea el análisis del fraude mediante la aplicación de herramientas que, soportadas en la teoría del triángulo del fraude, permiten detectar conductas sospechosas. Además, para esto se considerarán elementos de la conducta humana que se pueden derivar, por ejemplo, de la información que un empleado genera en su estación de trabajo. Proponemos el análisis automatizado de esta información para detectar patrones de comportamiento sospechosos que podrían evidenciar una conducta fraudulenta. Esto es un aporte importante a la detección temprana de fraude en una organización frente a mecanismos de auditoria tradicionales que no consideran el factor humano para la detección.

Un importante problema durante el análisis del fraude es encontrar evidencias sobre la existencia de este comportamiento y la elección de los datos que lo comprueben. Los investigadores utilizan conjuntos de datos reales para realizar evaluación y análisis de datos, pero cuando el acceso a esta información es restringida o inexistente, los conjuntos de datos generados sintéticamente pueden proporcionar una solución a este dilema. Además, nos permite un mejor y adecuado control de las características de los datos generados [19].

Para la generación de datos, el investigador puede controlar los detalles relacionados con la creación del conjunto de datos, también puede analizar el impacto de estos aspectos en la visualización de los resultados del tema relacionado a la investigación. Un beneficio adicional

sobre el conjunto de datos sintético es la capacidad de modificar las características del conjunto de datos generado [20] [21].

Una vez obtenido el conjunto de datos, se utilizarán técnicas de minería de texto y técnicas de aprendizaje automático, incluyendo LDA (Latent Dirichlet Allocation), NMF (Non-negative Matrix Factorization) y LSA (Latent Semantic Analysis), seleccionadas porque permiten analizar grandes cantidades de texto mediante la detección de temas específicos relacionados. En nuestro ámbito, estas herramientas permitirán identificar comportamientos sospechosos relacionados con fraude. Cuando se requiere descubrir de qué se trata un conjunto de datos, resulta imposible leerlo y resumirlo manualmente; para esto, el modelado de tópicos y el agrupamiento son técnicas utilizadas que requieren un número de categorías definidas con anterioridad para extraer temas latentes de un corpus de documentos. No existen etiquetas que dirijan este proceso, por lo tanto, se asocian a aprendizaje no supervisado.

Así, mediante la utilización de métodos de aprendizaje no supervisado y métodos para el modelado de tópicos, realizaremos el estudio de la información asociada a personas. Estos métodos serán evaluados con el objetivo de identificar la mejor alternativa para el análisis de tópicos. Una vez establecido el modelo idóneo, se establecerá, mediante a un parámetro definido como coherencia, el número adecuado de tópicos que definirán el alcance del estudio y alinearlo al triángulo del fraude.

En segunda instancia, y una vez obtenida la probabilidad de que un documento pertenezca a un determinado tópico, esto servirá como entrada para realizar el análisis de detección de fraude mediante un enfoque supervisado, utilizando métodos de clasificación. Este análisis tiene el objetivo de medir la efectividad de distintos métodos para la predicción y análisis de fraude. Igualmente se compararán todos los métodos de clasificación para identificar el que ofrezca mejor rendimiento. Finalmente, se contrastarán estas alternativas y los resultados obtenidos.

References

[1] El tiempo, "El 70 % de empresas ignoran el impacto del fraude interno," [Online]. Available: https://www.eltiempo.com/economia/empresas/impacto-del-fraude-interno-en-las-empresas-de-america-latina-436626.

[2] Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada, Ciberseguridad, 2017.

[3] Ministerio Coordinador de Seguridad, "Plan de agenda de Seguridad Integral," 2014. [Online]. Available: http://instrumentosplanificacion.senplades.gob.ec/documents/20182/21649/SeguridadIntegralPlanyAgendas2014-2017.pdf/4c537326-7db2-4b7e-ae28-1bd972257a94.

[4] S. H. a. H. Z. a. T. S. a. M. H. Breitner, "Fraud Prediction and the Human Factor: An Approach to Include Human Behavior in an Automated Fraud Audit," *2012 45th Hawaii International Conference on System Sciences,* 2012.

[5] C. Holton, "Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem," *Decision Support Systems,* pp. 853-864, 2009.

[6] M. J. a. N. L. a. K. Vanhoof, "Internal fraud risk reduction: Results of a data mining case study," *International Journal of Accounting Information Systems,* pp. 17-41, 2010.

[7] M. a. L. N. a. V. K. Jans, "A framework for internal fraud risk reduction at it integrating business processes," 2009.

[8] V. a. S. B. Kumar, "A review on data mining techniques to detect insider fraud in banks," *International Journal of Advanced Research in Computer Science and Software Engineering,* pp. 370-380, 2014.

[9] P. R. a. V. R. a. G. R. R. a. I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision Support Systems,* pp. 491-500, 2011.

[10] P. K. Panigrahi, "A Framework for Discovering Internal Financial Fraud Using Analytics," *International Conference on Communication Systems and Network Technologies,* 2011.

[11] R. J. a. V. S. a. J. J. Tamilselvi, "A framework for fraud detection system in automated data mining using intelligent agent for better decision making process," *International Conference on Green Computing Communication and Electrical Engineering,* 2014.

[12] D. Y. a. X. W. a. Y. W. a. Y. L. a. C.-H. Chu, "A Review of Data Mining-Based Financial Fraud Detection Research," *International Conference on Wireless Communications, Networking and Mobile Computing,* 2007.

[13] C. a. L. V. a. S. K. a. G. R. Phua, "A comprehensive survey of data mining-based fraud detection research," 2009.

[14] S. Wang, "A Comprehensive Survey of Data Mining-Based Accounting-Fraud Detection Research," *International Conference on Intelligent Computation Technology and Automation,* 2010.

[15] D. A.-J. a. A. H. a. A. M. a. H. T. a. G. S. a. J. Lunn, "The Development of Fraud Detection Systems for Detection of Potentially Fraudulent Applications," *International Conference on Developments of E-Systems Engineering,* 2015.

[16] E. A. L.-R. a. S. Axelsson, "A review of computer simulation for fraud detection research in financial datasets," *Future Technologies Conference FTC,* 2016.

[17] G. M. a. J. Mailley, "A tale of two triangles: comparing the Fraud Triangle with criminology's Crime Triangle," *Accounting Research Journal,* vol. 28, pp. 45--58, 2015.

[18] D. A.-J. a. A. H. a. Á. M. a. H. T. a. G. S. a. J. Lunn, "The Development of Fraud Detection Systems for Detection of Potentially Fraudulent Applications," *2015 International Conference on Developments of E-Systems Engineering (DeSE),* pp. 7-13, 12 Octubre 2015.

[19] Yvan Pereira dos Santos Brito and Carlos Gustavo Resque dos Santos and Sandro de Paula Mendonca and Tiago Davi Araujo and Alexandre Abreu de Freitas and Bianchi Serique Meiguins, "A Prototype Application to Generate Synthetic Datasets for Information Visualization Evaluations," *22nd International Conference Information Visualisation,* 2018.

[20] R. R. a. B. Srinivasan, "Criteria for a Comparative Study of Visualization Techniques in Data Mining," *Intelligent Systems Design and Applications,* pp. 609-620, 2003.

[21] Fraud Explorer, "Git-Hub," [Online]. Available: https://github.com/nfsecurity/the-fraud-explorer/blob/master/Application%20Dashboard/thefraudexplorer/core /rules/fta_text_english.json. [Accessed 2018].

14. INFRAESTRUCTURA Y EQUIPOS

- *Indicar la infraestructura y equipos **disponibles** para la ejecución del proyecto, con la ubicación actual de los mismos*

Infraestructura	Equipos	
Laboratorio	**Nombre del Equipo**	**Ubicación del Equipo**
Servidor de alta prestación	Equipos informáticos	Oficina 405 Departamento de Informática y Ciencias de la Computación

15. MONTO REQUERIDO

15.1 Monto y justificación del equipo requerido
No se requiere equipo adicional al disponible.

15.2 Monto y justificación del personal requerido
No se requiere personal adicional al director y colaborador.

15.4 Monto y justificación de los investigadores invitados
No se requiere investigadores invitados.

15.5 Monto y justificación de los viajes y salidas del campo requeridos
No se requiere.

16. FONDOS ADICIONALES

- *Otros fondos de otros organismos (si los hubiere)*

No hay otros fondos.

B. DATOS INFORMATIVOS

1. INFORMACIÓN DEL DIRECTOR, CODIRECTOR, COLABORADORES Y COLABORADORES TÉCNICOS

Apellidos y nombres	No. de Cédula	HSS*	Departamento	Rol	Título de mayor nivel y mención.
Estrada Jiménez José Antonio	1714672456	8	Electrónica, Telecomunicaciones y redes de Información	Director	MSc
Sánchez Aguayo Marco Polo (Profesor a tiempo parcial – Estudiante de doctorado de la EPN)	1711881977	6	Informática y Ciencias de la Computación	Colaborador	MSc

* HSS = Horas Semana Semestre: Es el número de horas que se dedica por semana a la investigación. Este número de horas se mantiene para todo el semestre

ESCUELA POLITÉCNICA NACIONAL

Proyecto de Investigación Interno

CRONOGRAMA DE ACTIVIDADES DEL PROYECTO

Título del Proyecto:

AÑO 1

Nº	Actividad	Presupuesto de la Actividad	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6				Mes 7				Mes 8				Mes 9				Mes 10				Mes 11				Mes 12			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**Objetivo específico 1. Realizar la revisión de literatura sobre la detección de fraude a través del análisis del comportamiento humano aplicando técnicas de minería de datos.**	$ -																																														
1,1	Estudio de los mecanismos disponibles de detección de fraude basados en el triángulo del fraude	$ -																																														
1,2	Análisis de mecanismos de detección de fraude basados en aprendizaje automático.	$ -																																														
2	**Objetivo específico 2. Mediante la teoría del triángulo del fraude detectar patrones inusuales de comportamiento en un conjunto de datos.**	$ -																																														
2,1	Obtención conjunto de datos con evidencia de fraude	$ -																																														
2,2	Identificación frases relacionadas fraude mediante analisis de topicos	$ -																																														
2,3	Análisis de probabilidad de tópicos mediante metodos de clasificación	$ -																																														
2,4	Comparativa métodos de clasificación y reseultados finales	$ -																																														