UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO DE SISTEMAS

CARRERA:
INGENIERÍA DE SISTEMAS

TEMA:
“EL CIBERACOSO POR REDES SOCIALES EN EL ECUADOR”

AUTOR:
JOHN ANGELO RECALDE MONAR

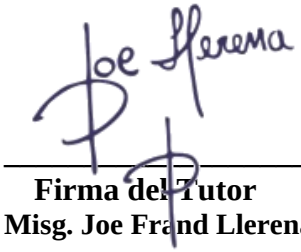
TUTOR:
Msg. JOE LLERENA IZQUIERDO

Junio 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **John Angelo Recalde Monar**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Nombre: Angelo Recalde
CI.: 0930265244



Firma del Tutor
Misg. Joe Frand Llerena Izquierdo

EL CIBERACOSO POR REDES SOCIALES EN EL ECUADOR

John Angelo Recalde Monar[1][0000-0003-1906-2204] and Joe Llerena Izquierdo[2][0000-0001-9907-7048]

[1]Universidad Politécnica Salesiana sede Guayaquil, Ecuador
jrecaldem@est.ups.edu.ec, jllerena@ups.edu.ec

Resumen. El ciberacoso se genera en distintas plataformas digitales, una de ellas son las redes sociales utilizadas por personas de todas las edades en diferentes sociedades. El problema es el incremento del acoso cibernético en redes sociales que causan toda clase de molestia en las personas y su entorno. El objetivo es determinar el estado actual del ciberacoso en redes sociales en el Ecuador para evidenciar el alcance de los efectos y consecuencias en las familias utilizando las denuncias de la Fiscalía General del Estado. Se utiliza el método deductivo y la investigación exploratoria para analizar la información suministrada por el ente regulador e identificar propuestas que detectan el ciberacoso en redes sociales. Esta investigación resultó en casos de ciberacoso en el Ecuador para su clasificación en los últimos 5 años, información obtenida del ciberacoso en redes sociales mediante técnicas estadísticas, y contrastar los resultados encontrados de ciberacoso para evidenciar falencias en la detección por los entes regulatorios. Se concluyó que las TIC's son un gran un aporte en las plataformas sociales, pero no todas garantizan una detección del ciberacoso; en Ecuador, al año 2020 la violación a la intimidad tuvo 118 denuncias con aumento del 18%, y la pornografía adolescente tuvo 2008 denuncias con aumento del 32%; la regresión lineal indica 7070 casos de ciberacoso para el año 2025 es decir 70% de crecimiento; es necesario mitigar los riesgos que existen en las redes sociales a través de algoritmos, arquitecturas, software o procesos; esta propuesta presentó un pequeño aporte para utilizar estas tecnologías.

Abstract. Cyberbullying is generated in different digital platforms, one of them is social networks used by people of all ages in different societies. The problem is the increase of cyberbullying in social networks that cause all kinds of discomfort in people and their environment. The objective is to determine the current state of cyberbullying in social networks in Ecuador to evidence the extent of the effects and consequences in families using the reports of the Attorney General's Office. The deductive method and exploratory research are used to analyze the information provided by the regulatory body and identify proposals that detect cyberbullying in social networks. This research resulted in cases of cyberbullying in Ecuador for its classification in the last 5 years, information obtained from cyberbullying in social networks through statistical techniques, and contrast the results found of cyberbullying to demonstrate shortcomings in the detection by regulatory bodies. It was concluded that ICTs are a great contribution in social platforms, but not all of them guarantee a detection of cyberbullying; in Ecuador, in 2020 the violation of privacy had 118 complaints with an increase of 18%, and adolescent pornography had 2008 complaints with an increase of 32%; the linear regression indicates 7070 cases of cyberbullying for the year 2025, that is 70%

growth; it is necessary to mitigate the risks that exist in social networks through algorithms, architectures, software or processes; this proposal presented a small contribution to use these technologies.

Keywords: Social Networks, Cyber bullying, Information Security, Cyber harassment.

1 Introducción

Conforme al avance de las Tecnologías de la Información y Comunicación (TIC) se presentan muchas facilidades y beneficios para sociedad; pero como algunas de las tecnologías tienen sus ventajas y desventajas, en este caso una desventaja es el ciberacoso que incrementa cada vez más con la ayuda de las redes sociales que muchos utilizan para mantener el anonimato con facilidad [1].

La web 2.0 ofrece las redes sociales para que las personas se conecten y expresen sus momentos a través de imágenes, texto y voz, además que se forman comunidades virtuales; la intimidación, el acoso cibernético e ingeniería social son varios de los problemas que se afrontan en los proyectos; otros inconvenientes son la gramática, terminología o jerga [2]; otras incertidumbres en estos espacios virtuales son: la intimidad, la participación intelectual, la seguridad de los consumidores, la privacidad de los datos personales, el acoso, engaño y acorralamiento cibernético.

Los inconvenientes con la gramática son más grandes que las abreviaciones, los mensajes contienen letras o caracteres para enviar insultos tales como f*ck; por lo general los textos son lingüísticamente incorrectos porque las frases son incompletas; otro inconveniente con la escritura de los mensajes es la utilización de palabras sin sentido obsceno, pero contienen una corriente sarcástica. En vista de estas formas de abreviar ciertas palabras lo usan bastante para no ser detectados con facilidad; los principales afectados son los niños y jóvenes, hoy en día casi todo joven tiene acceso a internet y un dispositivo móvil, y las redes sociales se han vuelto algo cotidiano para ellos [3]. Para mitigar esta corriente de acoso, actividad delincuente y ataques contra personalidades famosas las compañías de redes sociales como Instagram, Facebook, YouTube, Twitter y Wechat; el contenido violento en fotos y videos es suprimido por Facebook a través de inteligencia artificial; los mensajes posteados sobre odio son bloqueados o se deja de seguir en Twitter, además existen otras normas para auxiliar a una víctima abusada; el detectar el ciberacoso y noticias falsas es una tarea muy difícil porque esto genera un mal uso de cualquier plataforma [2].

El problema es el incremento del acoso cibernético en redes sociales que causan toda clase de molestia en las personas y su entorno.

Actualmente las redes sociales grandes tienen un despliegue alto en contra del ciberacoso, en sus políticas de uso y políticas de convivencia dentro de estas comunidades virtuales; en estas se promulga el compartir sin ofensas entre usuarios, contenidos aptos para todos, y usar etiquetas para definir contenido que no lo sea, como por ejemplo etiquetas restrictivas +18 o en muchas otras etiquetas Not Safe For World (NSFW).

¿Por qué es necesario un análisis para detectar el estado del ciberacoso en las redes sociales en el Ecuador?

Para generar información válida de redes sociales que permita mitigar el acoso y ayude a las autoridades a realizar el control de actividades inapropiadas basados en un modelo y procedimientos; además los resultados ayudan a detectar si hay un aumento en ciberacoso que las personas sufren, poder establecer medidas y controles más efectivos para identificar a los victimarios y recopilar evidencia para un posible proceso judicial.

La contribución es hacer respetar la privacidad y estar mejor protegido a través de la medición de textos invasivos en la red social y emisión de un informe del estado del ciberacoso en el país.

El objetivo es determinar el estado actual del ciberacoso en redes sociales en el Ecuador para evidenciar el alcance de los efectos y consecuencias en las familias utilizando las denuncias de la Fiscalía General del Estado.

2 Materiales y Métodos

Se utiliza el método deductivo y la investigación exploratoria para analizar la información suministrada por el ente regulador e identificar propuestas que detectan el ciberacoso en redes sociales.

El Ciberacoso, es abuso o intimidación por medio de la tecnología como mensajes o publicaciones, no es una amenaza física, esto desemboca en efectos negativos a nivel psicológico para las víctimas; normalmente el ciberacoso se da en menores de edad por su ingenuidad; este acoso, que es un hostigamiento o intimidación puede llevar al suicidio de la persona; aunque esto afecte también a los que están la mayor parte del tiempo en redes sociales nadie está exento del ciberacoso[4]. Algunas características son: se genera en cualquier momento, difícil de evadir, fácil de divulgar, representantes anónimos [5].

En Ecuador, existen dos artículos dentro de la Ley Orgánica de Educación Intercultural en contra del acoso, son el artículo 15 y el artículo 134; hasta el mes de septiembre de 2020 se desarrolló un estudio de una política denominada política pública por una internet segura para niños niñas y adolescentes[6]. Además a inicios del 2010 los usuarios de estas redes representaban el 9% de la población; actualmente el porcentaje de usuarios que usan las redes sociales esta entre 81% y 96% a nivel global [7].

Trabajos en ciberacoso [8], se detectó ciberbullying de redes sociales como: Twitter se revisó a través de clasificador bayesiano y Support Vector Machine; Instagram se revisó a través de Support Vector Machine; Facebook se revisó a través de Natural Language Processing; YouTube se revisó a través de clasificador Binary y Support Vector Machine; teléfonos celulares se revisó a través de lógica difusa; las páginas web se revisó a través de clasificador Naive Bayes.

La herramienta de [9] analiza las interacciones de los adolescentes y verifica señal temprana de ciberacoso, esta aplicación es utilizada por un responsable adulto, y solicita acceso por medio de inicio de sesión de Facebook del adolescente.

Método para detectar texto de ciberacoso de red Twitter, que utiliza varios algoritmos Machine Learning (SVM, Regresion logística, árbol de decisión, árbol aleatorio, gradiente, multicapa) para clasificar los tweets de la red social, los puntajes que entrega

el modelo son exactitud, precisión, recuerdo y medida F, se considera que el algoritmo que pase de 90% de precisión es más eficiente [10].

Un sistema para evadir sesiones para adultos en red social Facebook, dar seguridad al usuario contra suplantación de identidad, realizar análisis de comentarios a través Natural Language Processing , realizar análisis de imágenes a través de revisión de pixeles, y bloqueo de los mensajes o contenidos [4].

Con la utilización de dos herramientas los autores realizaron un análisis de sentimientos para detectar el acoso en Twitter, los resultados fueron sentimientos positivos y negativos; se describe un proceso de investigación, extracción de datos, y clasificación manual [11].

El sistema de [12] busca comportamientos relacionados al ciberacoso que están en foros online; utiliza algoritmos Machine Learning, para esto realizaron entrenamiento y pruebas a un conjunto de datos en lenguaje Python.

Se aplicó la predicción del ciberacoso en Instagram a través del algoritmo Machine Learning Clasificador de Regresión Logística; se analizaron texto, imagen y metadatos para obtener una predicción con precisión de 78% en un dataset de 10 características [13].

Los autores propusieron un prototipo de arquitectura para realizar auditorías sobre una red social, este proceso ayuda a determinar la existencia de ciberacoso; el algoritmo provee informe de auditoría para que un adulto o autoridad legal pueda utilizarlo[14]. El módulo para verificar acoso cibernético en idioma árabe en la red Twitter a través de una API, este programa para procesar los mensajes realiza un filtrado, extrae las palabras claves, asigna un peso para encontrar el supuesto abuso; está dirigido a padres y es detector en línea [15].

Aplica minería de datos a los datos extraídos de redes sociales, los parámetros son palabras claves, medidas y sentimientos; después de encontrar el acoso realiza una validación/evaluación de los mensajes; el proceso tiene precisión del 79% [16].

Obtención de información.

Se solicitó información a la Fiscalía General del Estado sobre ciberacoso desde el año 2016 al 2020, basados en el Artículo 18 de la Republica del Ecuador (acceso a la información de entidades públicas), el Artículo 1 de la Ley Orgánica de Transparencia y Acceso a la Información Pública (Apertura de publicidad), y del Artículo 472 del Código Orgánico Integral Penal (restricciones en la circulación de información); los parámetros entregados a la Fiscalía fueron:

- Periodo inicio y fin de análisis del pedido (día, mes, año): 01 de enero del 2016 al 31 de diciembre del 2020.
- Nivel de desagregación geográfica: Por Provincia.
- Artículo o tipo penal del Código Orgánico Integral Penal o del Código Penal: Art. 178 y 103.

Se tabularon los datos entregados por la Fiscalía para lograr los objetivos propuestos que se presentan en los resultados de este documento.

3 Resultados

3.1 Casos de ciberacoso en el Ecuador para su clasificación en los últimos 5 años

Desde 2016 la 2020 existen dos tipos de ciberacoso el primer caso es “Violación a la intimidad” y el segundo caso es “Pornografía con utilización de niñas, niños o adolescentes”; en el año 2016 el primer caso fueron 100 denuncias, el segundo caso fueron 1523 denuncias; al año 2020 el primer caso fueron 118 denuncias, el segundo caso fueron 2008 denuncias; es decir existe 18% y 32% en aumento de denuncias en cada caso respectivamente; la tendencia es al alza para ambos casos, pero es más pronunciada en el segundo caso (Fig. 1).

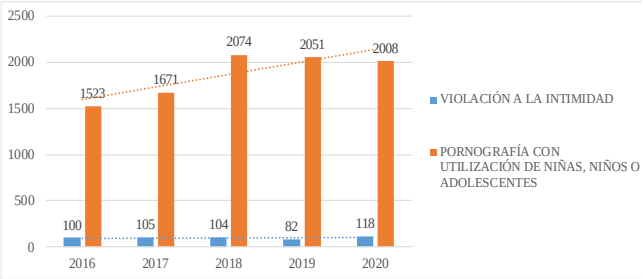


Fig. 1. Clasificación del ciberacoso.

En los últimos cinco años de un total de 9836 denuncias de ciberacoso; la pornografía es mayor cada año, a tal punto que ocupa 95% del ciberacoso, la violación ocupa el 5% del ciberacoso; es decir este delito es mayor hacia menores de 18 años (Fig. 2).

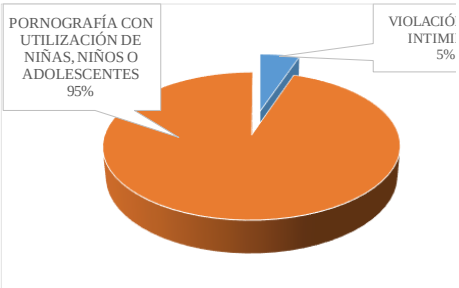


Fig. 2. Delitos por Ciberacoso.

3.2 Información obtenida del ciberacoso en redes sociales mediante técnicas estadísticas

A nivel de Ecuador, la provincia Guayas tiene la mayor cantidad de denuncias por ciberacoso 3027, desde el año 2016 al 2020 fueron 532, 577, 697, 602 y 609 por cada año respectivamente; la provincia Pichincha es la segunda con mayor cantidad denuncias 2154, desde el año 2016 al 2020 fueron 369, 395, 474, 462 y 454 por cada año respectivamente; la provincia Galápagos tiene la menor cantidad con 28 denuncias; se propuso el gráfico en Columnas Apiladas para mostrar las partes del total, los segmentos cambian al transcurrir el tiempo (Fig. 3).

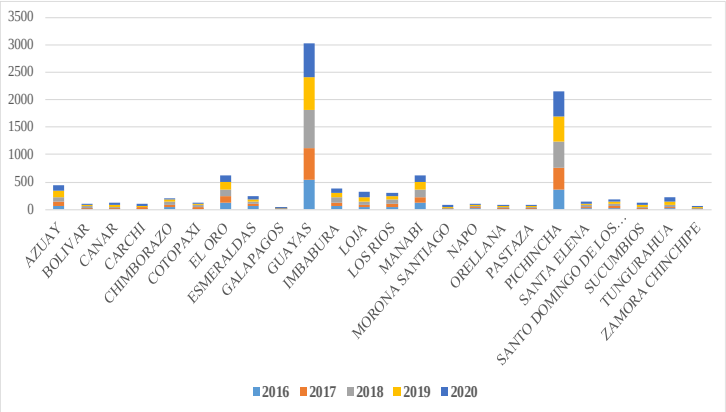


Fig. 3. Ciberacoso por provincias del Ecuador.

Los porcentajes por provincia representa los valores de las denuncias proporcionales a la frecuencia relativa entre el 2016 y 2020; Guayas contiene 31%, Pichincha 22%, Oro y Manabí contienen 6%; Azuay e Imbabura contiene 4% (Fig. 4).

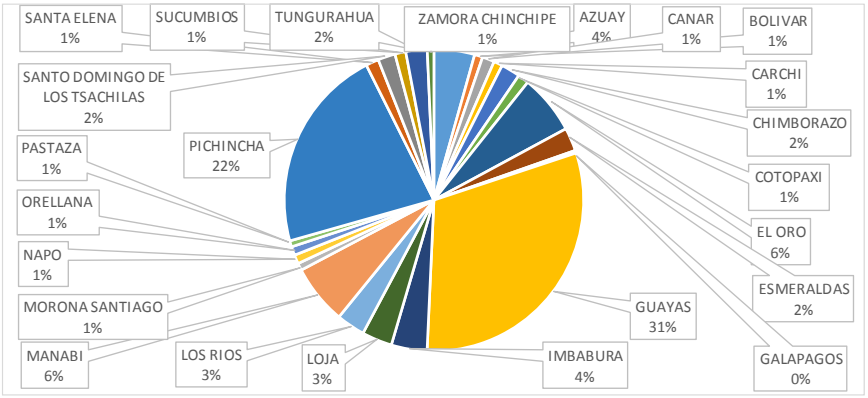


Fig. 4. Distribución del ciberacoso.

Se aplicó el método de Regresión Lineal para proyectar las denuncias por ciberacoso desde el año 2021 al 2025; en el año 2021 se proyectan 4154 denuncias, es decir un incremento del 17.55% respecto al año 2020; en el año 2025 se proyectan 7070 denuncias, es decir un incremento del 10.31% respecto al año 2024; en este periodo de tiempo 2021-2025 hay un incremento promedio del 13.45% anual. En la Fig. 5 la línea X son los años, la línea Y son las cantidades de denuncias que están representadas en las barras azules; la línea punteada color rojo es la tendencia.

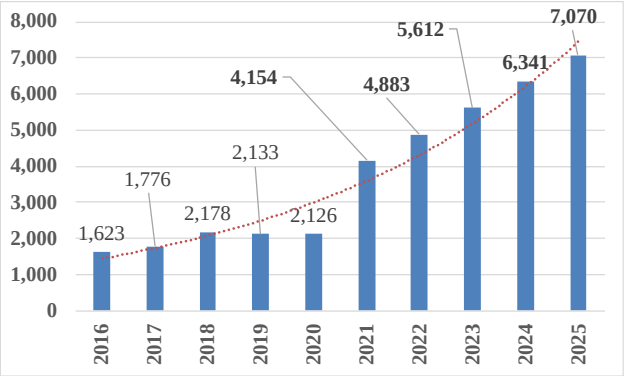


Fig. 5. Proyección lineal.

3.3 Contrastar los resultados encontrados de ciberacoso para evidenciar falencias en la detección por los entes regulatorios

Se evidenció un incremento en las denuncias de ciberacoso desde el año 2016 al 2020, y en la proyección desde el año 2021 al 2025 la tendencia sigue en alza; ante esto se presentan varias alternativas tecnológicas para detectar ciberacoso en las redes sociales y son útiles en evitar/disminuir falencias en la detección de ciberacoso para los entes regulatorios; son herramientas probadas de manera científica, es decir referencias de primer nivel. La tabla 1 presenta las alternativas que utilizan distintas tecnologías y distintos alcances para una revisión de red social.

Table 1. Alternativas tecnológicas.

Ref	Propuesta tecnológica	Alcance	Red social u otros
[4]	Análisis de comentarios a través Natural Language Processing	Texto	Facebook
[8]	Búsqueda a través de Clasificador bayesiano y Support Vector Machine; Natural Language Processing, Clasificador Binary, lógica difusa	Texto e imagen	Twitter, Instagram, Facebook, YouTube, teléfonos celulares, páginas web
[9]	Módulo de aprendizaje por niveles de riesgo	Texto	Facebook

[10]	Calsificar mensajes a través de Support Vector Machine, Regresion logística, árbol de decisión, árbol aleatorio, gradiente, multicapa	Texto	Twitter
[11]	Análisis de sentimientos a través de minería de datos con Sentimentl y Mr Tuit	Texto	Twitter
[12]	Busca comportamientos con algoritmos Machine Learning: Naive Bayes, Logistics Regression y Stochastics Gradient Descent	Texto	Foros online
[13]	Predicción del ciberacoso a través de Learning Clasificador de Regresión Logística	Texto, imagen y metadatos	Instagram
[14]	Prototipo de arquitectura realizar auditorías sobre una red social	Texto	Red social
[15]	Procesar los mensajes en tiempo real a través de módulo de refinamiento y módulo de identificación	Texto	Twitter
[16]	Clasificación de datos a través de minería de datos	Texto	Facebook, twitter

La base legal para solicitar información a la Fiscalía General del Estado sobre ciberacoso fue el Art. 18 de la Republica del Ecuador, el Art. 1 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, y el Art. 472 del COIP.

Esta investigación está en base a datos suministrados por la Fiscalía General, se utilizaron en el primer resultado para clasificar los casos de ciberacoso en el Ecuador, y en el segundo resultado para realizar estadísticas y proyecciones; esa tendencia de casos es un impulso para dar a conocer propuestas tecnológicas que ayuden a minimizar las posibles falencias en la detección de ciberacoso por parte de los entes regulatorios.

Se recomienda que en el conjunto de tecnologías que se utilizaron, no está considerado tiempos de implementación, ni infraestructura, ni personal técnico, ni costos en dinero; para conocer más falencias es necesario la vinculación de la universidad con los entes regulatorios en las áreas administrativas, legales, económicas e informática para realizar un estudio interdisciplinario a través de metodologías científicas.

La consecuencia teórica de esta propuesta es el inicio para probar o utilizar propuestas de tecnológicas del área científica en el área legal, los resultados obtenidos por las herramientas tecnológicas pueden servir como indicios/pruebas en un juicio.

4 Conclusiones

Se concluyó que las TIC’s son un gran un aporte en las plataformas sociales, pero no todas garantizan una detección del ciberacoso; en Ecuador, al año 2020 la violación a la intimidad tuvo 118 denuncias con aumento del 18%, y la pornografía adolescente tuvo 2008 denuncias con aumento del 32%; la regresión lineal indica 7070 casos de ciberacoso para el año 2025 es decir 70% de crecimiento; es necesario mitigar los riesgos que existen en las redes sociales a través de algoritmos, arquitecturas, software o procesos; esta propuesta presentó un pequeño aporte para utilizar estas tecnologías.

Es un desafío la mejora en detectar la intimidación para prevenir el ciberacoso, el aviso con alertas tempranas dirigidas a padres o autoridades civiles/legales; la

tecnología de prevención debe ser modelada de acuerdo con la red social para tener más confianza en publicaciones positivas y negar las negativas.

Las herramientas presentadas como alternativas realizan extracción sobre texto e imágenes, no solo por redes sociales se presenta el ciberacoso; por ello la seguridad y la privacidad deben aumentar en las distintas plataformas.

Agradecimientos

Fiscalía General del Estado Ecuatoriano.

Referencias

1. Rivadulla López, J.C., Rodríguez Correa, M.: Ciberacoso escolar: experiencias y propuestas de jóvenes universitarios. RIED. Rev. Iberoam. Educ. a Distancia. 22, 179 (2019). https://doi.org/10.5944/ried.22.2.23541
2. Al-Garadi, M.A., Hussain, M.R., Khan, N., Murtaza, G., Nweke, H.F., Ali, I., Mujtaba, G., Chiroma, H., Khattak, H.A., Gani, A.: Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. IEEE Access. 7, 70701–70718 (2019). https://doi.org/10.1109/ACCESS.2019.2918354
3. Toapanta Toapanta, S.M., Alfredo Espinoza Carpio, J., Mafla Gallegos, L.E.: An Approach to Cybersecurity, Cyberbullying in Social Networks and Information Security in Public Organizations during a Pandemic: Study case COVID-19 Ecuador. 2020 Congr. Int. Innov. y Tendencias en Ing. CONIITI 2020 - Conf. Proc. (2020). https://doi.org/10.1109/CONIITI51147.2020.9240375
4. Upadhyay, A., Chaudhari, A., Arunesh, Ghale, S., Pawar, S.S.: Detection and prevention measures for cyberbullying and online grooming. Proc. Int. Conf. Inven. Syst. Control. ICISC 2017. 4–7 (2017). https://doi.org/10.1109/ICISC.2017.8068605
5. Qonitatulhaq, S., Astin, N., Sarinastiti, W.: Creative Media for Cyberbullying Education. IES 2019 - Int. Electron. Symp. Role Techno-Intelligence Creat. an Open Energy Syst. Towar. Energy Democr. Proc. 622–627 (2019). https://doi.org/10.1109/ELECSYM.2019.8901646
6. NACIONAL, R.D.E.A.: Codigo Organico Integral Penal. Repub. DEL ECUADOR Asam. Nac. 268 (2018)
7. Intergeneracional, C.N. para la I.: Política pública por una internet segura para niños , niñas y adolescentes. 64 (2020)
8. Krithika, V., Priya, V.: A Detailed Survey on Cyberbullying in Social Networks. Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020. 1–10 (2020). https://doi.org/10.1109/ic-ETITE47903.2020.031
9. Silva, Y.N., Rich, C., Hall, D.: BullyBlocker: Towards the identification of cyberbullying in social networking sites. Proc. 2016 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2016. 1377–1379 (2016). https://doi.org/10.1109/ASONAM.2016.7752420

10. Zhang, J., Otomo, T., Li, L., Nakajima, S.: Cyberbullying Detection on Twitter using Multiple Textual Features. 2019 IEEE 10th Int. Conf. Aware. Sci. Technol. iCAST 2019 - Proc. (2019). https://doi.org/10.1109/ICAwST.2019.8923186
11. Tapia, F., Aguinaga, C.: Detection of Behavior Patterns through Social Networks like Twitter, using Data Mining techniques as a method to detect Cyberbullying. 111–118 (2018)
12. Pawar, R., Raje, R.R.: Multilingual cyberbullying detection system. IEEE Int. Conf. Electro Inf. Technol. 2019-May, 040–044 (2019). https://doi.org/10.1109/EIT.2019.8833846
13. Hosseinmardi, H., Rafiq, R.I., Han, R., Lv, Q., Mishra, S.: Prediction of cyberbullying incidents in a media-based social network. Proc. 2016 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2016. 186–192 (2016). https://doi.org/10.1109/ASONAM.2016.7752233
14. Toapanta Toapanta, S.M., Recalde Monar, J.A., Mafla Gallegos, L.E.: Prototype to Perform Audit in Social Networks to Determine Cyberbullying. In: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). pp. 145–153. IEEE (2020)
15. Mouheb, D., Abushamleh, M.H., Abushamleh, M.H., Aghbari, Z. Al, Kamel, I.: Real-time detection of cyberbullying in Arabic twitter streams. 2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work. (2019). https://doi.org/10.1109/NTMS.2019.8763808
16. Ting, I.H., Liou, W.S., Liberona, D., Wang, S.L., Bermudez, G.M.T.: Towards the detection of cyberbullying based on social network mining techniques. Proc. 4th Int. Conf. Behav. Econ. Socio-Cultural Comput. BESC 2017. 2018-January, 1–2 (2017). https://doi.org/10.1109/BESC.2017.8256403