Universidad Militar Nueva Granada | 2021

VI Congreso Internacional de Administración de la Seguridad y Salud en el Trabajo. Gestión del riesgo: una visión global e integral

I Encuentro de semilleros de investigación en Administración del Riesgo, Seguridad y Salud en el Trabajo

Universidad Militar Nueva Granada

Editorial Neogranadina

VI Congreso Internacional de Administración de la Seguridad y Salud en el Trabajo. Gestión del riesgo: una visión global e integral

Primera edición, 2021

Cómo citar:
UMNG. (2021). *VI Congreso Internacional de Administración de la Seguridad y Salud en el Trabajo. Gestión del riesgo: una visión global e integral*. Editorial Neogranadina.
DOI: https://doi.org/10.18359/litgris.6278

DOI: https://doi.org/10.18359/litgris.6278

Universidad Militar Nueva Granada
Sede Campus, edificio de posgrados, primer piso
Kilómetro 2, vía Cajicá-Zipaquirá, costado oriental
Teléfono: 650 00 00 Ext. 3092
editorial.neogranadina@unimilitar.edu.co

www.umng.edu.co

VI Congreso Internacional de Administración de la Seguridad y Salud en el Trabajo. Gestión del riesgo: una visión global e integral

I Encuentro de semilleros de investigación en Administración del Riesgo, Seguridad y Salud en el Trabajo

Facultad de Relaciones Internacionales, Estrategia y Seguridad
Programa de Administración de la Seguridad y Salud Ocupacional

CONTENIDO

Preliminares

Presentación

El *VI Congreso Internacional de la Administración de la Seguridad y Salud en el Trabajo. Gestión del riesgo: una visión global e integral* propone un espacio de discusión propicio para abordar diversos temas de actualidad referentes a la administración del riesgo, la seguridad privada y la seguridad y salud en el trabajo con enfoque integral. Dentro de estos, se contemplan los siguientes ejes temáticos:

- **Administración:** *Enterprise Risk Management*-ERM.
- **Seguridad Privada:** riesgos derivados de la intencionalidad humana.
- **Salud en el Trabajo:** gestión de la seguridad y salud en el trabajo.

Justificación

En concordancia con los Objetivos de Desarrollo Sostenible (ODS), Colombia debe realizar grandes esfuerzos en temas relacionados al fin de la pobreza; la salud y bienestar; la educación de calidad; el trabajo decente; el crecimiento económico; la producción y consumo responsables; las ciudades y comunidades sostenibles, entre otros. En línea con dichos objetivos, el *VI Congreso de la Administración de la Seguridad y Salud en el Trabajo* propende por el aporte a la empresa, la comunidad y la academia al orientar sus áreas de investigación a las áreas académicas propias de la formación profesional.

Como estipula el Ministerio de Cultura (2018), el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) consiste en el desarrollo de un proceso lógico y por

etapas basado en la mejora continua. Este incluye la política, organización, planificación, aplicación, evaluación, auditoría y acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo. La gestión de la Seguridad y Salud en el Trabajo (SST) tiene como propósito la estructuración de la acción conjunta entre el empleador y sus trabajadores en la aplicación de las medidas de SST a través del mejoramiento continuo de las condiciones y el medio ambiente laboral, así como del control eficaz de los peligros y riesgos en el lugar de trabajo. Este sistema aborda la prevención de los accidentes de trabajo y enfermedades laborales, y la protección y promoción de la salud de los trabajadores a través de la implementación de un método lógico llevado a cabo por etapas, cuyos principios se basan en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar). El desarrollo articulado de estos elementos permite cumplir con los propósitos del SG-SST.

Por su parte, el Instituto Nacional de Contadores Públicos (2018) establece que el *Enterprise Risk Management* (ERM) o Gestión de Riesgos Empresariales no es una función, cargo o departamento. Por el contrario, se trata del conjunto de hábitos, capacidades y prácticas propuestas para administrar efectivamente el riesgo que rodea a una compañía. Es decir, es una herramienta para identificar, administrar y mitigar los riesgos en todas las organizaciones, indistintamente de la forma en la que cumplan sus metas con respecto al cambio. Entre

los principales logros de su implementación en una organización se resalta el incremento del rango de oportunidades, la identificación y administración integral del riesgo, el incremento en los resultados positivos y las ventajas de la empresa; con la consecuente reducción de consecuencias negativas de los riesgos al permitir traducirlos en oportunidades de mejora.

En relación con los "riesgos derivados de la intencionalidad humana", se puede afirmar que la seguridad es un concepto de vital importancia dentro de las sociedades contemporáneas. El campo de acción de la seguridad se ha vuelto tan amplio que posee una naturaleza pluridimensional. Está conectado con las instituciones jurídicas, políticas, económicas, policiales o asistenciales conformando así un orden que demanda un nuevo tipo de sociedad.

Como sociedad, estamos enfrentados a continuas transformaciones que implican formas de riesgo que se apartan de las existentes en épocas pasadas. Por esta razón, existe la necesidad de imponer un nuevo modelo de seguridad capaz de enfrentar riesgos no limitados espacial, temporal o socialmente. Abriendo así las posibilidades de que el concepto de seguridad integral, hegemónicamente ligado al Estado y al ejercicio de la Defensa Nacional, se amplíe hacia nuevos espacios como el económico, social, ecológico y/o tecnológico.

Lo anterior, lleva a que este nuevo evento de la Facultad de Relaciones Internacionales, Estrategia y Seguridad contara con la participación de conferencistas,

nacionales e internacionales, expertos en temas relacionados con la gestión de riesgos. Quienes, a partir de su experticia, formularon alternativas para afrontar los retos que emergen de las problemáticas planteadas para abrir el escenario a las aportaciones de investigadores, docentes y estudiantes.

En el congreso se contemplaron dos formas de participación:

Ponencia: presentación de una propuesta aceptada por el comité del Congreso que puede ser expuesta por uno o más autores como forma de divulgación de resultados o avances de:

1. Pasantías o experiencias exitosas en gestión organizacional.
2. Proyectos de Iniciación Científica (PIC).
3. Proyectos de investigación.
4. Semilleros de investigación.

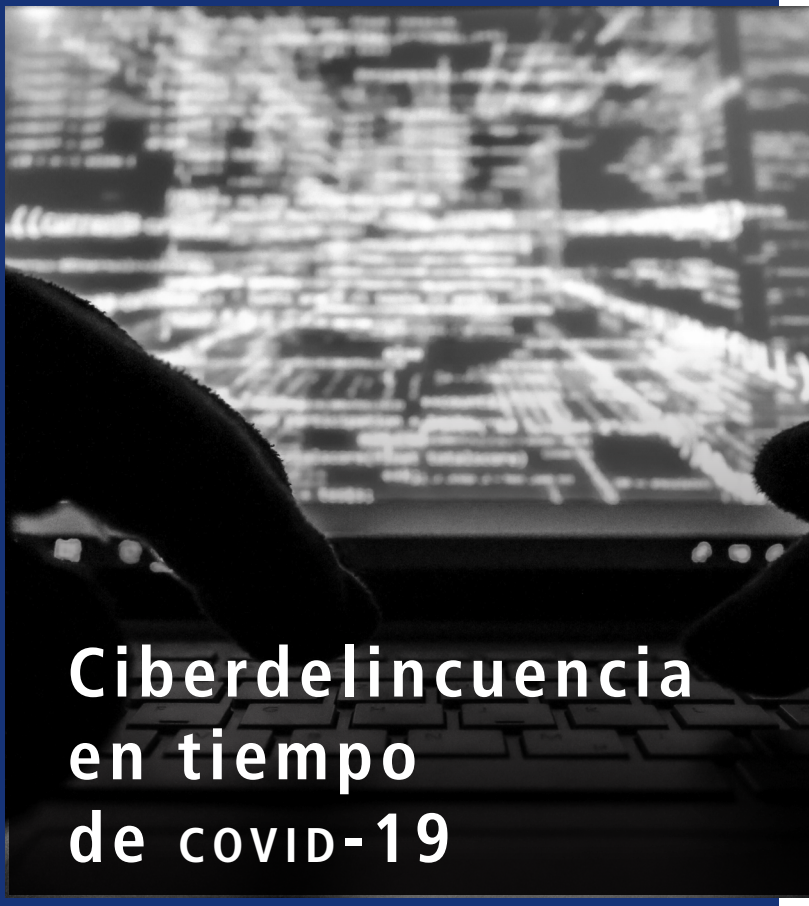
Poster: es una representación gráfica ampliada que contiene un título, el nombre de los autores, texto y figuras relacionadas con propuestas, avances y resultados de:

1. Pasantías o experiencias exitosas en gestión organizacional.
2. Proyectos de Iniciación Científica (PIC).
3. Proyectos de investigación.
4. Semilleros de investigación.

Declaración de compromiso ético

El congreso realiza la publicación de las memorias en medio digital e incluye a quienes se les haya aprobado su participación y, de forma voluntaria, deseen incluir su propuesta en las memorias. Todas las propuestas postuladas para este evento son originales e inéditas.

Cordialmente,
Comité organizador



Ciberdelincuencia en tiempo de COVID-19

Erika Cuastumal Benavides[a] · Andrea González Galeano[b]

a Universidad Militar Nueva Granada. Bogotá, Colombia. Correo electrónico: u0801230@unimilitar.edu.co
b Universidad Militar Nueva Granada. Bogotá, Colombia. Correo electrónico: u0801224@unimilitar.edu.co

Resumen: En tiempos de COVID-19, la ciberdelincuencia ha sido una de las grandes problemáticas para los colombianos. Esta, encaminada a atentar contra la integridad y la disponibilidad de los sistemas informáticos, afecta los datos sensibles de los individuos. Según estadísticas de la Policía Nacional de Colombia, durante el año 2020 los incidentes más representativos, dentro del periodo de marzo a septiembre, son: carta nigeriana, estafa, *fake news, malware, phishing, skimming, smishing y vishing*. Cada una de estas modalidades afecta directamente a los ciudadanos. De acuerdo con estos datos, es importante dar a conocer cuáles son los principales medios para cometer o perpetuar estos actos.

Las *fake news*, son cadenas masivas de noticias falsas que se difunden por diferentes

plataformas digitales; el phishing es spam a través de correos falsos; el *skimming* se refiere al robo de información de tarjetas de crédito por medios digitales; la estafa se da a través de la compra-venta por Internet; la carta nigeriana sucede por medio de correos electrónicos con incentivos monetarios atractivos; *malware* son amenazas informáticas o softwares maliciosos, el *smishing* se da con engaños a través de mensajes de texto; y, por último, *vishing* se utiliza para referirse a engaños a través de llamadas telefónicas.

No obstante, existen contramedidas para mitigar y minimizar estos ataques. Dentro de estas, es recomendable ser cuidadoso con mensajes, llamadas, contenidos de correos electrónicos, descargas de fuentes desconocidas de Internet, introducción de información personal en páginas web y acceso a redes wifi públicas. Asimismo, es recomendable actualizar el software de los dispositivos cada vez que estos lo requieran y emplear contraseñas de seguridad exclusivas para aumentar la protección de las redes que se utilizan. Todas estas medidas se encaminan a salvaguardar la información sensible dentro de los dispositivos electrónicos de los ciudadanos.

Palabras claves: ataques, ciberdelincuencia, COVID-19, contramedidas, seguridad informática.

Poster

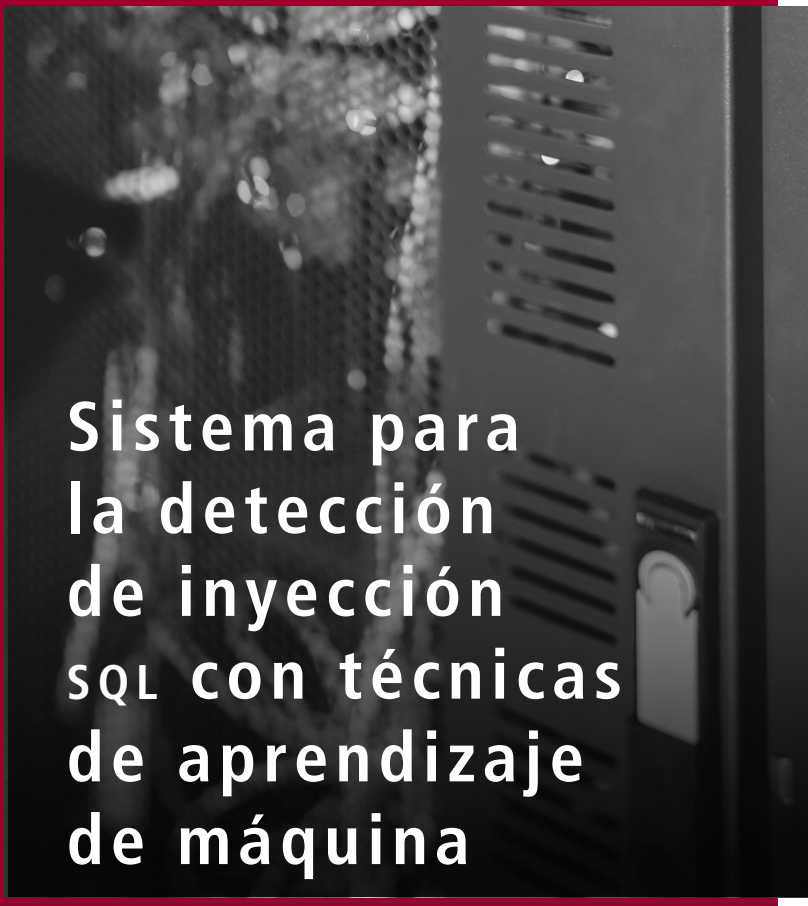

CIBERDELINCUENCIA EN TIEMPOS DE COVID-19
2020
01
CIBERDELINCENCIA
Esta ha sido una de las grandes problemáticas para los colombianos.
02
INCIDENTES MARZO-SEPTIEMBRE 2020
Fake News.
Phishing.
Skimming.
Estafa.
Carta Nigeriana.
Malware.
Smishing.
Vishing.


FAKE NEWS
03
1. FAKE NEWS: cadenas masivas de noticias falsas por diferentes plataformas digitales.
2. PHISIHING: spam a través de correos falsos.
3. SKIMMING: robo de información por medios digitales de tarjetas de crédito.
04
4. ESTAFA: compra y/o venta por internet.
5. CARTA NIGERIANA: correos electrónicos con incentivos monetarios atractivos.
6. MALWARE: amenazas informáticas o software malicioso.
2012
1040
Malware
control
05
1 new message received
7. SMISHING: engaños a través de mensajes de texto
8. VISHING: engaños a través de llamadas telefónicas.

Fuente: elaboración propia.

Referencias

Policía Nacional de Colombia. (2020, 4 de octubre). Centro Cibernético Policial. https://caivirtual.policia.gov.co/



Sistema para la detección de inyección SQL con técnicas de aprendizaje de máquina

Cristian Eduardo Carmona Carmona[a] ·
Misael Fernando Perilla Benítez[b]

a Universidad de Cundinamarca. Chía, Colombia. Correo electrónico: ccarmona@ucundinamarca.edu.co
b Universidad de Cundinamarca. Chía, Colombia. Correo electrónico: mperilla@ucundinamarca.edu.co

Resumen: Los ataques de inyección SQL son considerados como la mayor amenaza para las aplicaciones web de acuerdo a los reportes de entidades como OWASP o SANS. Este tipo de ataque se ha mantenido en el primer puesto entre los riesgos más críticos en aplicaciones web a nivel mundial desde el año 2010. Año desde el que, mediante la inserción de consultas con comandos de SQL en ubicaciones como campos de texto en aplicaciones y barra de direcciones en navegadores, estos logran ser ejecutados por el motor de la base de datos. Como consecuencia, se compromete la integridad, disponibilidad y confidencialidad de información sensible, dando al atacante la capacidad de robar, modificar, insertar y/o borrar los datos almacenados en la base de datos.

También, da la posibilidad de ejecutar aplicaciones con permisos del administrador de manera ilegítima.

La presente investigación, parte de la urgencia por detectar potenciales eventos directos sobre inyección de consultas SQL mediante el uso de métodos de aprendizaje de máquina. Las muestras tomadas para la construcción del conjunto de datos se dividen en dos categorías; la primera reúne las cadenas de texto comunes (como nombres de campos y tablas); y la segunda es el grupo de cadenas de textos propias de la sintaxis del lenguaje de consultas cuyo contenido corresponda a una declaración SQL. Posteriormente, estos datos se sometieron a un proceso de limpieza, extracción de características y etiquetado para ser usados en el entrenamiento de los modelos, los cuales son de clasificación dicotómica. El objetivo era analizar cuál de estos modelos arroja mejores resultados acordes al objetivo final de la investigación.

Una vez realizada la evaluación de los modelos (curvas ROC, matriz de confusión y validación cruzada), se comprobó que el modelo Naïve-Bayes presenta una exactitud del 97.7% frente a SVM, *Random Forest* y Regresión Logística.

Palabras claves: clasificación, detección, inyección, *Machine Learning*, SQL.

Introducción

Los ataques de inyección SQL son ataques dirigidos a aplicaciones de todo tipo donde se utilizan conexiones a bases de datos tipo SQL. En estos, se ingresa un código para tratar de acceder, leer, modificar y/o eliminar registros. Este mecanismo de ataque es "considerado como la mayor amenaza para aplicaciones web al ser comparado con otros tipos de ataques informáticos" (Varshney & Ujjwal, 2019, p. 2). Según la OWASP *(Open Web Application Security Project)*, organización sin ánimo de lucro que busca combatir las ciberamenazas, la inyección SQL se ha mantenido en el primer puesto de los diez riesgos más críticos para aplicaciones web a nivel mundial desde el año 2010. Para esta forma de ataques, se utilizan consultas (*queries*) que contienen códigos en lenguaje SQL *(Structured Query*

Language), tautologías lógicas, procesos almacenados, inyección SQL ciega, desbordamiento de memoria, etc., en campos de texto y barra de direcciones (barra de URLS). El objetivo de estos comandos es "ser ejecutados en la base de datos de la aplicación comprometida y, como consecuencia, el atacante logra tener acceso a información sensible almacenada en la misma" (Wang & Li, 2012, p. 1). Lo anterior, permite el acceso, robo, alteración y/o eliminación de información sensible o crítica de los usuarios como claves de acceso, datos personales, información médica y demás.

El software, actualmente, puede ser utilizado para ayudar a desarrollar procesos en casi toda actividad humana. Automatizando o agilizando procesos mecánicos, almacenando y/o gestionando diferentes tipos de información, permitiendo la toma de decisiones basándose en el análisis en tiempo real de los datos disponibles, entre otros. Esto ha propiciado un amplio abanico de nuevos tipos de sistemas informáticos adaptados a múltiples propósitos. Como ejemplo, existen las redes sociales, aplicaciones web, mensajería electrónica, etc., que, de manera independiente y diferente, pueden ser usados para actividades como la atención al cliente de manera remota o la venta de productos. Pero, la gran mayoría de estos usos requieren de una base de datos donde toda la información sea almacenada. La cual es la principal motivación de los ciberatacantes para perpetrar sus actos.

Es común que toda la información se centre en una base de datos donde reposa información personal del talento humano, clientes, colaboradores, organizaciones e incluso estados enteros. Y donde, dependiendo del tamaño de la organización, es habitual que toda la información repose sin los mecanismos de protección adecuados. Pues, a mayor criticidad de los datos, más herramientas y técnicas de protección se deben implementar.

La presente investigación, parte de la necesidad de detección de posibles incidentes de seguridad relacionados con el ataque de inyección de consultas SQL que muchas organizaciones tienen. Utilizando métodos con un alto nivel de efectividad en el descubrimiento de estos ataques, esta propuesta de solución trata de responder a la problemática implementando tecnologías de vanguardia, como la inteligencia artificial, donde este tipo de ataques maduran y evolucionan. Lo anterior, hace que se requieran soluciones de mayor complejidad para detectar dichas consultas maliciosas y sustituir los sistemas estáticos, cada vez menos eficientes, generando un sistema más robusto para detectar este tipo de anomalías.

Desarrollo

Para el desarrollo de este proyecto de corte mixto, se estableció el uso de la metodología de descubrimiento de conocimiento en bases de datos (KDD - *Knowledge Discovery in Databases*) siendo adaptada a las necesidades propias de la clasificación de los modelos de aprendizaje de máquina (*Machine Learning*) que se usan para la clasificación de posibles casos de ataques informáticos según la literatura consultada. Autores como Narudin *et al.*, han demostrado que los modelos bayesianos y *Random* Forest son muy eficientes en la detección de *malware* en dispositivos móviles, los cuales están en un escenario más hostil que otros tipos de dispositivos (2016). Mientras que, los modelos SVM y ANN (*Artificial Neural Networks*) son altamente efectivos en la detección de intrusos (Suleiman & Issac, 2018).

La KDD es una metodología más enfocada en la minería de datos y el *big data*, pues establece un proceso automático de descubrimiento y análisis de información partiendo de una base de datos dispersa. Sin embargo, varios de sus procesos y actividades comparten similitud con los que se proponen para la recolección, preparación y procesamiento de datos en el desarrollo y entrenamiento de modelos de *Machine Learning*. De acuerdo con Timarán Pereira *et al.,* "el proceso consiste en extraer patrones en forma de reglas o funciones, a partir de los datos, para que el usuario los analice" (2016, p. 101).

El método en este proyecto implica el preprocesar, hacer minería y presentar los resultados de datos que fueron estimados para esta investigación. Partiendo de las fases de preprocesamiento de los datos recolectados, se pasó al entrenamiento de los modelos de aprendizaje automático *Support Vector Machine* (SVM), Regresión Logística, *Random Forest y Naive Bayes*, para, finalmente, evaluar los resultados que cada modelo entrenado arrojó y seleccionar el de mejores datos. Las etapas que se adaptaron del proceso KDD son las siguientes:

- Selección/etiquetado.
- Preprocesamiento/limpieza.
- Transformación/reducción.
- Entrenamiento y validación.
- Análisis de errores.

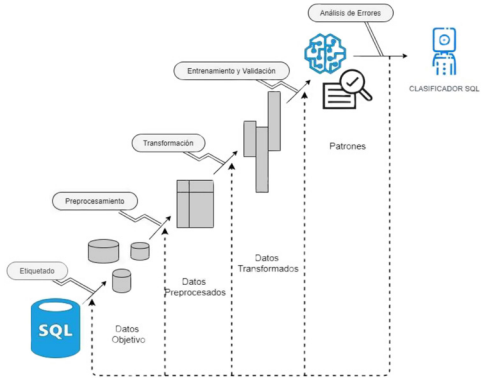


Figura 1. Gráfico de etapas KDD aplicado a Machine Learning[1].

Las etapas seleccionadas descritas en la figura 1 son de tipo lineal. En este caso no es posible pasar o saltar una etapa, pues cada una entrega o genera un archivo con transformaciones específicas que sirven de entrada para la subsiguiente. A continuación, se describe el desarrollo de cada una de estas.

Etapa de selección/etiquetado

Una vez identificado el objetivo del proceso KDD, se procede a realizar la recolección de datos. Para este proyecto, los datos fueron recolectados directamente de

1 Esta ilustración muestra las etapas de la metodología KDD adaptada al proyecto de investigación. Elaboración propia.

SecLists (listas utilizadas en auditorías de seguridad) y archivos CSV (valores separados por comas) compartidos en repositorios de GitHub, Kaggle y Datacamp. Como se implementaron varios modelos de aprendizaje de clasificación de máquina supervisados, fue necesario disponer de los datos debidamente etiquetados para evitar problemas de implementación y poder continuar con el resto de las etapas del procedimiento de entrenamiento.

Los datos de la muestra tomada para la construcción del conjunto de datos (*dataset*) se encuentran etiquetados en dos clases. La primera, corresponde a las cadenas de texto comunes (benignas). Normalmente, los usuarios finales de un paquete de software no son conocedores ni expertos en el manejo de lenguajes de uso específico. Por ello, utilizan las aplicaciones a la interfaz gráfica y el ingreso de datos solo cuando es necesario (como en formularios o menús de acceso). Las cadenas de texto comunes corresponden a los datos que los usuarios ingresan al aplicativo web mediante el uso de cuadros de texto sin ninguna intención de realizar un ataque informático el sistema, como lo serían las cajas de texto de una pantalla de *Login* (usuario-contraseña) o caja de comentarios, entre otros. La segunda clase de muestras son consultas SQL, catalogadas como maliciosas pues en sistemas informáticos no se espera que los usuarios digiten consultas en campos de búsqueda. Estas consultas maliciosas son ingresadas por un atacante.

Estos datos son etiquetados al momento de la construcción del conjunto de datos para que estas dos clases

puedan ser diferenciadas. Las cadenas de texto comunes se etiquetan como textos benignos (0), mientras que las declaraciones de inyección son etiquetadas como malignas (1). Así, se determina cuál conjunto de datos será de naturaleza dicotómica (con solo dos clases posibles). Una vez que los datos son ajustados a las características del modelo (texto y etiqueta), el tamaño del conjunto de datos total es de 32762 muestras, distribuidas de la siguiente manera:

- 20300 datos benignos (0).
- 12462 datos malignos (1).

Etapa de preprocesamiento/limpieza

En esta etapa se analiza la calidad de los datos que se usarán en el entrenamiento. Dado que de esto depende el desempeño del sistema final, así como su efectividad en la clasificación, el propósito es remover, corregir e, incluso, adicionar datos al conjunto de datos previamente generado en la primera fase para descartar cualquier posible error que pueda ocurrir o generar problemas en la siguiente etapa de entrenamiento. Para que el modelo pueda realizar la clasificación con un grado de efectividad aceptable (90% de precisión o superior), es necesario que los datos con ruido (*noisy data*), que son datos fuera del rango de los valores esperados, valores duplicados, datos nulos o incompletos, sean depurados o transformados según sea el caso.

Este procedimiento de limpieza se efectuó utilizando las librerías Pandas y Numpy para Python 3.x, dentro

de las cuales existen funciones y procedimientos para la estructuración de datos, limpieza y depuración, de manera automatizada. Además de seguir las buenas prácticas que se espera de este tipo de procesos de depuración de datos.

Etapa de transformación/reducción

En la etapa de transformación/reducción, se busca extraer las características relevantes (*features*) de los datos de acuerdo con lo estipulado en el proceso KDD. También, es importante implementar técnicas de normalización de los datos con la finalidad de que los datos del conjunto de datos se encuentren en una escala de valores similar, evitando problemas en el modelado y entrenamiento. Igualmente, se debe dar un formato adecuado según el modelo que se desea entrenar.

Los modelos de aprendizaje de máquina están diseñados para procesar vectores numéricos, pero en este punto varias características de los conjuntos de datos son textos o caracteres. Estos los consideraremos como datos no estructurados que no pueden ser analizados ni interpretados por los modelos de aprendizaje de máquina. Por lo que es necesario aplicar métodos de vectorización. Para este proceso se usaron las librerías Scikit Learn y NLTK (*Natural Language Tool Kit*) disponibles para Python 3.x, las cuales proporcionan las herramientas necesarias para realizar el proceso de vectorización de cadenas de caracteres. Se debe tener en cuenta que en este proceso de transformación de datos se realizan procesos muy ligados al procesamiento de lenguaje

natural NLP (*Natural Language Processing*), que es otra de las ramas donde actualmente se adelantan más avances y proyectos de investigación por parte de la comunidad científica del campo de la inteligencia artificial.

Etapa de entrenamiento y validación

En esta etapa de entrenamiento, se divide el conjunto de datos previamente tratado en las etapas anteriores. El procedimiento de entrenamiento consiste en dividir el *dataset* en subconjuntos de prueba y entrenamiento de manera aleatoria. Para este proyecto en particular, se realizó mediante la técnica de *K-Fold* con el fin de medir el rendimiento de los modelos de *Machine Learning* según sus predicciones.

Los resultados que se dan en esta etapa son temporales dado que el proyecto sigue en desarrollo, realizando optimizaciones a los modelos y al conjunto de datos. Para este punto, se realizó el entrenamiento de prueba con un *dataset* reducido de 4200 muestras, donde el set de entrenamiento contenía el 80% de los datos (3360) y el restante, 840, eran de prueba. Se eligieron cuatro modelos que, según el estado del arte recolectado, eran los más usados en la clasificación binaria y que fueron preparados haciendo uso del set de entrenamiento. Se eligió la palabra *label* como variable objetivo, siendo esta la etiqueta para diferenciar los datos de inyección (malignos) y los comunes (benignos).

Una vez fueron entrenados los cuatro modelos predictores, se procedió a realizar la validación del rendimiento

de cada uno. Lo cual sirve para determinar los posibles errores y/o mejoras que se puedan desarrollar para cada modelo. Se desarrolló una matriz de confusión para proveer información clave sobre el rendimiento de los predictores para así visualizar la cantidad de aciertos y errores como se presenta en la tabla 1:

Tabla 1. Resultados de la métrica matriz de confusión

	VP	VN	FP	FN
Logistic Regression	561	252	0	27
svc	540	234	18	48
Random Forest	517	252	0	71
Naive-Bayes	568	252	0	20

Una tabla de contingencia o matriz de confusión se utiliza para mostrar donde los datos están compuestos por solo dos clases, representados por estados (1, 0). Los datos VP (Verdadero Positivo) y VN (Verdadero Negativo) representan los recuentos de casos analizados como verdaderos positivos. En este caso, VP corresponde a los intentos reales de acceso con inyección de código SQL y VN a los intentos de validación del modelo, donde este predijo de manera acertada los datos usados en el set de testeo. Por su parte, FP (Falsos positivos) y FN (Falsos Negativos) recuentan las alertas validadas. Para el proyecto, FP representa los casos detectados inicialmente como inyección de código, pero erróneamente clasificados y posteriormente validados como eventos benignos.

Mientras que FN corresponde al número de errores de clasificación dentro de los modelos. Estos números son importantes no solo para mejorar la calidad de los datos de entrenamiento, sino también para optimizar los modelos y su detección.

De acuerdo con los datos obtenidos, se hizo necesario el uso de otras métricas que permitieran seleccionar el modelo de mejor desempeño y precisión para ser implementado. Para cumplir con este trabajo donde se busca evaluar la precisión, la exactitud (*accuracy*), el puntaje F1 y el puntaje ROC-AUC, primero se debe comprender los siguientes puntos:

1. Con la precisión se puede encontrar la relación entre las predicciones correctas y el número total de predicciones correctas previstas en el set de testeo. Esto permite medir la precisión del clasificador a la hora de predecir casos nuevos.
2. La exactitud corresponde a la relación que existe entre las predicciones correctas y el número total de predicciones. Se encarga de hallar la frecuencia sobre la cual el modelo acierta en su análisis.
3. El puntaje F1 (*F1-Score*) es una combinación entre la precisión y la sensibilidad del modelo.
4. El puntaje ROC-AUC permite saber qué tan bueno es el modelo predictor para diferenciar entre los dos modelos (Flach, 2003).

Los resultados son expuestos en la tabla 2, donde se especifican los puntajes de correspondientes a cada predictor:

Tabla 2. Resultados de la evaluación de los modelos

	Precisión	Exactitud	F1-Score	roc
Logistic Regression	0.903226	0.967857	0.949153	0.977041
svc	0.829787	0.921429	0.876404	0.923469
Random Forest	0.780186	0.915476	0.876522	0.939626
Naive Bayes	0.926471	0.976190	0.961832	0.982993

Etapa de análisis de errores

En esta etapa, se usa el indicador de rendimiento de la etapa de entrenamiento y evaluación para realizar un análisis de errores que nos permita concretar medidas para mejorar los resultados. La etapa conlleva desde recolectar más datos hasta extraer más características e, incluso, cambiar el modelo por uno más complejo o simple, según el caso (Martinez-Heras, 2020). La metodología kdd es dinámica e interativa y la ejecución no es estricta, por lo que podemos regresar a procesos anteriores para realizar cambios según se requiera. Asimismo, esta metodología permite que el trabajo se enfoque en la mejora de la precisión de los clasificadores. Esto gracias a la integración de procesos de preprocesamiento existentes en kdd como la selección de características y la discretización, los cuales favorecen los resultados del modelo Naïve-Bayes (Deshmukh *et al.*, 2015).

Conclusiones

Con los resultados obtenidos y gracias a la incorporación de las fases de preprocesamiento de KDD, el modelo Naïve-Bayes se puede calificar como el que mejor precisión presenta al comparar los resultados de este con los demás modelos entrenados. No obstante, es necesario realizar un despliegue del modelo sobre un servicio web con el objetivo de hacer una simulación de ataques de inyección SQL y efectuar una nueva evaluación del sistema de detección.

Se recomienda que antes de llevar a cabo la división de los datos en la fase de etiquetado, se implemente el proceso de estandarización de características como lo sugieren Deshmukh *et al.* (2015). Esto con el objetivo de eliminar los datos que puedan estar fuera de escala, mejorando su calidad y la eliminación del ruido que estos pueden generar.

Para, por consiguiente, mejorar la calidad de los resultados de los modelos entrenados.

Finalmente, se puede afirmar que el método de transformación y extracción de características usado durante el desarrollo del proyecto de experimentación no es el más adecuado para solucionar el problema de clasificación. Se recomienda explorar otros métodos como la tokenización de los datos, tanto malignos como benignos. Aunque este proceso genera un problema con el tratamiento de los datos benignos, ya que el uso de librerías para generar los tokens está enfocado, principalmente, en palabras del idioma inglés. Por lo cual, los análisis de contenidos en otros idiomas, como el español, son difíciles de encontrar y utilizar, y los resultados suelen ser difíciles de interpretar por la baja calidad respecto a los que se pueden conseguir en inglés.

Referencias

Deshmukh, D., H., Ghorpade, T., & Padiya, P. (2015). *Improving Classification Using Preprocessing and Machine Learning Algorithms on NSL-KDD* Dataset. Conference in 2015 International Conference on Communication, Information & Computing Technology (ICCICT). Mumbai, India.

Flach, P. A. (2003). The Geometry of ROC Space: Understanding Machine Learning Metrics through ROC Isometrics. *Proceedings, Twentieth International Conference on Machine Learning, 1*(August), 194–201.

Martinez-Heras, J. (2020, 19 de septiembre). *Las 7 Fases del Proceso de Machine Learning.* IArtificial. net.https://www.iartificial.net/fases-del-proceso-de-machine-learning/

Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing, 20*(1), 343–357. doi: https://doi.org/10.1007/s00500-014-1511-6

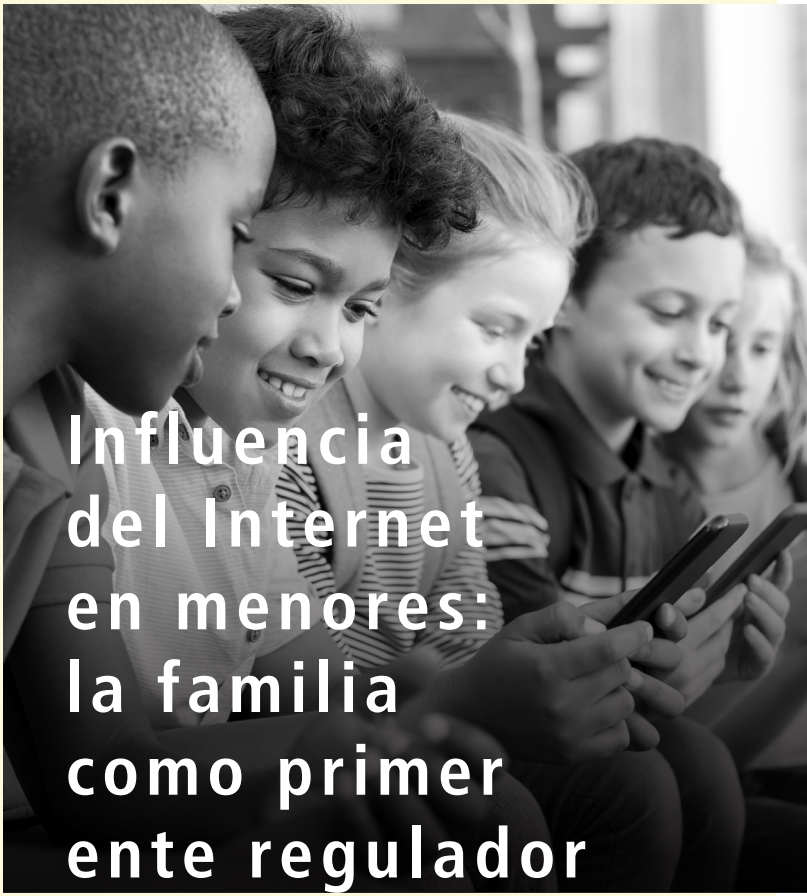
Suleiman, M. F., & Issac, B. (2018). *Performance Comparison of Intrusion Detection Machine Learning Classifiers on Benchmark and New Datasets.* [conference] in 28th International Conference on Computer Theory and Applications. Alexandria, Egypt.

Timarán Pereira, S. R., Hernández Arteaga, I., Caicedo Zambrano, S. J., Hidalgo Troya, A., y Alvarado Pérez, J. C. (2016). Descubrimiento de patrones de desempeño académico con árboles de decisión en las competencias genéricas de la formación profesional. *Descubrimiento de patrones de desempeño académico con árboles de decisión en las competencias genéricas de la formación profesional, 2016, 1*(1), 63–86. doi: https://doi.org/10.16925/9789587600490

Varshney, K., & Ujjwal, R. L. (2019). LSSQLIDP : Literature survey on SQL injection detection and prevention

techniques. *Journal of Statistics and Management Systems, 22*(2), 257–269. doi: https://doi.org/10.1080/09720510.2019.1580904

Wang, Y., & Li, Z. (2012). SQL injection detection via program tracing and machine learning. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* 7646 LNCS, 264–274. doi: https://doi.org/10.1007/978-3-642-34883-9_21



Influencia del Internet en menores: la familia como primer ente regulador

Andrea Julieth Acosta Sánchez[a] · Sindy Paola Ortegon Melo[b]

a Universidad Militar Nueva Granada. Bogotá, Colombia. Correo electrónico: u0801214@unimilitar.edu.co
b Universidad Militar Nueva Granada. Bogotá, Colombia. Correo electrónico: u0801240@unimilitar.edu.co

Resumen: La familia es el núcleo básico de la sociedad. Los padres son los primeros educadores; quienes se encargan de transmitir y plasmar las normas y valores. Por medio de las pautas y estilos de crianza, se pretende regular a los hijos sobre distintos aspectos, fenómenos, problemas sociales y/o dificultades netas de la vida. Los menores son una población vulnerable que puede llegar a ser víctima de diferentes delitos, entre ellos, los delitos informáticos. Estos, son consecuencia del uso inadecuado de las tecnologías de la información y las comunicaciones (TIC). En la actualidad, uno de los fenómenos que avanza con mayor rapidez es el uso de TIC, lo que conlleva un gran número de beneficios para sus usuarios, pero también puede traer problemas si no se les da el uso adecuado.

El presente trabajo tiene como objetivo determinar el rol de la familia como actor fundamental en la formación de un menor y cómo las pautas y estilos de crianza utilizadas controlan o permiten el acceso a las tecnologías de la información. Esta investigación se lleva a cabo por medio de una revisión documental que nos permite indagar, analizar, comparar e identificar cuáles son las pautas y estilos de crianza que permiten regular el uso de la tecnología por parte de niños y adolescentes dentro del entorno familiar. Entre los resultados más relevantes, se encontró que muchos de los padres consideran que sus hijos manejan con soltura y confianza las TIC. Por lo que piensan que el aprendizaje digital es algo innato en los jóvenes y esta es la principal razón para permitir el uso libre de dispositivos electrónicos, empleando un estilo de crianza permisivo.

Como investigadores, consideramos que la información recolectada permitirá crear un estudio que obtenga como resultado la reflexión individual y colectiva sobre la importancia de la familia como ente regulador de este fenómeno social.

Palabras claves: amenazas, ciberdelincuentes, estilos y pautas de crianza, familia, tecnologías de la información y las comunicaciones.

Introducción

"Las nuevas tecnologías de la información y las comunicaciones son una extraordinaria herramienta con tal implantación en el mundo desarrollado que en poco tiempo han revolucionado las relaciones sociales y numerosos aspectos de nuestra vida" (Labrador *et al.*, 2018, p.4). Para nadie es un secreto que son los niños y adolescentes los que se encuentran cada vez más inmersos en las nuevas tecnologías. "Los jóvenes de las nuevas generaciones crecieron con una tecnología que las ha definido por su familiaridad y confianza en las TIC" (Espinoza y Rodríguez, 2017, p. 4). Esto les sucede, especialmente, a aquellos que hacen parte de la Generación Z (nacidos a partir del año 2000), también conocidos como los verdaderos nativos digitales por haber nacido en la era del Internet y llevar la tecnología

en su código genético. Echenique (2012), citado por Espinoza y Rodríguez (2017), se refiere a ellos como:

> Los jóvenes que han crecido en un mundo digital y esperan utilizar estas herramientas para sus entornos avanzados de aprendizaje, como parte de su vida cotidiana, sus pasatiempos y su forma de interacción; se rodean del uso de videojuegos, reproductores de música, cámaras, mensajería instantánea y multimedia, lo que les ha dado la posibilidad de desarrollar habilidades en torno al procesamiento de información. (p. 151-170).

Los menores tienen cada vez más acceso a dispositivos electrónicos a edades tempranas y con estos tienen acceso a diferentes páginas web, dejando así la puerta abierta a todo tipo de peligros. Tal como lo señala García, *et al.*, (2014): "en la actualidad, el 91.2% de los menores de diez a quince años acceden habitualmente a Internet, elevándose este porcentaje con la edad hasta alcanzar el 96.5% a los quince años" (p.463). Por lo tanto, se han catalogado como un grupo de edad vulnerable dado al uso excesivo que hacen del Internet que día a día los expone a situaciones amenazantes y peligrosas para su seguridad física y mental, convirtiéndolos en las víctimas idóneas para los ciberdelincuentes.

Sin embargo, "la responsabilidad de educar en un uso razonable y saludable de las Nuevas Tecnologías,

previniendo los problemas derivados de una mala utilización, corresponde a padres y educadores" (Labrador *et al.*, 2018, p.64). Así mismo, "La familia representa el primer contexto social que acoge al individuo e interviene, en primera instancia, en su inmersión dentro de un contexto sociocultural específico" (Yubero *et al.*, 2018, p.2). Por esta razón, los padres tienen un papel fundamental en la socialización del uso de las redes. Los diferentes estilos de crianza en función del control que ejercen pueden fomentar en los hijos un empleo responsable de las nuevas tecnologías de la información y comunicaciones. Asimismo, un buen control parental puede disminuir las posibilidades de que los menores sean víctimas de diferentes delitos informáticos.

Planteamiento del problema

Aunque la generación Z haya crecido en el mundo de las tecnologías y las maneje con gran facilidad, esto no significa que estén haciendo un uso adecuado y correcto de las mismas. Si bien el Internet tiene grandes beneficios, también existen ciertos riesgos que debemos identificar y prevenir. Según un estudio de Webroot, compañía estadounidense especializada en seguridad en Internet, los "niños y jóvenes entre los 8 y 18 años pasan en promedio 44.5 horas por semana frente a los computadores y dispositivos" (Ministerio de tecnologías de información y las comunicaciones, 2019, p. 2). Igualmente, un estudio de la universidad EAFIT y Tigo-Une muestra que "el 20% de los menores de edad de entre 9 y 16 años deja de dormir o comer alguna vez por estar navegando en Internet" (Ministerio de tecnologías de información y las

comunicaciones, 2018, p. 3). En ese sentido la ciberdependencia hace cada vez más vulnerables a los niños y adolescentes de ser víctimas de otros riesgos asociados al uso de las TIC como el *grooming*, el *sexting*, el ciberacoso, el material de abuso sexual infantil, etc.

Según lo publicó el periódico El Tiempo (2019), en los últimos nueve años, se han presentado en el país 5.583 denuncias de casos por delitos como pornografía con menores de edad y delitos sexuales vinculados a acceso de internet. De estas, 1.038 fueron radicadas en lo corrido de este año. Allí había, entre otros, 202 casos de *grooming* (perfiles falsos usados por adultos para llegar a sus víctimas, especialmente menores de edad), 281 casos de sextorsión, 73 de *cyberbullying* y 93 casos de publicación de imágenes no autorizadas con contenido sexual. Ese tipo de delitos por internet se vienen incrementando cada año. En el 2018 fueron 1.445 reportes, en 2017 se recibieron 1.323 denuncias, en 2016 fueron 866 y en 2015 llegaron 518 reportes.

La educación sobre el adecuado uso del Internet puede ser la clave para prevenir todos los riesgos y vulnerabilidades a los que se encuentran expuestos los menores. Cabe aclarar que esta prevención debe ser constante. Se requiere no solo de la Policía, sino de la acción conjunta de los padres, tutores y centros educativos. En especial, el rol de los padres es fundamental para educar y acompañar a los menores en la utilización de las nuevas tecnologías con responsabilidad. Tal como lo señala Labrador *et al.* (2018):

> El papel de la familia como agente preventivo de primer orden es incuestionable, en el área de las Nuevas Tecnologías y en cualquier otra. Los padres tenemos la responsabilidad de informar a nuestros hijos de los riesgos que corren, enseñarles a hacer un uso razonable y responsable de estos recursos, pero, sobre todo, protegerlos con el ejemplo coherente de nuestros propios actos (p.9).

La pregunta principal que pretende abordar esta investigación "(¿cómo se regula en el entorno familiar el uso que los menores hacen de la tecnología?)" parte del razonamiento de que la familia es el agente principal de socialización, educación y formación de los menores.

Objetivos

Objetivo general

Determinar el rol de la familia como actor fundamental en la formación de un menor y cómo los estilos y pautas de crianza utilizados controlan o permiten libremente el acceso a las tecnologías de la información.

Objetivos específicos

1. Relacionar cómo los estilos y pautas de crianza influyen en el acceso a las tecnologías de la información y las comunicaciones (TIC).
2. Comprender por qué los menores se ven inmersos en delitos informáticos siendo víctimas de los abusos que se dan por medio de las TIC.
3. Explicar la importancia de la participación familiar en la crianza y la necesidad de controles para mitigar que los menores de edad sean víctimas de delitos informáticos.

Marco teórico

Para comenzar a desarrollar las variables de estudio es importante definir ciertos conceptos que servirán para comprender el artículo. Como principal variable se encuentra la familia; varios autores la definen desde distintos puntos de vista. Autores como Elizabeth Jelin afirman que "la familia es la institución social anclada en necesidades humanas universales de base biológica: la sexualidad, la reproducción y la subsistencia cotidiana. Sus miembros comparten un espacio social definido por relaciones de parentesco, conyugalidad y pater-maternidad" (2005, p.3). Otros autores definen este término desde el aspecto psicológico:

> la familia como la unión de personas que comparten un proyecto vital de existencia en común que se supone duradero, en el que se generan fuertes

> sentimientos de pertenencia a dicho grupo, en el cual existe un compromiso personal entre sus miembros y se establecen intensas relaciones de intimidad, reciprocidad y dependencia (Malde, 2012, citado por Gómez y Villa, 2014, pág. 16).

Por su parte, autores como Cámara *et al.* definen la crianza como una serie de "actitudes y comportamientos de los padres" (2007, p. 73). Pero, en definitiva, son los padres el principal vehículo determinante en la formación de los menores, tal como lo señalaba Córdoba en 2014: "la acción parental incide en el desarrollo cognitivo, emocional y social de niñas, niños y adolescentes dado que son las acciones y hábitos cotidianos, que padres y madres manifiestan, en respuesta a las demandas de sus hijos" (p.10). Los estilos de crianza y las pautas que se introduzcan en la formación de un menor de edad influyen directamente en los comportamientos que refleja el niño. Diana Baumrind, psicóloga clínica, en su estudio *Child care practices anteceding three patterns of preschool behavior* de 1967 analiza los tres posibles estilos de crianza: autoritario, democrático y permisivo.

En ese orden de ideas, es importante comenzar a definir los peligros en los que los menores de edad pueden verse inmersos por el uso inadecuado de las TIC. Uno de ellos es el *grooming* que el Instituto Nacional de Tecnologías de la Comunicación de España define como: "acoso o acercamiento a un menor ejercido por un adulto

con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña" (2013, p.5). Para expertos como la psicóloga Paula Cañeque el *grooming* consiste en una "serie de conductas y acciones deliberadamente emprendidas por un adulto, con frecuencia pederasta, con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional, con el fin del poder abusar sexualmente de él" (2015, párr. 2).

Otra amenaza es el *sexting* que según la RAE (2014) se define como el "envío de imágenes o mensajes de texto con un contenido sexual explícito a través de un dispositivo electrónico, especialmente un teléfono móvil" (párr.1). Otros autores coinciden con esta definición afirmando que el *sexting* es "el envío de contenidos eróticos o pornográficos entre dispositivos móviles, en la mayoría de las ocasiones, aunque también pueden utilizarse otras vías" (Molina y Navarro, 2015, p.40).

Por otra parte, Molina y Navarro mencionan: "el *ciberbullying* se describe como abuso psicológico entre iguales o de edad similar. En este caso, la diferencia con el *bullying* es el medio a través del cual se produce el acoso, puesto que en el ciberbullying se utilizan las nuevas tecnologías de la información y las comunicaciones" (2015, p.34). Asimismo, existe el ciberacoso que se diferencia del *ciberbullying* porque es exclusivamente cometido por una persona adulta, mientras este último puede ser cometido por un menor o adulto. Además, el ciberacoso puede convertirse en acoso sexual virtual al tener relación directa con chantajes, extorsiones y atosigamientos por

fotografías o videos eróticos enviados sin consentimiento en los que aparece el acosador y/o la víctima.

Otra gran amenaza a la que se ven expuestos los menores de edad es el acceso a contenido inadecuado. En Internet, los menores pueden acceder de manera voluntaria e involuntaria a materiales nocivos e inadecuados para su edad. Desde actos violentos hasta contenidos de sexo explícito o pornográfico. Si bien los delitos relacionados con la pornografía infantil no son un fenómeno exclusivamente informático, cada vez está más relacionado con el uso de la TIC. En la actualidad, la mayoría de los casos en los que se encuentra este tipo de material se dan a través de Internet (Gabrielli, 2019). La autora Norma Bouyssou (2015) afirma al respecto: "la pornografía infantil ha pasado de ser una actividad casi residual para adquirir indudable relevancia, lo que implica la explotación sexual de niños a nivel mundial, que abarca desde la exhibición de sus cuerpos hasta la violación y la tortura" (p.14).

Otra de las problemáticas que puede traer el uso abusivo y en exceso del Internet en los menores es la adicción al Internet. Es decir, una dependencia hacia Internet en donde se les hace casi imposible desprenderse de sus dispositivos electrónicos. Debe tomarse en cuenta que "la adicción es una enfermedad física y psicológica, la cual provoca un estado de dependencia hacia una sustancia o conducta, y posee una serie de características o síntomas como: pérdida del control, distorsiones del pensamiento y negación de dependencia, entre otros" (OMS, 2020, párr.1).

Metodología

El presente es un estudio en curso que está siendo desarrollado mediante una metodología cualitativa. Se considera una investigación descriptiva ya que reseña las características y rasgos del fenómeno objeto de estudio y no se limita a la recolección de datos. En ese sentido, pretende hacer una predicción e identificación de las relaciones que existen entre las variables. Por consiguiente, la investigación busca determinar de qué manera los diferentes estilos y pautas de crianza influyen en los menores para que tengan control o acceso libre a las tecnologías de la información (TIC). Al pretender describir un fenómeno y, a la vez, asociarlo con una variable, la investigación es de tipo descriptivo correlacional. En consecuencia, el método de recolección de información primordial es la revisión documental de la información publicada en artículos, bases de datos, libros y revistas científicas cuyos temas centrales son objeto de la investigación.

Teniendo presente el método fenomenológico de Edmund Husserl, se considera pertinente el aporte de Alfred Schutz y la incorporación de la teoría del significado para poder entender las variables de estudio. Según Schutz, existen fenómenos, ya sean reales, ideales o imaginarios, que hacen parte del sujeto que vive en el mundo social. Este sujeto está configurado por sus experiencias inmediatas, pues cada individuo vive experiencias únicas; sus padres, su crianza, su educación, sus intereses, deseos y motivos son elementos que nutren y aportan a la formación de personalidades únicas. El tiempo y espacio en el que se desarrollan dichas experiencias determinan las vivencias del individuo.

Cuando hablamos de la realidad debemos tener claro que cada individuo está sujeto a actos y acciones. Todas estas acciones tienen un sentido y significado que puede ser interpretado por otros. Aunque desde la observación directa no se puede determinar qué acciones son conductas significativas, sí se puede observar y comprender los componentes que integran estos actos. Un ejemplo de ello sería la definición de la conducta del sujeto, ya que la observación de actos conlleva a la apropiación e interpretación de los significados de ciertas acciones. Según lo anterior, se busca observar e interpretar los componentes que integran la personalidad del menor partiendo desde los estilos y pautas de crianza impartidas por sus padres. Así, además de comprender el grado de influencia que tiene la crianza en el menor, se quiere saber si esta tiene un efecto positivo para evitar que el menor cometa o sea víctima de delitos informáticos.

Resultados

Lo que se pretendía con esta investigación es determinar y relacionar cuáles de las pautas y estilos de crianza permiten regular el uso de la tecnología en el entorno familiar. Para esto, se llevó a cabo la revisión de artículos, revistas y tesis en las que se evidencia información que corrobora el objeto del estudio. El acceso a Internet y el uso de las TIC desde las primeras edades cada vez aumenta más, principalmente a través de un móvil propio. Muchos de los padres consideran que sus hijos manejan con soltura y confianza las TIC por lo que piensan que el aprendizaje digital es algo innato en ellos y permiten el uso de los aparatos digitales con total independencia. A partir de estas premisas se puede afirmar que los estilos y pautas de crianza de escaso control parental utilizados en el entorno familiar no son los

adecuados para regular el uso del Internet por parte de los niños y adolescentes.

En la revisión documental realizada se tomó en cuenta el estudio *Child care practices antecending three patterns of preschool behavior* de la psicóloga clínica Diana Baumrind, en donde se analizan tres posibles estilos de crianza: autoritario, democrático y permisivo. Tomando como guía los resultados de este estudio, se puede plantear que el estilo de crianza que podría considerarse más apropiado es el democrático. En este, el padre brinda la calidez y amor que el menor necesita, pero también le exige y le establece metas y expectativas que debe cumplir. No obstante, este estilo de crianza permite que el menor sea autónomo y se desarrolle libremente en determinados tiempos establecidos. Lo que permite la creación de un carácter propio y la toma de decisiones por sí mismo.

A través de la información recolectada se pretende establecer que la familia es el primer agente fundamental en la vida del menor. Los padres, quienes deben interesarse por los delitos informáticos y todo lo que conlleva el uso de las tecnologías de la información y las comunicaciones, son los encargados de orientar al menor en el uso de las TIC. Por lo anterior y según la información cotejada, se recomienda el estilo de crianza democrático expuesto por Baumrind. El cual permite que los padres guíen al menor en el uso de las herramientas informáticas, previniendo posibles riesgos y amenazas, sin coartar sus libertades de desarrollo.

Conclusiones

Las nuevas tecnologías se han convertido en herramientas muy valiosas que tienen grandes beneficios si su uso es adecuado. Sin embargo, conforme a este avance tecnológico se ha desarrollado, han aparecido nuevas formas de delitos informáticos frente a los que los niños y adolescentes son, en gran medida, las posibles víctimas. Ya que, cada vez son esta población la que se encuentra más involucrada en el mundo digital, pasando gran parte del día conectada a Internet. Lo anterior, puede llegar a convertir a los jóvenes en las víctimas idóneas para los ciberdelincuentes si estos hacen un uso incorrecto de las herramientas digitales sin acompañamiento de sus padres.

No obstante, esto no significa que se deba cohibir a los menores de usar las TICS. Lo importante es que los padres tengan conocimiento de las implicaciones de navegar

en Internet, se informen y actúen de manera proactiva para evitar que sus hijos sean víctimas de la ciberdelincuencia. Por lo tanto, los padres son los encargados de ser entes reguladores para mitigar que sus hijos puedan tener acceso abusivo a sitios prohibidos o no aptos para su edad.

Por todo lo anterior, es posible afirmar que las pautas y estilos de crianza elegidos por los padres para la educación de los menores influyen en gran medida en que cómo estos accederán a las tecnologías de la información y las comunicaciones. Por esta razón, la mejor manera de evitar que los jóvenes sean víctimas de la ciberdelincuencia es generar una crianza donde exista confianza, comunicación asertiva y una adecuada educación en cuanto a los beneficios y riesgos de las TICS. Asimismo, es importante establecer límites y restricciones para el uso de estas.

Referencias

Baumrind, D. (1967). Child care practices anteceding three patterns of preschool behavior. *Genetic Psychology Monographs, 75*(1), 43-88. https://scinapse.io/papers/1731952969

Bouyssou, N.I. (2015). *Los delitos de corrupción de menores y pornografía infantil.* (Tesis doctoral). Universidad de Sevilla, Sevilla.

Cámara, P., Diaz, M., Carpio, P., Esquivel, E., Acosta, I., y Torres, A. (2007). La contribución del bienestar subjetivo, las expectativas y la crianza maternas en los logros escolares de sus niños y en la valoración de la participación de los padres. *Acta Colombiana de Psicología, 10*(2), 71-82. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=2524841

Cañeque, P. (2015, 28 de abril) *¿Qué es el grooming?*. Paula Cañeque Psicóloga. https://www.paulacaneque-psicologa.com/que-es-el-grooming/

Córdoba, J. (2014). *Estilos de crianza vinculados a comportamientos problemáticos de niñas, niños y adolescentes* (Tesis de maestría). Universidad Nacional de Córdoba, Córdoba. Espinoza, L., y Rodríguez, R. (2017). El uso de tecnologías como factor del desarrollo socioafectivo en niños y jóvenes estudiantes en el noroeste de México. Revista Iberoamericana de las *Ciencias Sociales y Humanísticas, 6*(11), 151-170. doi: http://dx.doi.org/10.23913/ricsh.v6i11.113

Gabrielli, Omar. (2019). Pornografía infantil escala de Tanner, ¿utilidad o ficción? *Gaceta internacional de ciencias forenses, 6*(30), 28-33.

García, B., López & García, A. (2014). Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet. *Revista Latina de Comunicación Social*, 69, 462 - 485. doi: 10.4185/RLCS-2014-1020

Gomez, E. & Villa, V. (2014). Hacia un concepto interdisciplinario de la

familia. *Justicia juris, 10*(1), 11-20. http://www.scielo.org.co/pdf/jusju/v10n1/v10n1a02.pdf

Instituto Nacional de Tecnologías de la Comunicación. (2013). *Guía s.o.s contra el grooming padre y educadores*. Recuperado de: https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

Jelin, E. (2005). *La Familia en la Argentina: Modernidad, Crisis Económica y Acción Política.* Recuperado de: https://biblio.flacsoandes.edu.ec/catalog/resGet.php?resId=21180.

Justicia. (2019, 23 de Septiembre). Casi 4 denuncias al día se reciben por casos de explotación de menores. *El Tiempo.* https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

Labrador, F., Requesens, A., y Helguera, M. (s.f.). Guía para padres y educadores sobre el uso seguro de Internet, móviles y videojuegos. *Codajic.* http://www.codajic.org/node/3848

Real Academia Española. (2014). *Definición de sexting.* https://dej.rae.es/lema/sexting

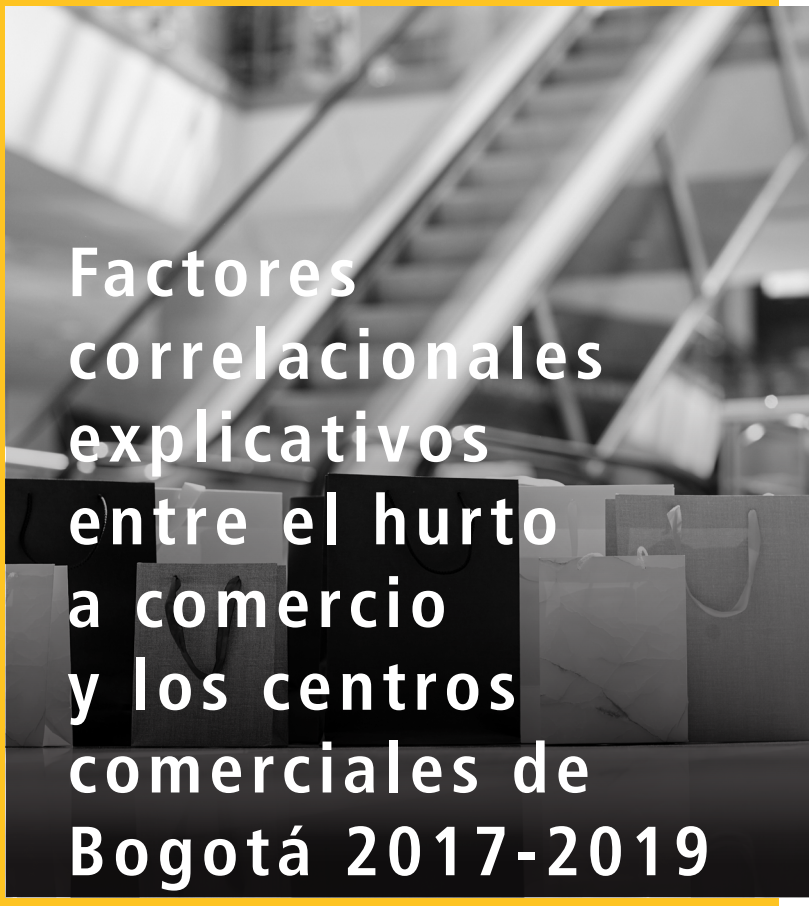
Ministerio de tecnologías de la información y las comunicaciones. (2018,13 de agosto). *Así usan redes sociales los niños y jóvenes en Colombia.* En TIC Confío. https://www.enticconfio.gov.co/Asi-usan-redes-sociales-los-ninos-y-jovenes-en-colombia

Ministerio de tecnologías de la información y las comunicaciones. (2019, 30 de septiembre). *La familia: clave para combatir la ciberdependencia.* En TIC Confío. https://www.enticconfio.gov.co/La_familia_clave_para_combatir_la_ciberdependencia

Molina del Peral, J. A. y Vecina, P. (2015). *Bullying, ciberbullying y sexting: ¿cómo actuar ante una situación de acoso?.* Recuperado de https://elibro.net/es/ereader/usta/115227?page=34

Organización Mundial de la salud. (2020). *La adicción*. Organización Mundial de la salud. https://www.who.int/es

Yubero, S., Larrañaga, E., Navarro, R., & Elche, M. (2018). Padres, hijos e Internet. Socialización familiar de la Red. Una relación compleja. *Universitas Psychologica,* 17(2), 1-13. doi: https://doi.org/10.11144/Javeriana.upsy17- 2.phis.



Factores correlacionales explicativos entre el hurto a comercio y los centros comerciales de Bogotá 2017-2019

Daniela García Vásquez[a]

a Universidad Militar Nueva Granada. Bogotá, Colombia. Correo electrónico: est.daniela.garcia3@unimilitar.edu.co

Resumen: La situación de inseguridad de los comercios en Bogotá plantea unas preocupantes cifras que reflejan la inseguridad ciudadana. En contraste, el auge de los centros comerciales en la Capital y sus medidas de seguridad hacen suponer que el nivel de riesgo frente a esta problemática es más bajo. No obstante, resulta importante determinar si el hurto en los centros comerciales está determinado por variables externas como el entorno o la inseguridad ciudadana.

Palabras clave: centros comerciales, entorno, hurto en comercio, riesgo.

Introducción

La situación de seguridad ciudadana en Colombia reviste varios tipos de análisis y, a su vez, representa la dificultad de determinar claramente cuáles son los factores de causalidad que mayor relevancia tienen para cada tipo de delito. Dentro de la perspectiva del riesgo, el hurto a comercio es un fenómeno de alto impacto no solo en el *retail*, sino también en los centros comerciales. Pese a esto, los centros comerciales de manera permanente desarrollan estrategias para lograr minimizar el hurto en los establecimientos que más se ven afectados, pero no obtienen los resultados esperados. Una prueba de ello es que el hurto a comercio ha crecido 62% entre los años 2017 y 2019. La falta de investigación académica en este campo se debe a la complejidad de obtener cifras claras sobre el hurto a los

locales comerciales. Lo anterior lo ocasionan, especialmente, los siguientes aspectos:

1. En muchas ocasiones, la marca no sabe qué le han hurtado hasta cuando hace inventario después y detecta faltantes.
2. En muchas ocasiones, la marca prefiere denunciar ante las autoridades y no vincular al centro comercial.
3. En otras ocasiones, sí se da el reporte al centro comercial, pero este no lo cuenta como hurto dado que el objetivo del centro comercial es proteger sus áreas comunes y la seguridad.

En este sentido, la obtención de información que permita desarrollar estrategias al interior de los centros comerciales para fortalecer la seguridad de los establecimientos que se encuentran en una zona gris reviste serias dificultades. Ante este vacío de información, pocos son los reportes que se tienen a nivel de las autoridades, en especial de la Policía Nacional. A pesar de la poca información, es probable que exista una relación entre el hurto a comercio y el hurto en los centros comerciales, toda vez que las cifras de la Policía están muy por debajo de la realidad de los centros comerciales.

Según lo anterior, las preguntas que esta investigación pretende resolver son: ¿existe alguna relación entre las cifras de hurto a comercio y hurto a comercio dentro de los centros comerciales? De no ser así, ¿podría ser la inseguridad de los centros comerciales el reflejo del tipo de entorno que se tiene? Esta ponencia

busca analizar el fenómeno del hurto a comercios por localidades en Bogotá como variable explicativa del hurto en centros comerciales.

Para cumplir con este objetivo, en la primera parte de la investigación se analizan las cifras de hurto a comercio de las diferentes localidades de Bogotá, delimitando el estudio a los años 2017, 2018 y 2019. La segunda parte pretende hacer un análisis de las estadísticas delictivas en los centros comerciales de Bogotá, así como el análisis del tipo de entorno que circunda a cada centro comercial. En la tercera parte, se establece la relación entre el hurto a comercio, el hurto en los centros comerciales y el tipo de entorno para determinar si existe alguna correlación entre estas variables.

Marco teórico

El hurto en los centros comerciales es un fenómeno altamente recurrente, pero poco estudiado desde el punto de vista criminológico. A nivel global, esta situación se ha estudiado desde el enfoque de la pérdida conocida y la pérdida desconocida; esta última es la diferencia que existe entre las existencias teóricas y las reales, una vez efectuada la auditoría contable (López-Bonilla y López-Bonilla, 2001). Asimismo, esta pérdida tiene tres factores concomitantes: el hurto interno, el hurto externo y los errores administrativos. Sin embargo, el concepto de merma se ha denominado tradicionalmente desde la perspectiva del *retail*. Es decir, desde las tiendas que venden al detalle que, para este caso, son las tiendas que se encuentran en los centros comerciales. Al respecto, Ceccato *et al.* (2018), argumentan que los centros comerciales están

compuestos por áreas públicas, semipúblicas y privadas, las cuales en ocasiones tiene un límite sutil entre ellas.

Lo anterior, confluye con lo planteado por González *et al.* (2019), donde las dinámicas públicas se vinculan al interior del centro comercial dada su condición de acceso al público en los diferentes modos de operación como son: centro comercial abierto, parcialmente abierto y cerrado. Por esto, uno de los aspectos que mayor incidencia se considera que tienen en la seguridad de los centros comerciales es el entorno. Es así como la investigación de Ceccato y Tcancecu (2018), se estudia cómo la influencia del entorno físico y social en los centros comerciales podría determinar la seguridad percibida por parte de los visitantes y compradores. Los autores concluyeron que, en general, hay lugares en el centro comercial que generan mayor sensación de inseguridad. Estos podrían también tener una mayor propensión a sentirse inseguros especialmente en horas de la noche. Por todo lo anterior, es posible considerar que el hurto en los centros comerciales está influido por factores de tiempo, modo y lugar. Sin embargo, para los centros comerciales colombianos esta relación podría no estar tan clara, siendo este el aspecto de principal interés por determinar para esta investigación.

Metodología

Se realizó una revisión en la base de datos del Observatorio del Delito en la página de la Policía Nacional. El periodo de tiempo determinado para este estudio fueron los años 2017, 2018 y 2019, donde se analizaron los reportes obtenidos sobre el hurto a comercio en cada localidad de Bogotá y el hurto en centros comerciales.

Paralelamente, para la elaboración de este análisis, se tomaron como referencia 36 centros comerciales de la ciudad de Bogotá. Para la elección de estos se tuvo en cuenta que tuvieran parqueadero y salas de cine. Igualmente, se hizo una investigación acerca de su año de inauguración para poder identificar si esto influía en el aumento de hurto a comercio de la localidad.

Análisis de las cifras de hurto a comercio en Bogotá

La seguridad ciudadana es la convergencia de innumerables variables y en este sentido la complejidad de entenderla a partir del comportamiento de las cifras. La inseguridad, bajo la perspectiva de Luhmann (1991), es la interacción de un sistema social influenciado por situaciones políticas, económicas, sociales y el alcance global que complejizan la situación de seguridad. En este escenario de diversa complejidad, obtener la información necesaria para explicar la fenomenología de inseguridad en los establecimientos a partir de la dinámica propia de las localidades podría brindar información clara que aporte al diseño de estrategias de protección efectivas. A continuación, se analizan las tendencias de inseguridad ciudadana en los comercios durante los años 2017, 2018 y 2019 para cada localidad de la ciudad de Bogotá.

Tabla 1. Hurto a comercio por localidades en Bogotá para los años 2017 a 2019

LOCALIDAD	HURTO A COMERCIO			TOTAL/ AUMENTO
	2017	2018	2019	
Usaquén	1.947	1.434	2.562	31,6%
Chapinero	1,191	1.630	1.547	29,9%
Usme	313	436	433	38,3%
Tunjuelito	327	369	294	-10,09%
Bosa	651	775	524	-19,5%

Kennedy	1.681	1.809	1.540	-8,4%
Fontibón	1.057	1.338	864	-18,3%
Engativá	1.837	2.041	1.677	-8,7%
Suba	1.698	1.979	1.767	4,06%
Barrios Unidos	551	713	610	10,7%
Teusaquillo	862	939	869	0,8%
Los Mártires	571	579	488	-14,5%
Antonio Nariño	638	799	704	10,3%
Puente Aranda	680	1.032	771	13,4%
Ciudad Bolívar	411	492	425	3,4%

Nota. Tabla elaborada a partir de los datos estadísticos de la Policía Nacional.

A partir de lo visto en la tabla 1, se puede evidenciar que las localidades que presentan más hurto a comercio son Usaquén, Suba y Kennedy. Lo cual, a través de un análisis de Pareto, se puede concluir que son X, Y y Z las localidades que aportan el 36.9% de las cifras totales de hurto a comercio en las localidades. Desde otro punto de vista, los mayores incrementos en hurto a comercio se han dado en las localidades de Usme, Chapinero y Usaquén a lo largo de los tres años objeto de estudio, donde los casos reportados a la Policía Nacional tuvieron un aumento entre el 26 y el 28%. Esta radiografía de la inseguridad en el comercio permite también analizar la dinámica propia que se relata en los centros comerciales, la cual es la ocurrencia de eventos de inseguridad en estos establecimientos que se ocultan dentro de

la dinámica de los sucesos de la seguridad comercial. Justamente, es esta última uno de los servicios que se brindan al interior de estos conglomerados de tiendas que hacen parte de la cadena de valor.

El hurto en los centros comerciales de Bogotá según las localidades

Como se ha planteado en la problemática de esta investigación, resulta compleja la identificación de variables determinantes del hurto en los establecimientos al interior de los centros comerciales puesto que en ocasiones no se denuncia, en otras no se puede determinar el momento del hurto y en otras el centro comercial en concreto puede no tener la información de dichos casos. En este sentido, se parte de las cifras de las denuncias interpuestas de casos que han ocurrido al interior de los centros comerciales, entendiendo que son las mejores cifras disponibles para el análisis. En la tabla 2 se presentan estas cifras y la cantidad de centros comerciales seleccionados por cada localidad objeto de estudio.

Tabla 2. Cantidad de centros comerciales y reporte de hurtos

LOCALIDAD	HURTO EN CENTROS COMERCIALES						
	2017		2018		2019		Total, hurtos
	Total, cc	Hurtos	Total, cc	Hurtos	Total, cc	Hurtos	
Usaquén	3	24	3	32	3	35	91
Chapinero	4	10	4	15	4	16	41
Usme	1	4	1	0	1	1	5
Tunjuelito	1	8	1	2	1	3	13
Bosa	1	6	1	4	1	5	15
Kennedy	2	4	2	19	3	15	38
Fontibón	3	10	4	29	4	20	59
Engativá	4	17	4	33	4	18	68
Suba	6	34	6	45	6	53	132
Barrios Unidos	3	6	3	7	3	14	27
Teusaquillo	2	11	2	10	2	8	29
Los Mártires	1	9	1	13	1	9	31
Antonio Nariño	1	4	1	21	1	11	36

Puente Aranda	1	9	1	17	1	8	34
Ciudad Bolívar	0	0	1	3	1	5	13

Nota. Tabla elaborada a partir de los datos estadísticos de la Policía Nacional.

Tomando como referencia los datos obtenidos, podemos identificar que el año 2018 fue el año que mayor cantidad de hurtos en centros comerciales se reportaron y el aumento con respecto al año 2017 es del 35%, mientras que para el año 2019 los hurtos se redujeron en un 14%.

Análisis de las estadísticas delictivas en los centros comerciales de Bogotá

Tomando como referencia la tabla 2, podemos identificar que la localidad de Suba es la que tiene mayor número de centros comerciales y, asimismo, es la localidad con mayor cantidad de hurtos a lo largo de los 3 años con 132 hurtos. Seguida de Usaquén que cuenta con tres centros comerciales y presenta un aumento progresivo en la cantidad de hurtos por año, teniendo 91 registros durante los años 2017 a 2019. En tercer lugar se encuentra Engativá, que es una de las localidades con mayor cantidad de centros comerciales y presentó 68 reportes de hurto en centros comerciales durante estos tres años. Siendo el 2018 el año con mayor número de casos registrados y reportando una disminución para el

año 2019. También se identificó que de las tres localidades donde aumentó la cantidad de centros comerciales solo en Ciudad Bolívar aumentaron los hurtos. Mientras que en Kennedy, al haber un centro comercial nuevo, los hurtos disminuyeron. En Fontibón, para el tiempo de apertura del cuarto centro comercial, los hurtos aumentaron notoriamente, pero al año siguiente disminuyeron.

Conclusiones

En el 46.7% de las localidades de Bogotá el hurto en centros comerciales aumentó durante el año 2018 y se redujo notoriamente en el año 2019. Mientras que en el 26.7% de estas localidades el hurto aumentó progresivamente en los años analizados y en el 26.6% restante la cantidad de hurtos disminuyó. En las localidades de Kennedy, Fontibón y Ciudad Bolívar se identificó la inauguración de centros comerciales durante 2018 lo que, según los datos obtenidos, influyó en el aumento de casos de hurto en centros comerciales.

Referencias

Castro J, D. (2019). *Una Mirada Desde El Liderazgo Transformacional en la Gestión Operativa de Seguridad en Centros Comerciales de Bogotá.* (Tesis de posgrado). Universidad Militar Nueva Granada, Bogotá.

Ceccato, V. y Tcacencu, S. (2018). Seguridad percibida en un centro comercial: un estudio de caso sueco. *En Crimen minorista.* Londres, Reino Unido: Palgrave Macmillan.

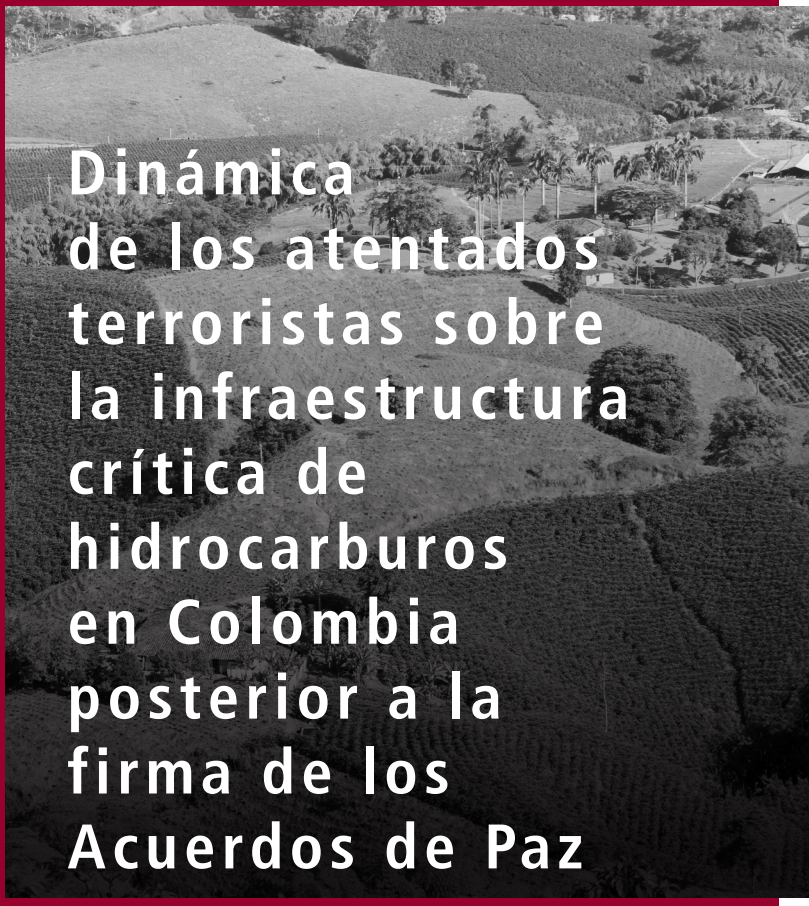
Ceccato, V., Falk, Ö., Parsanezhad, P. y Tarandi, V. (2018). Crimen en un centro comercial escandinavo. En *Retail Crime.* Londres, Reino Unido: Palgrave Macmillan.

González J, C., Fajardo C, H., y Ríos J. (2019). La prevención del riesgo de terrorismo en centros comerciales: hacia una seguridad pública en

Colombia para la protección de infraestructuras críticas. *Revista Ibérica de Sistemas e Tecnologias de Informação. E*(18), 471-484.

López-Bonilla, J. M., y López-Bonilla, L. M. (2001). El hurto en el comercio minorista. *Boletín Criminológico, E*(56), 1-4.

Luhmann, N.,(1991) *Sistemas Sociales: Lineamientos para una Teoría General,* Ciudad de México, México:Alianza Editorial.



Dinámica de los atentados terroristas sobre la infraestructura crítica de hidrocarburos en Colombia posterior a la firma de los Acuerdos de Paz

Stefania Rotavista Pardo[a]

a Universidad Militar Nueva Granada. Bogotá, Colombia. Correo electrónico: stefaniarotavista@gmail.com

Resumen: El objetivo del artículo es determinar el comportamiento de los atentados sobre las infraestructuras críticas energéticas de hidrocarburos en Colombia con posterioridad a la firma de los Acuerdos de Paz de La Habana (APH). Para lograrlo, el presente trabajo se divide en tres partes: primero se centra en realizar el levantamiento de información disponible en recursos periodísticos que hacen referencia a los atentados efectuados por grupos armados a infraestructuras críticas de hidrocarburos. En segunda instancia, compara reportajes y estudios que han expuesto los actos terroristas ocurridos antes de la firma de los Acuerdos de Paz con lo hallado anteriormente. Finalmente, la tercera parte analiza si hay reducción en el comportamiento de las actividades delictivas de los grupos terroristas

frente a las infraestructuras críticas de hidrocarburos. Después de realizar todo el análisis, se pudo concluir que los atentados tuvieron bajas cifras por un par de años, pero sufrieron una alteración aumentando en un 86.5%. Esto demuestra que los APH lograron el fin de estos actos a largo plazo. Aunque, queda la esperanza de que estas cifras disminuyan de acuerdo a los datos recogidos para el año 2019.

Introducción

En el presente artículo se analiza el comportamiento de los atentados a las infraestructuras de hidrocarburos en Colombia después de la firma de los Acuerdos de Paz en el gobierno de Juan Manuel Santos. El ELN (Ejército de Liberación Nacional) y las FARC (Fuerzas Armadas Revolucionarias en Colombia) han sido protagonistas de gran parte de los atentados previo a la firma del Proceso de Paz. Varios de los estudios previos, como los de la Fundación Ideas para la Paz, indican que estos grupos armados tienen como fin atacar la ganancia de poder jerárquico en el país y el aumento de sus riquezas por medio de extorsiones, homicidios, secuestros, sobornos, etc. Esta dinámica de ataques converge en serias afectaciones de lo que es el concepto de las infraestructuras críticas. Esto ha

desembocado en impactos económicos, sociales y de seguridad para el país. De acuerdo a cifras del Ministerio de Defensa Nacional, en total, durante los últimos diez años, se han presentado 1.673 atentados terroristas contra este tipo de infraestructuras. Este alto número de atentados convierte a Colombia en uno de los países con mayor afectación de sus infraestructuras críticas.

Según un especial de Semana Sostenible, desde 2012 al 2016, el índice de asaltos a estos oleoductos antes de la firma de los Acuerdos, sobrepasa los 600 atentados. Lo anterior demuestra que, desde el primer atentado que se presentó a este tipo de infraestructura en el año 1965, ha disminuido (345) el registro de atentados sufridos. Mediante una reconstrucción de fuentes periodísticas como El Tiempo, El Espectador, Noticias Caracol, Noticias RCN, etc., se pueden identificar los principales atentados a la infraestructura crítica del país que han afectado a las poblaciones cercanas, la flora y la fauna. Junto con esta información, bases de datos como las del Ministerio de Defensa Nacional permiten complementar el análisis de rigor de esta investigación.

Marco teórico

Atentados terroristas contra el sector hidrocarburos posterior a la firma de APH

El primer atentado ocurrido en Colombia a la infraestructura de hidrocarburos fue en 1965 cuando el ELN atacó una infraestructura en Barrancabermeja. En la década de los noventa y posteriores, las capacidades de los grupos al margen de la ley y los ataques se incrementaron visiblemente. No obstante, en la actualidad los ataques han sido discontinuos, no ha habido una regularidad (Issa, 2015). Por ejemplo, en el año 2000 en Colombia se presentaron 215 casos, en el 2005 hubo 155 y, hasta el año 2010, hubo una rápida disminución de los casos, año en el que, favorablemente, solo se presentaron 31 atentados (Issa, 2015). Sin embargo, según el especial de la Revista Semana de julio del

2019, en 2015 se reportaron 82 atentados en oleoductos, cifra que cambió la disminución continua que se venía presentando.

Después de la firma de los Acuerdos de Paz se suponía que los ataques debían cesar, pero el nombre de la banda criminal las FARC se volvió a ver implicado en ellos, mientras que el ELN es quien más predominaba en este campo. En el tiempo transcurrido desde la fecha de la firma de APH hasta la actualidad, abril del 2020, se siguen presentando ataques a este tipo de infraestructura. No obstante, este artículo sólo tiene como objeto de estudio el periodo desde la fecha de la firma de los Acuerdos de Paz hasta 2019.

De acuerdo con la recolección de datos en bases periodísticas, 12 fueron los atentados que se presentaron en el oleoducto de Caño Lima-Coveñas en Arauca, Boyacá, Casanare (OCC) y el oleoducto Transandino (OTA) desde el 26 de septiembre del 2016 hasta finales del mismo año. En 2017 se calcularon 43 atentados a estas mismas estructuras. Lamentablemente, en 2018 este número ascendió a 85 y las noticias al respecto demostraron que muchas veces no se determinaba el autor de cada ataque. Pero, cuando se lograba hallar al causante de estos crímenes, el ELN sobresalía. Pocas fueron las veces en las que las incidencias de las FARC de los sitios aledaños también fueron culpables de estos actos. Siguiendo con la línea de tiempo, en 2019 los ataques decayeron a 49. En esta ocasión se presentaron en el OCC, OTA y el

oleoducto Mansoyá Orito (OMO), pero no se determinó al causante de estos delitos.

La figura 1 muestra a detalle las cifras de los ataques al oleoducto Caño Lima-Coveñas. Según esta, se puede evidenciar el incremento de estos actos en los años siguientes a la firma del Proceso de Paz. El incremento es exponencial y solo hasta 2019 presenta una disminución en estos atentados. Al mismo tiempo, este incremento coincide con la presencia y crecimiento de las estructuras criminales en el departamento de Arauca, donde se encuentran. Principalmente, el ELN y las FARC.En esta gráfica también se detallan los atentados terroristas ocurridos al oleoducto Caño Lima-Coveñas que atraviesa los departamentos de Arauca, Boyacá, Casanare y Norte de Santander siendo estas, regiones de alta presencia de grupos como las FARC y el ELN.

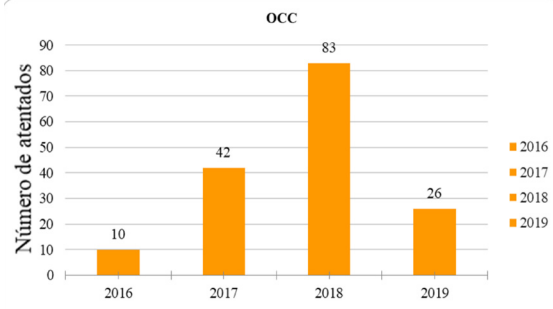


Figura 1. Número de ataques al oleoducto Caño Lima-Coveñas.
Fuente: elaboración propia.

La figura 2 expone los atentados terroristas ocurridos en el oleoducto Transandino, ubicado en el departamento de Nariño, región donde hay presencia de grupos al margen de la ley como el Clan del Golfo, las FARC, el ELN y muchos otros que se disputan el territorio.

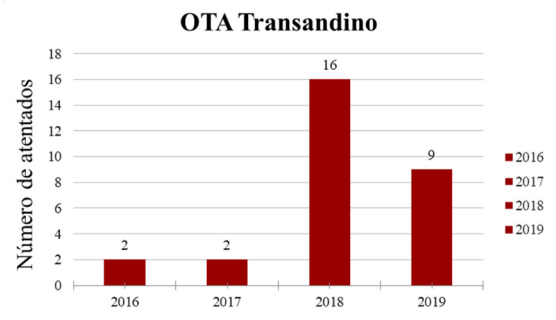


Figura 2. Número de ataques al oleoducto Transandino.
Fuente: elaboración propia.

En la figura 3 se detallan los atentados terroristas ocurridos en el oleoducto Mansoyá Orito que converge en los departamentos de Nariño y Pasto. Siendo estas regiones territorios de alta presencia de grupos como el Clan del Golfo, la Resistencia Campesina y el ELN. Para realizar esta gráfica en concreto se tuvo presente que si bien son bastantes los datos que se obtuvieron en la prensa, también existía la necesidad de buscar más fuentes que arrojaran cifras oficiales para lograr una buena comparación y observar cómo la tendencia disminuyó o aumentó a través de los años. Después de una

búsqueda, se logró obtener datos actualizados por el Ministerio de Defensa Nacional sobre atentados terroristas a infraestructuras críticas. Con ellos, se compararon algunas cifras, ya que los informes abarcan los atentados ocurridos cada año desde el 2007 hasta el 2020.

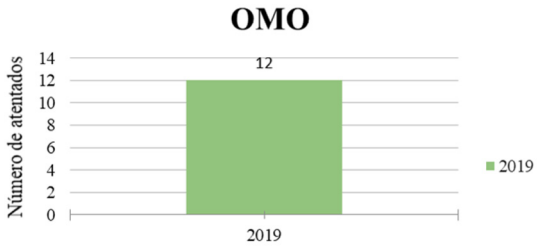


Figura 3. Número de ataques al oleoducto Mansoyá Orito.
Fuente: elaboración propia.

Figura 4. Total de atentados en los oleoductos OCC, OTA y OMO durante el periodo 2016-2019 dividido en porcentajes.
Fuente: elaboración propia.

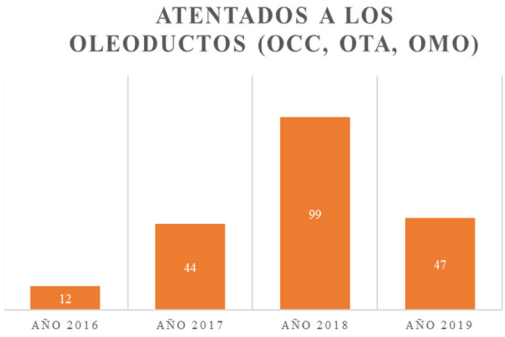


Figura 5. Número de atentados en los oleoductos OCC, OTA y OMO durante los años 2016-2019 según las fuentes periodísticas. **Fuente:** elaboración propia.

En las figuras 4 y 5 se evidencia que en el año en que más se cometió este tipo de atentados en el país fue en el 2018 con un total de 99 para un porcentaje del 47%. Por su parte, el 2016 es el año con menor número de ataques, presentando solo 12, el 6% del total. Sin embargo, estos datos no pueden considerarse completamente certeros pues al ser cifras que aparecen en medios de información, como noticias, artículos, publicaciones, etc., podrían estar incompletas. Prosiguiendo, las figuras 6 y 7 muestran los datos proporcionados por el Ministerio de Defensa organizados de igual manera a las anteriores:

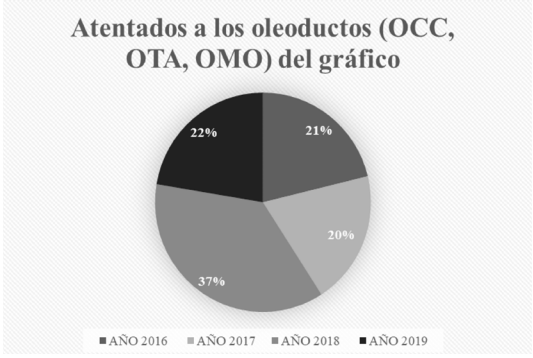


Figura 6. Total de atentados en los oleoductos OCC, OTA, OMO para los años 2016, 2017, 2018 y 2019 según el Ministerio de Defensa dividido en porcentajes.
Fuente: elaboración propia.

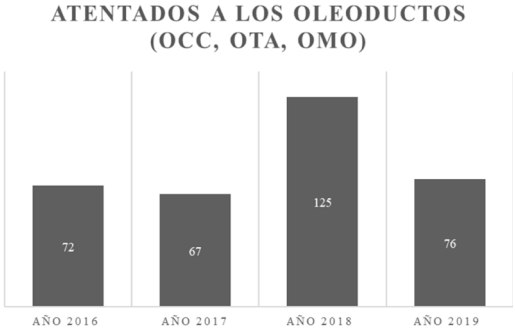


Figura 7. Número de atentados en los oleoductos OCC, OTA, OMO durante los años 2016, 2017, 2018 y 2019 según el Ministerio de Defensa.
Fuente: elaboración propia.

Según las cuatro gráficas anteriores, se puede empezar a observar ciertas similitudes. Por ejemplo: el 2018 fue la época en donde más atentados se desarrollaron. Al coincidir la información de las gráficas, se puede considerar a los datos recogidos en fuentes periodísticas como un apoyo verídico para la investigación.

Evolución de la tendencia

Para entender la evolución de la tendencia sobre los atentados a oleoductos en el país, se decidió tomar como punto de partida datos entre los años 2010 hasta 2015. Asimismo, se apoyó esta información con las cifras dadas por el Ministerio de Defensa.

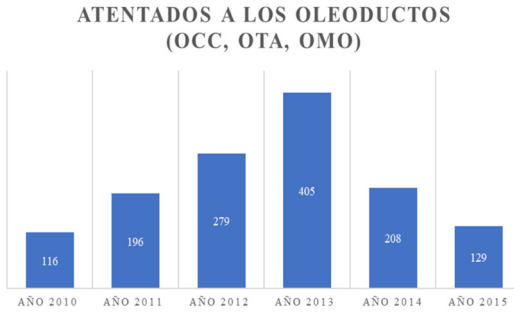


Figura 8. Número de atentados en los oleoductos OCC, OTA y OMO durante los años 2010 a 2015 según el Ministerio de Defensa. **Fuente:** elaboración propia.

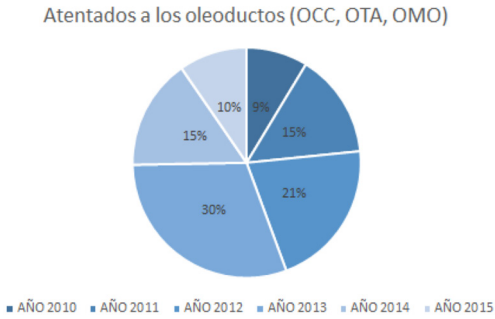


Figura 9. Porcentajes de atentados a los oleoductos OCC, OTA y OMO del 2010 al 2015 según el Ministerio de Defensa. **Fuente:** elaboración propia.

Las gráficas en las figuras 8 y 9 representan cómo, desde que se contempló una lucha contra la restitución de tierras y la atención a víctimas del conflicto armado, aumentaron los ataques. En 2012 se declaró oficialmente la negociación del APH. Es decir, desde esa fecha los ataques fueron en aumento hasta que en 2014 se fueron reduciendo de a poco hasta llegar al primer periodo del 2016. Esta fue una constante lucha en donde se logró reducir los ataques por un par de años, pero de igual manera se siguen viendo y, hoy por hoy, estos van en aumento.

Conclusiones

Después de analizar la información anterior, se puede concluir que los atentados tuvieron bajas cifras por un par de años, pero sufrieron una alteración aumentando en un 86.5%. Esto demuestra que los APH lograron el fin de estos actos a largo plazo. Aunque, queda la esperanza de que estas cifras disminuyan de acuerdo a los datos recogidos para el año 2019. Además, se pudo determinar que existen otros actores criminales que afectan de igual manera la infraestructura crítica de hidrocarburos. Entre ellos, se destaca, por ejemplo, la seguridad en las empresas, donde los actos delincuenciales se perpetuaron gracias a el robo de información y se ultrajaron diferentes oleoductos con válvulas ilícitas. Si bien es cierto que son muchos los factores que influirían para llegar a disminuir estos ataques, con una lucha constante por la paz lograrlo en el futuro no es imposible.

Referencias

Fundación Ideas para la Paz. (2015). El ELN y la industria petrolera: ataques a la infraestructura en Arauca. *Área Dinámicas del Conflicto y Negociaciones de Paz, 2015*(Abril), 1-49. http://cdn.ideaspaz.org/media/website/document/55411b8a3ccab.pdf

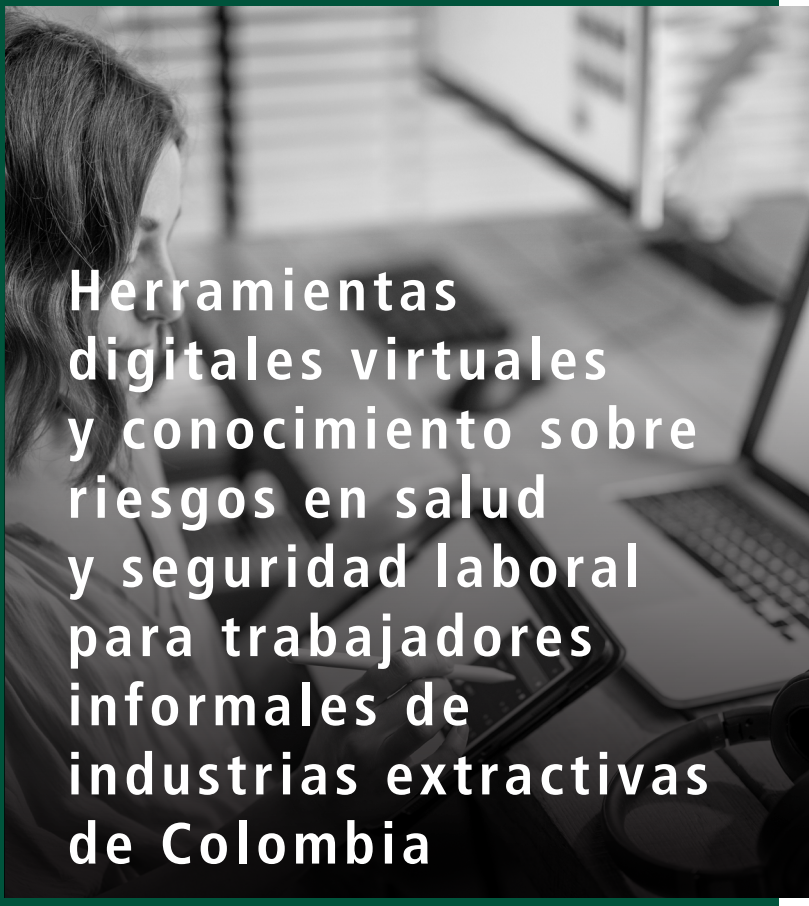
Ecopetrol. (2019, 17 de marzo). *Voladoras: Una cruda arma de guerra.* Editorial Semana. http://especiales.sostenibilidad.semana.com/voladuras-de-oleoductos-en-colombia/index.html

Issa Tejeda, L. F. (2015). Efectos del terrorismo en los oleoductos de Colombia. Universidad Militar *Nueva Granada, 2015*(1), 21. https://repository.unimilitar.edu.co/bitstream/handle/10654/7789/EFECTOS%20DEL%20TERRORISMO%20

EN%20LOS%20OLEODUCTOS%20DE%20COLOMBIA.pdf;jsessionid=628FB5E047EF0493F1DD05433FA3A719?sequence=1

Sáenz, J. (2020, 2 julio). *Petróleo, un beneficiado con la tregua con el ELN.* El Espectador. https://www.elespectador.com/noticias/economia/petroleo-un-beneficiado-con-la-tregua-con-el-eln/

Ministerio de Defensa Nacional de la República de Colombia. (2020). https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://ace7a1cda83a0586a637bea0316c7917



Herramientas digitales virtuales y conocimiento sobre riesgos en salud y seguridad laboral para trabajadores informales de industrias extractivas de Colombia

Gregorio Puello Socarrás[a] · Axel Rodríguez Peña[b]

a Corporación Universitaria Minuto de Dios. Bogotá, Colombia. Correo electrónico: gpuellosoca@uniminuto.edu.co
b Universitaria Virtual Internacional. Bogotá, Colombia. Correo electrónico: arodrgezp@uvirtual.edu.co

Resumen: El proyecto propuesto se enfoca en el desarrollo de productos digitales construidos con la población de trabajadores informales de industrias extractivas ubicadas en Ciudad Bolívar (Bogotá), Villavicencio y municipios PDET [1]. El problema de investigación propuesto aborda la comunicación en relación con el bienestar laboral con el objetivo de identificar factores de riesgo laboral en poblaciones de alto impacto. En especial, el proyecto se enfoca en trabajadores informales de industrias extractivas.

Este ejercicio busca implementar estrategias de co-creación en medios audiovisuales acerca de los factores de riesgo para su salud y seguridad laboral en estas comunidades de trabajadores. Para ello, se tomó como

1 Planes de Desarrollo con Enfoque Territorial.

base un muestreo no probabilístico de tipo "Bola de Nieve" de enfoque cualitativo en una población de cincuenta industrias extractivas formales e informales. En su estudio, se utilizaron instrumentos como la observación participante, la entrevista y la cartografía social que posteriormente fueron analizados mediante relatos y notas de campo en los informes de resultado de la investigación.

Por último, se creó un taller de co-creación que permite el desarrollo de una estrategia de comunicación digital. A partir de este ejercicio creativo, se espera la apropiación social del conocimiento en armonía con lo dispuesto en el ODS: "promover el crecimiento económico inclusivo y sostenible, el empleo y el trabajo decente para todos" (OIT, 2020). Se espera centrar la discusión en nuevas posibilidades del diseño digital en la salud y seguridad en el trabajo; específicamente en la comunicación de factores de riesgo laborales en poblaciones de trabajadores informales. De esta manera, se pretende plantear una discusión sobre los métodos y resultados de exploración y ponderación de las experiencias de este ejercicio transdisciplinario. Esto con el fin de refinar estrategias y sistematizar procesos de investigación y creación en espacios para la comunicación humana que incluyan el mejoramiento de condiciones laborales y fomento de objetivos de desarrollo sostenible necesarios para el cambio social.

Palabras clave: apropiación social del conocimiento, creación, diseño digital, investigación, riesgos laborales.

Introducción

Partiendo de la premisa fundamental definida por la Organización Internacional del Trabajo, "trabajo decente y crecimiento económico-promover el crecimiento económico inclusivo y sostenible, el empleo y el trabajo decente para todos" (OIT, 2018), el proyecto realizado en la vigencia 2020 y denominado C120-271: *Estrategia de Innovación social enfocada en la apropiación del conocimiento sobre factores de riesgo para la salud y seguridad laboral en trabajadores informales de industrias extractivas de territorios con pdet (Planes de Desarrollo con Enfoque Territorial) en el sur de Bogotá y en la ciudad de Villavicencio*, tuvo como uno de sus objetivos principales evaluar los riesgos a los que están expuestos los trabajadores informales de industrias mineras en sus

estaciones de trabajo. El fin era identificar factores de riesgo para, en una segunda etapa, integrar estos conocimientos de seguridad y salud laboral con los del diseño gráfico en pro de realizar estrategias de aprehensión del conocimiento en estas comunidades. Con respecto a estas estrategias, desde el diseño gráfico se establece:

> Para que las estrategias de comunicación afecten el conocimiento, las actitudes o el comportamiento de las personas, deben ser detectables, discriminatorias, atractivas, comprensibles y convincentes. Deben construirse sobre la base de una buena comprensión de la percepción visual y la psicología del conocimiento y el comportamiento, y deben considerar las preferencias personales, las habilidades intelectuales y el sistema de valores culturales de la audiencia objetivo. (Frascara, 2000)

En el texto anterior, la comunicación ha sido la función principal del diseñador gráfico. Al asumir este rol, es necesario encontrar una propuesta que brinde una solución al público objetivo desde el ámbito ocupacional y utilizando las diferentes herramientas de trabajo que caracterizan al comunicador visual. El campo de desarrollo de estas iniciativas también incluye el uso de Nuevas Tecnologías de la Información y la Comunicación (NTICS), medios en los que se vienen desarrollando

aplicaciones y plataformas que pueden dinamizar procesos y narrativas audiovisuales para convertirlos en productos transmedia.

En el campo de la seguridad y salud ocupacional, y más aún en el campo de las comunidades laborales informales, no se han producido desarrollos con la participación de la disciplina del diseño gráfico que permitan dinamizar los procesos de aprehensión del conocimiento. Por ende, el autocuidado es fundamental como una medida de control frente a los riesgos que se presentan para la salud y la seguridad laborales. Lo anterior, es la principal razón por la que esta iniciativa es un potencial innovador disruptivo sobre el trabajo en el área de la seguridad laboral. Pues fusiona la salud ocupacional y el diseño gráfico en las industrias mineras de Colombia.

Metodología

Esta etapa de construcción de la estrategia de conocimiento y diseño de las herramientas digitales virtuales del proyecto contó con las siguientes fases:

Tabla 1. Fases del proceso de investigación y creación a partir de la metodología del Parque Científico de innovación Social (PCIS) de Uniminuto

Fase	Tipo de investigación/ instrumentos utilizados	Observaciones
Fase 1: alistar	Revisión documental en Resúmenes Analíticos Especializados (RAES) sobre factores de riesgo laborales presentes	Se identifican los factores de riesgo para los trabajadores a partir de las normas legales

	en la normativa colombiana y sus aplicaciones en proyectos previos. Antecedentes de intervención en riesgos laborales con comunidades mineras informales.	vigentes en Colombia y la Guía Técnica Colombiana (GTC45).
Fase 2: entender y analizar	• Observación participante basada en Norma Técnica Colombiana (NTC4114). • Entrevista y cartografía social en trabajo de campo para aproximarse a la percepción de riesgo de los trabajadores.	Se espera poder realizar tres sesiones de observación participante para cada estudio de casos (población estimada de impacto: 90 empresas; muestra: tres estudios de caso). Desarrollo de *storyline, storyboard*

	● Con el concurso de la población laboral, aplicar técnicas de innovación y creatividad social.	y guión técnico de las piezas digitales, basadas en realidad mixta.
Fase 3: crear	Desarrollo de producción y postproducción del recurso multimedia digital con realidad mixta para permitir la interacción con la comunidad laboral interesada.	Diseño de un producto multimedia digital, basado en realidad mixta, para el conocimiento de factores de riesgo por parte de trabajadores de industrias extractivas en Colombia.

Es importante mencionar que en esta metodología se mezclan la salud ocupacional y el diseño gráfico a través de un proceso de investigación-creación. En este, la fase investigativa se construye sobre los conocimientos

de las disciplinas de la seguridad y salud en el trabajo (observación basada en NTC4114, análisis de riesgos basado en GTC45), sumado a otras técnicas de indagación (RAES, entrevistas y cartografía social), con los conocimientos del diseño gráfico en la etapa creativa, en la que se desarrolla el *storyline*, *storyboard*, guión técnico y piezas digitales basadas y proyectadas en sistemas de realidad mixta.

Resultados

Entendiendo el proceso de investigación y creación como un proceso de dos etapas: investigación en SST y diseño gráfico, los resultados se presentan de la siguiente manera:

1. Factores de riesgo laboral identificados a partir de conocimientos de seguridad y salud en el trabajo

Tabla 2. Riesgos laborales y efectos posibles identificados en el estudio a partir de la aplicación de la NTC4114, entrevista y cartografía social

Tipo de riesgo	Posibles efectos negativos identificados para la salud	Nivel bajo	Nivel medio	Nivel alto
Biomecánico	Trastornos osteomusculares.			X

Físico	Insolaciones, exposición a temperaturas extremas, enfermedades respiratorias por aspiración de virus y/o partículas (neumoconiosis).		X
Químico	Exposición a agentes químicos corrosivos.	X	
Biológico	Enfermedades respiratorias por aspiración de virus y/o partículas (COVID-19).		X
Condiciones de seguridad	Caídas a nivel, atrapamiento o quemaduras de contacto.	X	

Riesgo público	Robos y/o Lesiones personales.	X
Riesgo vial	Accidente vial.	X

Nota. Elaboración propia a partir de GTC45, 2010.

Como se puede apreciar en la tabla anterior, a partir de la matriz de identificación de peligros y valoración de riesgos definida en la GTC45, se identificaron tres factores de riesgo principales con valores importantes a ser considerados en la creación de la pieza audiovisual basada en realidad mixta para la comunicación de factores de riesgo laboral a los trabajadores de industrias extractivas.

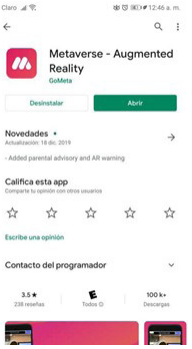
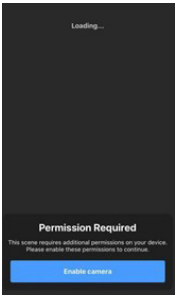
Los resultados de la observación bajo la norma NTC4114 de factores de riesgo en diferentes puestos de trabajo, pero en especial el puesto de trabajo foguista, indican que los principales factores de riesgo identificados son los correspondientes al riesgo biomecánico, físico y biológico. Estos resultados denotan una notable ausencia y deficiencia en el uso de elementos de protección personal (VRS), los cuales son una medida de control importante para evitar accidentes y enfermedades laborales. Los efectos posibles de estos riesgos son: afectación de vías respiratorias por aspiración de material irritante o infeccioso (neumoconiosis o COVID-19), así como los peligros derivados del manejo de cargas (ladrillos, material de construcción, herramientas y material mineral).

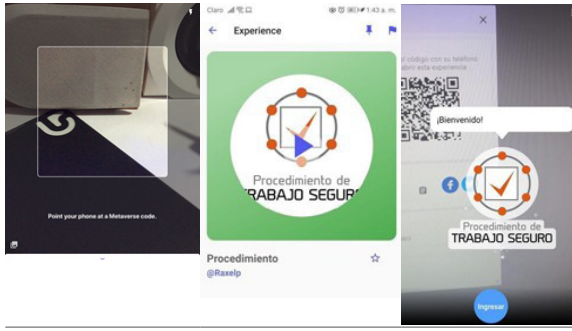
2. Diseño y desarrollo de piezas digitales basadas en realidad mixta para el conocimiento de factores de riesgo laboral

Para el diseño y desarrollo de las piezas digitales se realizó un proceso de diseño digital, teniendo en cuenta los resultados de la aplicación de instrumentos de investigación y lo establecido en la matriz de riesgo GTC45 (tabla 2). Se procede entonces con la etapa de creación de las bases de la narrativa visual necesaria para elaborar las piezas comunicativas sobre los factores de riesgo identificados a los que se ven expuestos los trabajadores de las industrias mineras,clasificados como los de mayor interés para ser trabajados. Para ello, se planteó el desarrollo de los siguientes pasos, presentados de manera resumida en esta ponencia, pero de manera amplia en otros productos de divulgación asociados al proyecto:

1. Desarrollo de *storyline* de las piezas comunicativas a ser organizadas en el programa Metaverse para ser proyectadas con la ayuda de las gafas VR (*Virtual Reality*).
2. Desarrollo de *storyboard* para definición de textos, voz y escenas de las piezas comunicativas.
3. Desarrollo de *wireframe* con los elementos gráficos necesarios para el diseño de las piezas comunicativas.
4. Culminación del proceso con una prueba de intro en la herramienta digital de realidad mixta Metaverse, como se muestra en la siguiente tabla:

Tabla 3. Procedimiento de revisión de piezas en la app Metaverse

		
Descargar la app en Play Store (Android) y App Store (Iphone). Abrir app.	Dar clik donde dice *Scan Code*.	Permitir el acceso a la cámara del *smartphone*.



Dentro del cuadro, enfocar el código QR.	Dar *click* en el icono de *play* para reproducir la experiencia.	Disfrutar del contenido de la realidad aumentada.

En la actualidad, este proceso creativo se encuentra en la etapa de pruebas de piezas piloto con la comunidad de trabajadores informales de industrias extractivas. Las cuales pueden ser observadas en cualquier dispositivo celular smartphone, de gama baja, media o alta, escaneando uno de los siguientes *Quick Response (QR) Codes*:

Figura 1. Códigos QR de las piezas digitales piloto sobre procedimientos de trabajo seguro desarrollados en la app Metaverse. **Fuente:** elaboración propia.

Discusión

Una experiencia divergente y altamente gratificante para el equipo investigador fue tener la posibilidad de realizar procesos multidisciplinarios y aplicar instrumentos de observación en diferentes áreas de conocimiento para atender situaciones que suponen desafíos para el desarrollo y poder aportar, desde la disciplina de comunicación visual, propuestas que ayuden a generar una comunicación directa y diferente. El ejercicio desarrollado en el campo de la Seguridad y Salud en el Trabajo requiere dinámicas comunicativas que fomenten una comprensión de los riesgos laborales para los trabajadores. Igualmente, requiere un cambio en sus hábitos y rutinas de trabajo que, según numerosos estudios y organizaciones multilaterales, ayudan a mitigar factores de riesgo desde la variable más importante de la estación de trabajo: el ser humano.

En un principio, el proyecto proponía una metodología totalmente diferente para realizar procesos de co-creación con los trabajadores informales, que serían la intención inicial. Pero debido a los drásticos cambios que se viven desde marzo en Colombia por la pandemia ocasionada por la covid-19, fue necesario replantear muchos aspectos esenciales del proyecto y luchar por la búsqueda de permisos en los sitios de trabajo para poder aplicar instrumentos de recolección de datos, desarrollar matrices de riesgo y acceder a la población de trabajadores informales y formales de industrias extractivas.

Por último, cabe notar que se pretende abrir la discusión sobre los procesos, procedimientos y técnicas utilizadas en este proyecto para mejorar día a día en el desarrollo de nuevas estrategias para que el diseño expanda su influencia y poder convertirnos en gestores de innovación social, apreciados en los campos de conocimiento por llevar a cabo ejercicios divergentes de frontera.

Limitaciones del estudio

El presente estudio estuvo limitado por las dificultades de acceso al trabajo con la población laboral informal en las industrias extractivas. Estas dificultades son propias del aislamiento preventivo obligatorio ocasionado por la pandemia asociada al covid-19. Por otro lado, los datos solo fueron tomados con base en instrumentos de observación enfocados en la población laboral formal y en inspecciones de puestos de trabajo desarrolladas al interior de las empresas. Ya que no existen, en la actualidad, instrumentos de recolección de datos estandarizados bajo Norma Técnica para estudios de población laboral informal.

Referencias

Bartlett, G. (2001). Systemic Thinking-a simple thinking technique for gaining systemic (situation-wide) focus. Final draft at the International Conference on thinking, "Breaktroughs 2001". Los Angeles, United States.

Bernal Cesar A. (2010). *Metodología de la Investigación.* Bogotá, Colombia: Editorial Pearson.

Cross, R.; Prusak, L. (2002) *The people who make organizations go or stop.* Watertown, Massachusetts: Harvard Business Review.

Departamento Administrativo Nacional de Estadística. (2017). *Principales Indicadores del Mercado Laboral. Mayo de 2017 (COM- 030-PD-001-r004).* Recuperado de https://www.dane.gov.co/

files/investigaciones/boletines/ech/ech/bol_empleo_may_17.pdf

Forrester, J. W. (1991). Systems Dynamics and the Lessons of 35 years. En: De Greene, K. (1991). *The Sistemic basis of Policy making in the 1990s. Sloan School of Management* (pp.1-35). Cambridge, United States: Massachusetts Institute of Technology.

Forum on Public-Private Partnerships for Global Health and Safety, Board on Global Health, Institute of Medicine, National Academies of Sciences, Engineering, and Medicine, (2016). *Approaches to Universal Health Coverage and Occupational Health and Safety for the Informal Workforce in Developing Countries: Workshop Summary.* Washington D.C., United States: National Academies Press.

Gómez, I., Castillo, I., Banquez-, A., Castro, A., y Lara, H. (2012). Condiciones de trabajo y salud de vendedores informales estacionarios del mercado de Bazurto, en Cartagena, *Revista Salud Pública, 14*(3), pp. 448-459. 2012; https://www.scielosp.org/pdf/rsap/v14n3/v14n3a08.pdf

Guataquí, J., García, A. y Rodríguez, M. (2011). El Perfil de la Informalidad Laboral en Colombia. *Serie documentos de trabajo, 16*(95), 91-115.

Gruenfield, D.H., Martorana, P.V., Fen, E.T. (2000). What do groups learn from their Worldliest members?; direct and indirect influence in dynamic teams. *Organizational Behavior and Human Decision Processes, 82*(May), 45-59.

Heller, F., Pusic, E., Strauss, G. & Wilpert, B. (1998). Organizational Participation. Myth and reality. Oxford, Reino Unido: Oxford University Press.

Hernández, A. (1997). *El tejido interactivo de la organización laboral : la dualidad formal-informal.* La Habana, Cuba: Centro de Investigaciones Psicológicas y Sociológicas (CIPS).

Ibáñez, J. (1.998) *El regreso del sujeto; la investigación social de 2do orden.* Ciudad de México, México: Siglo XXI Editores.

Lamertz, K. (2002). The social construction of fairness: social influence and sense making in organizations. *J. Organiz. Behav.*, 1(23), 19–37. doi:10.1002/job.128

Ley 1438 de 2011. Por la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones. 19 de Enero de 2011.D.O. No. 47957.

Ocampo, J. y Garzon, M. (2016). El sistema de riesgos laborales frente al trabajador del sector informal. *Opinión Jurídica, 15*(30), pp.183-204.

Organización Internacional del Trabajo, (2020). *Agenda 2030 de Desarrollo Sostenible.* ODS 8:Trabajo Decente y Crecimiento Económico. http://www.ilo.org/global/topics/sdg-2030/goal-8/lang--es/index.htm

Organización Internacional del Trabajo, (s.f.). *Estrategias de Desarrollo Local.* Sitio web de la Organización Internacional del Trabajo. http://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_policy/documents/publication/wcms_229866.pdf

Organización Internacional del Trabajo,– (2014). La transición de la economía informal a la economía formal. Conferencia en Conferencia Internacional del Trabajo 103.ª reunión 2014. Ginebra, Suiza.

Organización Internacional del Trabajo, (2015, 23 de marzo). *La economía informal, una actividad peligrosa.* OIT-ILO website. http://www.ilo.org/safework/areasofwork/hazardous-work/WCMS_356541/lang--es/index.htm

Parque Científico de Innovación Social de Uniminuto. (2018) *Innovación Social.* Sitio web de Uniminuto. https://www.uniminuto.edu/web/pcis/innovacion-Social

Puello-Socarrás, G., & Vargas Puentes, L. (2019). Salud Ocupacional y su enfoque social dentro de trabajos de grado en universidades de Bogotá. *Educación Médica Superior, 33*(1), 1-21.

Puerto, A., Torres, P., Roa, F., y Hernández, J. (2016). Modo de Vida de un grupo de trabajadores informales en Corabastos. *Revista Facultad Nacional de Salud Pública, 34*(1), 80-87. doi: 10.17533/udea.rfnsp.v34n1a10.

Rahman, M. y Borda, F.(1991) Acción y conocimiento: Rompiendo el monopolio con la IAP. *Revista Análisis Político*, (5), 46-55.

Restrepo, H., Vásquez, E., Soto, M., Yepes, J., Orozco, S. y Saldarriaga, K. (2008). *Diagnóstico nacional de*

condiciones de salud y trabajo de las personas ocupadas en el sector informal de la economía.Medellín, Colombia: Universidad de Antioquia y Ministerio de Protección Social.

Rojas, L. F. (2012). Estudio de Riesgos en el Trabajo en una Comunidad del Sector Informal de Bogotá (Tesis de maestría). Pontificia Universidad Javeriana, Bogotá.

Romero, J. y Farinos, J. (2011). Redescubriendo la gobernanza más allá del buen gobierno. Democracia como base, desarrollo territorial como resultado. *Boletín de la Asociación de Geógrafos Españoles, 56*(2011), 295-319.

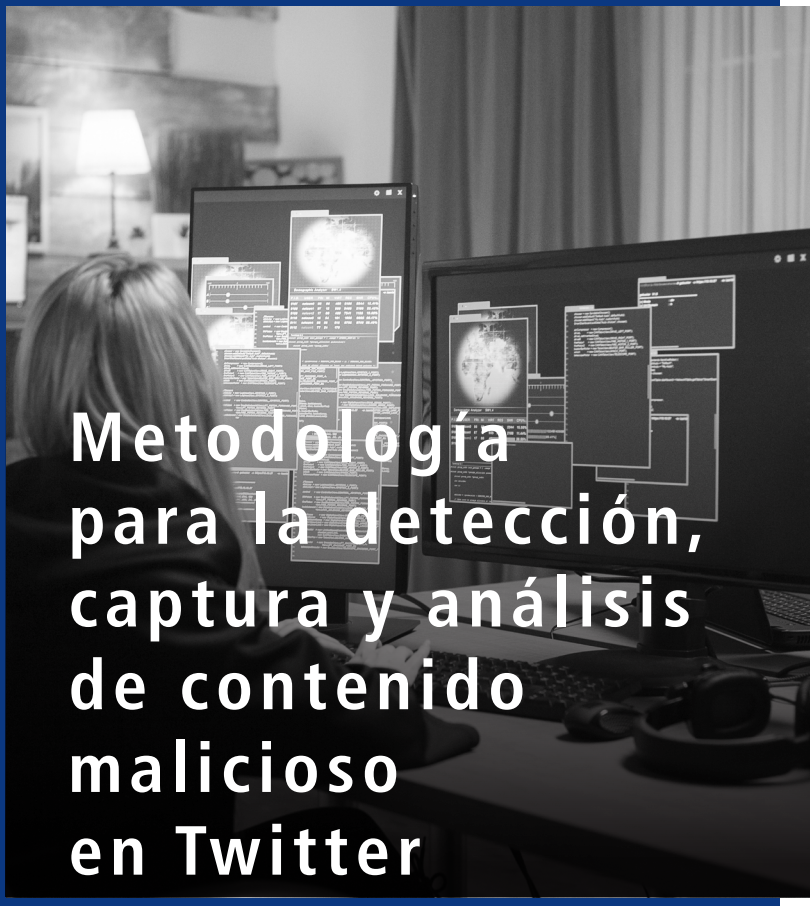
Sachs, J., Jeffrey, D., Schmidt-Traub, G., Kruk, M., Bahadur, C., Faye, M. & McCord, G. (2004). Ending Africa's Poverty Trap. *Economic Activity, Columbia University and UN Millenium Project, 1*(pp. 117-240).

Schneider, F. y Enste, D. (2002). Ocultándose en las sombras El crecimiento de la economía subterránea. En *Temas de Economía 30* (pp.1-26) Washington D.C., Estados Unidos: International Monetary Fund Publication Services.

Thaler, R. & Sunstein, C. (2008). *Nudge: improving decisions about health, wealth and happiness.* New Haven, United States: Yale University Press.

Viveros, A. y Salazar, V. (2013). Condiciones de salud y trabajo de la población informal que labora en las galerías del municipio de Popayán. *Revista Cubana de Salud y Trabajo, 14*(3), 11-23. http://bvs.sld.cu/revistas/rst/vol14_3_13/rst02313.htm

Weigo, (2012, Junio). *Salud y Seguridad Ocupacional para los trabajadores informales.* WEIGO. http://www.wiego.org/sites/default/files/resources/files/OHS_Newsletter_Junio_2012_Espanol.pdf



Metodología para la detección, captura y análisis de contenido malicioso en Twitter

Misael Fernando Perilla Benítez[a]

a Universidad Nacional de Colombia. Bogotá, Colombia. Correo electrónico: mperillab@unal.edu.co

Resumen: Dentro de las redes sociales más comunes, como Twitter, se han incrementado los casos de ciberataques que atentan contra la seguridad de la información. Para los usuarios de las empresas que utilizan estas plataformas para comercializar productos y servicios, contactar clientes y realizar campañas de marketing, este tipo de ciberdelitos se han incrementado tanto en cantidad como en dificultad para su detección. Muchos de estos sitios web maliciosos han sido creados bajo protocolos estándar con caracteres especiales de lenguaje internacional que facilitan generar portales web visualmente similares a los legítimos. Para la detección de estas amenazas, se diseñó una metodología de selección de publicaciones en Twitter mediante una API de desarrollador. Realizando así un proceso de recolección de información

mediante una “bolsa de palabras” con el objetivo de generar un conjunto de datos para su posterior estudio y evaluación de caracteres especiales, signos, iconos, emojis y emoticones en el mensaje conocido como tweet. También, se buscó establecer la presencia de una URL, recortada por servicios externos e internos de Twitter, en un cuerpo característico del mensaje que permite realizar un proceso de recuperación de la URL original para su posterior análisis. Asimismo, también permite que los datos obtenidos de la cuenta que pública o responde un *tweet*, tales como edad, cantidad de seguidores, favoritos y otros, faciliten, de manera automática, la detección de contenido potencialmente peligroso.

Palabras clave: análisis, contenido malicioso, detección, metodología, twitter.

Introducción

El *phishing* es definido por el Anti-Phishing Working Group (APWG) como "un crimen que implementa tácticas de ingeniería social y engaño para robar datos de identificación personal y financieros" (2020, p.2). En este tipo de ataque se crean sitios web falsos que visualmente suelen ser bastante similares a los sitios legítimos de empresas, bancos o entidades reconocidas como Amazon, Google, y Netflix o, localmente, Bancolombia, Davivienda y el Fondo Nacional del Ahorro. De acuerdo con reportes presentados por grupos *antiscam* y *antiphishing*, los ataques de fraude o engaño usando redes sociales como Twitter se han incrementado en los últimos años, buscando comprometer las cuentas de correo empresariales y/o corporativas

mediante contenidos de sitios web ficticios, instalación de *malware* y estrategias de ingeniería social para el robo de información.

El procedimiento del *phishing* consiste en enviar previamente mensajes por correo electrónico, mensajes de texto o a través de las redes sociales con contenidos que buscan atraer a la potencial víctima para que ingrese a la dirección web (URL) señalada. De tal manera que, mediante variadas estrategias de engaño, ingrese datos sensibles como el número de identificación e información personal en campos tipo formulario; los cuales son capturados por los ciberatacantes para, posteriormente, ser usados en diversos tipos de delitos.

Como lo señalan Oest *et al.* (2019), en la actualidad, la medida más eficiente para la detección de sitios de *phishing* es el uso de las listas negras donde los navegadores web utilizan servicios como los ofrecidos por Google Safe Browsing, Microsoft SmartScreen o Phishtank por mencionar algunos. Estos son implementados como repositorios donde las direcciones web son comparadas con las registradas. La detección depende de los reportes que la comunidad de usuarios haga al encontrar e identificar estos sitios maliciosos. Por lo que, en muchos casos, un nuevo sitio web para campañas de *phishing* puede tardar un tiempo considerable para ser denunciado y bloqueado. Adicionalmente, los ataques y las tácticas usadas por los cibercriminales cambian de acuerdo a las nuevas medidas que existen tanto a nivel tecnológico como a nivel personal.

No obstante, como lo indica Check Point en su informe, gracias a la capacitación del personal en la identificación de mensajes o direcciones web potencialmente peligrosas, las cuentas de correo electrónico "son el vector de ataque predilecto, los malos actores están usando una variedad de trucos para obtener información sensible, incrementando el *phishing* involucrando mensajes de texto SMS usando mensajería de redes sociales y plataformas de videojuegos" (2020, p. 15). Un ejemplo al respecto es el envío de mensajes engañosos mediante cadenas en WhatsApp como se muestra en la figura 1. En esta se puede apreciar el uso de palabras en mayúscula y un enlace a un sitio web con protocolo TLS/SSL, que se interpreta como un sitio seguro por un navegador.

Figura 1. Ejemplo de mensaje con contenido de *phishing* en WhatsApp.
Fuente: elaboración propia.

Los ataques y campañas de *phishing* evolucionan y se adaptan a las diferentes contramedidas que las organizaciones crean. En ese sentido, las medidas que se implementan van quedando rezagadas frente a las nuevas acciones y métodos de engaño, como el ocultamiento de caracteres en nombre de dominio internacionales, reemplazando caracteres como la n por la letra b (con valor en Unicode 0042) por una similar como la letra b en cirílico (con valor en Unicode de 0412) o la n (Unicode 006E) por la letra n del hebreo (Unicode 0578). Sumado a lo anterior, muchos de los sitios web maliciosos son lanzados en hostings con HTTPS como se muestra en los datos reportados desde el año 2015 por APWG: "para el final del 2019 el 74% de todos los sitios de *phishing* usaban los protocolos TLS/SSL" (Anti-Phishing Working Group, 2020, p. 3). Mostrando así, el incremento de casos llegado al segundo cuartil del 2020 a un valor cercano al 80% (Anti-Phishing Working Group, 2020).

Las amenazas anteriormente expuestas se unifican con otra serie de prácticas para generar un mayor impacto y engaño en los usuarios de redes sociales; como el uso de mensajes o contenidos en Twitter con emojis, palabras o frases que son recurrentes en diferentes mensajes fraudulentos. El enmascaramiento de las URL mediante servicios de acortamiento de las direcciones web (URL *Shorters*), así como las estrategias propias para confundir y engañar usuarios, buscan que los usuarios, incluso aquellos que apliquen buenas prácticas como utilizar aplicaciones oficiales, contar con software

de seguridad entre otras como las mencionadas por Shahriar *et al.* (2015), sean ineficientes.

En este documento se presenta una metodología diseñada para la identificación temprana y automática de potenciales sitios web maliciosos publicados en la red social Twitter basándose en los contenidos de los mensajes, el análisis de la dirección web posterior al proceso de recuperación de la URL original o no acortada (URL *unshorting*), junto con valores propios de la cuenta que postea el contenido.

Con base a todo lo expuesto, se crea una metodología que permite dar solución a las múltiples necesidades de seguridad existentes para los usuarios de la red social Twitter en los equipos de cómputo y/o dispositivos móviles a los que acceden y con los que interactúan. Especialmente en los dispositivos en los que es habitual que, por el tamaño reducido de la pantalla, no es posible ver las direcciones web (URL) por su longitud o por las diferentes estrategias implementadas para que sea difícil identificarlas como no legítimas. Esto conlleva a la falta de soluciones que funcionen de manera efectiva en dispositivos móviles. Junto a las reducidas capacidades de procesamiento en estos últimos, se origina que existan limitadas opciones de protección. A lo cual se debe sumar los hábitos y conocimientos que se ven limitados en los usuarios de redes sociales para la detección de sitios de *phishing*, facilitando el trabajo a los atacantes (Baadel *et al.*, 2019).

Desarrollo

Durante el desarrollo de un sistema para la detección automática de *phishing* en Twitter mediante la implementación de modelos de aprendizaje automático, se inició utilizando la metodología expuesta por Dann (2015). Pero, esta demostró limitaciones frente a las nuevas amenazas y estrategias utilizadas por los cibercriminales, así como frente a los cambios que la plataforma de Twitter ha sufrido con el paso de los años. Esto junto con las tendencias en el desarrollo de campañas de *phishing* y *scam*, llevan a plantear una metodología compuesta por ocho fases generadas con el objetivo de capturar datos de Twitter de una manera más precisa y eficiente. Facilitando el análisis de la información obtenida y la detección de contenidos potencialmente peligrosos.

El propósito de la metodología propuesta en la figura 2 es generar un marco de trabajo común para las empresas, organizaciones e investigadores que deseen iniciar o mejorar sus propios desarrollos de soluciones para combatir las amenazas a la integridad, disponibilidad y confidencialidad de los datos e información de usuarios en la red social Twitter, con el objetivo de detectar amenazas basadas en el engaño y robo, como ocurre en ataques de *phishing*.

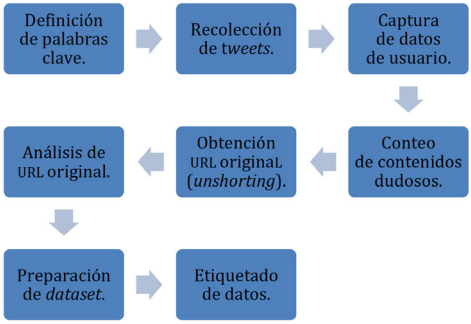


Figura 2. Metodología Propuesta para la detección de contenidos maliciosos en Twitter.
Fuente: elaboración propia.

La metodología está compuesta por ocho fases, cada una de ellas generada para ser implementada en diferentes plataformas y lenguajes de programación. A continuación, se utilizarán herramientas y librerías para Python. Sin embargo, se pueden seguir las mismas fases buscando sus equivalentes en otros contextos.

Fase 1. Definición de palabras clave

Para la recolección de los mensajes en Twitter conocidos como tweets, se deben considerar que los mensajes que buscan atraer víctimas suelen contener palabras de connotación positiva e invitan a que los usuarios crean que se les está dando una oportunidad para ganar o recibir un beneficio. En este sentido, se buscan publicaciones que contengan palabras que haga atribución a premios, descuentos y obtener objetos o servicios que son de pago de manera gratuita.

Esta fase se encuentra inspirada en el concepto de la bolsa de palabras (*bag of words*). Según este, dependiendo del contexto y el objetivo de estudio, se seleccionan palabras relacionadas o conjuntos de ellas que puedan ser usadas dentro de los contenidos de una campaña de *phishing*. Un ejemplo puede ser el caso del *phishing* con la temática de la pandemia por el COVID-19, donde se encontraron mensajes a través de Whatsapp, correos electrónicos y redes sociales como Facebook donde se promocionan cuentas "gratis" de Netflix durante la cuarentena, obtener ayudas como mercados o apoyos económicos de parte de empresas o el Gobierno (Lubeck, 2020), e, incluso, suplantan a la Organización Mundial de la Salud (OMS) con falsos consejos, mecanismos de diagnóstico y alternativas naturales para prevenir, combatir o curar la enfermedad (World Health Organization, 2020).

En la tabla 1 se pueden identificar las palabras o combinaciones de palabras más frecuentes utilizadas en

campañas de *phishing* en Twitter. Estas palabras llevan el conector más (+) para indicar que se desea capturar mensajes que incluyan dichas palabras junto a las previamente señaladas. Mientras que el símbolo (-) se usa para indicar que se desean capturar mensajes donde las palabras con este símbolo no deben estar presentes.

Tabla 1. Bolsa de palabras clave más comunes para campañas de phishing general y relacionadas con el COVID-19

Palabras comunes	Palabras con temática de COVID-19
Precio	Covid+vacuna
Info o información	Covid+cura
Descuento	Coronavirus+cura
Premio	Covid+inmunidad
Oferta	Coronavirus+vacuna
Ganar	Covid+mercado
Crédito	Covid+donar o donación
Gratis	Covid+ayuda o ayudas
Invertir	Covid+detección o diagnóstico

Fase 2. Recolección de tweets

Una vez que se ha definido la bolsa de palabras a utilizar, se deben usar herramientas de software para la captura mediante el API de desarrollador ofrecida por Twitter para acceder a los mensajes y los métodos de búsqueda.

Para desarrollar esta tarea, existen variadas alternativas de software, tanto pagas como gratuitas. Dentro de las más conocidas y con mejores opciones se encuentran las librerías de Python, como TweePy (disponible en http://docs.tweepy.org/en/latest/) y TwitterSearch (disponible en https://pypi.org/project/TwitterSearch/), las cuales requieren de la creación de una cuenta de desarrollador en Twitter para poder utilizar los datos de consumo (*consume_key, consume_secret*) y los de acceso (*access_token, access_token_secret*) como se muestra en la figura 3.

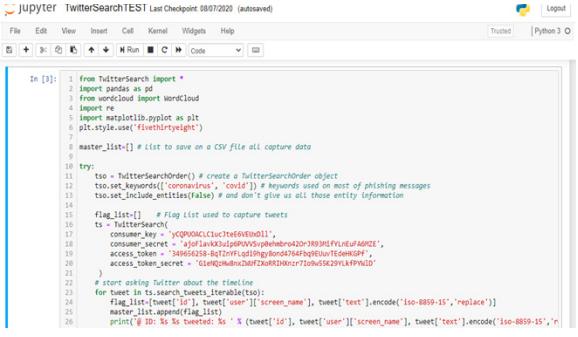


Figura 3. Uso de la librería TwitterSearch con lenguaje Python y palabras clave para búsqueda de tweets relacionados con el COVID-19.
Fuente: elaboración propia.

Una alternativa que no requiere de estas credenciales o la creación de cuentas de desarrollador es Mozdeh. Esta ha sido implementada en muchos proyectos de *big data* y análisis de sentimientos de datos obtenidos no solo en Twitter, sino también de otros medios sociales como Facebook o YouTube (Mozdeh, 2020).

Una vez elegida la herramienta a utilizar, se instala o configura para iniciar la búsqueda y captura de tweets usando las palabras clave que se han definido previamente. Dependiendo de la herramienta, se debe indicar qué datos se desean extraer. Para lo cual se debe conocer la estructura de los tweets que son objetos bajo estructuras JSON y el uso de las entidades existentes como son los medios (imágenes, URLS, hashtags, entre otros). Para el caso de Mozdeh, esta herramienta extrae por defecto quince elementos: AuthorName, AuthorURL, *content (Blank)*, EntryID, FavoriteCount, *geo, label, language, published,* retweets, *source,* tweet *(Title)*, timezone, UserFollowersCount y UserStatusesCount. En el caso de herramientas como TweePy y TwitterSearch, se deben elegir usando la estructura y el tipo de acceso que provea la cuenta de desarrollador, donde los datos permitidos en cuentas gratuitas son limitados a máximo treinta días atrás y solo dos niveles de profundidad en la estructura JSON. Esto indica que para obtener mejores resultados se debe pagar.

Independientemente de la herramienta utilizada, los datos mayormente útiles para el análisis son: AuthorName (nombre expuesto en Twitter del usuario que publicó

el mensaje, puede contener caracteres especiales o emojis), EntryID (identificación única del tweet), FavoriteCount (cantidad de usuarios que han indicado que les gustó la publicación), retweets (cantidad de veces que el *tweet* ha sido compartido), *source* (si fue publicado desde Android, iOS, web u otros servicios), tweet *(Title)* (mensaje completo publicado), UserFollowersCount (cantidad de usuarios que siguen a la cuenta que publicó el mensaje) y UserStatusesCount (cantidad de tweets o publicaciones de la cuenta desde que se creó).

Finalmente, se debe utilizar el campo de EntryID para filtrar y eliminar tweets repetidos pues dentro de las búsquedas es posible que los retweets en fechas posteriores sean capturados, generando ruido en los datos y duplicidad en los mismos.

Fase 3. Captura de datos de usuarios

Una vez se tienen los datos recolectados con la herramienta, se procede a las validaciones donde el contenido se analiza. El primer elemento por considerar es la presencia de una URL en el mensaje. Esta dirección se realiza mediante el uso de expresiones regulares en el texto. Para el caso de Python, se usa la librería Regular Expressions (RE), tal como se observa en la figura 4.

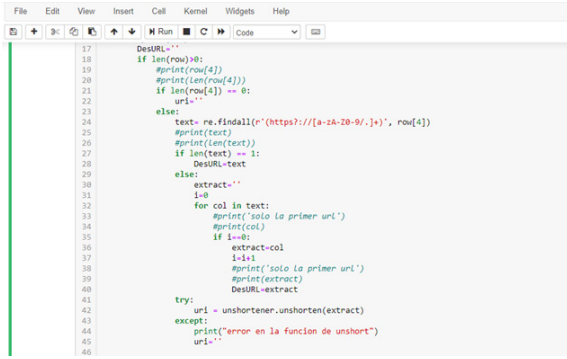


Figura 4. Importación y uso de las librerías Regular Expressions (RE) y UnshortenIt en Jupyter Notebook para detectar direcciones web en mensajes de Twitter y extraer la URL original del mensaje. **Fuente:** elaboración propia.

La expresión regular debe ser usada para buscar en el campo donde se encuentra el texto del tweet capturado. Luego, el mensaje junto con la URL separada se almacenan en una estructura interna; una matriz, un dataframe, como los de la librería Pandas, o, directamente, un archivo de texto plano como .txt o .csv. Esto dependiendo del tamaño final de los datos y la capacidad de almacenamiento existente. En este caso, se recomienda usar los archivos de texto plano para realizar la trazabilidad de los datos, así como implementarlos en diferentes herramientas a posteriori.

Fase 4. Conteo de caracteres dudosos

Del contenido presente en el cuerpo del tweet que se ha extraído en la fase 1, se procede a extraer contenidos que delatan los intentos de atraer la atención de las potenciales víctimas. Tomando en cuenta caracteres especiales (¡¡!!, ¿?,), letras en mayúscula, utilizadas para dar mayor interés, y emojis; por ejemplo: cara feliz, aplauso, entre otros que son extraídos y contados. Para la extracción y conteo de los caracteres especiales se usan expresiones regulares, mientras que para la extracción y conteo de los emojis se usan listas que contienen elementos en formato Unicode. En cuanto al proceso de comparación, se realiza a través de la función match de los objetos de tipo expresión regular (re), como se muestra en la figura 5.

Figura 5. Captura de emojis con expresiones regulares y listas en Jupyter Notebook.
Fuente: elaboración propia.

Los emojis deben ser ingresados en una lista para su validación mediante expresiones regulares. Un ejemplo de una lista de este tipo de emoticones se encuentra disponible en https://unicode.org/emoji/charts/full-emoji-list.

html. También, es importante utilizar listados que cuenten con códigos Unicode para que puedan ser usados dentro del código fuente de las herramientas.

Fase 5. Obtención de URLs originales

Dentro de Twitter existe un límite de 280 caracteres para la redacción de los mensajes. Por ello, se recurre a servicios acortadores de direcciones web conocidos como URL *Shorteners* (acortadores de URL) que, en el caso de los cibercriminales, se usan no solo con este propósito, sino también como medio para enmascarar o esconder el sitio web malicioso. Los servicios de acortamiento más conocidos son https://bitly.com/, https://tiny.cc/ o https://cutt.ly/. Aunque Twitter utiliza de manera automática un servicio propio conocido como http://t.co. El cual dada una dirección web la acorta de manera automática. Por esto es importante obtener la dirección original que es utilizada en el mensaje y para ello existen varias librerías. La más utilizada y versátil en lenguaje Python es UnshortenIt, como aparece en la figura 6 (disponible en https://pypi.org/project/unshortenit/). A diferencia de otras opciones como Urlparse (nativa de Python 3.x) o Urlunshort (disponible en https://pypi.org/project/urlunshort/), esta es fácil de instalar y usar, además de soportar la mayoría de servicios acortadores existentes actualmente, incluyendo el https://t.co de Twitter.

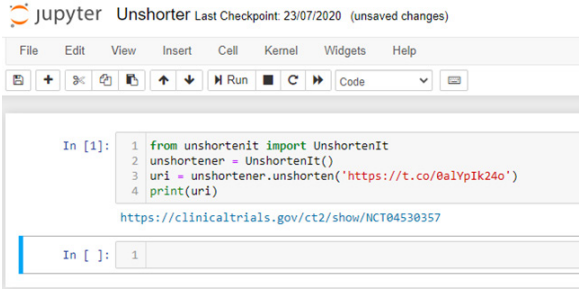


Figura 6. Uso de librería *UnshortenIt* 1.0.2 en Jupyter Notebook con dirección https://t.co para obtener URL original.
Fuente: elaboración propia.

Fase 6. Análisis de URLs originales

Para descubrir si la URL desenmascarada (*unshorted* u original como se le llama en este documento) es potencialmente peligrosa, se pueden realizar dos procesos. El primero es utilizar servicios como el de la API de Phishtank o Google Safe Browsing para buscar la URL en sus registros. La limitante es que solo funciona si el sitio ha sido previamente reportado. El segundo es realizar un análisis de la dirección mediante técnicas que buscan comparar patrones y elementos dentro de esta dirección que son comunes en sitios web fraudulentos.

Estos métodos se encuentran relacionados con otros en lo que también se realiza la búsqueda y conteo de caracteres pertenecientes a alfabetos poco comunes (hebreo, cirílico, armenio, etc.), para mejorar el enmascaramiento de sitios web maliciosos, como es el caso

de los ataques de tipo IDN (*Internacionalized Domain Names*) holográficos (Thao, 2020). Asimismo, en la presencia de extensiones de archivos como *.html, .php, .aspx*, entre otros, la verificación del sitio para comprobar si es HTTP o HTTPS y otros recuentos de los contenidos está ampliado en la figura 7. Cada uno de los recuentos depende del tipo de contenido que se analiza. En algunos casos, se realiza mediante la función *count* de listas; como en el caso de contar una cantidad de caracteres o medir la longitud de las comparaciones encontradas en el contenido mediante la función *findall* de expresiones regulares. Para la validación de palabras sospechosas, estas son definidas y almacenadas en una lista para, posteriormente, usar expresiones regulares y que estas sean buscadas dentro de la URL.

La búsqueda de palabra sospechosas dentro de la URL es importante puesto que muchos de los ataques de *phishing* suelen usar nombres de grandes empresas como Apple, Google y Microsoft o también de servicios como Netflix y Dropbox como se puede ver en la figura 7. Por esta razón, este listado puede ser alimentado de la lista de palabras generada en la fase 1 con el propósito de obtener una URL potencialmente maliciosa y extraer de esta última las características de la tabla 2.

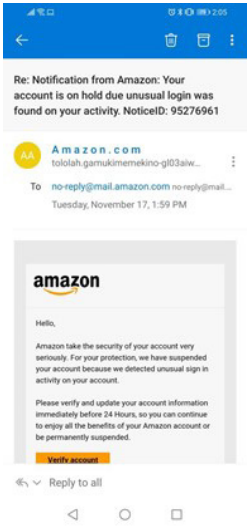


Figura 7. Ejemplo de correo con contenido malicioso referente a Amazon en e-mail asociado a cuenta de Twitter.
Fuente: elaboración propia.

```
    if len(row) > 0 :
        b=[row,#Analized_URL
            row.count('.'), #DotsCount
            row.count('/'), #SlashCount
            row.count('&'), #AmpersandCount
            row.count('='), #EqualCount
            row.count('?'), #IncognitCount
            row.count('-'), #DashCount
            row.count('@'), #AtCount
            row.count('~'), #TildeCount
            row.count('%'), #PercentCount
            row.count('#'), #NumCount
            row.count('_'), #UnderlineCount
            row.count('//'), #DoubleSlachCount
            row.count(':'), #DoubleDotCount
            row.count('('), #OpenParenthesisCount
            row.count(')'), #CloseParenthesisCount
            row.count('<'), #OpenAngleBrackets1Count
            row.count('>'), #CloseAngleBrackets1Count
            len(row), #URLLenght
            len(re.findall(r"[jJ]ava\S+", str(row))), #JavaScript_Functions >>>> 'file' 'html_tags' 'suspicious_words
            #len(re.findall(Suspicious, row)), #JavaScript_Functions >>>> 'file' 'html_tags' 'suspicious_words
            row.count('http'), #HTTP_Site
            row.count('https'), #HTTPS_Site
            len(re.findall('.html', str(row))), #HTML_Extension
            len(re.findall('.php', str(row))), #PHP_Extension
            len(re.findall('.htm', str(row))), #HTM_Extension
            len(re.findall('.net', str(row))), #NET_Extension
            len(re.findall('.js', str(row))),#JS_Extension
            len(re.findall('.asp', str(row))),#ASP_Extension
            len(re.findall('.aspx', str(row))),#ASPX_Extension
            len(''.join(re.findall('\d+', str(row))))#NumbersOnURL
```

Figura 8. Conteo de elementos sensibles en direcciones URL.
Fuente: elaboración propia.

Tabla 2. Listado de caracteres, extensiones y valores sensibles buscados y contados en URL.

Carácter	Nombre	Carácter	Nombre	Carácter	Nombre
.	Cantidad de puntos	&	Cantidad de ampersand	?	Cantidad de incógnitas
/	Cantidad de slash	=	Cantidad de iguales	-	Cantidad de signos menos
%	Cantidad de numerales	@	Cantidad de arrobas	~	Cantidad de virgulilla
#	Cantidad de numeral	_	Cantidad de barra al piso	//	Cantidad de doble slash
:	Cantidad de punto doble	(	Cantidad de abrir paréntesis	)	Cantidad de cerrar paréntesis

<	Cantidad de abrir llaves de ángulo	>	Cantidad de cerrar llaves de ángulo	'http'	Existencia de sitio HTTP (binario)
'https'	Existencia de sitio HTTP (binario)	'.html'	Existencia de extensión HTTP (binario)	'.php'	Existencia de extensión HTTP (binario)
'.htm'	Existencia de extensión HTM (binario)	'.net'	Existencia de dominio .net (binario)	'.js'	Existencia de extensión JavaScript (binario)
'.asp'	Existencia de extensión ASP (binario)	'.aspx'	Existencia de extensión ASPX (binario)	'.xyz'	Existencia de dominio .xyz (binario)

Numbers	Cantidad de números en URL	Capital	Cantidad de letras en mayúscula en URL	Suspicious	Cantidad de palabras sospechosas en URL

Fase 7. Preparación del *dataset*

Las fases anteriores entregan un conjunto de datos que contienen las cuentas de usuario, conteo de palabras y/o caracteres en los mensajes y conteo de caracteres, palabras y extensiones en las URL publicadas. Estos datos deben ser normalizados y estandarizados para evitar que información con valores que estén fuera de rango o en escalas diferentes afecten el entrenamiento de los modelos.

Mediante el proceso establecido en esta metodología se enumeran un total de cuarenta y dos características para la construcción de un conjunto de datos (*dataset*), el cual está compuesto por:

- Ocho características del mensaje o tweet: cantidad de caracteres especiales, cantidad de caracteres holográficos y cantidad de emojis, conteo de favoritos, ID del tweet o mensaje, origen de publicación (*source*) y retweets.
- Tres características de la cuenta de usuario: AuthorName, *UserFollowersCount y UserStatusesCount.*

- Treinta y una características extraídas de la URL original: expuestos en la tabla 2, donde algunas como puntos (.) o ampersand (&) son contadas, mientras que otras como "http" o ".net" son de tipo binario (0 si no están presentes y 1 si lo están en la dirección analizada).

Las características que contienen palabras, como por ejemplo *suspisious*, deben ser tokenizadas previamente al proceso de entrenamiento y análisis de los modelos de aprendizaje automático o de aprendizaje profundo. En este caso, se utilizó la librería NLTK, la cual es una de las más conocidas y utilizadas en proyectos de inteligencia artificial.

Fase 8. Etiquetado de datos

Finalmente, se realiza el etiquetado de los datos para que este sea implementado en herramientas de *big data*, analizadores de sentimientos o para entrenar modelos de inteligencia artificial como el aprendizaje automático o modelos de aprendizaje profundo que, según Singh & Meenu (2020), aprenden las características de sitios web para *phishing.* Además de predecir nuevas características, existiendo muchos algoritmos como Naïve-Bayes, árboles de decisión, *Support Vector Machine, Random Forest,* redes neuronales artificiales, redes neuronales convolucionales, K-Nearest Neighbor, cada uno con una diferentes variaciones y niveles de precisión que son utilizados para la clasificación de *phishing.*

Resultados

Como resultados de la aplicación de esta metodología, después de capturar datos durante los meses de diciembre de 2019, enero y febrero de 2020, se generó un conjunto final de 64.535 datos, usando las palabras clave generales de la tabla 1. En este proceso se recolectaron más de un millón de mensajes, los cuales fueron depurados mediante la presente metodología para permitir ahorrar tiempo y estandarizar el proceso en futuros proyectos.

Se concluyó que la captura y análisis de los mensajes se debe realizar de manera constante y en un ciclo definido de manera periódica. Esto se debe a que muchos de los sitios web maliciosos estarán fuera de línea después de un tiempo, sea porque son reportados o porque los atacantes ya cumplieron su cometido y los dan de baja. Lo anterior es el motivo principal del desarrollo de la presente metodología. El objetivo es que las personas y entidades que deseen

implementar medidas para detectar y generar defensas frente a potenciales ataques de *phishing* partan de un proceso definido y claro que les permita ahorrar tiempo y generar mejores resultados, tanto en el análisis como en el posterior uso de los datos.

Las dos fases que más toman tiempo son la primera segunda (recolección de tweets) y la quinta (*unshortening* de URL). Pues las dos dependen de conexiones externas para el consumo de APIS, el tiempo de consulta-respuesta de servidores y la velocidad de conexión a Internet. Además de verse interrumpidas frente a cortes eléctricos, fallos del hardware local y problemas de red. Por lo tanto, se recomienda que estas fases sean realizadas mediante servicios de computación en la nube como Azure o que tengan muchas menos probabilidades de ser afectadas por estas amenazas.

A pesar de tener algunas limitaciones, el uso de software libre, como el lenguaje Python y la plataforma Jupyter Notebook, junto con otras alternativas, mediante el proceso señalado y la recolección adecuada de datos, permite realizar un análisis apropiado para generar sistemas de detección temprana de ataques de *phishing*. Asimismo, tal como afirma Márquez (2020), no limita a este tipo de crímenes digitales, siendo útil también para la detección de intentos de spam, *ransomware* y, en general, el uso de la ingeniería social.

Referencias

Anti-Phishing Working Group. (2020). *Phishing Activity Trends Report 4th Quarter 2019*. Recovered from https://apwg.org/

Anti-Phishing Working Group. (2020). *Phishing Activity Trends Report Q2 2020*. Recovered from https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

Baadel, S., Thabtah, F., & Majeed, A. (2019). Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users. Conference in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference*. Vancouver, Canada.

Heck Point. (2020). *Cyber Security Report 2020*. Recovered from doi: https://doi.org/10.9785/ag-2019-641919

Dann, S. (2015). Twitter Data Acquisition and Analysis: Methodology and Best Practice. *Advances in Marketing, Customer Relationship Management, and E-Services (AMCRMES) 1*(November), 280–296. doi: https://doi.org/10.4018/978-1-4666-8408-9.ch012

Lubeck, L. (2020). *Nuevas campañas de phishing vía WhatsApp que utilizan el COVID-19 como excusa*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/03/26/phishing-whatsapp-utilizan-covid-19-excusa/

Mozdeh. (2020). *Mozdeh Big Data Text Analysis*. Recovered from http://mozdeh.wlv.ac.uk/

Oest, A., Safaei, Y., Doupe, A., Ahn, G. J., Wardman, B., & Tyers, K. (2019). PhishFarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. *Proceedings - IEEE Symposium on Security and Privacy, 2019*(May), 1344–1361. doi: https://doi.org/10.1109/SP.2019.00049

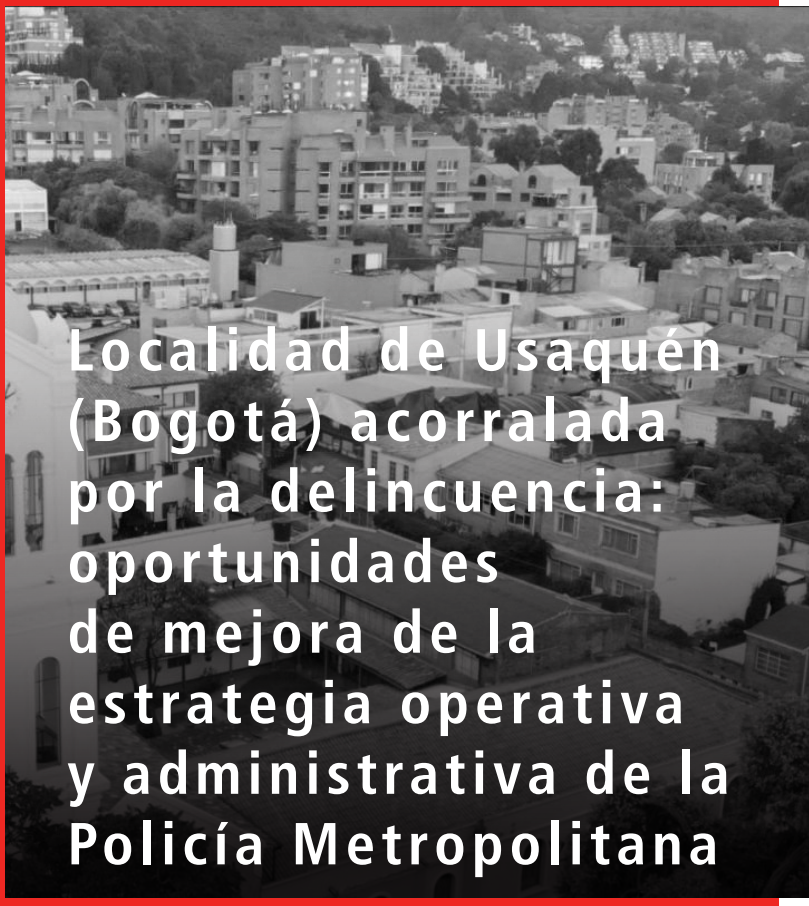
Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile Phishing Attacks and Mitigation Techniques. *Journal*

of Information Security, 06(03), 206–212. doi: https://doi.org/10.4236/jis.2015.63021

Singh, C., & Meenu. (2020). Phishing Website Detection Based on Machine Learning: A Survey *2020*. Conference in 6th International Conference on Advanced Computing and Communication Systems. *CACCS 2020*, 398–404. Tamil Nadu, India. doi: https://doi.org/10.1109/ICACCS48705.2020.9074400

Thao, T. P. (2020, september 17th). *Beware of criminals pretending to be WHO*. World HealthOrganization website. https://www.who.int/about/communications/cyber-security

Thao, T. P. (2020, september 17th). *Improving Homograph Attack Classification.* World Health Organization website. http://arxiv.org/abs/2009.08006



Localidad de Usaquén (Bogotá) acorralada por la delincuencia: oportunidades de mejora de la estrategia operativa y administrativa de la Policía Metropolitana

Juan Diego Fonseca Betancourt[a]

a Universidad Militar Nueva Granada. Bogotá, Colombia.
Correo electrónico: est.juand.fonseca@unimilitar.edu.co

Introducción

Desde inicios del siglo XXI, se ha planteado que la mejor estrategia en todos los campos siempre ha sido el trabajo armónico y conjunto entre las autoridades y la sociedad. Esto permite el logro de objetivos con mayor rapidez y con un mayor beneficio común (Bonett, 2006). En general, la estrategia de participación conjunta debe darse en todo tipo de organizaciones. Principalmente, en las organizaciones sociales (Bonett, 2006) que agrupan a importantes sectores de la ciudadanía. Esto implica que dentro de las organizaciones empresariales también es de suma importancia que siempre haya un trabajo coordinado entre los ciudadanos pertenecientes a ellas y las autoridades. Es por esto que el MNVCC articula esta estrategia acercándose a la comunidad y a la sociedad

civil con el único propósito de mejorar la convivencia y seguridad ciudadana. Lo que conlleva, directamente, a contrarrestar delitos como el hurto a personas.

Basados en el Modelo de Sistema Viable (MSV), las estrategias planteadas para mejorar la seguridad no deben ser vistas finales o definitivas porque la evolución de la violencia plantea revisiones constantes (Carrión *et al.*, 2006). Lo anterior, teniendo en cuenta que el MSV es útil para diagnosticar los fundamentos operativos de las organizaciones en general (Páez *et al.*, 2020) y se entiende como una herramienta que permite establecer los componentes de un sistema y sus diferentes niveles de recursión a partir de la identificación de tres aspectos fundamentales: entorno, administración y operaciones (Brocklesby, 2012), teniendo en cuenta que los entornos ciudadanos son altamente cambiantes.

Al mismo tiempo, proponer una estrategia administrativa y operativa es una actividad esencial dado que su desarrollo le permite a un equipo (en este caso los cuadrantes) concentrarse en un mismo objetivo y una misma visión, siguiendo las pautas para alcanzarlo. Si bien se considera que la elaboración de un plan de acción o estrategia puede tomar tiempo al inicio, durante su ejecución servirá para ahorrar tiempo, esfuerzos y recursos (Organización de las Naciones Unidas, 2009).

Desarrollo

Al hablar de estrategia no se puede separar la organización de su ambiente o entorno (Biggadike, 1981). Por eso, para el caso de estudio de este trabajo, no se puede separar a la localidad de su ambiente. Lo anterior, entendiendo al ambiente o entorno como el conjunto de cambios que ocurren a través del tiempo generando diferentes combinaciones de retos y problemáticas.

Asimismo, al hablar de estrategia, se debe tener presente que esta está relacionada con la definición de objetivos planteados, usualmente, a largo plazo. La estrategia influye en el desarrollo del plan o curso de acción, sin descuidar los recursos que se necesitarán para el logro de los objetivos (Chandler, 1962). El autor Igor Ansoff (1965), planteó que la estrategia une las actividades de la

organización con el producto mercado. Esto implica, según el mismo autor, que al hablar de estrategia también se está hablando de definir la naturaleza esencial de los negocios o el entorno en el cual está la organización y sus planes hacia futuro.

Considerando los problemas de seguridad de la localidad y en función de optar por un modelo de estrategia teórico, se plantea la utilización de la estrategia adaptativa. Esta propone una constante evaluación de las condiciones internas y externas con el fin de ajustar las condiciones de la organización al objetivo de alineación con los riesgos y oportunidades del ambiente o entorno (Chaffee,1985). De esta forma, se propone integrar los conceptos teóricos de estrategia a la administración y operación de los cuadrantes de policía de la localidad de Usaquén (Bogotá) para contrarrestar y disminuir el hurto a personas.

Desde el año 1995, se ha hecho más evidente que la seguridad ciudadana es una prioridad para las autoridades nacionales y locales. Estas se enfocan en prevenir los delitos de mayor impacto como el hurto a personas, los homicidios, las riñas, entre otros (Acero, 2002). Tales situaciones han generado que incluso en la Policía Nacional haya evolucionado el modelo de vigilancia. Para dar un contexto general, desde el año 1997 se cambió el abordaje de las problemáticas con la introducción de la Policía Comunitaria y, a partir del 2006, la Vigilancia Comunitaria. En el 2009, se creó el Plan Nacional de Vigilancia Comunitaria con un programa piloto en las

principales ciudades de Colombia y hacia el año 2014 se implementó el Modelo Nacional de Vigilancia Comunitaria por Cuadrantes (Policía Nacional de Colombia, 2015). Estos modelos de vigilancia no son novedosos, ya que desde hace más de treinta años se han venido implementando programas similares en diferentes países. Algunos de ellos son DART (Brown, 1987), COP (Tom & Savage, 1996), Policía de Barrio (Muller, 2010), entre otros.

Estos modelos de vigilancia comunitaria (DART, COP, Policía de Barrio, MNVCC) han permitido generar una mayor cercanía con la comunidad. Particularmente en Colombia, a partir de 2014, se tiene una asignación, estabilidad y jurisdicción concreta de los policías en los cuadrantes de cada localidad e, incluso, un número telefónico para contacto del cuadrante cercano en cada barrio. Esto genera para los integrantes del cuadrante una responsabilidad individual y promueve un servicio policial integral que puede responder a las nuevas demandas sociales de seguridad (Policía Nacional de Colombia, 2015). Según Sherman (1986), los esfuerzos planeados por los policías pueden controlar en gran medida el crimen, mejorar la calidad de vida de los habitantes de un sector y establecer buenas relaciones entre la policía y la comunidad. El autor también plantea que para la atención de delitos recurrentes se debe considerar una estrategia de cuatro pasos que consiste en analizar, diagnosticar, generar planes de acción y hacer seguimiento a los resultados.

En concordancia con el concepto de Sherman y teniendo en cuenta el enfoque teórico organizacional de contemplar una estrategia unificada e integrada que se diseña para asegurar que el objetivo será alcanzado (Mintzberg, 1987), la presente investigación propondrá una estrategia administrativa y operativa orientada a la reducción del hurto a personas. Así, también pretende ser una guía general que brinde una estructura organizada de las actividades que se requieren para lograr el objetivo. A nivel organizacional, sin perder de vista el concepto de estrategia administrativa y operativa que se pretende aplicar a la gestión de los cuadrantes del MNVCC en la localidad de Usaquén, se plantea que el rol de administrador/estratega debe tener cinco acciones que comprenden tres niveles diferentes: personas, información y acción (Mintzberg, 1997). Estos son:

1. Comunicación: dentro de la estrategia se debe velar por recibir y tener información que se pueda compartir con otros de manera interna y externa.
2. Controles: significa utilizar la información generada con el fin de controlar el trabajo de otros. Para este caso, se tendrán en cuenta resultados periódicos e indicadores clave de desempeño (KPI).
3. Liderazgo: empoderar a las personas para que tomen acción. Implica liderazgo individual (*mentoring, coaching*) y liderazgo grupal (resolución de conflictos).

4. Vincular: trabajo en comunidad generando vínculos internos y externos para fortalecer redes y poder ejercer influencia cuando se requiera. Muchas veces debe gestionarse desde la Dirección.
5. Hacer-ejecutar: tomar acción directamente desde aspectos que están bajo la dirección del estratega. Esto incluye la ejecución de proyectos internos y negociación de aspectos externos en función de poder gestionar cambios, tanto de estructura (internos) como de entorno (externos).

De esta forma, considerando que la operacionalización de los cuadrantes del MNVCC se basa en un plan de trabajo con tareas y actividades claras que también se registran en la Tabla de Acciones Mínimas Requeridas (TAMIR), se plantea generar la estrategia en torno a ciertas actividades incluidas en la operacionalización. Posteriormente, se evalúa su utilidad en la reducción del delito hurto a personas, sin dejar de lado que el plan de trabajo utilizado para operar los cuadrantes está alineado con los componentes habituales:

1. Acciones a desarrollar
2. Responsable del desarrollo de las acciones
3. Tiempo de ejecución
4. Plazo para realizarlas
5. Resultados esperados

Es importante aclarar que la construcción de dichos planes de trabajo, que al final hacen parte de la estrategia administrativa y operativa, siempre se realiza bajo un ambiente de concertación y participación.

Como preámbulo de la metodología a utilizar, se hace referencia a las palabras de Robert Kaplan (2004), quien plantea que todas las organizaciones de hoy crean valor sostenible apoyadas en activos intangibles como: recursos humanos, datos, procesos de alta calidad, relacionamiento, innovación y cultura. Estos aspectos se relacionan directamente con el planteamiento de una estrategia administrativa y operativa para la Policía Nacional de Colombia, la cual se plantea como propuesta de trabajo de grado. Para el desarrollo de esta, se utilizará la siguiente metodología:

Etapa 1. Selección y recolección de datos.

Se tendrán en cuenta los datos reportados por el SIEDCO de la Policía Nacional relacionados con el hurto a personas a nivel de localidades entre los años 2016 y 2019. También, se planteará la posibilidad de revisar variables adicionales como: género, edad, nivel de pobreza, nuevas modalidades de hurto, entre otras. Asimismo, se consultarán documentos académicos relevantes e información importante que aporte al plan de acción como: encuestas de percepción ciudadana, informes de la Secretaría de Seguridad, Convivencia y Justicia, entre otros.

Etapa 2. Análisis de datos y simulación

Se realizará el análisis de información, la construcción de gráficos y la generación de comparativos que permitan generar las bases para la estructuración del plan de acción.

Etapa 3. Propuesta de estrategia

Tendrá un enfoque práctico que permitirá definir la estrategia compuesta por cuatro fases:

Primera fase: revisión de los aspectos organizacionales que se deben tener en cuenta. Asimismo, se debe involucrar al equipo encargado de ejecutarlo para incrementar el sentido de pertenencia.

Segunda fase: definición del propósito y el alcance. Es decir, sentar las bases del plan y/o estrategia.

Tercera fase: planificar detalladamente los plazos, las actividades, los recursos, las áreas involucradas y los responsables. Esto implica involucrar a los participantes con los componentes del plan y los objetivos.

Cuarta fase (opcional): aplicación y evaluación del plan. Se ponen en marcha las actividades predefinidas articuladas con las áreas y personas responsables, los plazos, entre otros.

Conclusiones

Se espera que la estrategia administrativa y operativa a plantear como resultado del trabajo de investigación pueda impactar directamente, desde un enfoque administrativo, la operación de los cuadrantes del Modelo Nacional de Vigilancia Comunitaria por Cuadrantes (MNVCC) en la localidad de Usaquén (Bogotá). Por lo tanto, el documento de grado busca proponer la estrategia administrativa y operativa para luego estimar si la aplicación de esta reduce el hurto a personas en la zona.

Referencias

Ansoff, I. (1965). *The Corporate Strategy.* New York, USA: McGraw Hill.

Biggadike, E., (1981): The Contributions of Marketing to Strategic Management". *Academy of Management Review*, (6), 621-632.

Brown, L. (2018). American Academy of Political and Social Science Innovative Policing in Houston. *Sage Journals,3*(494).

Bonett Locarno, M. J. (2006). Seguridad Integral. *Estudios En Seguridad y Defensa, 1*(2), 32. doi: https://doi.org/10.25062/1900-8325.163

Brocklesby, J. (2012). Using the Viable Systems Model to examine multi-agency arrangements for combatting transnational organized crime. *Journal of the Operational*

Research Society, 63(3), 418-430. doi: https://doi.org/10.1057/jors.2011.43

Carrión, F., Pontón, J., y Armijos, B. (2009). 120 *Estrategias y 36 experiencias de seguridad ciudadana.* Quito, Ecuador: FLACSO Sede Ecuador.

Chandler, A. (1962). *Strategy and Structure.* Cambridge, United Kingdom: MIT Press.

Kaplan, R. S., & Norton, D. P. (2004). The strategy map: guide to aligning intangible assets. *Strategy & Leadership, 32*(5), 10–17. doi: https://doi.org/10.1108/10878570410699825

Mintzberg, H. (1987). The Strategy Concept 1: 5 Ps for Strategy. *California Management Review*, *30*(1), 11–24.

Mintzberg, H. (1997). Managing on the edges 131. *Managing on the edges. 10*(3), 131–153.

Muller, M. (2010). Community Policing in Latin America: Lessons from Mexico City. *European Review of Latin American and Caribbean Studies, 88*(88), 21–37.

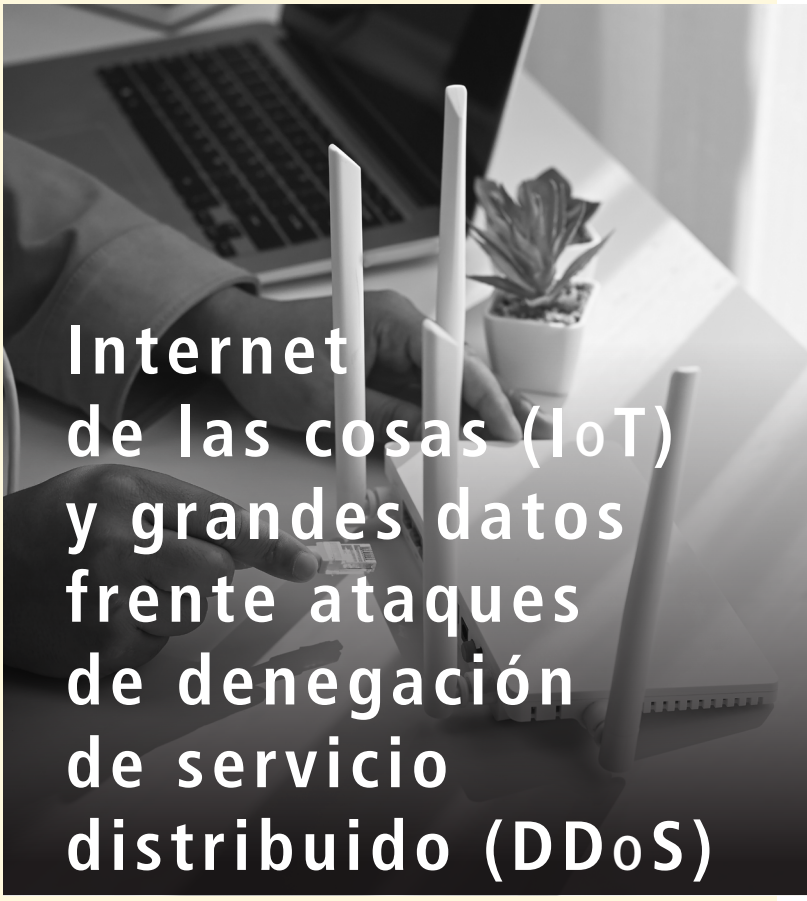
Químicas (2009), United Nations Institute for Training and Research (UNITAR).

Paez Murillo, C. A., Sandoval Garrido, L. E., y Peón Escalante, I. E. (2020). Caracterización del modelo nacional de vigilancia comunitaria por cuadrantes en Bogotá desde un enfoque sistémico. *Revista Científica General José María Córdova, 18*(30), 307–331. doi: https://doi.org/10.21830/19006586.591

Policía Nacional-Dirección General (2013-2016), *Modelo Nacional de Vigilancia Comunitaria por Cuadrantes* (MNVCC).

Savage, E. G. (1996). CITIZEN PERCEPTION OF COMMUNITY: Policing Impact. *Public Administration Quarterly, 20*(2), 163–179.

Sherman, L. W. (1986). Policing Communities: What Works? In Crime and Justice. *The University of Chicago Press Journals 8*, doi: https://doi.org/10.1086/449127



Internet de las cosas (IoT) y grandes datos frente ataques de denegación de servicio distribuido (DDoS)

Jairo Eduardo Márquez Díaz[a]

a Universidad de Cundinamarca. Chía, Colombia.
Correo electrónico: jemarquez@ucundinamarca.edu.co

Resumen: El Internet de las Cosas (IoT) ha supuesto un desarrollo tecnológico sin precedente alguno para la sociedad contemporánea. En la actualidad, miles de millones de dispositivos conectados a Internet registran información de diversa índole, transmitiendo datos permanentemente para su posterior análisis mediante técnicas relacionadas con el *big data*. Este análisis converge, finalmente, en la toma de decisiones en materia energética, sanitaria, de transporte, seguridad, impacto ambiental, entre otros. Esta información, que se recopila y fluye por dispositivos relacionados con el IoT, está sujeta a potenciales ciberataques provenientes de diferentes fuentes y técnicas. Una de las más utilizadas, es la técnica de denegación de servicio distribuido (DDoS), que constituye uno de los factores de intrusión de más alto riesgo

en una red estándar e híbrida debido a que compromete la información en diversos grados de seguridad.

Con esto en mente, se realizó un estudio en el que se exponen las vulnerabilidades a las que están expuestos los dispositivos del IoT, así como las implicaciones de seguridad que estas conllevan para la sociedad. En este sentido, también se consideró para la investigación el impacto y las repercusiones en materia de seguridad de la información en sus diferentes niveles, tanto del IoT como del manejo de datos masivos y las tecnologías que los acompañan; la inteligencia artificial, la nube informática, entre otras.

Palabras clave: amenazas persistentes avanzadas, *big data*, ciberseguridad, inteligencia artificial, Internet de las cosas, *ransomware*.

Introducción

El Internet de las cosas (IoT) estándar y aquel mediado por la inteligencia artificial (IA) presenta un nivel de seguridad discutible. Esto se puede atribuir, en parte, a fallas de diseño y fabricación de los dispositivos. Proceso donde no se ha tomado en cuenta que, aunque los sistemas operativos de los dispositivos estén soportados bajo protocolos y estándares propios de Internet, no implica que estén exentos de llegar a ser explotados por algún tipo de *malware* o técnica intrusiva. En este sentido, realizar ciberataques a estos sistemas permite sustraer datos no solo de hogares, sino también de armamento, drones, equipo médico, infraestructuras críticas, industrias, tecnología vestible, vehículos, entre otros.

Por otra parte, los elementos, como cámaras digitales, electrodomésticos, impresoras, juguetes, sistemas robóticos y demás, que se puedan conectar a Internet de forma alámbrica o inalámbrica y sean gestionados a través de un dispositivo móvil pueden ser intervenidos de forma maliciosa si su acceso no está configurado correctamente. Usualmente, los ciberataques dirigidos a estos dispositivos suelen atribuirse a las *botnets*; que, por medio de la técnica de distribución de denegación de servicio (DDoS), buscan sobresaturar el acceso de tráfico a Internet, inhabilitándolo y tomando el control de la red a la que se encuentran conectados los dispositivos IoT. En general, es importante mencionar que se presentan dos tipos ataque de denegación de servicio:

1. El estándar o simple (DoS), caracterizado por consumir recursos computacionales y/o de red hasta hacerlas colapsar, anulando la disponibilidad de los servicios donde el uso de *malware* es restringido.
2. El DDoS, se vale de miles, incluso de millones de sistemas (*botnet*), para no solo atacar y hacer colapsar una red anulando la disponibilidad sino, además, escalar el sistema, robar y/o secuestrar información empleando una gama de *malware*.

Con el DDoS el atacante busca recolectar la mayor cantidad de información de la víctima que lo lleve a tener acceso a las claves bancarias, las del correo personal y/o corporativo, las de redes sociales y todo tipo de

claves que le permita escalar privilegios en la red hasta llegar a la información sensible para su sustracción. Una vez capturada la información deseada, se presentan diversos escenarios: destrucción, secuestrar el sistema con fines extorsivos, vender la información sustraída a la competencia (ciberespionaje industrial), destruir instalaciones críticas (con fines militares y/o terroristas), entre otros.

Por su parte, uno de los mayores problemas de las *botnets* es que estas crecen conforme a las vulnerabilidades con las que se encuentran a su paso. En ese orden de ideas, lo que se espera para los próximos años es un aumento exponencial de cientos de millones de dispositivos conectados a Internet. Incluyendo, por supuesto, el IoT con todas sus variantes; lo que supone un potencial peligro para las organizaciones y la sociedad en general. Esta afirmación se sustenta en el hecho de que el número de dispositivos IoT conectados con otras tecnologías disruptivas está creciendo de forma exponencial. Además, electrodomésticos y todo tipo de dispositivos electrónicos están siendo gestionados y/o administrados permanentemente a través de redes locales y externas con una puerta de acceso a Internet. Haciéndolos más vulnerables a diversos tipos de ciberataque cuando no se toma en consideración ningún protocolo de seguridad al interior de la organización u hogar.

Desarrollo

Internet de las cosas (IoT)

El Internet de las cosas se define como el conjunto de dispositivos electrónicos alámbricos e inalámbricos dispuestos en diferentes medios y entornos conectados vía web que permiten el monitoreo de diversos tipos de variables. Su versatilidad concede compartir y/o centralizar datos de diversa índole en sistemas en la nube, lo que conlleva a dinamizar y optimizar procesos de monitoreo y toma de decisiones por parte del usuario o industria, según sea el caso. Aunque, esto está cambiando rápidamente debido a la integración de la inteligencia artificial, quien es la que toma las decisiones en vez del ser humano.

El IoT se encuentra presente en diversos contextos: agricultura, educación, hogar, industria, milicia, salud, transporte,

entre otros, incluyendo, por supuesto, todo lo relacionado con la industria 4.0 (cobots). Ejemplos puntuales de aplicaciones se encuentran en sistemas de detección y respuestas ante desastres; industrias y servicios para la gestión de procesos y logística. Algunos de ellos se presentan en:

- El sector sanitario: monitoreo y registro de signos vitales in situ dentro y fuera del centro clínico.
- La seguridad pública: a través de cámaras de video, controles de acceso y drones.
- Los sistemas de transporte e infraestructuras críticas de una ciudad: puentes, viaductos, edificios, hospitales, centrales eléctricas, etc.
- El hogar: por medio de electrodomésticos, control de persianas, luces, control de acceso biométrico, robots de limpieza, espejos, ventanas inteligentes entre otros.

En la industria energética Hao *et al.*, señala que "con el fin de optimizar procesos de comunicación y eficiencia de la banda ancha ha surgido el *Internet of Things-Grid* (IoT-G)" (2019, p. 82), cuya integración inmediata está centralizada en las ciudades inteligentes o *Smart Cities*.

Por otra parte, la tecnología móvil también aporta avances al IoT mediante tecnología vestible o usable como bandas fitness, bandas de muñeca, biosensores desechables, botas, exoesqueletos para la industria, gafas virtuales, guantes, *smartwatch,* entre otros a los que recientemente se les ha integrado inteligencia artificial por medio

de algoritmos de aprendizaje máquina (*Maquine Learning*) y aprendizaje profundo (*Deep Learning*).

Como el IoT se diversifica cada vez más, su integración con tecnologías 5G y 6G e inteligencia artificial (IAoT) implica desarrollos sin precedentes en sistemas de monitoreo y registro de datos combinados con tecnologías como la computación en el borde. Con este tipo de integración, se presupone un aumento a más de un billón de dispositivos solo para esta década. En ese sentido, "los investigadores, científicos e ingenieros enfrentan desafíos en el diseño de sistemas basados en IoT que permitan integrar de manera eficiente esta tecnología con las comunicaciones inalámbricas 5G" (Ejaz, 2016, p. 10310).

En términos técnicos, el IoT trabaja bajo el modelo TCP/IP (figura 1), que a diferencia del modelo OSI, opera diversos protocolos relacionados con la transferencia de datos. Por ejemplo, el protocolo IP (*Internet Protocol*) es el que permite la interoperabilidad entre dispositivos, donde la versión IPv4 se sustituyó definitivamente por la IPv6 y una variante IPv4+ en el 2020. Ampliando y mejorando, de esta manera, la organización de las direcciones IP de equipos y dispositivos en diversos tipos de redes de comunicación.

Figura 1. Comparación de capas entre el modelo OSI (Open System Interconnection) y el modelo TCP/IP (Transmission Control Protocol/Internet protocol).
Fuente: elaboración propia.

En materia de seguridad, el modelo TCP/IP exhibe vulnerabilidades en cada una de sus capas tal como señalan Acharya y Tiwari (2016), y Kak (2021). Por ejemplo, en la capa de red se encuentran problemas relacionados con la confidencialidad y el control de acceso. Estos son vulnerados directamente por medio del hardware de una red mal configurada, al igual que los propios dispositivos IoT conectados a la misma (DoS Santos et al., 2020). En esta capa, los ataques se enfocan a modificar o anular los datagramas asociados a una IP al emplear

técnicas como el *sniffing*, la suplantación en el protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*) o la desactivación del filtro MAC (*Media Access Control*).

En el nivel de infraestructura de red, la capa de transporte se encarga de transmitir datos a través de los protocolos TCP o UDP sobre los datagramas IP. En este punto, los problemas de seguridad se presentan en la autenticación, la integridad y la confidencialidad de la información. Estos se pueden realizar por medio de ataques de DDoS, obstruyendo el tránsito de datos e inhabilitando la comunicación entre cliente-servidor. Otros ataques que se pueden presentar son: "ataque de subdominio pseudoaleatorio (PRSD) *IP Flooding, ataque de tipo distribuido, snork, ping of death, smurf, Spoofing for SYN flood DoS attacks TCP/SYN, flooding y teardrop,* amplificación NTP, ataques ICMP (ping), UDP Flood, HTTP Flood, SSL/TLS renegotiation, entre otros" (Márquez, 2020, p. 14).

Otros componentes de seguridad a tener en cuenta están relacionados con el uso de tecnologías de redes de sensores inalámbricos (WSN), sistemas de comunicación de campo cercano (NFC) y sistemas de identificación de radiofrecuencia (RFID) implementados en dispositivos móviles que demuestran tener sus propias vulnerabilidades (Santiago *et al.*, 2018). Cada tecnología requiere de protocolos específicos (Márquez, 2019), a lo que se suma la tecnología 5G, cuyas aplicaciones emergentes abren un sinfín de oportunidades para nuevos ataques, por ejemplo, aplicaciones de tipo *HealthTech* y *BioTech.*

En cuanto a protocolos como Ethernet, WiFi, LiFi, Bluetooth, GSM y demás, estos operan en la capa de aplicación que diseñan, específicamente, como productos propios de una empresa sin estandarización alguna hasta el momento. Por ejemplo: MFI, Nest, Open Interconnect Consortium (OIC) y The AllSeen Alliance. Bajo este panorama, cada industria que trabaja con IoT desarrolla sus propios protocolos; LoRA, LTE, NB-IoT, NB-FI, Sigfox, Weightless, entre otros, o implementan algunos ya estandarizados. Por lo que no hay garantía de compatibilidad con dispositivos de otros fabricantes. El resultado de todo esto, es una brecha a nivel de seguridad de los dispositivos IoT que puede ser aprovechada por la ciberdelincuencia. Un ejemplo al respecto fue un ataque ocurrido en el año 2020 a Estados Unidos, empleando el *malware Drovorub* (NSA & FBI, 2020), cuyo objetivo estuvo encaminado a hackear de manera masiva dispositivos IoT para poder acceder a redes de comunicación más amplias.

Denegación de servicio distribuido

El IoT se encuentra en diversos dispositivos como señala Márquez: "en electrodomésticos, teléfonos inteligentes, ropa inteligente, wearables (pulseras, gafas de realidad virtual, etc.), televisores inteligentes, videoconsolas, sistemas de transporte, edificios (cámaras de seguridad, climatización, controles de acceso, etc.), infraestructuras públicas (puentes, autopistas, parques, etc.), servicios

públicos, componentes industriales" (2019, p.89); estos últimos en sistemas SCADA (Pliatsios *et al.*, 2020).

Tomando en cuenta que los dispositivos IoT trabajan bajo el modelo TCP/IP y protocolos propios diseñados a la medida, los problemas de seguridad son inminentes como se anotó anteriormente. Esto, en parte, por el escalamiento de la tecnología que no va en paralelo con determinados protocolos base de Internet, los cuales aún presentan debilidades desde su creación. El escenario plantea grandes desafíos como afirman Rose *et al.*: "hay ataques a dispositivos conectados a Internet, en la que hay temor a la vigilancia y preocupación por la privacidad" (2015, p. 6). Lo anterior, como señala Barrio, se debe a que "el IoT se presenta como una fuente de recolección de datos que crece exponencialmente y, en consecuencia, todo objeto pasa a ser un origen de información" (2018, p. 25).

Una debilidad del IoT en materia de seguridad, con mayor riesgo por su alto impacto, está relacionada con los ataques por denegación de servicio distribuido (DDoS) (Márquez, 2020). Cuyo objetivo está centrado en inhabilitar la comunicación de los dispositivos conectados a una red, afectando las tablas conmutadas de flujo de datos, el ancho de banda y la latencia. Esto se logra aprovechando las debilidades del modelo OSI (*Open System Interconnection*), efectuando así ataques en las capas de transporte, red y aplicación, al igual que ataques de tipo amplificación de DNS, SMURF y ACK, entre otros.

Algunos efectos de los ataques mencionados consisten en realizar múltiples peticiones a los servidores de la empresa víctima con el objetivo de saturar la red hasta hacerla colapsar. También, se pueden realizar ataques de fuerza bruta a través de *malware* especializado que se encarga de escanear la red en busca de dispositivos IoT. Lo anterior con el fin de obtener contraseñas e información que permita secuestrar y unir, finalmente, los dispositivos a una *botnet*. Posteriormente, esta se interpreta como *malware* especializado que se instala en los computadores y/o servidores aprovechando las vulnerabilidades de los navegadores y errores humanos.

La característica principal de una *botnet* consiste en infectar la mayor cantidad de redes de computadores y servidores, secuestrando sus recursos para formar la denominada "red zombie". Este tipo de red se controla mediante servidores de tipo *command & control* que aumentan la capacidad de un ataque DDoS, spam, *ransomware* o combinación de ambos (RDoS), entre otros, dirigidos a objetivos específicos. Normalmente, los objetivos son empresas, infraestructuras críticas como transporte, servicios públicos esenciales, sector salud, sector alimenticio, educación, etc. Aunque no se descartan ataques dirigidos a un individuo en particular que se dan, usualmente, por contrato. Un ejemplo reciente es el *botnet* QBot que emplea Windows Defender como cebo para que la víctima habilite las macros de archivos enviados en formato Excely, una vez hecho esto, instala un *ransomware* para secuestrar y encriptar la información del sistema.

Mitigación frente a un ataque DDoS

Frente a los desafíos de ciberseguridad que una organización debe afrontar está, precisamente, establecer qué mecanismos son los más apropiados basándose en las características particulares sobre determinados ciberataques, como los de tipo DDoS. A esta incertidumbre se suman los recursos técnicos y tecnológicos limitados destinados para la protección de toda la infraestructura. Cuyos costos en la mayoría de organizaciones están prohibidos. En consecuencia, la manifestación de riesgos potenciales atribuidos a tecnologías como el IoT, se expresan a través de fallos de seguridad que crecen día a día. No solo por el número de dispositivos, sino por su diversificación en múltiples campos de la industria y hogar. Convirtiéndose en un problema de seguridad mundial que demanda ser atendido con prontitud.

Ante este panorama planteado, se presenta una dinámica compleja derivada por la multiplicidad de vulnerabilidades que permiten ser explotadas tanto de la propia tecnología de los dispositivos IoT, como de los procedimientos de gestión y administración de los mismos. Para el caso de ataques por DDoS, se requiere de redes de computadores y servidores mal configurados o redes con niveles de seguridad escasos que, una vez

secuestrados, se conectan a una "red zombie" tal como se observa en la figura 2. [1]

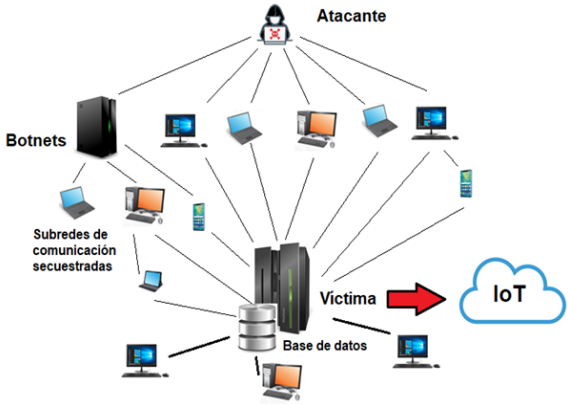


Figura 2. Representación gráfica de un ataque DDoS y su relación con el IoT.
Fuente: elaboración propia.

Esta estrategia aplicada a dispositivos IoT permite el uso de otras herramientas de *malware* especializado que pueden ser utilizadas con diferentes fines delictivos. Ampliando así la cobertura de la "red zombie" potenciando a miles o millones de veces las peticiones a los servidores de la víctima. Este tipo de redes están

1 Se emplean *botnets* encargadas de realizar el ciberataque, en este caso a un servidor que gestiona una red interna corporativa, incluyendo el IoT. El resultado del ataque culmina con el acceso a la información alojada en la base de datos del servidor y el control de la red.

creciendo rápidamente en la *Darknet*, en la que se pueden alquilar a módicos precios e, incluso, conseguir kits para efectuar pequeños ataques según el objetivo al cual se quiera atacar.

Para el caso de la seguridad metropolitana, es común encontrar sistemas de información geográfica, tecnologías de videovigilancia inteligentes compuestas por cámaras de alta resolución, control de tráfico e iluminación inteligentes, cámaras y micrófonos con aplicaciones específicas (detección de trazas digitales de audio), drones de monitoreo y seguimiento, sistemas biométricos, sensores y biosensores conectados vía dispositivos IoT distribuidos por toda la ciudad que pueden ser gestionados por diversos recursos TIC.

Bajo este escenario, un ciberataque a las infraestructuras críticas de una ciudad pondría al descubierto el acceso a una infinidad de datos e información. El ciberataque no solo estaría orquestado por delincuencia organizada y grupos terroristas, sino por los propios gobiernos a través de su milicia y organizaciones de seguridad con el fin exclusivo de monitorear a cada individuo y sociedad de forma permanente e impune, vulnerando de facto los derechos humanos. Por ejemplo, China bajo su régimen (Nardi, 2019), posee la mayor información de su población empleando diversas tecnologías biométricas, como sistemas de registro y reconocimiento facial, integrados con grandes bases de datos (incluye bases de datos de ADN), gestionados y administrados a través de la inteligencia artificial. Otro ejemplo, es la Agencia

Nacional de Seguridad (NSA) y la CIA, que de manera recurrente violan los derechos humanos espiando no solo a la propia comunidad estadounidense, sino al mundo entero (Bignami, 2018), bajo el argumento de protección ante el terrorismo. Al igual que agencias de otros países (Lemieux, 2019) que emplean las mismas estrategias de ataque y espionaje sin que la población se dé por enterada.

Las técnicas de mitigación de un ataque DDoS son discutibles en cuanto a su efectividad a gran escala. Esto se debe, en parte, a la eficiencia y complejidad de poder implementarlas. Por ejemplo, una reciente propuesta se sustenta en el uso de las tecnologías *blockchain* y *smart contracts* (Feliu, 2018) que disponen de la infraestructura necesaria para conservar el diseño y estabilidad de una red en el marco de desarrollo de un protocolo que soporte ataques de tipo DoS, DDoS o RDoS. La propuesta toma como soporte la computación en la nube que dispone de un alto grado de seguridad debido a la forma como se filtran los paquetes de datos. En esta, el sistema consta de un conjunto de dispositivos o programas (*Firewalls y Proxy*) configurados para limitar el paso y acceso de datos en una red restringida gobernada por un conjunto de reglas y protocolos.

Seguridad en dispositivos IoT

El IoT presenta diversas debilidades representadas tanto por una manufactura cuestionable como por una gestión deficiente de los mismos en materia de seguridad TI. No solo el DDoS saca partido, sino otras variantes como el DDoS de baja velocidad (LDDoS) (Savchenko,

2020), que oculta su tráfico de manera equivalente al tráfico normal. Adicional a esto, otro tipo de debilidad se atribuye al proveedor de servicios (DPS), entendido en aquellos casos donde el servicio es deficiente, presentando disminución en el rendimiento de la red contratada.

Otro factor de seguridad a mencionar es cuando los ciberdelincuentes se aprovechan de las fallas humanas relacionadas a no cambiar las contraseñas predeterminadas al configurar los dispositivos IoT, o deshabilitar el acceso administrativo remoto de los mismos. En estos casos, se emplean proxis anónimos para transmitir datos de forma ilegal en forma de amenazas, pornografía y ataques que hacen que el ancho de banda disminuya y, a la par, se incremente el consumo de energía de la red. A esto se suma la posibilidad de que el contenido delictivo fluya por la red de la organización si las autoridades logran rastrear este tipo de ataque. Lo que conlleva implicaciones legales serias para los encargados y sus dueños.

Existen propuestas en materia de seguridad para el IoT como son: la defensa colaborativa a través de las funciones "de red virtual (VNF), intercambio de eventos basado en FLow (FLEX), uso de protocolos DOTS (DDoS *Open Threat Signaling)*" (Márquez, 2019, p. 2) y técnicas de ofuscación, entre otros. Estas propuestas, aunque buenas, no dejan de lado el problema de normalizar que los protocolos de conectividad no permiten contrarrestar ataques DDoS y sus variantes a gran escala. Problemática de la que se espera su incremento para los próximos años, conforme el número de redes aumenta en todo el mundo.

Por su parte, aunque el uso de la Inteligencia Artificial (IA) permite, en principio, la detección temprana de un ataque mediante técnicas empleando redes neuronales avanzadas (Wang, Lu y Qin, 2019) y aprendizaje automático (*Machine Learning*), abre también un nuevo nicho para la creación e implementación de la seguridad informática inteligente y/o adaptativa; llevando con ello a un nuevo hito de la ciberseguridad disruptiva.

La nube informática y grandes datos

Incibe define la nube informática (*Cloud Computing*) como "un modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet" (s.f, p. 5). En este contexto, los recursos computacionales y servicios se ofrecen bajo demanda, representados bajo tres modelos: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS), tal como se observa en la figura 3.

Debido a las características escalables de la computación en la nube, el manejo es limitado en cuanto a la información para la gestión de tecnologías IoT y proyectos relacionados como el *big data*, analítica avanzada, inteligencia artificial entre otros. Por lo que compañías grandes, medianas y pequeñas contratan este tipo de servicio ya que no requieren de infraestructura tecnológica propia. De esta manera, minimizan los costos operativos y de funcionamiento, al igual que disponen de la información en cualquier momento y lugar. Por ejemplo, proveedores de servicio en la nube como Amazon Web Services, Azure y Google con sus

soluciones Cloud, Cloud Armor y Cloud Load Balancing han sido diseñados bajo estándares que les permiten soportar ataques masivos DDoS. Estos sistemas se están convirtiendo rápidamente en soluciones plausibles para aquellas empresas que emplean dispositivos IoT en sus instalaciones y servicios.

Figura 3. Modelo de servicios en la nube, Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS).
Fuente: elaboración propia.

Nota. Los cuadros en color azul corresponden a los servicios que gestiona la propia empresa y los cuadros de color rojo representan los servicios tercerizados.

Para el caso de los grandes datos o *big data*, se emplean modelos de gestión y análisis de información para encontrar patrones repetitivos que permitan generar conocimientos expresos a través de tendencias, correlaciones y preferencias. En muchos casos, convergen a sistemas predictivos, entrando en acción la IA a través del aprendizaje máquina. Como consecuencia

de ello, el volumen de datos se ha incrementado en los últimos años en órdenes que se acercan rápidamente a los exabytes (10^{18}). Exhibiendo así diversos tipos de datos, estructurados, no estructurados y semiestructurados, que demandan gran cantidad de recursos a nivel computacional, donde el IoT con sus diversas variantes como el IIoT (*Industrial IoT*) (Khan *et al.*, 2020), IoRT (*Internet of Robotized Things*) (Simoens *et al.*, 2018) y el IoTotBF (*IoT on the Battlefield*) (Márquez, 2019) entre otros, no son la excepción.

Lo anterior, presupone el desarrollo de políticas de protección de grandes datos en todos los niveles; propiedad de datos, seguridad, privacidad, marco ético, entre otros que permitan lidiar con los avances propios de la tecnología y las técnicas de ciberataque que vienen consigo. Bajo esta óptica, hace algunos años se afirmaba la inmunidad del *cloud computing* frente a los ataques de todo tipo de *malware*. Sin embargo, esto cambió rápidamente demostrándose que ningún sistema es infalible y menos con ataques de DDoS y de RDoS. De hecho, tal como señalan Deshmukh y Devadkar (2015), existen evidencias de ataques DDoS y taxonomía de los mismos sobre sistemas en la nube, exponiendo los tipos y diversas medidas de contraataque (técnicas de detección, prevención y tolerancia) para mitigar este tipo de intrusiones.

Ahora bien, para poder perpetrar un sistema en la nube, el atacante ha logrado tener acceso a ciertos privilegios como a un nodo del sistema. Por lo que puede

hacer lo que quiera con los datos e información encontrada, poniendo en serios aprietos a una organización. Estas fallas no suelen atribuirse a factores de índole técnico, sino a errores humanos, bien por negligencia o complicidad de un trabajador.

Por otra parte, la sinergia de diversas tecnologías disruptivas permitiría crear una infraestructura tecnológica sin igual para el registro, análisis, procesamiento y almacenamiento de datos masivos donde la intervención del ser humano va a ser menos necesaria. En consecuencia, como se mencionó anteriormente, con el aumento progresivo de dispositivos IoT en todo el mundo se espera que el nivel de seguridad también aumente. Garantizando que la información esté bien resguardada con un riesgo mínimo. Sin embargo, las técnicas de ataque de tipo DDoS o RDoS son dinámicas, por lo que van a evolucionar dando paso a otra clase de denegación de servicio distribuido inteligente (IDDoS). Por ende, se presupone la integración de la inteligencia artificial con algoritmos avanzados que se adaptaran a aquellas infraestructuras inteligentes. Es decir, se está hablando de IA atacando a otras IA.

Ransomware

El *ransomware* consiste en un ciberataque caracterizado por encriptar y codificar archivos resguardados en un computador, red o servidor. En este, la víctima debe pagar un rescate por medio de criptomonedas, razón por la cual se torna difícil, sino imposible, rastrear su origen o destino. Este tipo de ataque evoluciona

permanentemente empleando nuevos algoritmos de encriptación más robustos y complejos que buscan obligar a la víctima a pagar por el rescate de la información. De este modo, no se le da posibilidad alguna de que pueda desencriptarla, incluso, si eso implica contratar servicios de terceros. El ciberataque se potencia al conjugarse con el DDoS, transformándose en un ataque de clase RDoS. Los objetivos del ataque buscan comprometer la información y operatividad de los mismos del sector empresarial, industrial, financiero, gubernamental, militar y de infraestructuras críticas.

El *ransomware* solo requiere secuestrar unos pocos computadores que no estén actualizados o instalarse mediante engaños a sus víctimas a través de correo malicioso enviado por medio de subterfugios informáticos y acciones directas humanas. De igual manera, este *malware* puede instalarse en sistemas de tipo SCADA (Ibarra, 2019), que no necesariamente están conectados a Internet y, de estarlo, sus medidas de seguridad son inexistente o deficientes. Lo crítico de este tipo de ataque es que presenta un comportamiento escalable, si la seguridad de las redes lo permiten. Esto sucede cuando existen software y/o hardware vulnerables como routers y otros dispositivos mal configurados, en mal estado u obsoletos. También, el atacante puede hacer uso de otros tipos de *malware*, como troyanos, para abrir paso al *ransomware* y secuestrar más información al interior de una red hasta llegar a la data que circula por los dispositivos IoT.

En la última década, el *ransomware* se ha vuelto un gran recurso económico para el crimen organizado. Incluso, en tiempos de pandemia y post pandemia le ha permitido adaptarse para crear *malware* multiplataforma con la potencialidad de infectar cualquier tipo de sistema operativo. Al ingresar a un sistema, este *malware* informático puede cifrar todos los archivos (*Cryptolockers*), bloquear el acceso a la pantalla del computador (*Lockscreen*), bloquear el o los discos duros, incluyendo las copias de seguridad si estas se encuentran resguardadas en el mismo sistema o se tiene acceso a la nube, bloquear el acceso a cualquier dispositivo móvil, entre otros.

El problema no termina aquí; cuando es secuestrada la información el atacante tiene acceso a la misma de manera ilimitada, permitiéndole rastrear otras potenciales víctimas como los socios de la organización, clientes, familiares de los trabajadores, etc. En esta instancia, se ha vuelto común la triple extorsión que se presenta cuando la empresa se niega a pagar, consiste en llamar directamente a los afectados y amenazarlos. Si no funciona, se pasa a extorsionar a los clientes y si persiste la negativa a sus familiares.

Desde una perspectiva más general, la característica principal de un ataque *ransomware* es restringir el acceso a la información. Para ello, se requiere instalar un *malware* dentro de un fichero que al ser ejecutado por la víctima, bien al abrir un mensaje de correo falso, descargar archivos de redes P2P (*Peer Two Peer*) o

de sitios de software pirata, empieza a realizar cambios internamente en el sistema operativo, en sus registros; inactivando el antivirus, el acceso al teclado y otras funciones críticas del equipo y la red a la cual está conectado. El siguiente paso para el atacante es conectarse a la red de la víctima, lo que supone vulnerable, e ingresar vía conexión remota del escritorio del equipo, empleando diversos protocolos como RDP (Protocolo de Escritorio Remoto). Previamente, mediante ingeniería social, también se puede adivinar la contraseña o emplear un ataque de fuerza bruta para dar con ella entre otras argucias informáticas.

Para realizar este tipo de ataque se cuenta con gran diversidad de herramientas de *malware*, tanto gratuitas como pagas, que permiten cifrar la información incluyendo bases de datos corporativas, copias de seguridad (que normalmente se encuentran a los servidores físicos o en la nube) y datos almacenados en unidades de red. Finalizada la encriptación, la víctima recibe un mensaje en la que se le indica el pago inmediato por la información secuestrada mediante algún tipo de criptomoneda (bitcoin, ethereum, namecoin, dash, etc.), de lo contrario será destruida.

Desencriptar un *ransomware* no es fácil porque emplean algoritmos de cifrado asimétrico y simétrico como el de Galois/Counter (GCM) mode3, que es uno de los últimos cuyo grado de complejidad es alto en la actualidad. Con este panorama a la vista la empresa puede pagar, pero no hay garantía que se le devuelva el acceso

a la información, y si llegara a suceder, el riesgo de iniciar de nuevo el secuestro de la misma información más otros sistemas es considerablemente alto. Pues volverá a pedirse un pago por su recuperación.

Para prevenir daños irreparables, lo aconsejable es aplicar la regla 3-2-1, que significa: realizar tres copias de seguridad de la información a proteger en dos lugares físicamente diferentes y una de ellas que esté offline. Este consejo se aplica sobre todo para las empresas que quieren sobrevivir a un ataque de tipo *ransomware*. De manera adicional, para mitigar los daños, se sugiere al personal de TI a cargo realizar varios puntos de restauración que, aunque se pierdan datos, no se perderá todo. Emplear diferentes medios de almacenamiento (SSD, HD o NAS) y elegir las mejores soluciones de copia de seguridad. Finalmente, establecer planes de contingencia ante este tipo de eventos.

Amenazas persistentes avanzadas e Inteligencia artificial

En la actualidad, la inteligencia artificial (IA) presenta muchos campos de acción; uno de ellos es la seguridad informática; detectando vulnerabilidades en un sistema, tanto en hardware como en software. De hecho, ya es común que empresas de seguridad utilicen modelos predictivos basados en aprendizaje automático y redes neuronales, más que otras tecnologías disruptivas, con el fin de anticipar ciberataques a sus redes y detectar cualquier tipo de irregularidad en las mismas. Desde esta perspectiva, la delincuencia emplea de manera recurrente la ingeniería inversa para encontrar fallas y vulnerabilidades en un sistema que facilite un

ciberataque, donde algoritmos de IA pueden ser empleados para tal fin. Al igual que atacar un sistema mediante *malware* "inteligente".

Lo anterior, supone un problema a gran escala que las autoridades han empezado a mirar con detenimiento basándose en sus implicaciones en términos de defensa, seguridad y protección de la información, sumado a la ética que implica el uso de la IA. Esto no es para menos. Un ciberataque artificial podría, en teoría, comprometer toda la seguridad de un sistema, incluyendo la vida de personas inocentes. En este escenario, entra en juego el uso de diversos modos de ataque como las amenazas persistentes avanzadas (APT, *Advanced Persistent Threat*) combinadas con *ransomware*, DDoS, RDoS y otros *malware* inteligentes. Las APT las define Roa como:

> Amenaza: Identifica el uso de amenazas digitales para materializar el o los ataques. Persistente: indica que la naturaleza encubierta de la amenaza hace intentos reiterados de establecer el acceso a sistemas e información sensible de la organización. Avanzada: significa la capacidad de superar los sistemas de detección de intrusos y mantener un acceso constante a la red objetivo de manera segura. (2020, p. 6)

Al combinar las APT con *ransomware* se formula el objetivo de secuestrar sistemas críticos. Bien para inhabilitarlos temporalmente o, en su defecto, destruirlos

(dependiendo del contrato, misión o idealismo en juego), de tal manera que colapse cualquier operación que se ejecute en el ciberespacio, red corporativa, máquina (en este caso los PLC o microcontroladores que pueden hackearse su firmware) o industria en general. Este proceso requiere de una planificación sistemática que converge al instalar las APT en los servidores corporativos de la víctima mediante técnicas como "Spear-Phishing, DND Spoofing a través de Man in the Middle, exploits zero day, o mediante dispositivos de inserción USB, CD, DVD, etc." (Novoa *et al.*, 2016). Adicionalmente a estas técnicas, se realizan búsquedas de información corporativas, tanto en la red convencional como en la *Darknet*, relacionadas con las actividades comerciales, socios, clientes e información técnica de la página web. Además, se pueden hallar bases de datos "obsoletas" y documentación privada que ha sido filtrada (p. ej. información financiera, propiedad intelectual, información de los trabajadores, etc.).

Combinar las APT con la IA no solo amenaza la seguridad de una organización o industria, sino que puede ser escalada hasta comprometer la seguridad de las infraestructuras críticas de una nación. Este escenario puede ser orquestado por bandas criminales o por grupos financiados directamente por gobiernos, demostrando con ello una connotación geopolítica de alto impacto social y económico. Al ser *malware* especializado, las APT se diseñan para infectar e inhabilitar redes y equipo industrial especializado por lo que su uso está dirigido

al robo, modificación, destrucción, espionaje y sabotaje industrial o corporativo.

Cabe señalar, que las APT emplean técnicas complejas de cifrado combinadas con avanzados algoritmos polimórficos. Márquez señala que "los APT pueden perdurar en un sistema informático por mucho tiempo sin ser detectado, aprovechando las vulnerabilidades propias de la red o de la misma arquitectura de los protocolos de comunicación en el empaquetado de datos en una red" (2017, p. 52). En este contexto, una APT puede considerarse como una ciberarma diseñada para realizar ataques específicos, normalmente a infraestructuras críticas. Desde esta perspectiva, un sistema de IoT sería más susceptible a una APT ya que puede interceptar la comunicación entre dispositivos e inhabilitarla, modificarla o, simplemente, espiarla.

Las APT no son un *malware* que abunde en internet puesto que su diseño e implementación demanda recurso humano calificado y tecnología de vanguardia. Esto implica que sus gestores son gobiernos, corporaciones rivales y sindicatos criminales que cuentan con los suficientes recursos financieros para emprender tal empresa. De hecho, Sánchez y Urrutia señalan que: "existen puntos de unión de estas organizaciones con Estados y su respaldo económico. Empresas de ciberinteligencia como Fireye o Symantec catalogan a estos grupos mediante un número APTXX o un término escogido según las campañas realizadas" (2020, p. 5). Bajo este modelo, Ahmad *et al.*, señalan que "se emplea una variante de

las APT denominada S-APT, cuya acción está centrada en crear vectores de ataque basado en estrategias de desinformación en el marco de la milicia" (2019, p. 407).

Para finalizar este aparte, en el contexto de la IoT e industria 4.0, la incorporación de la inteligencia artificial y la ciencia de los datos crece día a día buscando mejorar no solo la conectividad, sino también la gestión de la información; empleando para ello la tecnología móvil y la ubicuidad que los acompaña. Sin embargo, no se puede bajar la guardia sobre los nuevos desarrollos de IoT inteligentes porque actualmente existen en la industria dispositivos IoT obsoletos, con fallas de diseño e inseguros que exponen un riesgo muy alto a las mismas. Este hecho, conduce a establecer estrategias delictivas encaminadas a introducir una APT con miras de buscar y aprovechar vulnerabilidades de estos sistemas. Ya sea cuando se encuentren en el mercado o desde su propia fabricación. Por lo tanto, se abren un sinnúmero de escenarios plausibles para realizar ciberataques desde drones, vehículos autónomos, robots avanzados, redes eléctricas inteligentes e, incluso, la propia infraestructura IoT con que cuenta una ciudad inteligente. Asimismo, la preocupación de errores de programación en sistemas basados en IA tiene mucho sentido porque se pueden explotar y aprovechar para vulnerar otros sistemas, como fue demostrado por el sistema inteligente DeepXplore (Pei *et al.*, 2019).

Discusión

Actualmente, la seguridad de la información no solo contempla la protección de equipos de cómputo y redes, sino que involucra otras tecnologías disruptivas como el IoT que, debido a su constante evolución e implementación en diversos entornos, ha demostrado tener fallas tanto en su manufactura como en su implementación, gestión y/o administración. Por ejemplo, dejar activos servicios de red que son prescindibles o son inseguros, facilitando al atacante asumir el control de cualquier otro servicio. También, se encuentran fallas en el diseño de las interfaces que gestionan los dispositivos IoT, tales como aplicaciones móviles, la página web corporativa (webApp), repositorios de datos en la nube y las API del *backend*. Todas estas fallas obedecen

a vulnerabilidades de cifrado débil aplicadas sobre los datos que circulan por la red. Sumado a esto, está la ausencia de filtros de entrada/salida.

Otros errores muy comunes en sistemas IoT están relacionados con dispositivos conectados a Internet y la red corporativa sin la debida autorización o errores de autenticación entre dispositivos maestro-esclavo. También, se suelen encontrar accesos remotos de dispositivos sin autorización o escaneos de la red en la misma situación. A nivel de software, los errores más comunes son la falta de actualización del *firmware*, cambios de la versión de los mismos sin cerciorarse que son estables o el uso de comandos potencialmente peligrosos que pueden habilitar accesos no autorizados, en particular en los PLC, entre otros.

Las fallas mencionadas no terminan aquí, ya que es muy común no actualizar el *firmware* de los dispositivos IoT. Igualmente, se tiende a no actualizar el cifrado en tránsito y no validar las actualizaciones que se realizan sin los procedimientos apropiados conforme a las políticas de seguridad corporativas. Lo que implica verificar que los componentes y librerías de software sean seguros, estén actualizados y provengan de fuentes confiables. También, se tiende a hacer uso inadecuado de información personal almacenada en dispositivos IoT, donde los procesos de seguridad son cuestionables pues no existe un permiso formal o consentimiento, ni un cifrado de datos o control de acceso a los mismos.

Recientemente, han salido al mercado aplicaciones que minimizan los riesgos mencionados. Por ejemplo: "Azure Defender for IoT" que inspecciona de forma pasiva el tráfico de red, enviando alertas a una instancia en la nube denominada "Azure Sentinel". Esta es una de varias propuestas plausibles para aquellas empresas que trabajan con IoT y desean garantizar seguridad en sus servicios y a sus clientes.

Es innegable que el IoT con todas sus variantes muestra grandes beneficios para la industria y sociedad. Pero, a la vez, representa grandes retos en materia de seguridad, bien desde el proceso directo de manufactura, como desde su integración con otras tecnologías,que permiten la gestión de múltiples dispositivos en diversos entornos. Esta tendencia debe ser tomada en consideración no solo por los fabricantes y gobiernos, sino por la propia sociedad. Ya que, el riesgo de acceso no autorizado a información sensible por parte de terceros es alto y la incertidumbre del manejo de la misma queda en entredicho. De hecho, también se presentan cuestionamientos acerca de la transparencia del manejo de la información por parte de los gobiernos y las grandes corporaciones porque, al parecer, el problema se agudizará aún más con las tecnologías venideras.

Sobre los ciberataques realizados mediante la DDoS combinado con otras técnicas señaladas en el presente estudio no excluyen al IoT. Demostrando así ser vulnerable en diversos aspectos. Por ejemplo, ataques de tipo

DDoS de día cero o aquellos basados en volumen (se dirigen a enlaces de red, a equipos y servidores DNS o de aplicaciones) que son difíciles de evitar debido a la rapidez con que se ejecutan. Existen otros tipos de ataques más sofisticados altamente destructivos y selectivos, que asumen el control de un sistema, como los de protocolo dirigido a redes que se comunican con servidores, *firewall* (físicos y lógicos), *gateways* y equilibradores de carga, cuyo daño a una infraestructura puede ser grave. Máxime cuando un ataque, al ser escalable, puede aumentar de miles de bits por segundo a millones o, incluso, billones en poco tiempo.

A lo anterior se suma la vulneración directa de "la propiedad, derechos, uso, explotación, mantenimiento y licencias para la administración de los datos masivos, que son un gran peso económico, legal, de imagen y de seguridad para las organizaciones y/o personal a cargo de gestionar y administrar sus activos" (Márquez, 2020, p. 12) En relación con este tema, los ataques de *malware* mencionados en el presente estudio cuestan millones de dólares a las empresas. Por lo que no es recomendable bajar la guardia, más aún cuando los sistemas de comunicación y redes incorporan nuevas tecnologías permanentemente y el nivel de seguridad se torna cada vez más complejo.

Lo recomendable para una empresa es siempre robustecer los sistemas con miras de reducir sus vulnerabilidades o *hardening* (Ibor y Obidinnu, 2015). Así

como tener planes de contingencia y políticas de seguridad actualizadas que les permita actuar de manera rápida e inteligente ante cualquier ataque mencionado. El tiempo de respuesta es factor crítico para minimizar daños irreparables haciendo que la estancia del *malware* sea mínima. Aquí, las acciones de monitoreo de la red son fundamentales, al igual que tener siempre presente que en materia de ciberseguridad el eslabón más débil son las personas.

Conclusiones

La preocupación por el acceso no autorizado a información sensible gubernamental, corporativa e industrial está más que fundamentada. Principalmente, cuando son concentrados y gestionados a través de diversas tecnologías como la inteligencia artificial, la ciencia de datos, el *Cloud Computing* y el IoT (con todas sus variantes), entre otras disciplinas. Los ciberataques están a la orden del día bajo diferentes modalidades y motivaciones (económica, social, corporativa, política, militar y terrorista) que evolucionan conforme a la tecnología lo hace. Esto los hace ideales para grupos delincuenciales organizados, gobiernos e industrias que buscan partido en vulnerar sistemas de sus contrapartes con el fin de secuestrar, extorsionar y/o destruir información crítica de las mismas.

Además, existen zonas grises sobre la formulación de políticas públicas que garanticen un resguardo adecuado sobre la propiedad de los datos, protección y prohibición de su uso con otros fines, tal como afirma Porcelli: "existe un vacío legal que es un riesgo colateral a todos los avances digitales y tecnológicos, porque ni los gobiernos ni entes reguladores van al paso de los cambios" (2020, p. 11). Por ende, se espera que para los próximos años se tomen cartas sobre este asunto, lo que demandará la colaboración de diversos grupos de expertos y disciplinas técnico-científicas que busquen minimizar los riesgos, tanto en el manejo de datos masivos como de los ciberataques por diversos medios de tecnologías emergentes como el IoT.

Para finalizar, no sobra mencionar que se puede minimizar el riesgo de un ciberataque por DDoS simplemente implementando las políticas de seguridad corporativas, instalando los parches y actualizaciones del caso para mantener a salvo y funcionando los sistemas. Asimismo, es importante tener siempre presente el sentido común cuando se navega en Internet. Este actuar debe acentuarse aún más ya que las modalidades de trabajo han venido cambiando. Un ejemplo de ello es el trabajo remoto que ha pasado rápidamente de ser una moda a ser una necesidad, todo por cuenta de la COVID-19. En ese sentido, se ha vuelto un objetivo ideal para ataques de tipo *ransomware*, aprovechando las condiciones particulares en la que se encuentran los usuarios, exponiendo el acceso no autorizado sin que se percaten de ello.

Referencias

Acharya, S. & Tiwari, N. (2016). Survey of DDoS Attacks Based On TCP/IP Protocol Vulnerabilities. *OSR Journal of Computer Engineering (IOSR-JCE), 18*(3), 68-76. doi: http://doi.org/0.9790/0661-1803046876

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack. *Computers & Security, 86*(2019), 402-418. doi: http://doi.org/10.1016/j.cose.2019.07.001

Barrio, A. M. (2018). *Internet de las cosas.* Madrid, España: Editorial REUS.

Bignami, F. (2018). Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance.

GWU Law School Public Law Research, (67), 1-20.

Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS Attack & its Effect in Cloud Environment. *Procedia Computer Science, 49*(49), 202–210. doi: http://doi.org/10.1016/j.procs.2015.04.245

Dos Santos, D., Stanislav, D., Wetzels, J. and Amri, A. (2020). Amnesia:33. How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices. (Research report). Forescout Research Labs.

Ejaz, W., Anpalagan, A., Imran, M. A., Jo, M., Naeem, M., Qaisar, S. B., & Wang, W. (2016). Internet of Things (IoT) in 5G Wireless Communications. *IEEE Access, 4*(4), 10310–10314. doi:10.1109/access.2016.2646120

Feliu, R. (2018). Smart Contract: Concepto, ecosistema y principales cuestiones del Derecho privado. *La Ley mercantil*, 47, 7- 10.

Hao, H., Wang, Y., Shi, Y., Li, Z., Wu, T. & Li, C. (2019). IoT-G: una arquitectura de comunicación inalámbrica de energía privada de baja latencia y alta confiabilidad para redes inteligentes.

Seminario en IEEE International de 2019 Conferencia sobre tecnologías de comunicaciones, control y computación para redes inteligentes (SmartGridComm). Beijing, China.

Ibarra, J., Javed Butt, U., Do, A., Jahankhani, H., & Jamal, A. (2019). *Ransomware* Impact to SCADA Systems and its Scope to Critical Infrastructure. Conference in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). London, United Kingdom.

Ibor, A., & Obidinnu, J. (2015). System Hardening Architecture for Safer Access to Critical Business Data. *Nigerian Journal of Technology, 34*(4), 788. doi:10.4314/njt.v34i4.17

Incibe (s.f). *Cloud computing. Una guía de aproximación para el empresario*. Instituto nacional de ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf

Kak, A. (2021). *TCP/IP Vulnerabilities and DoS Attacks: IP Spoofing, SYN Flooding, and The Shrew DoS Attack*: Lecture Notes on "Computer

and Network Security". Personal Collection ofA, Kak, Purdue University, West Lafayette, Indiana.

Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering, 81*(2020), 106522. doi: http://doi.org/10.1016/j.compeleceng.2019.106522

Lemieux, F. (2019). *Intelligence and state surveillance in modern societies: an international perspective.* Howard House, United Kingdom: Emerald Publishing Limited.

Márquez, J. (2017). Armas cibernéticas. Malware Inteligente para ataques dirigidos. *Ingenierías USB-Med,* 8(2), 48-57. doi: http://doi.org/10.21500/20275846.2955

Márquez, J.. (2020). Internet of Things and Distributed Denial of Service as Risk Factors in Information Security. *IntechOpen.* doi: https://doi.org/10.5772/intechopen.94516.

Márquez, J. (2019). Nanotecnología. Internet de las cosas. doi: http://doi.org/ 10.13140/RG.2.2.33697.66402

Márquez, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista Biòtica i Dret. Rev Bio y Der. 2019*(46) 85-100. doi: https://doi.org/10.1344/rbd2019.0.27068

Nardi, D. (2019). *Country update: China. Religious Freedom in China's High-Tech Surveillance State.* Washington, DC., United States of America: United States Commission on International Religious Freedom (USCIRF).

Novoa, R. K. S., Vargas, V. J. y Berdugo, R. E. O. (2016). La amenaza persistente avanzada (apa) y su método de delincuencia. *Visión electrónica, 10*(2), 224–229. doi: https://doi.org/10.14483/22484728.11740

National Security Agency Federal Bureau of Investigation Cybersecurity Advisory (2020). *Russian GRU 85th GTsSS. Deploys Previously*. Undisclosed Drovorub Malware. (1). Recovered from https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/

CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Pei, K., Cao, Y., Yang, J. & Jana, S. (2019). DeepXplore: automated whitebox testing of deep learning systems. *Communications of the ACM, 11*(62), 137-145. doi: http://doi.org/10.1145/3361566.

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys & Tutorials, 22*(3), 1–1. doi:10.1109/comst.2020.2987688

Porcelli, A. M. (2020). Un hito jurídico sobre Internet de las Cosas: la Ley de California n° 327 del año 2018 vigente a partir del 1 enero del 2020. *Revista Direito GV, 16*(1), 953. doi: https://doi.org/10.1590/2317-6172201953

Roa, S. J. (2020). *Amenazas persistentes avanzadas. Un enemigo en las sombras.* (26). Recuperado de https://www.csirt.gob.cl/media/2020/12/AN2-2020-26.pdf

Rose, K., Eldridge, S. y Chapin, L. (2015, 15 de octubre). *La internet de las cosas - Una breve reseña para*

entender mejor los problemas y desafíos de un mundo más conectado. Internet Society (ISOC). https://www.internetsociety.org/es/resources/doc/2015/iot-overview/

Sánchez, G. y Urrutia, R. (2020, 17 de febrero). *Amenazas Persistentes Avanzadas (APT) como medida de disuasión en el ciberespacio.* Instituto Español de Estudios Estratégicos.http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO12_2020GABSAN_Submarinos.pdf

Santiago, A., Castro, C., Uvidia, M., Samaniego, G., Radicelli, C. y Maggi, D. (2018). Modelo de Seguridad para Garantizar la Integridad de Pagos Móviles sobre Near Field Communication (NFC). *Revista Espacios, 39*(19), 6-30.

Savchenko, V. (2020). Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research. 8. 2019-2025. 10.30534/ijeter/2020/90852020.

Simoens, P., Dragone, M., & Saffiotti, A. (2018). The Internet of Robotic Things. *International*

Journal of Advanced Robotic Systems, 15(1), 172988141875942. doi:10.1177/1729881418759424

Wang, M., Lu, Y. & Qin, J. (2019). A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback. *Computers & Security, 8*(101645), 1-15. doi: https://doi.org/10.1016/j.cose.2019.101645