Implementación de un Sistema de Soporte a la Decisión (DSS) orientado a la gestión de alertas de seguridad de la información de las Instituciones de Educación Superior (IES)

Guamaní Proaño, Wilmer Orlando

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gestión de Sistemas de Información e Inteligencia de Negocios

Trabajo de titulación, previo a la obtención del título de Magister en Gestión de Sistemas de Información e Inteligencia de Negocios

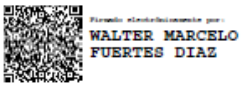
Ing. Fuertes Díaz, Walter Marcelo, PHD

30 de abril de 2021

Documento Tesis V3-Corr-WG-WF.docx

Scanned on: 19:21 March 31, 2022 UTC

Identical Words	983
Words with Minor Changes	132
Paraphrased Words	0
Omitted Words	1770



UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Implementación de un Sistema de Soporte a la Decisión (DSS) orientado a la gestión de alertas de seguridad de la información de las Instituciones de Educación Superior (IES)**" fue realizado por el señor **Guamaní Proaño, Wilmer Orlando** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 30 de abril de 2021

Firma:

WALTER MARCELO FUERTES DIAZ

Firmado digitalmente por WALTER MARCELO FUERTES DIAZ
Nombre de reconocimiento (DN): c=EC, o=SECURITY DATA S.A. 2, ou=ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN, serialNumber=0907201 14120, cn=WALTER MARCELO FUERTES DIAZ
Fecha: 2021.04.30 21:34:44 -05'00'

.....

Ing. Walter Marcelo Fuertes Díaz, PhD

Director

C.C.: 1707017701

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo **Guamaní Proaño, Wilmer Orlando**, con cédula de ciudadanía n° 0503070344, declaro que el contenido, ideas y criterios del trabajo de titulación**: "Implementación de un Sistema de Soporte a la Decisión (DSS) orientado a la gestión de alertas de seguridad de la información de las Instituciones de Educación Superior (IES)"** es de mí autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 30 de abril de 2021

Firma

Firmado electrónicamente por:
WILMER ORLANDO
GUAMANI PROAÑO

.....

Ing. Guamaní Proaño, Wilmer Orlando

C.C.: 0503070344

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Guamaní Proaño, Wilmer Orlando,** con cédula de ciudadanía n° 0503070344, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: "**Implementación de un Sistema de Soporte a la Decisión (DSS) orientado a la gestión de alertas de seguridad de la información de las Instituciones de Educación Superior (IES)**" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 30 de abril de 2021

Firma

Firmado electrónicamente por:
WILMER ORLANDO GUAMANI PROAÑO

……..

Ing. Guamaní Proaño, Wilmer Orlando

C.C.: 0503070344

Dedicatoria

A Dios por darme salud y vida. Quien ha estado conmigo siempre y me ha enseñado como vivir en la vida.

A quienes han estado junto a mi durante toda la vida con apoyo incondicional en todo momento: mi familia; mis amados padres: Gonzalo y Gloria; mis queridos hermanos: Jaime, Edwin, David Guamaní Proaño y amig@s.

Wilmer Guamaní Proaño

"Nunca tomen el estudio como una obligación, sino como la envidiable oportunidad de aprender a conocer la influencia liberadora que ejerce la belleza sobre el Reino del Espíritu"

A. Einstein

Agradecimiento

Por sobre todo a Dios.

A Ing. Walter Fuertes, PhD como persona ejemplar y Tutor de Tesis.

A Ing. Jaime Guamaní Proaño por su valioso aporte.

A Ing. Edwin Guamaní Proaño por su valioso aporte.

A Ing. David Guamaní Proaño por su valioso aporte.

Infinitas gracias a mis padres y hermanos, por su colaboración incondicional.

A toda mi familia.

A la Universidad de la Fuerzas Armadas ESPE.

A CEDIA.

Gracias.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Resumen

Este estudio busca establecer estrategias que fortalezcan la seguridad de la información de las Instituciones de Educación Superior (IES) del Ecuador. Su enfoque se centra en desarrollar soluciones relacionadas con la detección de intrusos, detección de anomalías, detección de vulnerabilidades y detección de incidentes de seguridad. Estas actividades forman parte de los principales servicios de un Equipo de Respuesta ante Incidentes de Seguridad Informático (CSIRT). Sin embargo, actualmente la gestión de alertas tempranas se realiza de forma manual, lo que puede derivar en incidentes de seguridad. A esto se suma que en las IES dado el incremento del teletrabajo y la teleeducación, se ha aumentado el número de amenazas, vulnerabilidades, ataques cibernéticos, fallos en los bugs de aplicaciones y sistemas operativos, lo que conlleva a buscar soluciones para proteger a los activos (física y lógicamente) en estas organizaciones.

Este estudio tiene como objetivo incrementar los niveles de seguridad de la información de las IES, para reducir el número de incidentes, que se registran diariamente. Como metodología general, se inició con la revisión del estado del arte, el análisis de la información para definir las fuentes de datos a ser utilizados, y la evaluación y selección de técnicas y herramientas de aprendizaje automático que mejor se adapten a la gestión de alertas de seguridad de la información. Posteriormente se diseñó el modelo de minería de datos y la base de conocimientos de la que se derivó la implementación de un sistema de soporte a la toma de decisiones (DSS) para la gestión de alertas de seguridad. Para esto, se aplicó la metodología de Investigación – Acción, bibliográfica, descriptiva y causal.

Dentro de los resultados esperados, se obtuvo un prototipado DSS, para mostrar, mediante una interfaz de usuario, información que sirva de apoyo a las IES en la toma de decisiones ante eventos de seguridad de la información.

Palabras Clave:

- **APRENDIZAJE AUTOMÁTICO**
- **MINERÍA DE DATOS**
- **ALERTAS DE SEGURIDAD DE LA INFORMACIÓN**
- **GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**

Abstract

This study seeks to establish strategies that strengthen the information security of Higher Education Institutions (IES) of Ecuador. Its focus is on developing solutions related to intrusion detection, anomaly detection, vulnerability detection, and security incident detection. These activities are part of the primary services of a Computer Security Incident Response Team (CSIRT). However, early warning management is currently done manually, which can lead to security incidents. Added to this is the fact that in IES, given the increase in teleworking and Tele-education, the number of threats, vulnerabilities, cyber-attacks, bugs in applications and operating systems has increased, which leads to the search for solutions to protect users assets (physically and logically) in these organizations.

The main of this study is to increase the information security levels of IES to reduce the number of incidents, which are recorded daily. As a general methodology, it began with the review of state of the art, the analysis of the information to define the data sources to be used, and the evaluation and selection of techniques and machine learning tools that are best adapted to the management of alerts information security. Subsequently, the data mining model and the knowledge base from which the implementation of a decision support system (DSS) for the management of security alerts derived was designed.

To do this, the Action Research methodology combined with a bibliographic and descriptive research were applied. Among the expected results, a DSS prototyping was obtained to show, through a user interface, information that serves as support to IES in making decisions in the face of information security events.

Key words:

- **MACHINE LEARNING**
- **DATA MINING**
- **INFORMATION SECURITY ALERTS**
- **INFORMATION SECURITY MANAGEMENT**

Capítulo I: Introducción

Antecedentes

Según la norma ISO 27001, para el mejoramiento continuo de la seguridad de la información, un aspecto importante es la gestión de alertas y de incidentes, que coadyuve a la protección de la confidencialidad, integridad y disponibilidad de los sistemas y datos de las Instituciones de Educación Superior (IES). Sin embargo, las organizaciones no lo realizan adecuadamente, debido a que se enfocan más en temas de índole tecnológico y no en los temas de gestión (ISO - the International Organization for Standardization, 2016).

Frente a este escenario, la Institución para el desarrollo de la Investigación y la Academia (IDIA), tiene como propósito fomentar, promover y coordinar el desarrollo de la investigación científica y la academia, ofrece entre sus principales servicios el Equipo de Respuesta ante Incidentes de Seguridad Informático (CSIRT), el cual realiza la gestión de alertas tempranas de presencia de amenazas que pueden derivar en incidentes de seguridad en TIC en las IES (Reyes-Mena, 2018) (Rodrigo Padilla Verdugo, 2017). Sin embargo, IDIA no cuenta con un sistema de gestión de alertas automatizado que permitan disminuir los incidentes.

Ante esta problemática, se ha creado mediante financiamiento de este organismo el Grupo de Trabajo (GT) en Analítica de Datos e Inteligencia Artificial aplicado a la Ciberseguridad de IDIA, cuyos intereses de investigación son principalmente, la ciberseguridad en los sistemas de información. En este ámbito uno de sus fines es establecer un framework de los componentes de un sistema de soporte a la toma de decisiones (DSS) que se acople al entorno de las IES y permita tener una guía sobre el cumplimiento con la normativa local e internacional relacionada con la ciberseguridad. Además, que permita mejorar sus procesos de gestión ante incidentes informáticos utilizando soluciones de máquinas de aprendizaje y BIG Data (Rodrigo Padilla Verdugo, 2017).

Para el desarrollo del proyecto en mención, el CSIRT de IDIA dispone de Datasets históricos de alertas de seguridad de información de las IES, sobre el cual se realizó el análisis y procesamiento.

El Problema de Investigación

Contexto del Problema

Una amenaza puede causar un incidente no deseado, que puede provocar daños o pérdidas de todo tipo en la organización (ISO - the International Organization for Standardization, 2016). Estas pérdidas pueden proceder de un ataque directo o indirecto sobre el sistema de información. Los ataques son principalmente en forma de revelación, de destrucción, de modificación no autorizada, de indisponibilidad o de pérdida de la información (Aguilera, 2011). Hay circunstancias diversas que pueden permitir que una amenaza se materialice y cause daño. Por ejemplo, la ausencia de un mecanismo de control de acceso a la vulnerabilidad que podría permitir la materialización de la amenaza de intrusión (Bertolín, 2008).

Sobre esta problemática, propuestas similares han empezado a desarrollarse en otras universidades del mundo, como la presentada por la Universidad de Nottingham de Reino Unido junto con la Universidad de Carnegie Mellon de USA en el trabajo de investigación Online Cyber Security Decision Support System (OCYSS) (Carniege Mellon University, 2017), que inició en abril del 2017 y finalizará en noviembre del 2020. Este estudio busco aplicar el uso de aprendizaje automático para evaluar las posibles vulnerabilidades existentes en base a boletines oficiales emitidos por las autoridades Nacionales de seguridad y fabricantes.

En este sentido, la propuesta del GT-Ciberseguridad de IDIA, es trabajar sobre un marco de referencia para la gestión de incidentes, que considera las técnicas de Analítica de datos, Inteligencia Artificial, Big Data y DSS (Reyes, 2018) (Sinnott, 2015). De esta manera se abordó el análisis de datos para poder detectar anomalías o

patrones que puedan ser generados por amenazas o ataques de seguridad. Además, la generación de esta cantidad de información, a grandes velocidades y de diferentes fuentes, de diversos lugares geográficos, permitió aplicar principios de BIG Data (Sinnott, 2015).

Planteamiento del Problema

El número de incidentes de seguridad de la información se incrementa continuamente. Los incidentes están relacionados con la explotación de vulnerabilidades dirigidas a comprometer la seguridad de un sistema o red (Bertolín, 2008). Bajo este contexto, el número de amenazas, vulnerabilidades y ataques cibernéticos se incrementan en todas las IES (datos IDIA y NIST), lo que ha incrementado el número de incidentes de seguridad de la información y los riesgos.

En las IES han aumentado los ataques cibernéticos, fallos en los bugs de aplicaciones y sistemas operativos, lo que lleva a una pérdida o mal uso significativo de los activos de información (Vieites, 2013). Cuando se detecta una nueva vulnerabilidad se registra en una alerta de seguridad donde se indica el evento detectado, las condiciones en las que aparece, las soluciones u opciones de mitigación (Vieites, 2013). En este contexto, se ha identificado, que las IES no disponen de sistemas de Gestión de alertas automatizado, no tienen planes de capacitación, ni han invertido en suficiente tecnología, lo cual disminuye los niveles de seguridad de la información de las IES.

Ante esta problemática, las organizaciones se enfocan más en soluciones de tecnología y no tienen procesos de gestión, generan altos costos en inversión de tecnología para reducir el incremento de alertas de seguridad y sin embargo no logran reducir el número de incidentes de seguridad (Vieites, 2013). “Las IES con el apoyo de IDIA han enfocado sus esfuerzos en herramientas para análisis preventivos de

ataques, así como soluciones físicas para reducir amenazas que pueden derivar en incidentes de seguridad" (Walter Fuertes, 2017).

Además, las alertas de seguridad de la información, es identificada por una serie de eventos indeseados o inesperados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio (Cardona, 2015).

Por otro lado, dado que las IES están ubicadas en lugares geográficos distintos y distantes, es necesario enfrentar al exceso de data desde diversas fuentes de información, lo que complica el análisis de información capturada en tiempo real en un enfoque global y por cada una (Valladares, 2017). Frente a este escenario, se implementó un modelo de minería de datos con el fin de obtener un DSS, para mostrar, mediante una interfaz de usuario, información que sirva de apoyo en la toma de decisiones ante eventos de seguridad.

Objetivos

General

Diseñar e implementar un DSS[1] para la gestión de alertas de seguridad de la información de las IES basado en herramientas de analítica de datos y aprendizaje automático.

Específicos

OE1: Realizar el estado del arte, relacionado a herramientas de minería de datos para la gestión de alertas de seguridad de la información mediante SMS/SLR[2].

[1] DSS (Decision Support System) Herramienta de Business Intelligence el cual ayuda a la toma de decisiones compilando información útil sobre los datos sin procesar.

[2] SMS (Systematic Mapping Study) método definido para construir un esquema de clasificación y estructurar un campo de interés que proporciona un resumen visual de sus resultados, SLR (Systematic Literature Review) es un método se estudió secundario.

OE2: Evaluar los algoritmos y herramientas de minería de datos utilizando estudios de Benchmarking existentes en el Internet, para seleccionar la que más se adapte a la gestión de alertas de seguridad de la información.

OE3: Diseñar el modelo de minería de datos e implementar un sistema de soporte a la decisión (DSS) para la gestión de alertas de seguridad de la información, con el fin de incrementar los niveles de seguridad de la información de las IES.

OE4: Evaluar y validar el modelo implementado mediante pruebas funcionales y no funcionales de Ingeniería de Software con el fin de ponerlo en producción.

Hipótesis

La implementación de un DSS basado en herramientas de analítica de datos y aprendizaje automático para la gestión de alertas de seguridad de la información en las IES, permitirá incrementar el nivel de seguridad de la información.

Señalamiento de Variables:

Variable dependiente: Nivel de seguridad de la información a través de predicción de incidentes.

Variable independiente: Técnicas de aprendizaje supervisado para procesar alertas de seguridad.

La contrastación de la hipótesis planteada se realizará mediante la aplicación de herramientas de analítica de datos y aprendizaje automático y validando el modelo mediante métricas de evaluación destinadas a análisis de datos.

Justificación Importancia y Alcance

La gestión exitosa de incidentes que amenazan la seguridad informática de una organización es una tarea compleja (Tejada, 2015). El enfoque principal de una organización está en los aspectos de respuesta de los incidentes de seguridad, lo que

resulta en su incapacidad para gestionar los incidentes más allá de simplemente reaccionar ante eventos amenazantes (Dorofee, 2018).

Para lograr el mejoramiento continuo de la seguridad de la información en una entidad es fundamental establecer la metodología de gestión de riesgos (Tejada, 2015), la cual debe comprender una identificación, análisis, evaluación y tratamiento de los riesgos en seguridad de la información presentes en la entidad y por otra parte, el proceso de gestión de los incidentes de seguridad de la información, que le permita estar preparada para responder ante la presencia de uno o varios incidentes de seguridad que comprometan la continuidad de sus procesos vitales (Gonzalez Díaz, 2013).

Frente a este escenario, las universidades y escuelas politécnicas buscan establecer estrategias que les permita fortalecer su seguridad de la información y de manera especial resolver la inseguridad generada por el ciber espacio. Y para incrementar el nivel de seguridad en las IES es importante gestionar las alertas de seguridad y evitar incidentes de seguridad informática (Tejada, 2015). En consecuencia, implementar un sistema DSS que permita la toma de decisiones a nivel gerencial para la gestión de seguridad de la Información.

Esta investigación realizó la recolección y análisis de la información para definir las fuentes de datos a ser utilizados, luego procedió a la evaluación y selección de los algoritmos y herramientas de minería de datos que mejor se adapte a la gestión de alertas de seguridad de la información y posterior el diseño del modelo de minería de datos que permita la implementación de un DSS para la gestión de alertas de seguridad utilizando el algoritmo y herramienta seleccionados. Con esto se procedió a evaluar los resultados conjuntamente con expertos de las IES y determinar si los resultados obtenidos son óptimos.

Preguntas de Investigación

A continuación, se describen los cuestionamientos que son los orientadores del proceso de investigación.

OE1–RQ1.1: ¿Cuáles son los estudios relacionados sobre gestión de alertas de seguridad de la información?

OE1-RQ1.2: ¿Cuáles son los estándares internacionales del sistema de gestión de seguridad de la información (SGSI), gestión de incidentes?

OE1–RQ1.3: ¿Cuáles son las técnicas de minería de datos aplicadas a alertas de la seguridad de la información?

OE2–RQ2.1: ¿Cuáles son las técnicas y herramientas de minería de datos que se adaptan a la gestión de alertas de seguridad de la información?

OE2–RQ2.2: ¿Cuáles serían los criterios y argumentos técnicos para realizar un proceso de evaluación de las técnicas o herramientas de minería de datos?

OE3–RQ3.1: ¿Qué metodología, método de minería de datos se debe aplicar para el diseño del modelo de gestión de alertas de seguridad de la información?

OE3-RQ3.2: ¿La información generada por el modelo de minería de datos permite implementar un DSS para la gestión de alertas de seguridad de la información?

OE3-RQ3.3: ¿Cuáles son los componentes de un DSS que permita la gestión de alertas de seguridad de la información?

OE4–RQ4.1: ¿Cuáles serían los criterios y argumentos de Ingeniería de Software para realizar las pruebas funcionales y no funcionales del modelo?

OE4–RQ4.2: ¿Cuál es el nivel de confianza o satisfacción alcanzado, mediante pruebas funcionales y no funcionales de Ingeniería de Software?

Metodología de Investigación

Para la ejecución de la investigación se aplicó la metodología Investigación – Acción. Esta metodología hace un acercamiento al objeto de estudio, se parte de un diagnóstico inicial, punto de vista, opiniones, sobre un tema o problemática susceptible de cambiar. Lewin presenta lo que denomina ciclos de acción reflexiva: planificación, acción y evaluación de la acción. (Colmenares E, 2012). Además, durante su desarrollo se utilizó las metodologías de investigación bibliográfica, descriptiva y causal. En la Tabla 1 se muestra el desarrollo de los objetivos específicos.

Tabla 1.

Metodología de investigación

CICLO	OBJETIVO	ACCIONES
1	**OE1:** Realizar el estado del arte, relacionado a técnicas de minería de datos para la gestión de alertas de seguridad de la información mediante SMS/SLR.	Revisión de literatura sobre gestión de alertas de seguridad de la información mediante SMS/SLR. Revisión de literatura sobre técnicas de minería de datos para la gestión de alertas de seguridad de la información mediante SMS/SLR.
2	**OE2:** Evaluar los algoritmos y herramientas de minería de datos utilizando estudios de Benchmarking existentes en el Internet, para seleccionar la que más se adapte a la gestión de alertas de seguridad de la información.	Evaluar los algoritmos y herramientas de minería de datos utilizando estudios de Benchmarking. Evaluar los algoritmos con métricas de evaluación destinadas a análisis de datos y realizar un cuadro comparativo entre los algoritmos y herramientas más utilizados. Para la selección se revisará que algoritmo (reglas de asociación, clusterización o arboles de decisión, entre otros) se adapta mejor a nuestro requerimiento.

CICLO	OBJETIVO	ACCIONES
3	**OE3:** Diseñar el modelo de minería de datos e implementar un sistema de soporte a la decisión (DSS) para la gestión de alertas de seguridad de la información, con el fin de incrementar los niveles de seguridad de la información de las IES.	Analizar las fuentes de datos con que cuenta la organización y que puedan ser útiles. Hacer un análisis previo con gráficos de dispersión que permita ver la distribución de los datos para identificar valores atípicos. Comparar y seleccionar la metodología a utilizar como CRISP-DM o KDD-Process. Seleccionar la herramienta que nos servirá para la implementación del DSS. Verificar que los tipos de datos a utilizar para la implementación sean los adecuados. En caso de que la data no se ajuste automáticamente buscar la manera de convertir los datos para que se ajuste al modelo a implementar.
4	**OE4:** Evaluar y validar el modelo implementado mediante pruebas funcionales y no funcionales de Ingeniería de Software con el fin de ponerlo en producción.	Evaluar y validar el modelo mediante métricas de evaluación destinadas a análisis de datos. Evaluar y validar el modelo a través de pruebas funcionales y no funcionales de Ingeniería de Software. Evaluar los resultados conjuntamente con expertos de las IES y determinar si los resultados obtenidos son óptimos.

Estado del Arte

Para llevar a cabo el análisis del estado del arte se utilizó un proceso SMS/SLR, definido para construir un esquema de clasificación y estructurar un campo de interés que proporciona un resumen visual de sus resultados (Sinoara, 2017), que incluye las fases de criterios de inclusión y estrategias de búsqueda, como fuentes de

búsqueda de la información se usaron las siguientes bibliotecas digitales: ACM Digital Library, IEEE Xplore, Springer y Scopus.

Definición del objetivo: El objetivo del estudio del estado del arte está enfocado en resolver las preguntas de los objetivos específicos planteados en la sección 1.5.1.

Definición de los criterios de inclusión y exclusión: Con el fin de determinar que estudios fueron relevantes para las preguntas de investigación se tomaron en cuenta los títulos y resúmenes, en los cuales se consideraron los siguientes criterios.

Criterios de Inclusión

- Artículos publicados a partir del 2010.
- Artículos científicos y documentos de conferencias publicados en idioma inglés.
- Artículos que contenga información referente a técnicas de minería de datos para la gestión de alertas de seguridad de la información.

Criterios de Exclusión

- Artículos con temas de minería de datos no relacionados con gestión de alertas de seguridad de la información.
- Artículos que no estén en idioma inglés.
- Artículos publicados antes del 2010.

Definición de la estrategia de búsqueda

Revisión Inicial: Se realiza una indagación inicial en las distintas bibliotecas digitales para buscar estudios relacionados con las preguntas de investigación.

Validación cruzada de estudios: En esta etapa se procede a verificar que los estudios cumplan con los criterios de inclusión y exclusión, con el fin de obtener el

listado inicial de documentos académicos con los cuales se va a trabajar en las siguientes fases del estudio.

Integración del grupo de control: Está conformado por los estudios que cumplen con los criterios de inclusión y exclusión, con lo cual se realiza el análisis del título, resumen, introducción, conclusiones y palabras claves. Los estudios seleccionados para el grupo de control se muestran en la tabla 2.

Tabla 2.

Estudios bases para formar el grupo de control

Grupo de Control	Título	Palabras Clave
EC1	Information management and decision support in critical infrastructure emergencies at the local level.	critical infrastructure protection; emergency operations; data fusion; decision support; data mining.
EC2	Survey of Attack Projection, Prediction, and Forecasting in Cyber Security	Cyber security; intrusion detection; situational awareness; prediction; forecasting; model checking; data mining.
EC3	Research on The Network Security Management Based on Data Mining	Network Security Management; data mining; intelligent analysis
EC4	Dimensional Data Model for Early Alerts of Malicious Activities in a CSIRT	CSIRT; Data warehousing; BI; Early Warning to Computer Attacks; ETL Process; OLAP cubes; Dimensional Data Model
EC5	Towards Predicting Cyber Attacks Using Information Exchange and Data Mining	Attack prediction, Collaborative security, Information exchange, Data mining
EC6	A User-Centric Machine Learning Framework for Cyber Security Operations Center	user-centric; Machine Learning system; cyber security operation center; risky user detection

Construcción de la cadena de búsqueda: Se definió un conjunto de palabras clave para formar los términos de búsqueda a partir de los estudios del grupo de control. Se definieron los siguientes contextos: Minería de datos, Big Data, Gestión de Seguridad Informática. (ver tabla 3)

Tabla 3.

Construcción de la cadena de búsqueda

Contexto	Palabra Clave	EC 1	EC 2	EC 3	EC 4	EC 5	EC 6	Número de Repeticiones
Minería de datos	Data mining	x	x	x		x		4
	Machine Learning		x				x	2
	Intelligent analysis			x				1
	Data Visualization		x					1
Big Data	ETL Process				x			1
	Attack prediction		x		x	x	x	4
	Decision support	x						1
	Data warehousing				x			1
	OLAP cubes				x			1
	Dimensional Data Model				x			1
Gestión de Seguridad Informática	Cyber security		x	x			x	3
	Information exchange					x		1
	Collaborative security					x		1
	Network security Management			x				1
	CSIRT				x			1
	Critical infrastructure protection	x						1

Los términos presentes en cada grupo se combinaron utilizando el operador booleano “OR” y todos los grupos se combinaron utilizando el operador booleano “AND”, de esta manera se seleccionó la cadena de búsqueda para obtener la mayor cantidad de información relevante, donde se aplicaron los criterios de inclusión y exclusión.

((Machine Learning OR data mining) AND (information security alerts) AND (information security management))

La identificación del estudio se realizó mediante búsquedas de estudios realizados en tres bibliotecas digitales: ACM Digital Library, IEEE Xplore, Springer Link (Sinoara, 2017). Las bibliotecas digitales cubren una amplia gama de publicaciones en el campo de la ciencia de la Ingeniería.

Se aplicó las siguientes expresiones de búsqueda general tanto en el título como en las palabras clave, cuando el motor de búsqueda de la biblioteca digital lo permite.

Se generó la consulta mediante las cadenas de búsqueda y se ejecutó en las bases de datos electrónicas más relevantes considerando el título, el resumen y las palabras clave, y los trabajos publicados desde el 2010. Las bases de datos utilizadas son IEEE Xplore, ACM Digital Biblioteca, y Springer.

Resultados del SLR

El número de estudios encontrados en cada base de datos se presenta en la tabla 4. Debido a las diferentes características de los motores de búsqueda, en algunos casos, la consulta se implementó utilizando una estrategia individual para cada base de datos. Para dividir la cadena de búsqueda en fragmentos pequeños, se ejecutó cada uno por separado y se unió los resultados. Al final de esta etapa, se obtuvo un conjunto de 1346 estudios.

Tabla 4.

Cadenas de búsqueda en base de datos

Cadena	Biblioteca Digital	Resultado
(((data mining) AND algorithm) AND cyber security)	IEEE	231
	ACM	37345
	Springer Link	4839
(((data mining) AND information security alerts) AND information security management)	IEEE	9
	ACM	197942
	Springer Link	5410
((((Machine Learning) OR data mining) AND information security alerts) AND information security management)	IEEE	18
	ACM	1216
	Springer Link	112

En la segunda etapa, los estudios repetidos fueron descartados, dejando como resultado 473. En la tercera etapa, los criterios de inclusión/exclusión se aplicaron en los estudios restantes, y se incluyó o excluyó un artículo leyéndolo en el siguiente orden: título, resumen, introducción, conclusión y todo el trabajo si es necesario. Al final de esta etapa, se obtuvo un conjunto de diez publicaciones. Finalmente, en el último paso, se utilizaron citas y la lista de referencias de los documentos encontrados para identificar otros estudios admisibles y se identificaron dos artículos adicionales. Por lo tanto, el conjunto final se compone de 12 publicaciones que se muestra en la tabla 5.

Tabla 5.

Grupo control de estudios primarios

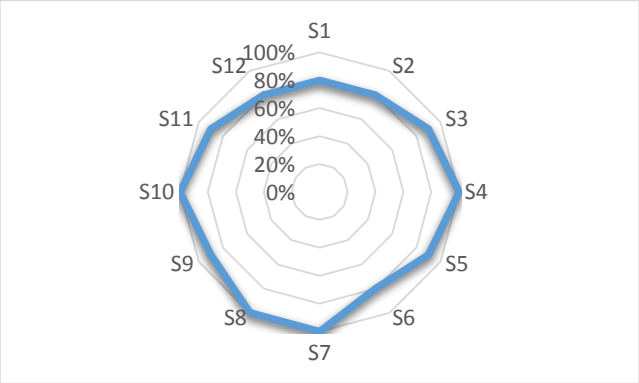
Año	Ítem	Study	Name
2017	S1	[5]	A user-centric Machine Learning framework for cyber security operations center

Año	Ítem	Study	Name
2017	S2	[10]	Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design
2019	S3	[11]	Network Intrusion Detection in Smart Grids for Imbalanced Attack Types Using Machine Learning Models
2016	S4	[12]	CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities
2010	S5	[13]	MARS: Multi-stage Attack Recognition System
2013	S6	[6]	An approach to the correlation of security events based on Machine Learning techniques
2010	S7	[14]	Using vulnerability information and attack graphs for intrusion detection
2018	S8	[15]	Enhancing the Accuracy of Intrusion Detection Systems by Reducing the Rates of False Positives and False Negatives Through Multi-objective Optimization
2016	S9	[4]	Intrusion Alert Correlation to Support Security Management
2011	S10	[16]	Towards a Multiagent-Based Distributed Intrusion Detection System Using Data Mining Approaches
2016	S11	[17]	New Types of Alert Correlation for Security Information and Event Management Systems
2016	S12	[18]	DDoS Attacks Detection in Cloud Computing Using Data Mining Techniques

En la Figura 1. Se muestra la relevancia de las investigaciones y los pesos de selección.

Figura 1.

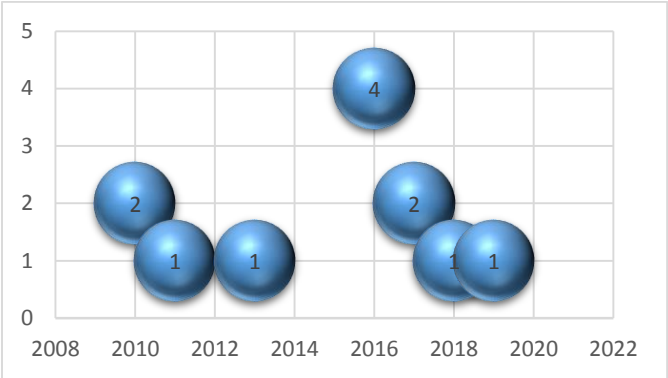
Percent agreement



En la Figura 2. Se muestra los años en los cuales los artículos fueron publicados, en el 2016 refleja que se realizó un mayor hincapié de publicaciones enfocados en la gestión de alertas de la información mediante técnicas de minera de datos.

Figura 2.

Distribución de publicaciones por años



De los resultados obtenidos se realizó la revisión de los documentos encontrados, los cuales se listan a continuación los documentos con más relevancia:

Towards Predicting Cyber Attacks Using Information Exchange and Data Mining

Presenta una evaluación empírica para predecir las actividades de los atacantes en base al intercambio de información y la extracción de datos. Recopilando

las alertas de seguridad cibernética compartidas dentro de la plataforma SABU, en las que comparten cada día alrededor de 220000 alertas de sensores heterogéneos distribuidos geográficamente (sistemas de detección de intrusos y honeypots). Entre los métodos de minería utilizaron reglas secuenciales para identificar patrones de ataque comunes y para derivar reglas de predicción de ataques. Con esto pueden predecir, primero, qué hará el atacante a continuación y cuándo. En segundo lugar, pueden predecir dónde impactará el ataque, por ejemplo, cuando un atacante está apuntando a varias redes a la vez" (Husák M. &.-5., 2018)**.**

Data Mining for Malicious Code Detection and Security Applications (Thuraisingham, 2011)**.**

Este artículo, trata sobre la minería de datos para aplicaciones de seguridad cibernética. Por ejemplo, las técnicas de detección de anomalías podrían usarse para detectar patrones y comportamientos inusuales. La clasificación se puede usar para agrupar varios ataques cibernéticos y luego usar los perfiles para detectar un ataque cuando se produce. La predicción se puede usar para determinar posibles ataques futuros dependiendo de la información obtenida sobre los terroristas a través de correo electrónico y conversaciones telefónicas. La minería de datos también se está aplicando para la detección de intrusiones y auditorías. Otras aplicaciones incluyen la extracción de datos para la detección de códigos maliciosos, como la detección de gusanos y la gestión de políticas de firewall.

A heuristic attack detection approach using the "least weighted" attributes for cyber security data (Dali, 2017)**.**

Este artículo, busca emplear técnicas de minería de datos en un entorno basado en la nube, mediante la selección de atributos y características apropiados con la menor importancia en términos de peso para la clasificación. A menudo, el estándar es seleccionar características con mejores ponderaciones mientras se

ignoran las que tienen menos ponderaciones. En este estudio, busca averiguar si se puede hacer predicciones utilizando esas características con menos ponderaciones. La motivación es que los adversarios utilizan el sigilo para ocultar sus actividades de lo obvio. emplean la ganancia de información para seleccionar atributos con los pesos más bajos y luego aplican Machine Learning para clasificar si una combinación, en este caso, de los puertos de origen y destino son atacados o no.

Classification of cyber attacks based on rough set theory (Amin, 2015)**.**

Este estudio, utiliza la teoría de conjuntos aproximados (RST), un enfoque de toma de decisiones basado en reglas para extraer reglas para la clasificación de ataques de intrusión. Realizaron experimentos en datos disponibles públicamente para explorar el rendimiento de cuatro algoritmos diferentes, por ejemplo. Algoritmo genético, algoritmo de cobertura, LEM2 y algoritmos exhaustivos. La clasificación de RST basada en el algoritmo genético para la generación de reglas produce el mejor rendimiento en comparación con otros algoritmos de generación de reglas mencionados. Además, al aplicar la técnica en el conjunto de datos disponibles públicamente sobre ataques de intrusión, los resultados muestran que el enfoque propuesto puede predecir completamente todos los ataques de intrusión y también proporciona información útil previa a los ingenieros de seguridad o desarrolladores para llevar a cabo una acción obligatoria.

Survey of Attack Projection, Prediction, and Forecasting in Cyber Security (Husák M. K.-H., 2018)**.**

Este artículo proporciona un estudio sobre la predicción y los métodos de pronóstico utilizados en la seguridad cibernética. Discuten temas principales como, la proyección de ataques y el reconocimiento de la intención, en los que es necesario predecir el siguiente movimiento o las intenciones del atacante, la predicción de intrusiones, en la que es necesario predecir los próximos ataques cibernéticos y la

situación de seguridad de la red previsiones, en las que proyectaron la situación de ciberseguridad en toda la red. Analizan, comparan y contrastan ambos métodos basados en modelos discretos, como los gráficos de ataque, las redes bayesianas y los modelos de Markov, y los modelos continuos, como las series temporales y los modelos en gris. Además, de Machine Learning y los métodos de extracción de datos, que han ganado mucha atención recientemente y parecen prometedores para un entorno en constante cambio, que es la seguridad cibernética.

A study on association rule mining of darknet big data (Ban, 2015)

Este artículo, presenta un estudio sobre la caracterización de los ataques cibernéticos, muestra que el aprendizaje de las reglas de asociación en la transmisión de datos de la red puede admitir la contramedida estratégica de ataques cibernéticos de las siguientes maneras. Las estadísticas calculadas a partir de reglas específicas de malware pueden conducir a una mejor comprensión de la tendencia global de los ataques cibernéticos en Internet. Las fuertes reglas de asociación pueden llevar a una mayor comprensión de la naturaleza de las herramientas de ataque y, por lo tanto, acelerar el diagnóstico. Luego, el descubrimiento de nuevos ataques emergentes puede llevar a una detección temprana y una pronta prevención de los incidentes, evitando daños en la infraestructura de TI y pérdidas financieras importantes. Finalmente, explorar el conocimiento de los patrones de ataque frecuentes puede permitir la predicción precisa de futuros ataques de los hosts analizados, lo que podría mejorar el rendimiento de los sistemas Honeypot.

Predictability-oriented defense against adaptive adversaries (Colbaugh, 2012)**.**

Este artículo adopta una perspectiva de defensas contra adversarios adaptativos, aprovechando la relación entre atacantes y defensores para obtener métodos para predecir y contrarrestar los ataques y para limitar la medida en que los adversarios pueden aprender acerca de las estrategias de defensa. El enfoque

propuesto combina la teoría de juegos con el aprendizaje automático para modelar la adaptación del adversario en el espacio de características del aprendiz, lo que produce clases de defensas predictivas y de "objetivo en movimiento" que tienen una base científica y son aplicables a problemas de escala y complejidad del mundo real.

Cyber security meets artificial intelligence: a survey (Li, 2018)**.**

Existe una amplia gama de intersecciones interdisciplinares entre la seguridad cibernética y la inteligencia artificial (IA). Por un lado, las tecnologías de la inteligencia artificial, como el aprendizaje profundo, pueden introducirse en la seguridad cibernética para construir modelos inteligentes, para implementar la clasificación de malware y la detección de intrusos y atacar la detección de inteligencia. Por otro lado, los modelos de IA se enfrentarán a varias amenazas cibernéticas, que perturbarán su muestra, aprendizaje y decisiones. Por lo tanto, los modelos de IA necesitan tecnologías de protección y defensa de seguridad cibernética específicas para combatir el aprendizaje de máquinas adversas, preservar la privacidad en el aprendizaje de máquinas, el aprendizaje federado seguro, etc. Este artículo hace una revisión de la intersección de IA y la seguridad cibernética. Resumen los esfuerzos de investigación existentes en términos de combatir los ataques cibernéticos utilizando la IA, incluida la adopción de métodos de aprendizaje automático tradicionales y las soluciones de aprendizaje profundo existentes.

An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence (Walter Fuertes, 2017)**.**

Los ataques cibernéticos han aumentado en severidad y complejidad. Eso requiere que el CERT / CSIRT investigue y desarrolle nuevas herramientas de seguridad. Este estudio se centra en el diseño de un modelo integral basado en Business Intelligence (BI), que proporciona servicios reactivos y proactivos en un CSIRT, para alertar y reducir cualquier actividad sospechosa o malintencionada en

sistemas de información y redes de datos. Para lograr este propósito, han reunido una solución que genera almacenes de información y se compila a partir de una transmisión de red continua de varias fuentes internas y externas de una organización. Diseñaron e implementaron sistemas de BI utilizando las fases de la metodología de Ralph Kimball, ETL y los procesos OLAP. Además, implementaron una aplicación de software utilizando la metodología SCRUM, que permitió vincular los registros obtenidos al sistema de BI para la visualización en paneles dinámicos, con el fin de generar alertas tempranas y construir consultas complejas utilizando la interfaz de usuario a través de estructuras de objetos.

A User-Centric Machine Learning Framework for Cyber Security Operations Center

En este estudio, desarrollan un marco de aprendizaje de máquina centrado en el usuario para el centro de operaciones de seguridad cibernética en un entorno empresarial real. Discuten fuentes de datos típicas en el centro de operaciones de seguridad (SOC), su flujo de trabajo y cómo aprovechar y procesar estos conjuntos de datos para construir un sistema de aprendizaje automático efectivo. El artículo está dirigido a dos grupos de lectores. El primer grupo está formado por científicos de datos o investigadores de aprendizaje automático que no tienen conocimientos de dominio de seguridad cibernética. No obstante, desean desarrollar sistemas de aprendizaje automático para el centro de operaciones de seguridad. El segundo grupo de audiencias, son aquellos profesionales de seguridad cibernética que tienen un profundo conocimiento y experiencia en seguridad cibernética, sin embargo, no tienen experiencias de aprendizaje automático y desean construir una por sí mismos. usaron el sistema que construyeron en el entorno de producción de Symantec SOC como ejemplo para demostrar los pasos completos desde la recopilación de datos, la creación de etiquetas, la ingeniería de características, la selección de algoritmos de

aprendizaje automático, las evaluaciones de desempeño de modelos, hasta la generación de puntajes de riesgo (Feng, 2017)**.**

Respuesta a preguntas de Investigación

De la investigación realizada y documentos seleccionados, se respondieron las preguntas de investigación planteadas.

- RQ1: ¿Cuáles son los estudios relacionados sobre gestión de alertas de seguridad de la información?

En la mayoría de los estudios tratan la gestión de alertas de seguridad de la información, tal es caso de los estudios (Kawakani, 2016), (Stroeh, 2013), (Franklin, 2017), (Hachmi, 2019), (Granadillo, 2016) que presentan la importancia de realizar la gestión de las alertas de seguridad mediante técnicas de minería de datos que se pueden utilizar para el análisis de una gran cantidad de alertas de intrusión y encontrar patrones interesantes y resumirlos en estructuras de información mejoradas. En este trabajo (Kawakani, 2016), proponen un nuevo enfoque para ayudar al analista de seguridad en el análisis de alertas de intrusión. El enfoque propuesto se compone de dos elementos: el correlacionador fuera de línea y el correlacionador en línea.

- RQ2: ¿Cuáles son los estándares internacionales del sistema de gestión de seguridad de la información (SGSI), gestión de incidentes?

En (Garae, 2017), presentan varios estándares de seguridad cibernética y los evalúan con el propósito de resaltar la importancia de cómo los estándares de sistema de gestión de seguridad de la información ayudan a gestionar y reducir los posibles ataques cibernéticos.

La tabla 6 muestra los estándares de seguridad cibernética. Desde una perspectiva práctica, ISO 27001 proporciona formalmente una guía de gestión de riesgos de información a través de controles de seguridad de la información en una

organización. Por ejemplo, el ISO / IEC 27001: 2005 proporcionó el ciclo “PDCA (Planificar-Hacer-Verificar-Actuar / Ajustar) o Demingcycle”. ISO27032 no es el otro estándar de certificación de seguridad de Internet en seguridad (Garae, 2017). En cualquier estándar de seguridad, se implementan políticas y directrices para incluir y mantener todos los aspectos en los eventos de seguridad.

Tabla 6.

Estándares relacionados con la seguridad cibernética

ISO/IEC 27000 SERIES	
ISO Codes	Description
ISO/IEC 27000	Information Security Management System (ISMS) -- overview
ISO/IEC 27001	Information Technology: Security Techniques in ISMS
ISO/IEC 27032	Guideline for Cybersecurity

- RQ3: ¿Cuáles son las técnicas de minería de datos aplicadas a alertas de la seguridad de la información?

En el sistema del estudio (Feng, 2017), experimentan varios algoritmos de aprendizaje automático, incluida la Multi-layer Neural Network (MNN) con dos capas ocultas, Random Forest (RF) con 100 árboles Ginisplit, Support Vector Machine (SVM) con núcleo de función de base radial y Logistic Regression (LR). En la práctica, descubren que la Multi-layer Neural Network y Random Forest funcionan bastante bien para el problema.

El estudio (Stroeh, 2013), separa en meta-alertas que representan ataques de falsas alarmas es una tarea ideal para las técnicas de aprendizaje automático. Verifican cómo se comportan las técnicas modernas, como las SVM y las Bayesian Networks, dentro de la capa de clasificación.

- RQ4: ¿Cueles son las herramientas de minería de datos que se adaptan a la gestión de alertas de seguridad de la información?

Los softwares o herramientas de minería de datos permiten elaborar modelos predictivos, descubre patrones y tendencias en datos estructurados y no estructurados, modela los resultados y reconoce factores que influyen en ellos (Mikut, 2011).

Para la aplicación de minería de datos con licencia libre se puede mencionar: MiningMart, Orange; TariyKDD, ARMiner y WEKA; por el lado comercial: Cart; SAS Enterprise Miner, Tiberius, Kxen, IBM SPSS Modeler, entre otros (Mikut, 2011). En la tabla 7 se muestra un comparativo entre algunas de estas herramientas.

Tabla 7.

Comparativo entre algunas herramientas

Característica	**IBM SPSS Modeler**	**SAS Enterprise Miner**	**Tarlykdd**	**Weka**	**Jupyter Notebook**
Licencia libre	No	No	Si	Si	Si
Requiere conocimientos avanzados	No	No	No	No	No
Acceso a SQL	Si	No	Si	Si	Si
Multiplataforma	No	Si	Si	Si	Si
Requiere bases de datos especializadas	No	--	No	No	No
Métodos de máquinas de soporte vectorial	Si	Si	No	Si	Si
Métodos bayesianos	Si	--	No	Si	Si
Puede combinar modelos	Si	Si	No	Si (no resulta	Si

Característica	IBM SPSS Modeler	SAS Enterprise Miner	Tarlykdd	Weka	Jupyter Notebook
				muy eficiente)	
Modelos de clasificación	Si	Si	Si	Si	Si
Implementa arboles de decisión	Si	Si	Si	Si	Si
Modelos de regresión	Si	Si	No	Si	Si
Clustering y agrupamiento	Si	Si	No	Si	Si
Interfaz amigable	Si	Si	Si	Si	No
Permite visualización de datos	Si	Si	Si	Si	Si

- RQ5: ¿Cuáles serían los criterios y argumentos técnicos para realizar un proceso de evaluación de las técnicas o herramientas de minería de datos?

(Hoffmann, 2019) Realizó un estudio de benchmarking. Los modelos de clasificación se comparan en conjuntos de datos de comportamiento relacionados con la ciberseguridad. Las comparaciones estadísticas de rendimiento con análisis de curvas de aprendizaje demuestran dos hallazgos importantes. Esboza pautas para un benchmarking en aprendizaje automático, principios de benchmarking, estimación de precisión y validación de modelos. Proporciona referencias a repositorios y concursos establecidos y discute los objetivos y limitaciones del benchmarking.

Benchmarking es clave para progresar en el aprendizaje automático, ya que permite una comparación sin prejuicios entre métodos alternativos. Presenta pautas y mejores prácticas para la evaluación comparativa en clasificación y regresión. Establece principios benchmarking y analiza las métricas de rendimiento para un análisis comparativo estadístico sólido donde lista los criterios, objetivos y

restricciones que determinan la preferencia entre algoritmos de aprendizaje alternativos, diseños y parametrizaciones que incluyen los siguientes aspectos:

- La complejidad del modelo es un aspecto importante en la selección de un método particular, ya que afecta el rendimiento de la predicción, la complejidad computacional y la interpretabilidad.
- La complejidad computacional involucra principalmente los recursos algorítmicos requeridos para aprender un modelo de los datos de entrenamiento. Además, también se refiere a la cantidad de cálculo requerido para predecir la respuesta en la fase de consulta.
- La escalabilidad es un problema estrechamente relacionado, ya que refleja la capacidad de manejar grandes volúmenes de datos o problemas con un espacio de características de alta dimensión. La cantidad de datos recopilados en Internet, comercio, industria y ciencias aumenta exponencialmente.

(Hoffmann, 2019).

(De Cnudde, 2020) define que el alcance del estudio de benchmarking está delineado por el tipo de datos analizados y las técnicas de clasificación comparadas, también presenta el procedimiento de evaluación. Los componentes del estudio de benchmarking y las medidas de desempeño para realizar un proceso de evaluación de las técnicas o herramientas de minería de datos son:

Datos

Datos de comportamiento

Procedimiento de selección de conjunto de datos

Colección de conjunto de datos

Técnicas de clasificación

Medidas de desempeño

Área bajo curva ROC (AUC)

Prueba de significación estadística

Curvas de aprendizaje

Propuesta

El número de incidentes de seguridad de la información se incrementa continuamente. Los incidentes están relacionados con la explotación de vulnerabilidades dirigidas a comprometer la seguridad de un sistema o red (Bertolín, 2008). Bajo este contexto, el número de amenazas, vulnerabilidades y ataques cibernéticos se incrementan en todas las IES (datos IDIA y NIST), lo que ha incrementado el número de incidentes de seguridad de la información y los riesgos.

Frente a este escenario, se implementó un modelo de minería de datos con el fin de obtener un DSS, y mostrar, mediante una interfaz de usuario, información que sirva de apoyo en la toma de decisiones ante eventos de seguridad.

La implementación de un DSS para la gestión de alertas de seguridad de la información de las IES se basó en herramientas de analítica de datos y aprendizaje automático.

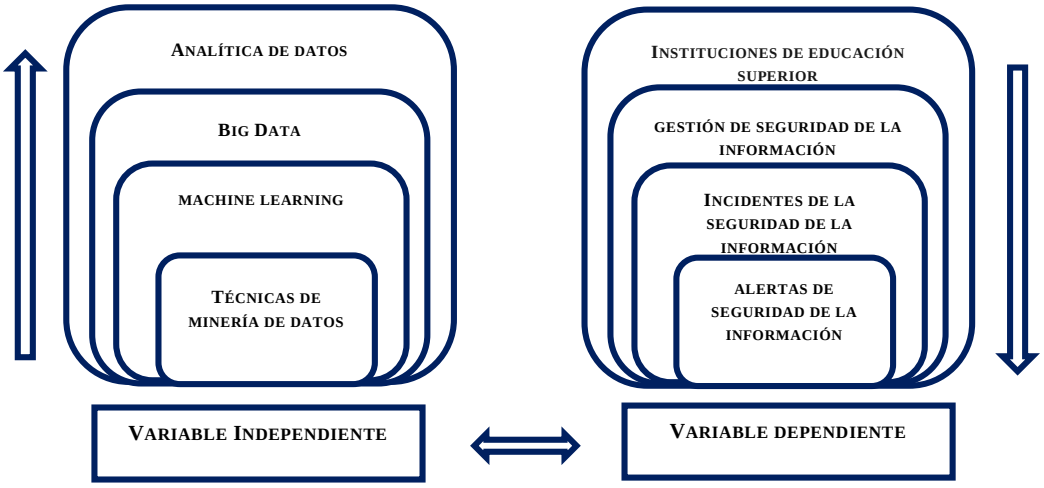
El DSS basado en herramientas de analítica de datos y aprendizaje automático para la gestión de alertas de seguridad de la información en las IES, permite incrementar el nivel de seguridad de la información.

Capítulo II: Marco Teórico

La fundamentación teórica tiene el propósito de generar una congruencia de la teoría con la hipótesis, para esto se realiza un análisis de la teoría a partir de las variables de la hipótesis, con el fin de investigar jerárquicamente cada categoría hasta llegar a la categoría que comprende y explica las variables dependientes e independientes del tema de estudio, para lo cual en la figura 3 se plantea la siguiente jerarquía de estudio:

Figura 3.

Variables dependientes e independientes para el marco teórico



Fundamentación de la variable Independiente

Analítica de datos

Implica los procesos y actividades diseñados para obtener y evaluar datos para extraer información. Es la ciencia de examinar datos en bruto (crudos) con el propósito de obtener conclusiones acerca de la información contenida en ellos. Se utiliza en muchas industrias para permitir a organizaciones y empresas mejoras en la toma de decisiones. Este término se utiliza en el campo de la inteligencia de negocios (business intelligence), y según los fabricantes de herramientas de software pueden abarcar una gran variedad de términos: OLAP, CRM, dashboard (tableros de control).

Existe variedad de herramientas de software que se utilizan en analítica de datos y métodos. Las técnicas más utilizadas son: consultas e informes (quering y reporting), visualización, minería de datos, análisis de datos predictivos, lógica difusa, optimización, streaming de audio, video o fotografía, etc (Aguilar, 2016).

Big Data

Representa una nueva era en la explotación y utilización de datos, las características definitorias de Big Data son: volumen, variedad, velocidad, variabilidad, veracidad, visualización y valor. Big Data es un activo de información de alto nivel, alta velocidad y/o gran variedad que exige costos efectivos, formas innovadoras de procesamiento de información que permiten una visión mejorada, toma de decisiones y procesos de automatización. Se aplica a la información que no se puede procesar o analizar mediante procesos o herramientas tradicionales (Zikopoulos, 2011).

Machine Learning

El aprendizaje automático se refiere a los cambios en los sistemas que realizan tareas asociadas con la Inteligencia Artificial (IA). Dichas tareas implican reconocimiento, diagnostico, planificación, control de robots, predicción, entre otros. El agente de Inteligencia Artificial modela su entorno y calcula las acciones apropiadas, talvez anticipando sus efectos. Los cambios realizados a cualquiera de sus componentes pueden contar como aprendizaje, se podría emplear diferentes mecanismos de aprendizaje dependiendo de qué subsistema se esté cambiando (Nilsson, 1996).

Machine Learning, analiza datos a gran escala y con distintos algoritmos, detectando patrones y modelos en un período muy corto de tiempo, identificando oportunidades rentables y evitando riesgos que podrían ser imperceptibles a la experiencia humano (Chema Alonso, 2018).

En ciberseguridad, el Machine Learning y el Deep Learning se aplican en detección y clasificación de spam, malware, botnets, fraude en tarjetas de crédito, ciberterrorismo en redes sociales, reconocimiento del habla y lenguaje natural, sentimientos (Reyes, 2018).

Hoy en día Machine Learning es importante ya que, junto a otras tecnologías como Big Data, IoT. Abre una gran cantidad de aplicaciones que están cambiando múltiples áreas como la ciberseguridad (Valladares, 2017).

Técnicas de Minería de Datos

La clasificación inicial de las técnicas de minería de datos distingue entre técnicas predictivas, en las que las variables pueden clasificarse inicialmente en dependientes e independientes (similares a las técnicas del análisis de la dependencia o métodos explicativos del análisis multivariante), técnicas descriptivas, en las que todas las variables tienen inicialmente el mismo estatus (similares a las técnicas del análisis de la independencia o métodos descriptivos del análisis multivariante) y técnicas auxiliares (Hernández Orallo, 2004).

Las técnicas predictivas especifican el modelo para los datos en base a un conocimiento teórico previo. El modelo supuesto para los datos debe contrastarse después del proceso de minería de datos antes de aceptarlo como válido (Hernández Orallo, 2004).

En las técnicas descriptivas no se asigna ningún papel predeterminado a las variables. No se supone la existencia de variables dependientes ni independientes y tampoco supone la existencia de un modelo previo para los datos. Tanto las técnicas predictivas como las técnicas descriptivas están enfocadas al descubrimiento del conocimiento embebido de datos (Hernández Orallo, 2004).

Las técnicas auxiliares son herramientas de apoyo más superficiales y limitadas. Se trata de nuevos métodos basados en técnicas estadísticas descriptivas,

consultas y enfocados en general hacia la verificación (Hernández Orallo, 2004). El campo que abarca Machine Learning es amplio y sus tipos, pueden ser:

Técnicas de aprendizaje no supervisado

En las técnicas de aprendizaje no supervisado no tienen una variable de salida para predecir, solo se tiene variables de entrada. En vez de ajustar el modelo a las variables de entrada para predecir la variable de salida, estas técnicas buscan descubrir patrones dentro de los volúmenes de información (Gorakala & Usuelli, 2015).

Por tanto, la máquina debe de ser capaz de encontrar la estructura existente de datos. Este tipo de aprendizaje es muy útil para reducir la dimensionalidad de los datos reduciendo la pérdida de información. Como la segmentación de alertas de seguridad de la información, en la que, a partir de toda una serie de características, el Machine Learning es capaz de encontrar un número de grupos con características similares definido por el analista de datos humano. Y se puede representar gráficamente estos grupos para poder visualizarlos y tener así una mejor comprensión (Aurélien Géron,2017). En el aprendizaje no supervisado los algoritmos se pueden dividir en dos grupos:

Clustering: Son técnicas exploratorias de análisis de datos que se usan para organizar o segmentar la información en grupos, cada grupo o segmentación comparte características similares dando como resultado grupos diferentes en función de sus características. Los modelos que se pueden emplear son k-Means, Hierarchical Cluster Analysis (HCA) y Expectation Maximization.

Visualización y reducción de la dimensión: Reducen la dimensión de los datos por medio de la correlación entre las variables para eliminar el ruido que existe en los datos. Los modelos que se emplean son Principal Component Analysis (PCA),

Locally-Linear Embedding (LLE) y t-distributed Stochastic Neighbor Embedding (t-SNE).

Técnicas de aprendizaje supervisado

Trabaja con datos etiquetados, además de los datos necesarios para realizar la predicción se necesita conocer para cada instancia la característica del objetivo. Es una técnica para deducir una función a partir de datos de entrenamiento. Los datos de entrenamiento consisten en pares de objetos, por un lado, los datos de entrada y por otro lado el resultado deseado. Los datos que se emplean suelen ser valores históricos lo que permite a etiquetar los datos de forma correcta, la etiqueta de los datos se realiza en el proceso de entrenamiento del modelo debido a que es la etapa de prueba donde se comprueba la calidad de la predicción. Entre los algoritmos que son parte están (Aurélien Géron,2017):

- K-NN;
- Regresión lineal;
- Regresión Logística;
- SVM;
- Decision Trees;
- Random Forests;

Dentro del aprendizaje supervisado, se puede dividir en (Macías Macías, Peguero Chamizo, & García Orellana, 2016):

- Clasificación: la salida del sistema debe ser asociada a una de entre un conjunto discreto de clases Ck con k=1, 2, …, e;
- Regresión: cuando la salida del sistema representa a los valores de una variable continua;

(Aurélien Géron,2017).

En ambos casos para resolver el problema desde el punto de vista matemático, tanto el patrón de entrada como el de salida, vienen definidos por un vector numérico.

Fundamentación de la variable dependiente

Instituciones de Educación Superior

Las instituciones de Sistema Nacional de Educación Superior Ecuatoriano tienen como misión la búsqueda de la verdad, el desarrollo de las culturas universal y ancestral ecuatoriana, de la ciencia y tecnología, mediante la docencia, la investigación y la vinculación con la colectividad.

El Sistema de Educación Superior del Ecuador, se encuentra compuesto por 64 Universidades y Escuelas Politécnicas divididas en 28 Publicas, nueve Particulares cofinanciadas y 27 Particulares autofinanciadas, Además por 300 Institutos técnicos y tecnológicos (Larrea, 2012).

Gestión de Seguridad de la Información

Según la ISO 27000, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. La ISO/IEC 27000 es unan norma internacional referente para la gestión de seguridad de la información que cubre todo tipo de organización, y especifica los requisitos para establecer, implementar, supervisar y mejorar un sistema de seguridad de la información. Ofrece un método sistemático y bien estructurado que protege la confidencialidad de la información, asegura la integridad de los datos y mejora la disponibilidad de los sistemas de tecnologías de la información (ISO - the International Organization for Standardization, 2016).

Incidentes de la Seguridad de la Información

Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones

comerciales y amenazar la seguridad de la información (ISO - the International Organization for Standardization, 2016).

Alertas de Seguridad de la Información

Ocurrencia identificada de un sistema, servicio o estado de red que indica un incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. Esto puede incluir intentos de ataques o fallas que exponen vulnerabilidades de seguridad (ISO - the International Organization for Standardization, 2016).

Capítulo III: Diseño e Implementación de la solución

Este capítulo describe la arquitectura del DSS y de manera general las etapas del modelo de proceso CRISP-DM. Las etapas que componen al modelo de proceso CRISP-DM se relacionan entre sí. Estas se llevan a cabo en un ciclo iterativo hasta llegar al descubrimiento del conocimiento deseado. Contiene seis etapas de la metodología tales como el entendimiento del negocio, entendimiento de los datos, preparación de los datos, modelado, evaluación y despliegue.

Arquitectura del DSS

La arquitectura de un DSS está compuesta generalmente por tres componentes: Base de datos (Base de conocimiento), un modelo de contexto de decisión y los criterios del usuario, y la interfaz de usuario. Los usuarios son también componentes importantes de la arquitectura. Estos elementos o capas pueden variar dependiendo del criterio de elaboración del sistema:

- Capa del Cliente;
- Capa de Datos;
- Capa de Negocios;

Capa Cliente: Es donde el cliente interactúa por medio de un navegador Web. En este estudio, reside en un servidor la tecnología Kibana.

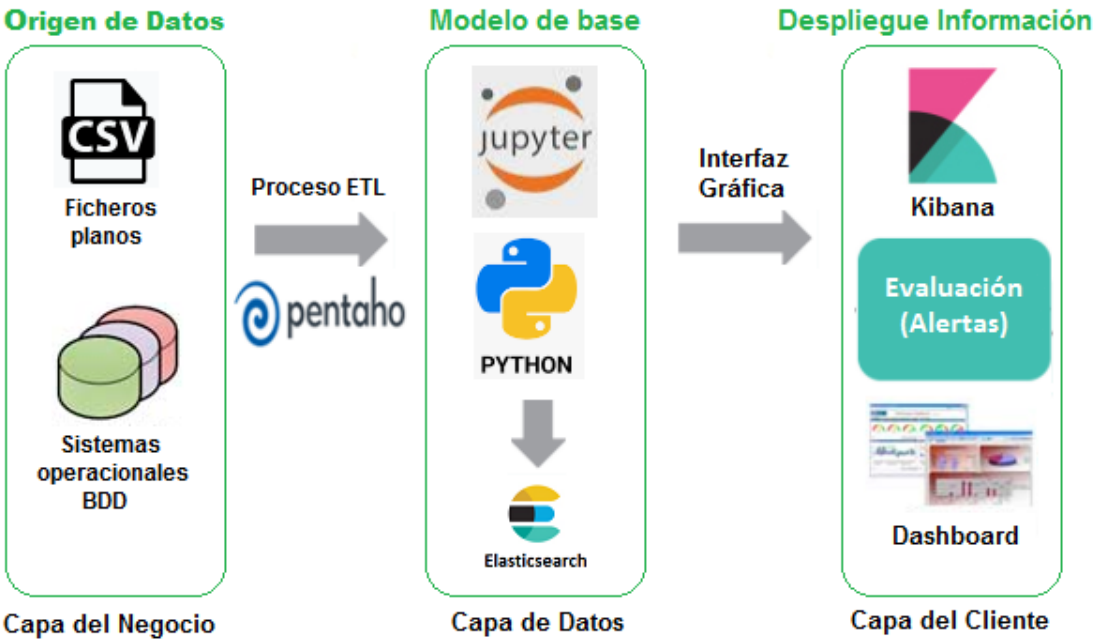
Capa de Negocio: En esta capa está la información origen del negocio. Consiste de las tecnologías aplicadas como los sistemas operacionales, archivos de datos csv. En esta capa se realiza el proceso ETL con la herramienta Pentaho.

Capa de Datos: Se encuentran tecnologías como Jupyter, Python y ElastcSearch. En donde se realiza el proceso de Machine Learning.

Cada una de estas funcionalidades estarán sustentadas en las herramientas Pentaho, Jupyter, Kibana, ElasticSearch. La arquitectura para su utilización se definió de la siguiente manera, tal como se visualiza en la figura 4.

Figura 4.

Arquitectura DSS



Pentaho Data Integration: Es una de las herramientas o componentes de Pentaho Suite que permite utilizar técnicas ETL, implementar procesos de extracción, transformación y carga de datos. Además, ofrece datos analíticos muy precisos, al eliminar las complejidades involucradas en la codificación al proporcionar bibliotecas (Roldán, 2013).

Jupyter: Es el intérprete de comandos de Python, una aplicación web de código abierto que le permite crear y compartir documentos que contienen código en vivo, ecuaciones, visualizaciones y texto narrativo. Los usos incluyen: limpieza y transformación de datos, simulación numérica, modelado estadístico, visualización de datos, Machine Learning (Shmueli, 2019).

Python: Es un lenguaje de programación interpretado o de script dinámico, fuertemente tipado, multiplataforma y orientado a objetos. Se ejecuta con un programa intermedio llamado intérprete, en lugar de compilar el código a lenguaje máquina que pueda comprender y ejecutar directamente una computadora (Shmueli, 2019).

Clúster ElasticSearch: Se utiliza para indexar y contener los datos. Inicialmente el clúster tendrá un solo nodo, según la cantidad de los datos y requerimientos se podría incrementar el número de nodos. (Collier, 2019).

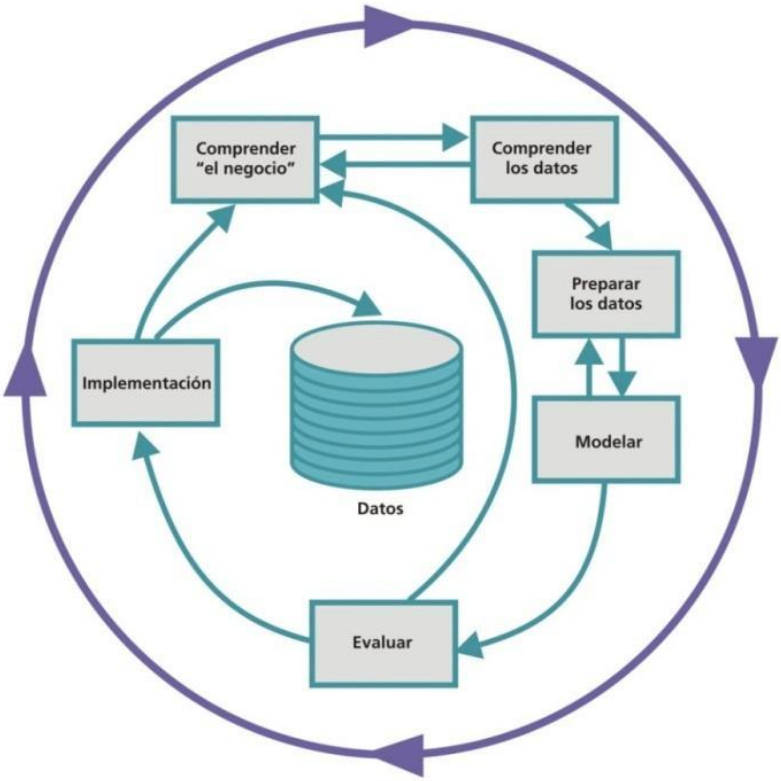
Interfaz de Kibana: Para visualizar los datos en el índice. Kibana y ElasticSearch están incluidos en un mismo contenedor Docker para su sencilla distribución.

Metodología CRISP-DM

En la figura 5 se muestra el ciclo de vida del modelo CRISP-DM. Las flechas indican relaciones más habituales entre las fases, aunque se pueden establecer relaciones entre cualquier fase. El círculo exterior simboliza la naturaleza cíclica del proceso de modelado (Galán Cortina, 2016).

Figura 5.

Ciclo de vida modelo CRISP-DM. Tomado de (Galán Cortina, 2016).



Entendimiento del negocio

El CSIRT de IDIA realiza procedimientos de recibir, atender y procesar los eventos de seguridad que se presentan, los principales procedimientos que realiza el CSIRT de IDIA son:

- Definición del impacto, alcance del evento;
- Definición de la causa del evento;
- Identificar las amenazas que genera el evento;
- Implementar estrategias de respuesta con apoyo de las instituciones miembros de IDIA como especialistas de TI, seguridad de la información (ISO), gerentes de negocios, ejecutivos, relaciones públicas, recursos humanos y asesoría legal;
- Difundir la información sobre los riesgos, amenazas, ataques, exploits y estrategias de mitigación a través de alertas, avisos;

- Coordinación y colaboración con equipos externos como ISP, grupos de seguridad y CSIRTs;
- Mantenimiento del repositorio de datos sobre los incidentes, vulnerabilidades y actividades relacionadas con la elaboración de tendencias para mejorar la seguridad y los procesos de gestión de incidentes;

El CSIRT de IDIA a las instituciones miembros ofrece los siguientes servicios de soporte:

- Respuesta a incidentes;
- Coordinación de incidentes;
- Resolución de incidentes;
- Genera estadísticas referentes a incidentes que ocurren en IDIA o a las instituciones miembros;

El CSIRT de IDIA detecta flujos continuos de datos y entre los principales eventos que maneja se describen a continuación:

- Botnets;
- DNS Open Resolver;
- Sinkhole;
- Ataques de amplificación basados en UDP;
- Honeypots;
- Ingenieria Social;
- Phishing;
- Gusanos;
- Degradación de sitios web;
- Ataque de fuerza bruta;

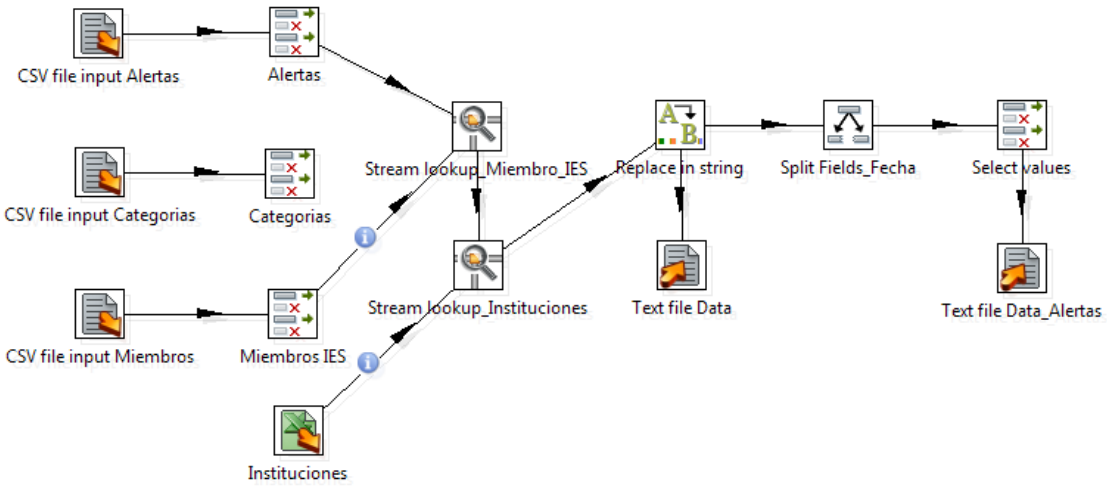
Entendimiento de los datos

Comprende la recolección inicial de datos, en orden a que sea posible establecer un mejor contacto con el problema, con la identificación de la cantidad de los datos y establecer las relaciones más evidentes que permitan establecer las primeras hipótesis.

Para obtener el dataset se realizó la extracción y transformación necesaria para realizar el análisis y mejor entendimiento de los datos, la extracción se ejecutó mediante la utilización de la herramienta Pentaho, en la figura 6 se observa el proceso que se siguió para conseguir el dataset a analizar, representa el flujo final del ETL de la limpieza de la información.

Figura 6.

Proceso de extracción de datos ETL. Ilustración derivada del software Pentaho.



El dataset que se obtuvo del proceso de extracción y transformación, se importó con la herramienta Jupyter que permite representar diferentes tipos de tablas, información de tipo estadística y gráficas, que relacionan atributos que contiene la base de datos.

El dataset contiene 15 variables en cada registro que se indican en la tabla 9, en los cuales se describen diferentes características de cada conexión y diferentes tipos o categorías de alertas las cuales se describen en la tabla 8.

Tabla 8.

Categorías de alertas

Ítem	**Categoría Alerta**	**Ítem**	**Categoría Alerta**
1	botnet_drone	35	tc-dipnet
2	dns_openresolver	36	tc-fastflux
3	microsoft_sinkhole	37	tc-malwareurl
4	sinkhole_http_drone	38	tc-mydoom
5	scan_mdns	39	tc-nachi
6	scan_mssql	40	tc-openresolvers
7	scan_netbios	41	tc-phabot
8	scan_ntp	42	tc-phishing
9	scan_portmapper	43	tc-proxy
10	scan_ssdp	44	tc-routers
11	scan_ssl_poodle	45	tc-scanners
12	scan_tftp	46	tc-sinit
13	scan_xdmcp	47	tc-slammer
14	compromised_website	48	tc-spam
15	cwsandbox_url	49	tc-spreaders
16	scan_chargen	50	tc-stormworm
17	scan_elasticsearch	51	tc-toxbox
18	scan_ipmi	52	cleanmx-viruses
19	scan_memcached	53	cleanmx-portals

Ítem	Categoría Alerta	Ítem	Categoría Alerta
20	scan_mongodb	54	cleanmx-phishing
21	scan_ntpmonitor	55	hma-openproxy
22	scan_qotd	56	n6
23	scan_snmp	57	cediahp-scan
24	scan_ssl_freak	58	cediahp-fail
25	spam_url	59	cediahp-success
26	ssl_scan	60	cediahp-wget
27	open_proxy	61	certbrspampot
28	tc-beagle	62	certbrglobal
29	tc-blaster	63	scsummary
30	tc-bots	64	zone-h-accepted
31	tc-bruteforce	65	scan_isakmp
32	tc-dameware	66	sh-bots
33	tc-ddosreport	67	sh-cyc
34	tc-defacement	68	sh-botnetcc

Tabla 9.

Variables de los registros de base de datos

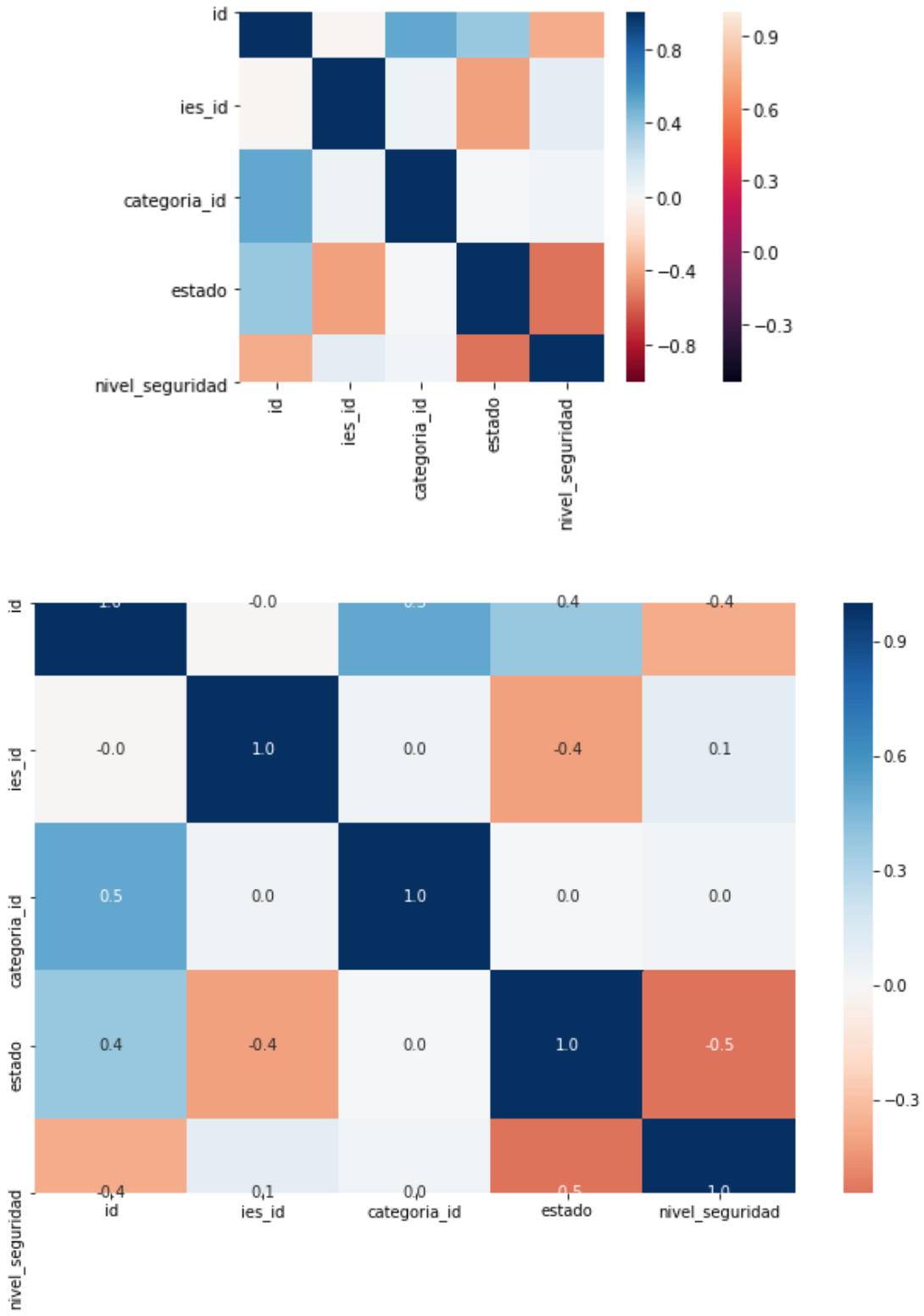
CARACTERÍSTICA	DESCRIPCIÓN	TIPO
ID	Identificador registro del evento.	Continuo
IES_ID	Identificador de la Institución de Educación Superior miembro de IDIA.	Continuo
CATEGORIA_ID	Identificador de categoría alerta.	Continuo
FECHA_REGISTRO	Fecha registro del evento.	Continuo

CARACTERÍSTICA	DESCRIPCIÓN	TIPO
HORA_REGISTRO	Hora registro del evento.	Continuo
IP	Dirección IP del host destino.	Continuo
FECHA_PROCESO	Fecha proceso del evento.	Continuo
HORA_PROCESO	Hora proceso del evento.	Continuo
LLAVE_ELECTRÓNICA	Token de seguridad o token criptográfico.	Discreto
ESTADO	Estado de eventos que se encuentran procesados o pendientes.	Continuo
NIVEL_SEGURIDAD	Clasifica los eventos en Alto, Medio, Bajo.	Continuo
CATEGORIA_ALERTA	Nombre categoría de la alerta registrada.	Discreto
IES	Nombre de la Institución de Educación Superior miembro de IDIA.	Discreto
ACRÓNIMO_IES	Acrónimo de la Institución de Educación Superior miembro de IDIA.	Discreto

En la Figura 7, se observa un mapa de calor de la tabla de correlaciones, que muestra todas las correlaciones entre las variables numéricas. Los tonos más oscuros corresponden a una correlación más fuerte (positiva o negativa). Es fácil detectar rápidamente las correlaciones altas y bajas. El uso de azul / rojo se utiliza en este caso para resaltar correlaciones positivas versus negativas. En la imagen se visualiza que no presentan correlaciones altas entre las variables numéricas.

Figura 7.

Mapa de calor de la tabla de correlaciones entre las variables numéricas. Ilustración derivada del software Jupyter.

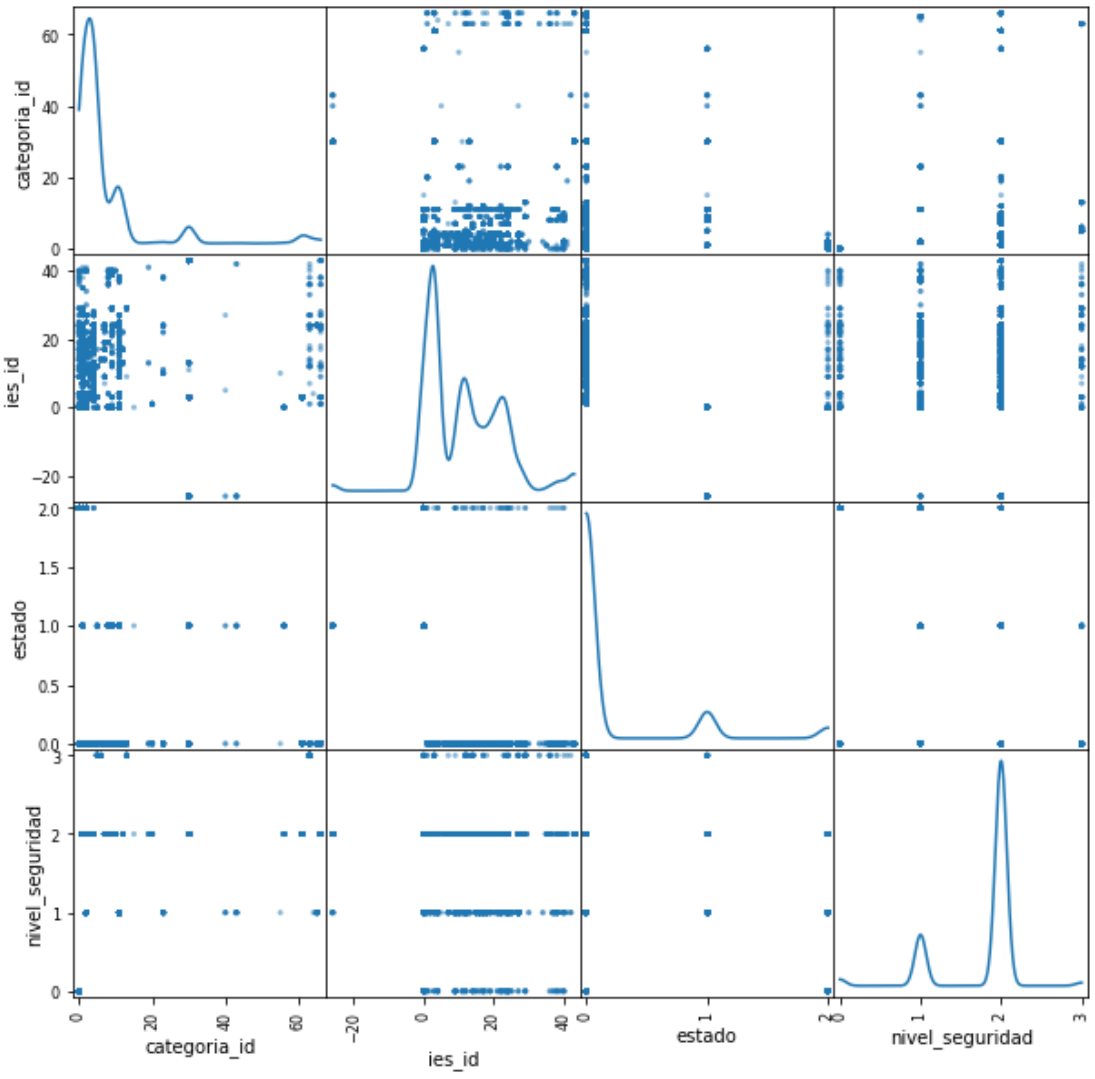


En la Figura 8 se visualiza una matriz de diagrama de dispersión con nivel_seguridad y tres predictores. El nombre de la variable indica la variable del eje y. Por ejemplo, todas las gráficas en la fila inferior tienen nivel_seguridad en el eje y (que permite estudiar las relaciones individuales de resultado-predictor). Se puede visualizar diferentes tipos de relaciones de diferentes formas (por ejemplo, una relación muy sesgada entre ies_id y categoría_id), que puede indicar las transformaciones necesarias. Donde solo está involucrada una sola variable, en la figura 8 se muestra la distribución de frecuencia para esa variable.

Figura 8.

Matriz de diagrama de dispersión para MEDV y tres predictores numéricos.

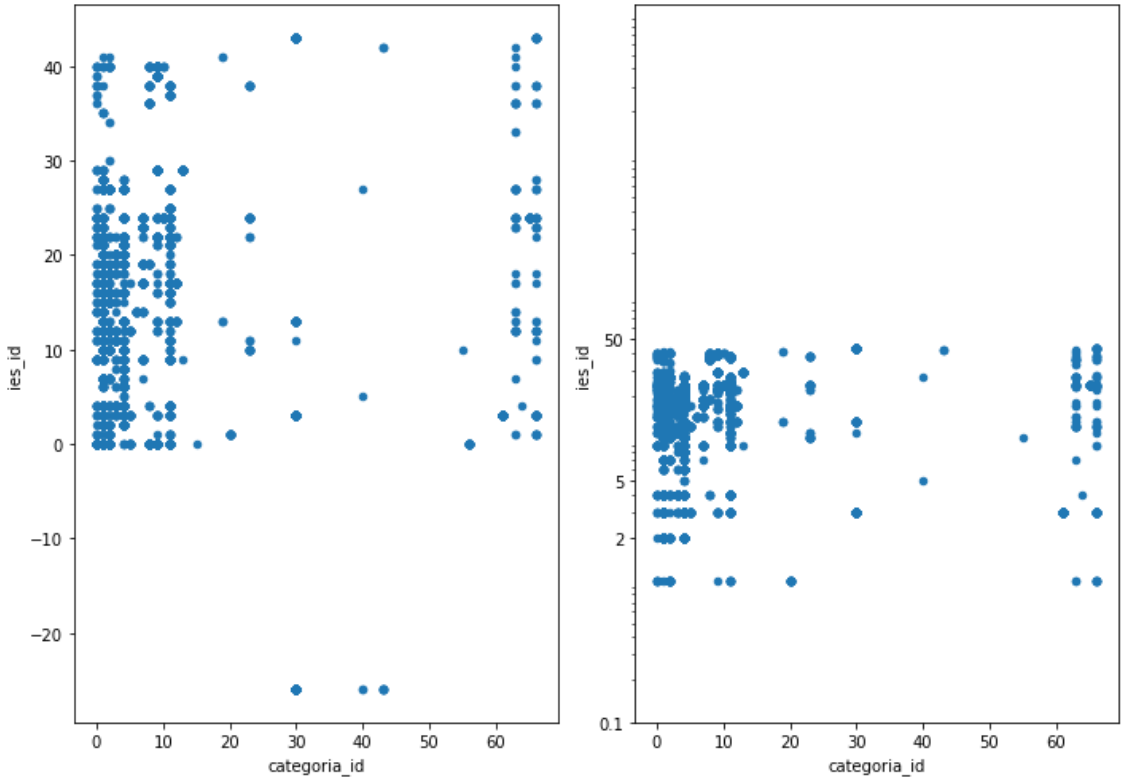
Ilustración derivada del software Jupyter



En las figuras 9 y 10 se cambia la escala para mejorar la trama y enfocar las relaciones, el efecto de cambiar ambos ejes del diagrama de dispersión figura 9 y el eje y de un diagrama de caja figura 10 a escala logarítmica (log). Mientras que las figuras originales son difíciles de entender, los patrones se hacen visibles en la escala logarítmica. En los histogramas, la naturaleza de la relación entre ies_id y categoría_id es difícil de determinar en la escala original, porque muchos de los puntos están "llenos" cerca del eje y. El cambio de escala elimina esta aglomeración y permite una mejor vista de la relación lineal entre las dos variables (lo que indica una relación de registro-registro).

Figura 9.

Cambio de escala de las tramas. (a) escala original, (b) escala logarítmica. Ilustración derivada del software Jupyter

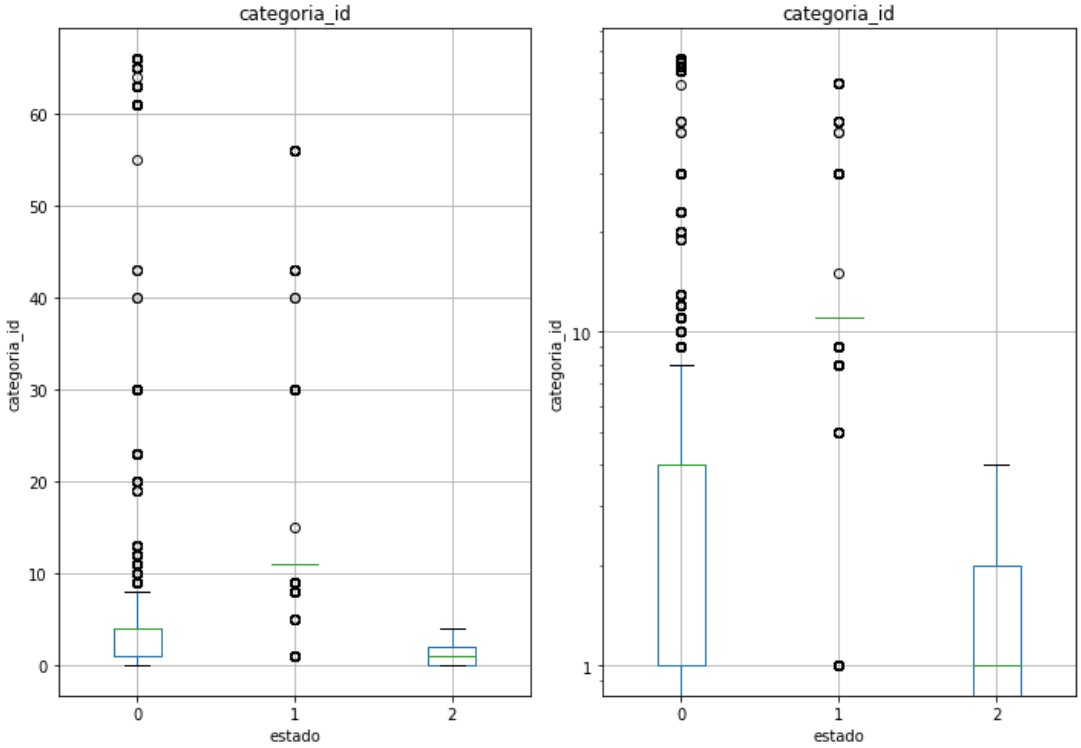


En el diagrama de caja figura 10, mostrar el apiñamiento hacia el eje x en las unidades originales no permite comparar los dos tamaños de caja, sus ubicaciones,

valores atípicos inferiores y la mayoría de la información de distribución. El cambio de escala elimina el efecto de "apiñamiento al eje x", lo que permite una comparación de los dos gráficos de caja.

Figura 10.

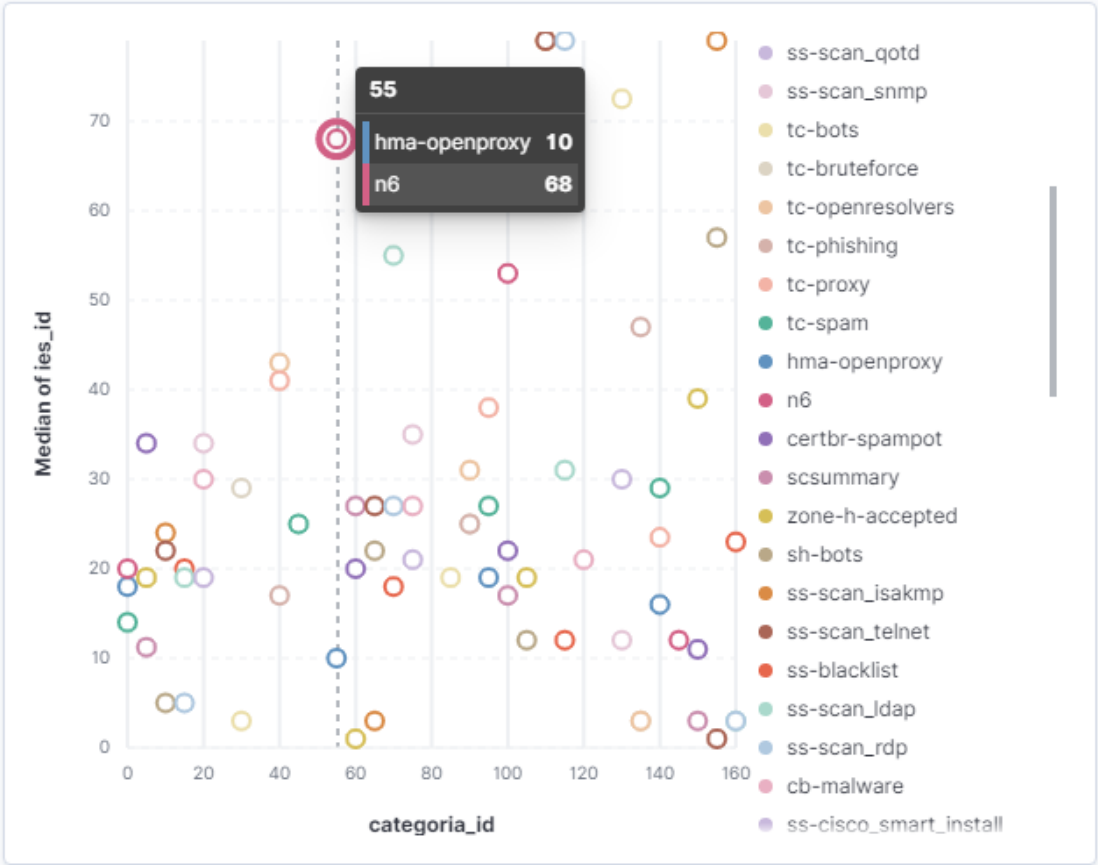
El cambio de escala puede mejorar las tramas y revelar patrones. (a) escala original, (b) escala logarítmica. Ilustración derivada del software Jupyter



El uso de etiquetas puede ser útil para una mejor exploración de valores atípicos y clústeres. En la Figura 11 se muestra diferentes utilidades en un diagrama de dispersión que compara el *ies_id* con *categoría_id*. Se podría agrupar los datos y utilizar algoritmos de agrupamiento para identificar grupos que difieren notablemente con respecto al *ies_id* y la categoría_*id*. La Figura 11 con las etiquetas, ayuda a visualizar estos grupos y sus miembros. Se visualiza que las alertas hma-openproxy y ns se presenta solo en una Institución, además las categorías de alertas se presentan en pocas Instituciones como es el caso de tc-openresover, tc-proxy.

Figura 11.

Diagrama de dispersión con puntos de etiquetas. Ilustración derivada del software Kibana.



Preparación de los datos

Incluye las tareas generales de selección de datos a los que se va aplicar la técnica de modelado (Variables y muestras), limpieza de los datos, generación de variables adicionales, integración de diferentes orígenes de datos y cambios de formato.

En la Figura 12 se visualiza un mapa de calor que ayuda a visualizar el nivel y la cantidad de valores faltantes en el conjunto de datos. Surgen patrones, variables, así como grupos de filas a las que les faltan valores.

Se puede visualizar en color gris la ubicación de los elementos perdidos en el conjunto de datos (usando el código Python). Existen tres variables con datos faltantes

o vacíos, que se podría descartar fecha_proceso, hora_proceso, otras_entradas. Al descartar dichas variables del conjunto de datos se tiene como resultado las variables que se muestran en la figura 13.

Figura 12.

Mapa de calor de los valores faltantes en el conjunto de datos. Ilustración derivada del software Jupyter.

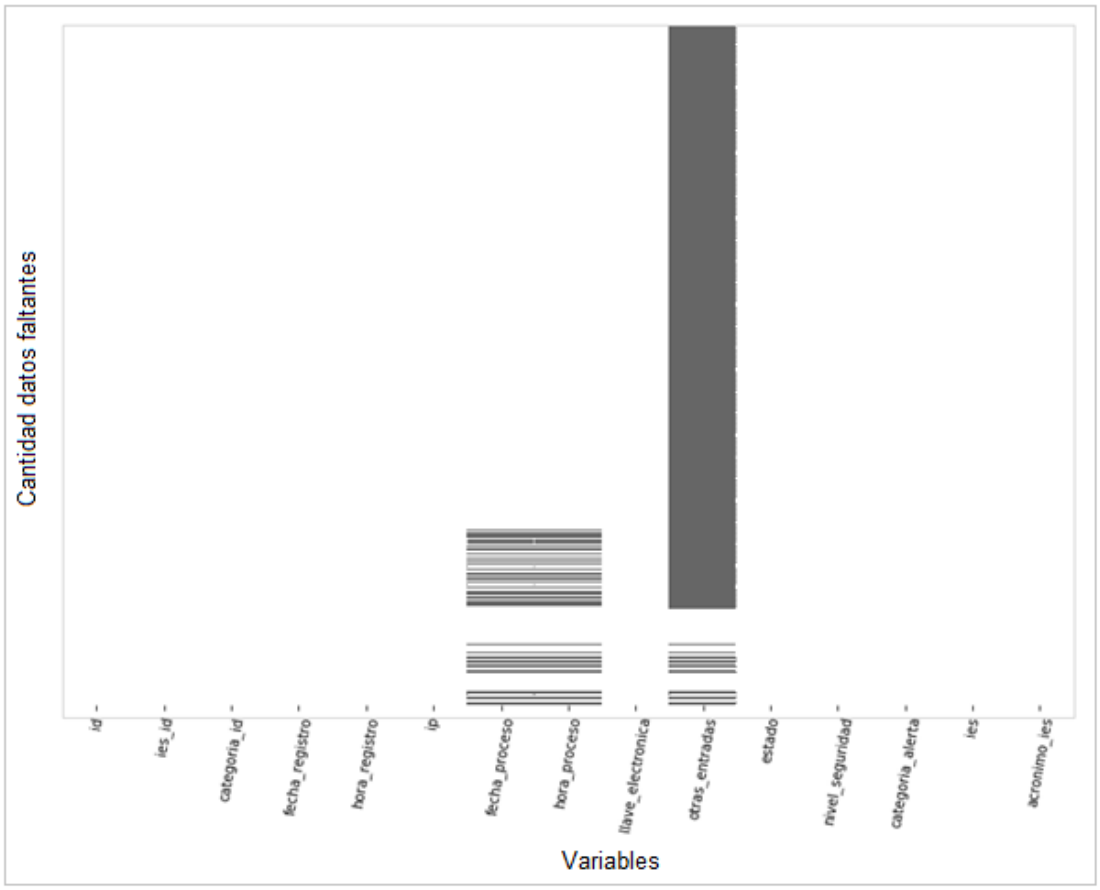


Figura 13.

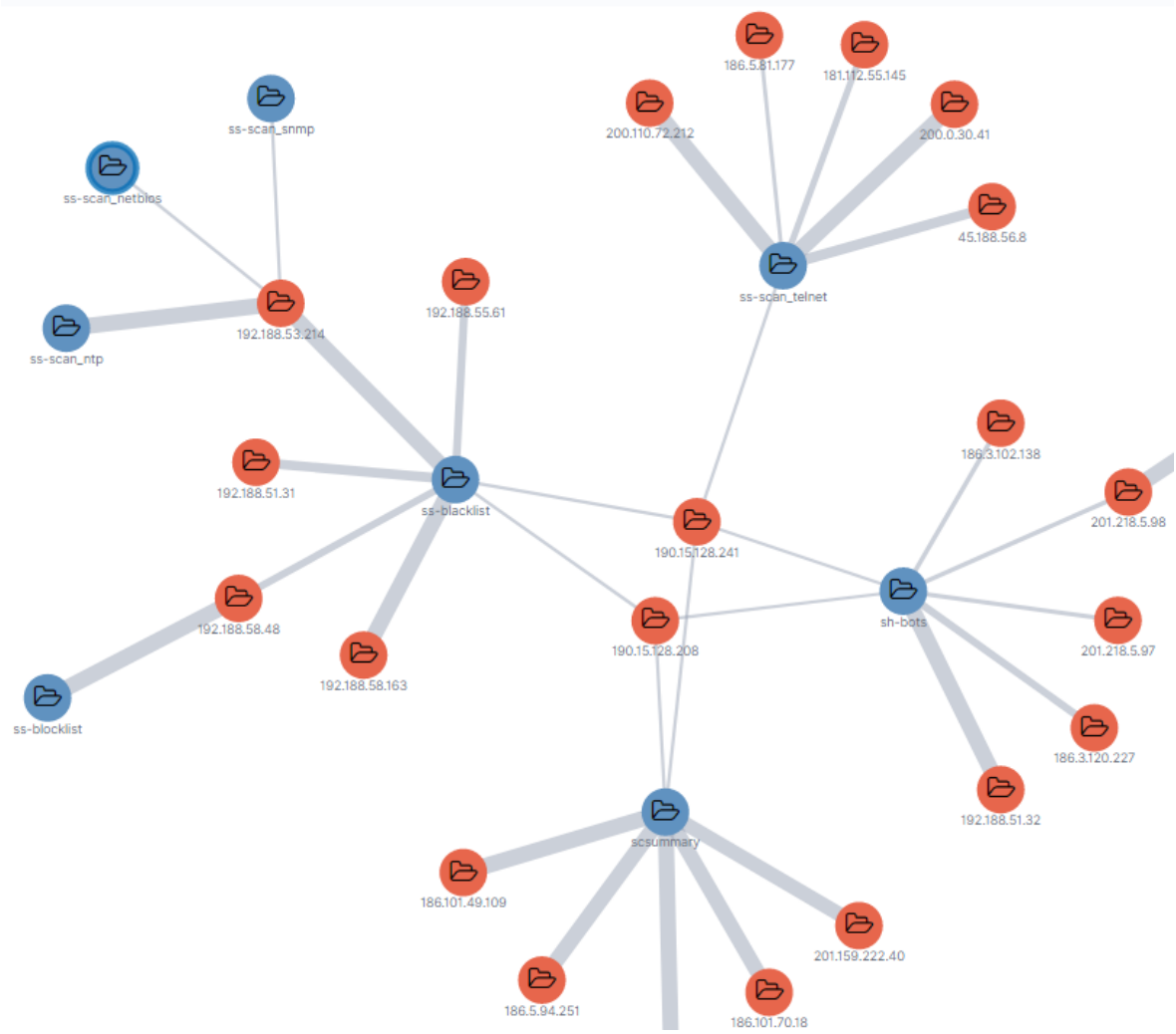
Matriz de datos resultante

id	ies_id	categoria_id	fecha_registro	hora_registro	ip	Categoria_alerta	estado	acronimo_ies
100686933	31	9	22/11/2020	5:58:21	201.159.223.113	ss-scan_portmapper	1	institucion 31
100686936	31	9	22/11/2020	5:58:21	201.159.223.113	ss-scan_portmapper	1	institucion 31
100686950	68	1	22/11/2020	4:03:11	190.15.134.3	ss-botnet_drone	1	institucion 68
100686951	1	1	22/11/2020	16:22:24	192.188.58.15	ss-botnet_drone	1	institucion 1
100686969	103	1	22/11/2020	0:27:44	179.49.2.130	ss-botnet_drone	1	institucion 103
100687028	5	1	22/11/2020	1:16:43	181.39.156.98	ss-botnet_drone	1	institucion 5
100687070	68	1	22/11/2020	4:03:11	190.15.134.3	ss-botnet_drone	1	institucion 68
100687074	5	1	22/11/2020	5:22:15	186.101.67.158	ss-botnet_drone	1	institucion 5
100687075	5	1	22/11/2020	5:32:55	181.39.138.180	ss-botnet_drone	1	institucion 5
100687076	5	1	22/11/2020	7:19:15	181.39.156.98	ss-botnet_drone	1	institucion 5
100687081	5	1	22/11/2020	12:21:29	186.5.88.108	ss-botnet_drone	1	institucion 5
100687082	5	1	22/11/2020	12:38:33	186.3.97.122	ss-botnet_drone	1	institucion 5
100687083	5	1	22/11/2020	12:45:00	186.5.94.118	ss-botnet_drone	1	institucion 5
100687086	5	1	22/11/2020	13:08:05	181.39.151.126	ss-botnet_drone	1	institucion 5
100687107	5	1	22/11/2020	14:40:46	186.5.88.108	ss-botnet_drone	1	institucion 5
100687120	5	1	22/11/2020	15:25:03	186.3.65.146	ss-botnet_drone	1	institucion 5
100687138	1	1	22/11/2020	16:22:24	192.188.58.15	ss-botnet_drone	1	institucion 1
100687191	5	1	22/11/2020	22:25:36	190.95.163.4	ss-botnet_drone	1	institucion 5
100687233	68	4	22/11/2020	0:33:22	190.15.134.22	ss-sinkhole_http_drone	1	institucion 68
100687236	68	4	22/11/2020	0:33:22	190.15.134.22	ss-sinkhole_http_drone	1	institucion 68
100687241	68	56	23/11/2020	4:00:01	190.15.134.3	n6	1	institucion 68
100687242	38	61	23/11/2020	5:32:01	190.15.130.90	certbr-spampot	1	institucion 38
100687243	38	61	23/11/2020	5:32:01	190.15.130.90	certbr-spampot	1	institucion 38
100687244	38	61	23/11/2020	5:32:01	190.15.130.90	certbr-spampot	1	institucion 38
100687245	38	66	23/11/2020	6:11:01	190.15.130.90	sh-bots	1	institucion 38
100687246	68	66	23/11/2020	6:11:01	190.15.134.22	sh-bots	1	institucion 68

En la figura 14 se visualiza un conjunto de transacciones entre una red de direcciones IP y las categorías de alertas. Los círculos de color tomate representan las direcciones IP y los círculos de color azul representan la categoría de alertas. Se puede ver que las alertas interactúan con varias IP.

Figura 14.

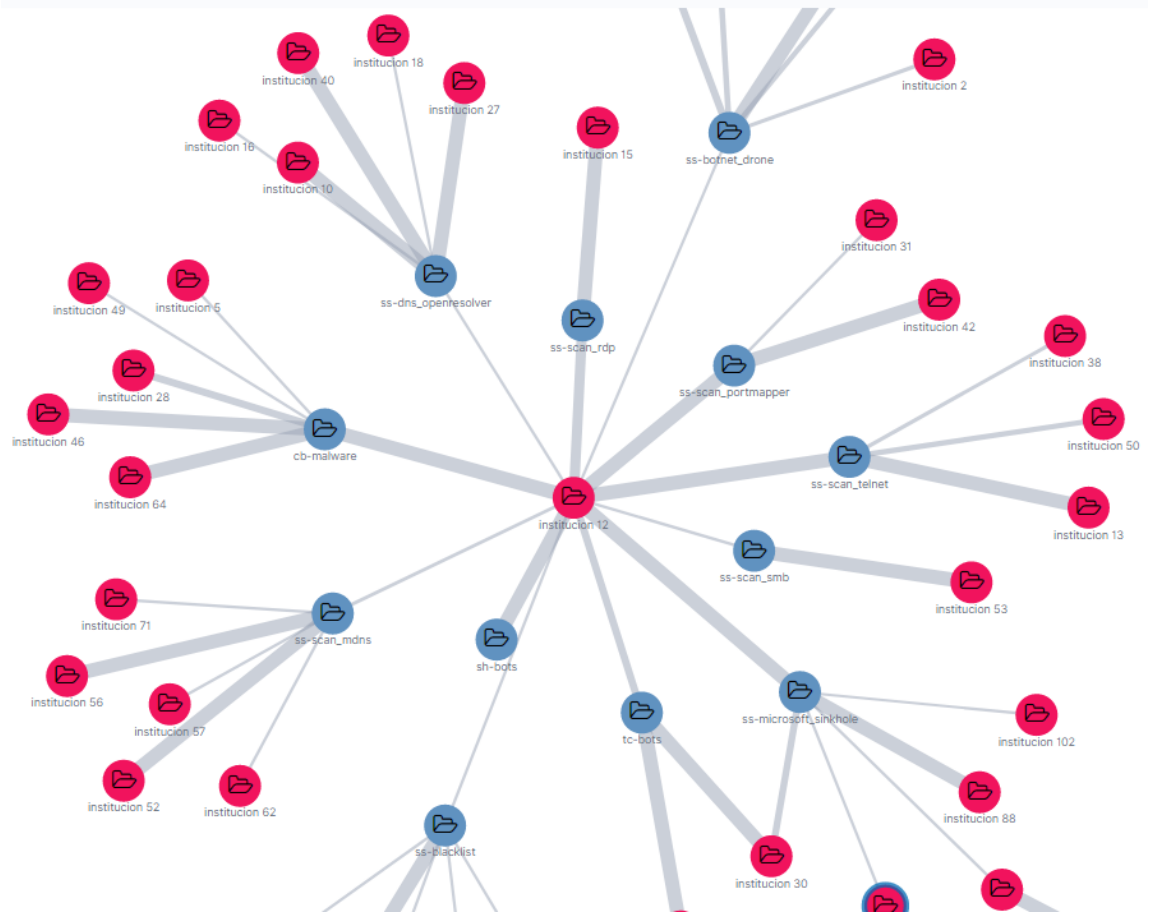
Trama de red de direcciones ip y categoria_alerta. Ilustración derivada del software Kibana.



En la figura 15 se puede ver un conjunto de transacciones entre una red de las IES y las categorías de alertas. Los círculos de color rojo representan las IES y los círculos de color azul representan las categorías de alertas. Se puede distinguir que las Instituciones de Educación superior interactúan con varias alertas. Además, se observa que las alertas interactúan solo con una Institución.

Figura 15.

Trama de red de acronimo_ies y categoria_alerta. Ilustración derivada del software Kibana.

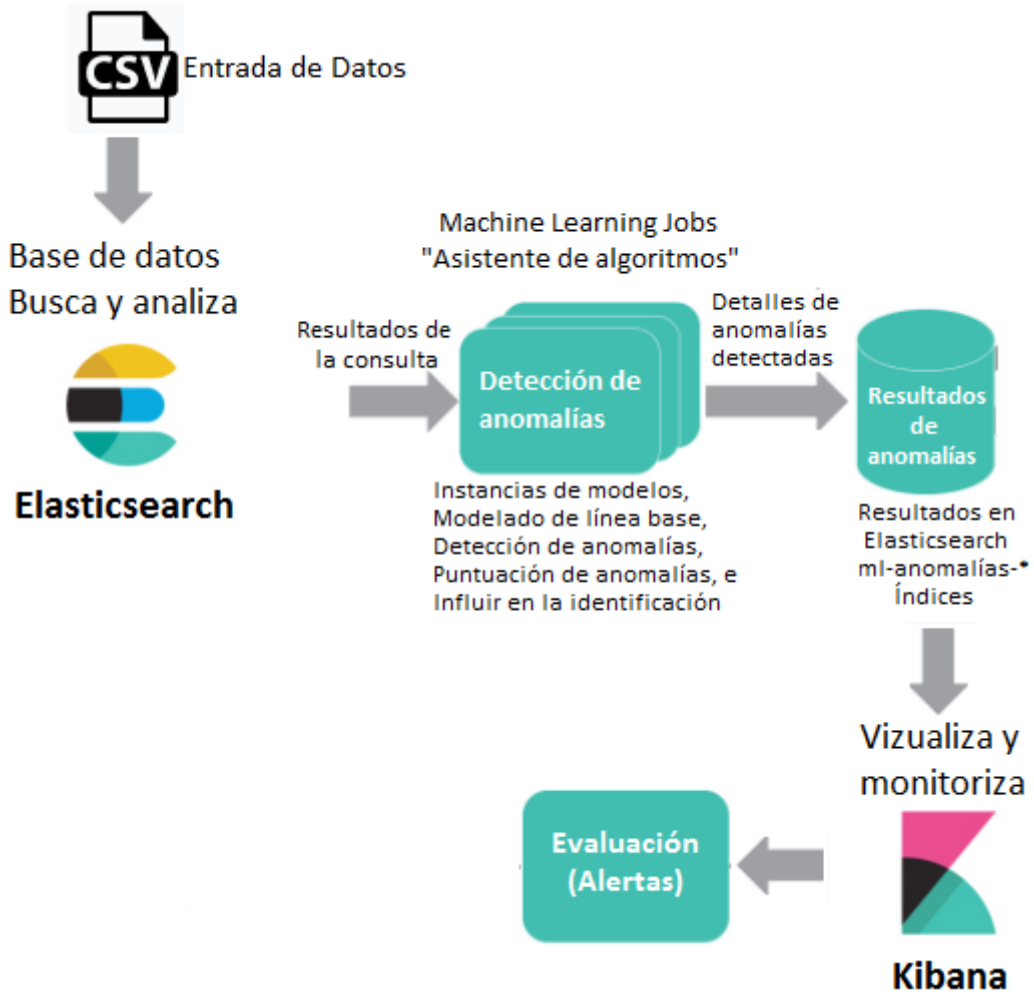


Modelado

Para el modelado de Machine Learning se siguió el flujo de trabajo de implementación tal como se ilustra en la figura 16. En ella se describe cómo los elementos del modelo se implementan y cómo estos se organizan de acuerdo a los nodos específicos en el modelo del despliegue.

Figura 16.

Flujo de trabajo de implementación del modelo de Machine Learning, adaptado de (Hassan, 2019).



Se seleccionaron las técnicas de modelado más apropiadas para el proyecto de minería de datos, aplicadas a las alertas de la seguridad de la información. Una de las técnicas utilizadas es Naive Bayes classifier aplicado a los datos de alertas.

Después de convertir todos los predictores a categóricos y crear dummies, los datos se dividieron en conjuntos de entrenamiento (80%) y validación (20%), y luego se aplicó un clasificador Naive Bayes al conjunto de entrenamiento.

Con esto se genera la tabla dinámica para el resultado frente a cada uno de los predictores, usando el conjunto de datos de entrenamiento, para obtener probabilidades condicionales cómo se muestra en la tabla 10.

Tabla 10.

Tabla dinámica de probabilidades condicionales

categoria_alerta	**Probabilidad**
sinkhole_http_drone	0.3683
botnet_drone	0.2804
scan_ssl_poodle	0.1077
dns_openresolver	0.0630
tc-bots	0.0386
scan_portmapper	0.0223
microsoft_sinkhole	0.0186
certbrspampot	0.0165
scan_netbios	0.0161
scan_ntp	0.0160
sh-bots	0.0053
scsummary	0.0040
scan_tftp	0.0037
scan_mdns	0.0033
scan_snmp	0.0032
scan_ssdp	0.0024
scan_isakmp	0.0020
scan_xdmcp	0.0020
n6	0.0014
scan_mssql	0.0011
tc-proxy	0.0008
scan_mongodb	0.0007
scan_memcached	0.0004
tc-openresolvers	0.0003

Para evaluar el rendimiento del clasificador de Naive Bayes para los datos, se usó la matriz de confusión, las tablas de ganancias y levantamiento. La matriz de confusión para la validación del conjunto de datos se muestra en la tabla 11 y se visualiza que el nivel de precisión general es de alrededor del 80% para los datos de validación.

Tabla 11.

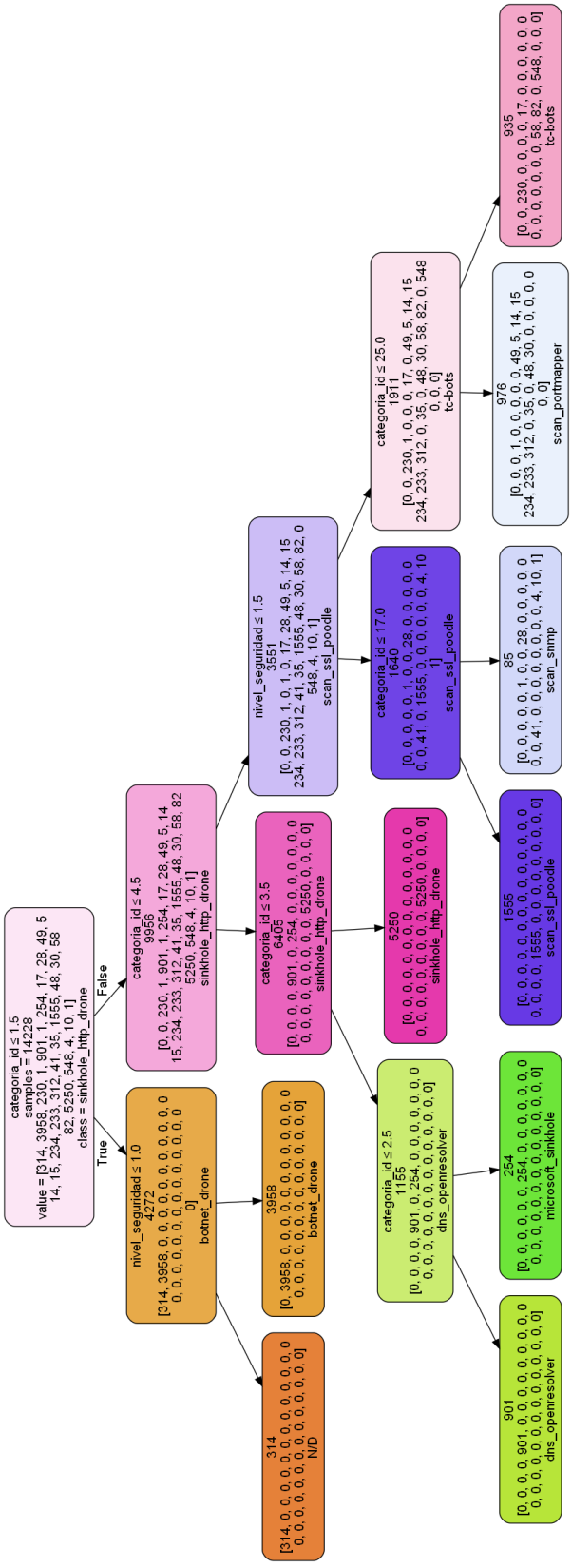
Matriz de Confusión del clasificador Naive Bayes. Tabla derivada del software Jupyter

Confusion Matrix (Accuracy 0.8665)																			
	Prediction																		
Actual	botnet_drone	certbrspampot	cwsandbox_url	dns_openresolver	hma-openproxy	microsoft_sinkhole	n6	scan_isakmp	scan_mdns	scan_memcached	scan_mongodb	scan_mssql	scan_netbios	scan_ntp	scan_portmapper	scan_snmp	scan_ssdp	scan_ssl_poodle	scan_tftp
botnet_drone	535	0	0	0	0	85	3	0	0	2	0	0	7	4	0	0	0	0	0
certbrspampot	0	42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
cwsandbox_url	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
dns_openresolver	0	0	0	183	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
hma-openproxy	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
microsoft_sinkhole	21	0	0	0	0	18	0	0	0	0	0	0	1	0	0	0	0	0	0
n6	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
scan_isakmp	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0
scan_mdns	0	0	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	0
scan_memcached	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
scan_mongodb	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0
scan_mssql	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
scan_netbios	0	0	0	0	0	0	0	0	0	0	0	0	51	0	0	0	0	0	0
scan_ntp	0	0	0	0	0	0	0	0	0	0	0	0	0	51	0	0	0	0	0
scan_portmapper	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
scan_snmp	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0
scan_ssdp	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
scan_ssl_poodle	0	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0
scan_tftp	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
scan_xdmcp	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
scsummary	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
sh-bots	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
sinkhole_http_drone	66	2	0	0	0	30	0	0	0	2	0	0	1	0	0	0	0	0	0
tc-bots	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
tc-openresolvers	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
tc-proxy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
zone-h-accepted	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Otra de las técnicas de modelado que se utilizó es el árbol de decisión por clasificación. La razón por la que el método se denomina algoritmo de árbol de clasificación es que cada división se puede representar como una división de un nodo en dos nodos sucesores. La primera división se muestra como una ramificación del nodo raíz de un árbol. En la figura 17 se ilustra el árbol con las cinco primeras divisiones. El árbol tiene más divisiones por la cantidad de categorías de alertas que tiene los datos.

Figura 17.

Representación del árbol de decisión por clasificación. Ilustración derivada del software Jupyter



En las tablas 12 y 13 se puede observar las matrices de confusión para el árbol de clasificación. Se visualiza que los datos de entrenamiento están bien clasificados (precisión = 0.9788), mientras que los datos de validación tienen una precisión menor (0,8797).

Tabla 12.

Matriz de confusión y precisión para el árbol de clasificación, en los datos de entrenamiento. Tabla derivada del software Jupyter.

Confusion Matrix (Accuracy 0.9788)																									
	Prediction																								
Actual	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2345	1	0	0	0	0	0	0	0	0	9	2	3	0	0	0	2	0	0	1	10	0	0	0
2	0	4	139	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	3	4	0	0
3	0	0	0	547	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	1	0	0	160	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	1	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	27	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
8	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	1	0	0	0	0	0	0	3	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	3	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	5	2	0	0	0	0	0	0	0	0	122	0	2	0	0	0	1	0	0	1	2	4	0	0
12	0	5	0	0	0	0	0	0	1	0	0	0	121	1	0	0	0	0	0	0	0	0	0	0	0
13	0	4	0	0	0	0	0	0	0	3	0	15	2	164	0	0	0	1	0	0	0	0	2	0	0
14	0	0	0	1	0	0	0	0	0	0	0	0	0	0	27	0	0	0	0	0	0	0	0	0	0
15	0	2	0	0	0	0	0	0	0	0	0	4	2	2	0	5	0	1	0	0	0	0	3	0	0
16	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	934	0	0	0	0	0	0	0	0
17	0	0	2	0	0	0	0	0	0	0	0	3	2	1	0	2	0	17	0	0	0	0	6	0	0
18	0	0	0	0	0	0	0	4	0	0	1	0	0	0	0	0	0	0	13	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	37	0	0	0	0	0
20	0	2	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	37	1	0	0	0
21	0	15	0	0	2	0	0	0	0	0	0	5	0	3	0	0	0	2	0	0	0	3108	0	0	0
22	0	2	7	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	313	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	6

Tabla 13.

Matriz de confusión y precisión para el árbol de clasificación, en los datos de validación. Ilustración derivada del software Jupyter.

Confusion Matrix (Accuracy 0.8797)																											
	Prediction																										
Actual	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
0	126	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1360	2	0	0	0	24	0	0	0	0	0	0	6	7	8	0	1	0	1	0	0	7	169	0	0	0	0
2	0	1	71	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	2	0	0	0	0	2	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	350	0	0	0	1	0	0	0	0	0	0	0	2	0	1	0	0	0	0	0	0	0	0	0
5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	12	0	0	0	0	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	57	0	0	0	0
7	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	1	0	0	0	6	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	10	0	0	3	0	0	0	0	0	0	0	6	2	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	7	0	0	0	1	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
13	0	1	2	0	0	0	0	0	0	0	0	0	0	74	2	3	0	4	0	3	0	0	0	1	5	0	0	0
14	0	4	0	0	0	0	0	0	0	0	0	0	0	3	94	4	0	0	0	0	0	0	0	0	0	0	0	0
15	0	10	1	0	0	0	0	0	0	0	0	1	0	16	2	85	0	0	0	5	0	0	0	0	1	0	0	0
16	0	0	0	0	8	0	0	0	1	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0
17	0	0	1	0	0	0	0	0	0	0	0	0	0	3	0	3	0	2	0	2	0	0	0	1	4	0	0	0
18	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	618	0	0	0	0	0	0	0	0	0
19	0	2	1	0	0	0	0	0	0	0	0	0	0	1	1	3	0	3	0	3	0	0	0	0	1	0	0	0
20	0	0	0	0	0	0	0	0	0	7	0	0	3	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	20	0	0	0	0	0	0
22	0	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	35	2	0	0	0	0
23	0	185	0	0	0	0	18	0	0	0	0	0	4	0	3	0	0	0	2	0	0	0	1903	0	0	0	0	0
24	0	1	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	213	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0
27	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Despliegue de la información

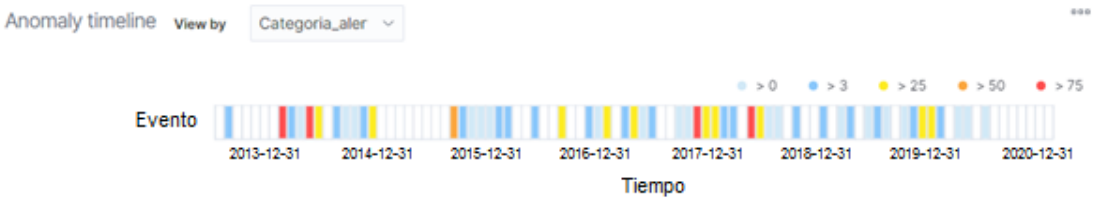
Normalmente los proyectos de Machine Learning no terminan en la implantación del modelo, sino que se debe documentar y presentar los resultados de manera comprensible en orden a lograr un incremento del conocimiento. Además, en la fase de explotación se debe asegurar el mantenimiento de la aplicación y la posible difusión de los resultados.

Para la implementación del DSS se utilizaron Elasticsearch y Kibana que generan un panel de visualización de datos de código abierto para que los científicos de datos visualicen redes semánticas y trabajen con ellas. Proporcionan capacidades de visualización además del contenido indexado en un clúster de Elasticsearch. Permiten crear gráficos de barras, líneas y dispersión, o gráficos circulares y mapas sobre grandes volúmenes de datos (Collier, 2019).

La figura 18 es la línea de tiempo para los resultados de la detección de anomalías. Los bloques en azul muestran recuento normal, los amarillos muestran advertencia menor, los naranjas muestran advertencia mayor y los rojos muestran recuentos críticos de categoría de alerta.

Figura 18.

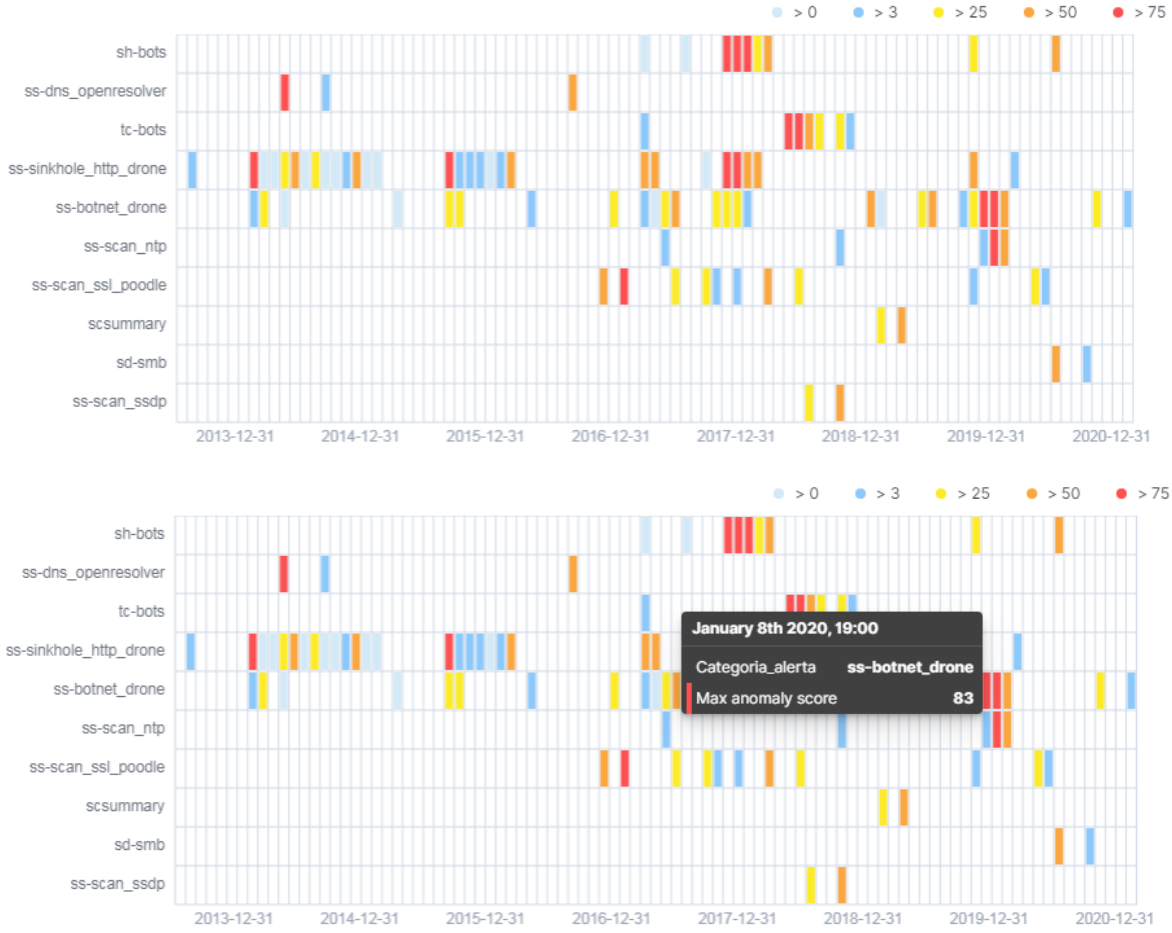
Anomaly Detection Timeline. Ilustración derivada del software Kibana.



La figura 19 muestra la categoría de alertas objetivo para la implementación de nuestro caso. La leyenda en bloque negro es el desplazamiento sobre el bloque rojo de la categoría alerta ss-botnet-drone. Son los resultados de enero los que muestran una puntuación máxima de anomalías de 83.

Figura 19.

Categoría alerta bajo consideración. Ilustración derivada del software Kibana.



La figura 20 muestra los recuentos de las anomalías principales de las categorías de alertas generales del datasets. La figura 21 muestra el detalle completo de la anomalía detectada con la función de detección de alta entropía. Los resultados con el conjunto de datos de entrenamiento y la lógica de ML son comparables. Es la representación en texto del resultado crítico.

Figura 20.

Influencers Count in Anomaly detection. Ilustración derivada del software Kibana.

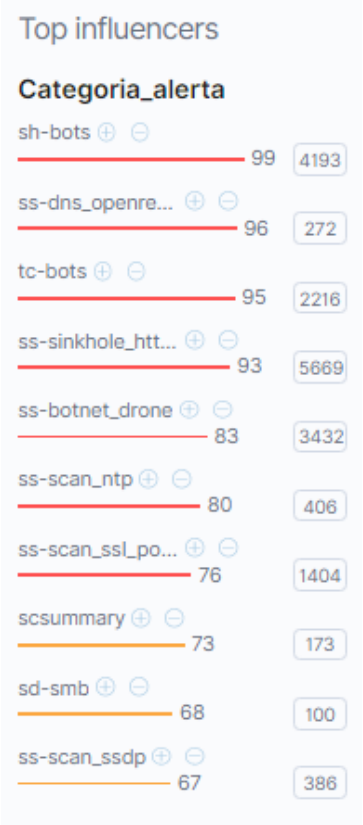


Figura 21.

Detalle de anomalías. Ilustración derivada del software Kibana.

Anomalies

Severity threshold: critical

Interval: Auto

time	severity	detector	found for	influenced by	actual	typical	description	actions
February 5th 2020	80	distinct_count(acronimo_ies) partitionfield= Categoria_alerta	ss-scan_ntp	Categoria_alerta: ss-scan_ntp	8	1.74	5x higher	
February 1st 2020	82	distinct_count(acronimo_ies) partitionfield= Categoria_alerta	ss-botnet_drone	Categoria_alerta: ss-botnet_drone	1	15.8	16x lower	
January 31st 2020	75	distinct_count(acronimo_ies) partitionfield= Categoria_alerta	ss-botnet_drone	Categoria_alerta: ss-botnet_drone	5	17	3x lower	
December 31st 2019	80	distinct_count(acronimo_ies) partitionfield= Categoria_alerta	ss-botnet_drone	Categoria_alerta: ss-botnet_drone	4	15	4x lower	

En la anomalía de mayor puntuación de categoría alerta ss-botnet-drone, que muestran una puntuación máxima de anomalías de 83, se puede desplegar la descripción de la anomalía como se muestra en la figura 22.

Figura 22.

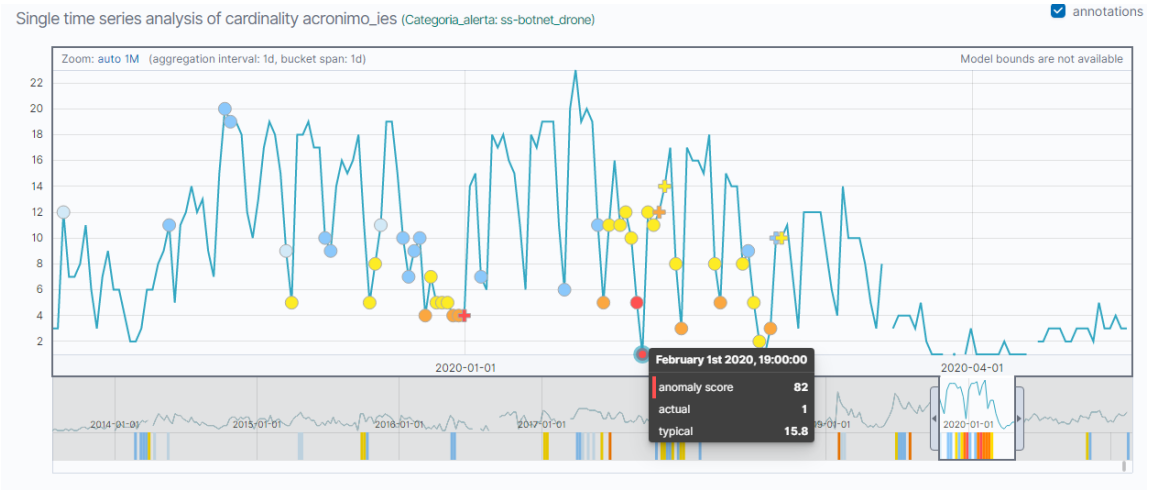
Descripción de anomalía critica. Ilustración derivada del software Kibana.

La probabilidad de la observación de la categoría alerta ss-botnet-drone en este punto en el tiempo se calculó en 2.6155513863726616e-9. Este valor tan pequeño quizás no sea tan intuitivo para la mayoría de la gente. Como tal, Machine Learning tomará este cálculo de probabilidad y, mediante un proceso de normalización de cuantiles, volverá a emitir esa observación en una escala de gravedad entre 0 y 100, donde 100 es el nivel más alto de inusualidad posible para ese conjunto de datos en particular. En la figura 23, el cálculo de probabilidad de 2.6155513863726616e-9 se normalizó a una puntuación de 82. Esta puntuación normalizada es útil para evaluar la gravedad de la anomalía con fines de alerta.

Figura 23.

Machine Learning calcula la probabilidad de caída de valor en esta serie de tiempo.

Ilustración derivada del software Kibana.



Capitulo IV: Evaluación de Resultados

Validación del modelo

Kibana proporciona métricas de errores de entrenamiento, que representan qué tan bien se desempeñó el modelo en el conjunto de datos de entrenamiento. También proporciona métricas de error de generalización, que representan qué tan bien se desempeñó el modelo en los datos de prueba. Se evalúa el modelo, no desde el punto de vista de los datos, si no del cumplimiento de los criterios del éxito del problema. Al realizar la evaluación de regresión se puede verificar que se obtiene los siguientes resultados que se muestran en la tabla 14.

Tabla 14.

Evaluación de regresión derivada del software Kibana.

Generalization error		**Training error**	
Mean squared error	0.0182	Mean squared error	0.0271
Mean squared logarithmic error	0.000169	Mean squared logarithmic error	0.00019
R squared	1	R squared	1
Pseudo Huber loss function	0.00573	Pseudo Huber loss function	0.0065

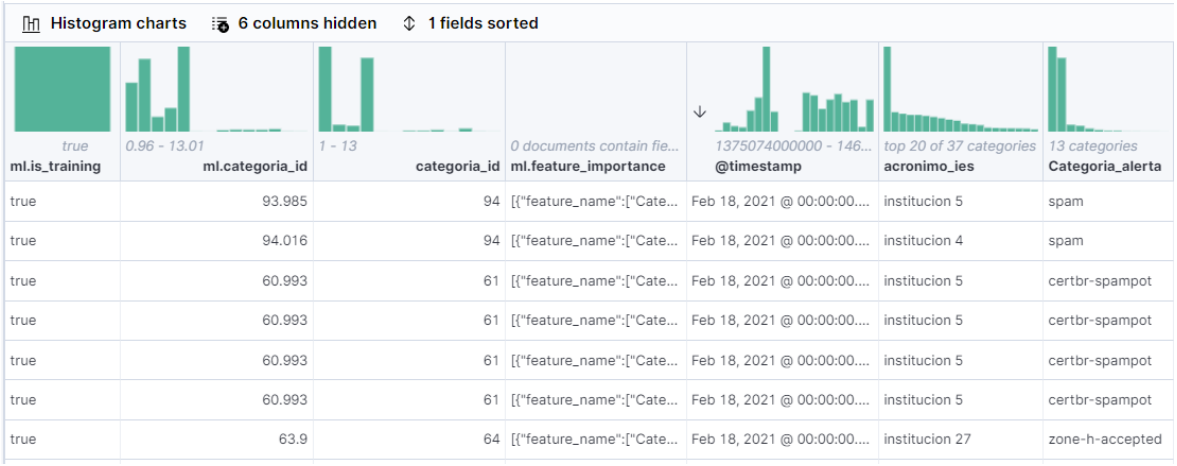
Un error cuadrático medio (MSE) de cero significa que los modelos predicen la variable dependiente con perfecta precisión. Este es el ideal, sin embargo, normalmente no es posible. Del mismo modo, un valor R cuadrado de 1 indica que toda la varianza en la variable dependiente puede explicarse por las variables características. Normalmente, se compara los valores de MSE y R-cuadrado de varios modelos de regresión para encontrar el mejor equilibrio o ajuste para los datos.

El resultado de la regresión tiene un nuevo índice que contiene una copia de sus datos de origen con predicciones para su variable dependiente. La figura 24

muestra los resultados de la regresión en Kibana, que muestra el contenido del índice de destino en un formato tabular.

Figura 24.

Resultados de la regresión. Ilustración derivada del software Kibana.



true ml.is_training	0.96 - 13.01 ml.categoria_id	1 - 13 categoria_id	0 documents contain fie... ml.feature_importance	1375074000000 - 146... @timestamp	top 20 of 37 categories acronimo_ies	13 categories Categoria_alerta
true	93.985	94	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 5	spam
true	94.016	94	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 4	spam
true	60.993	61	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 5	certbr-spampot
true	60.993	61	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 5	certbr-spampot
true	60.993	61	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 5	certbr-spampot
true	60.993	61	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 5	certbr-spampot
true	63.9	64	[{"feature_name":["Cate...	Feb 18, 2021 @ 00:00:00....	institucion 27	zone-h-accepted

El resultado de la figura 24, muestra una columna para la variable dependiente (categoría_id), que contiene los valores reales que se está tratando de predecir con el análisis de regresión. Además muestra una columna para los valores de predicción (ml.categoria_id) y una columna que indica si el documento se usó en el conjunto de entrenamiento (ml.is_training).

Otras de las funciones que permite Kibana es que puede filtrar la tabla para mostrar solo datos de prueba o entrenamiento y puede seleccionar qué campos se muestran en la tabla. Además, puede habilitar gráficos de histograma para comprender mejor la distribución de valores en sus datos.

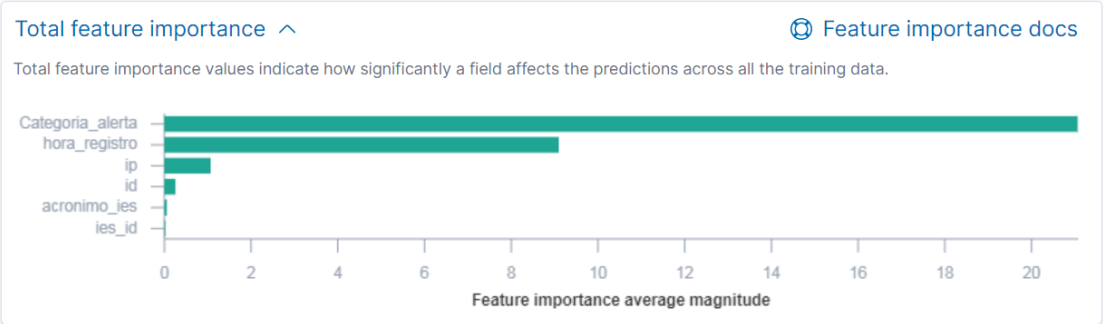
Si se elige calcular la importancia de la característica, el índice de destino también contiene objetos ml.feature_importance. A cada campo que se incluye en el análisis de regresión (conocido como una característica del punto de datos) se le asigna un valor de importancia de la característica. Este valor tiene una magnitud y una dirección (positiva o negativa), lo que indica cómo cada campo afecta a una predicción en particular. Solo los valores más significativos (en este caso, los cinco

primeros) se almacenan en el índice. Sin embargo, los metadatos del modelo entrenado también contienen la magnitud promedio de los valores de importancia de la característica para cada campo en todos los datos de entrenamiento. En la figura 25 se puede ver la información resumida en Kibana

Figura 25.

Información resumida de la importancia de las características en la predicción.

Ilustración derivada del software Kibana.

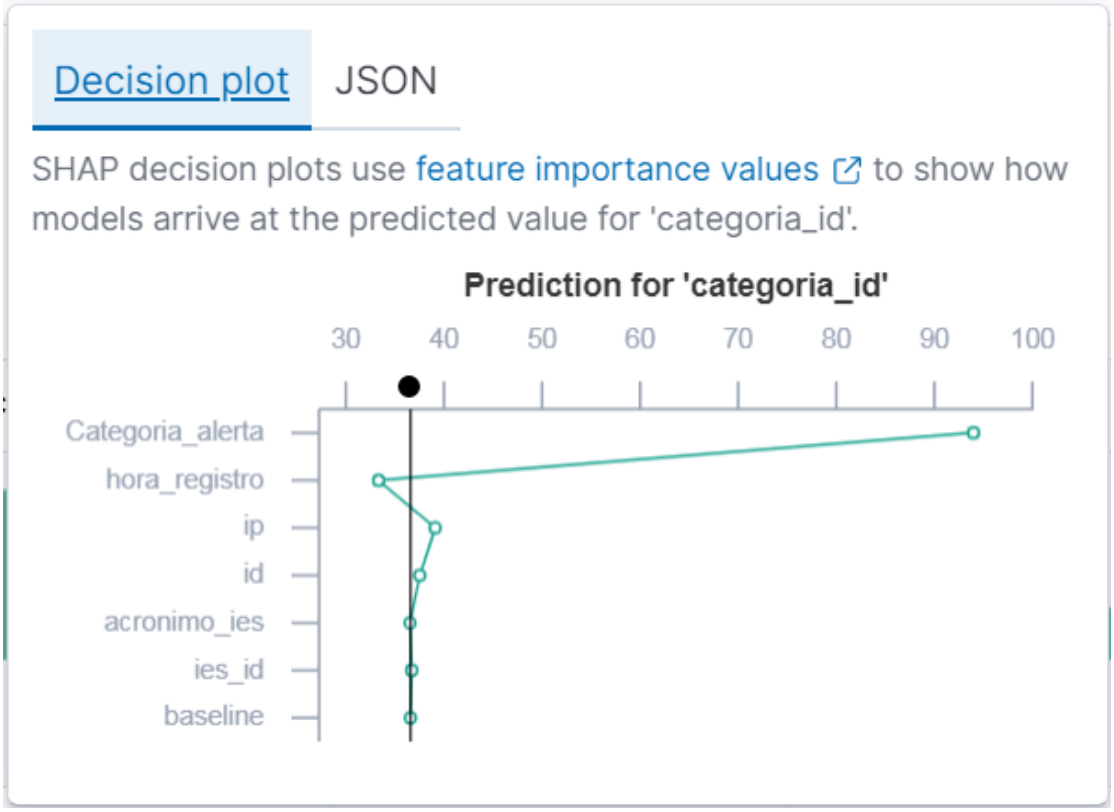


Además, se puede visualizar en la figura 26 los valores de importancia de la característica para cada predicción individual en forma de un gráfico de decisión. La ruta de decisión comienza en una línea de base, que es el promedio de las predicciones para todos los puntos de datos en el conjunto de datos de entrenamiento. A partir de ahí, los valores de importancia de la característica se agregan a la ruta de decisión hasta que llega a su predicción final. Las características con el impacto positivo o negativo más significativo aparecen en la parte superior.

Por lo tanto, las características relacionadas con las categorías de alertas tuvieron la influencia más significativa en predecir el valor de categoría id. Este tipo de información puede ayudarnos a comprender cómo los modelos llegan a sus predicciones. También puede indicar qué aspectos de su conjunto de datos son más influyentes o menos útiles cuando se está entrenando y ajustando su modelo.

Figura 26.

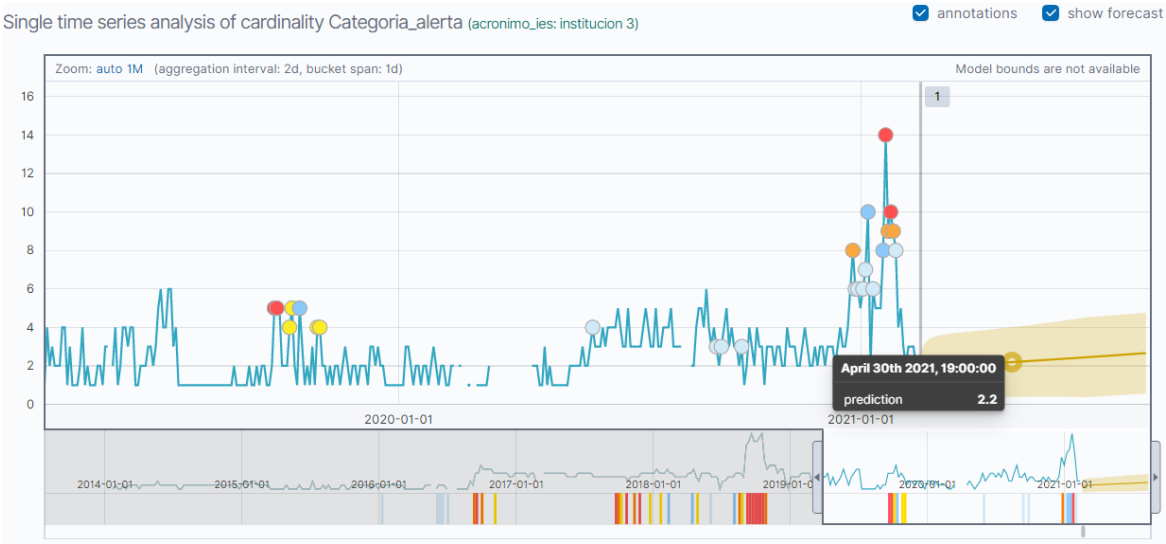
Importancia de la característica para cada predicción individual. Ilustración derivada del software Kibana.



A continuación, en la figura 27 se muestra una gráfica obtenida en Kibana sobre la predicción realizada por 90 días. Para el 30 de abril la Institución tres tiene una predicción del 2.2 que se dé la categoría alerta ss-botnet-drone.

Figura 27.

Valores reales vs los valores predichos. Ilustración derivada del software Kibana.



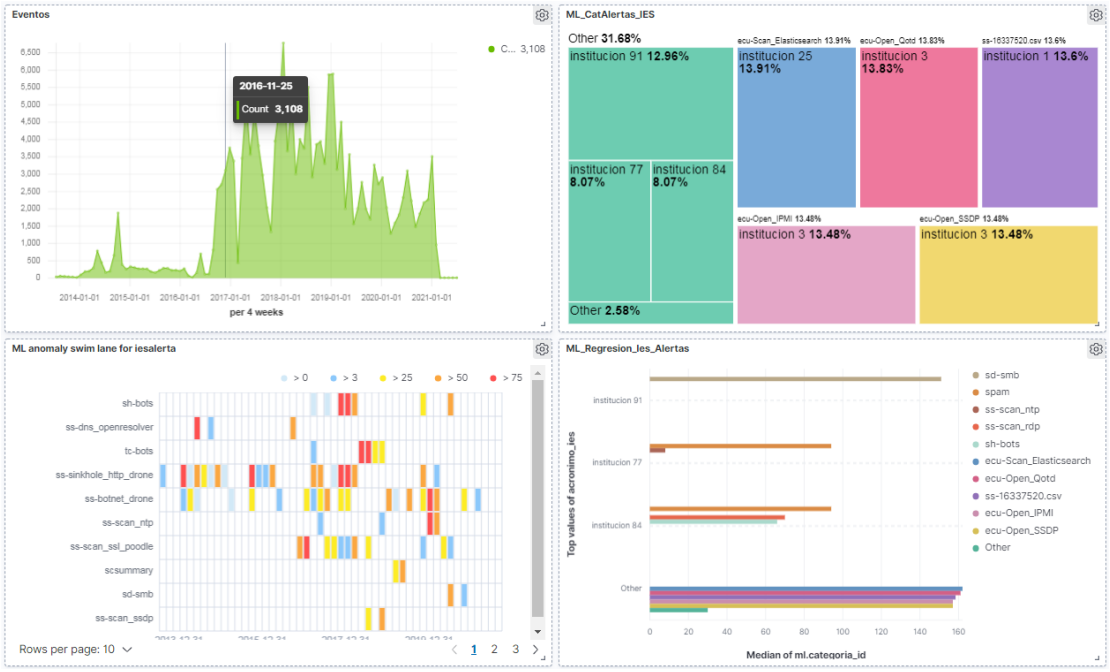
Visualización de los datos en dashboard

La mejor forma de comprender los datos es visualizarlos. Con los paneles, se puede convertir los datos de uno o más patrones de índice en una colección de paneles que aportan claridad a los datos, cuentan una historia sobre los datos y permiten concentrarse solo en los datos que son importantes. Se configuro cada panel para mostrar los datos en un gráfico, tabla, mapa, luego se comparó los paneles uno al lado del otro para identificar los patrones y conexiones de los datos.

En la figura 28, se muestra un dashboard con algunos paneles que muestran la historia de los datos, además, las líneas de tiempo de la detección de anomalías de las categorías de alertas y en las IES.

Figura 28.

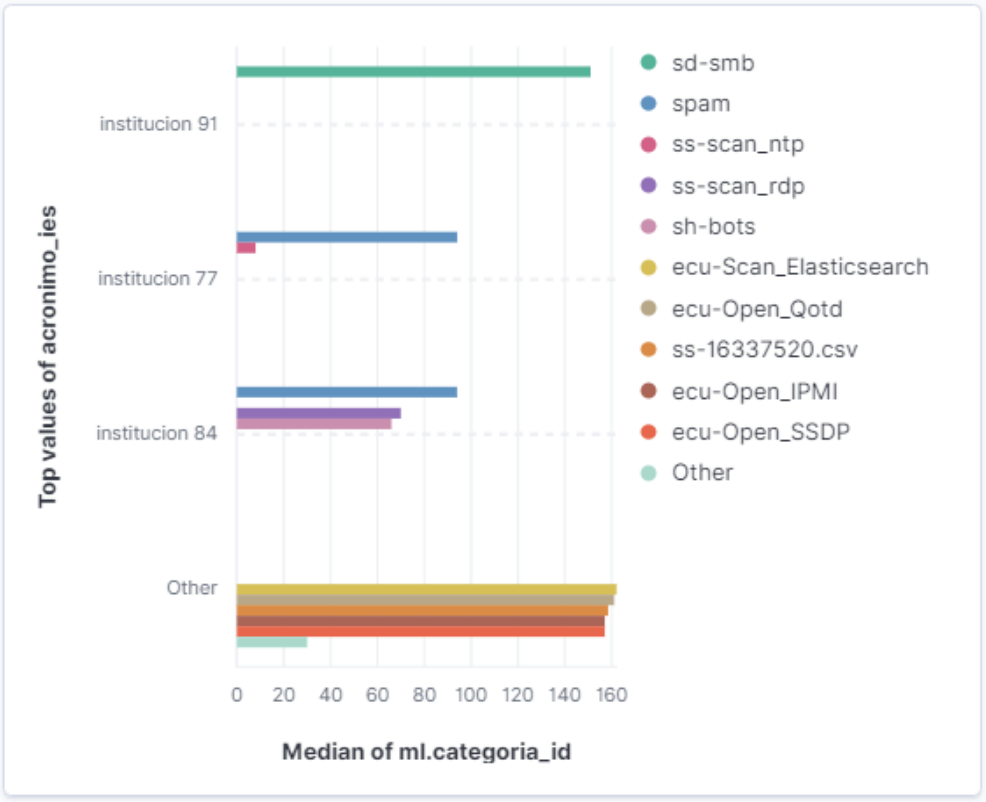
Dashboard líneas de tiempo de anomalías y Machine Learnig. Ilustración derivada del software Kibana.



En la Figura 29 se visualiza el resultado del algoritmo por regresión y se puede observar a las categorías alertas con más probabilidades que pueda suceder, además, de la universidad que puede estar involucrada con tal categoría alerta. En la figura 30 se muestra el mismo resultado con la diferencia que en este caso es con el algoritmo de clasificación. Si se comparan los dos resultados las probabilidades que se pueda dar una categoría alerta son similares.

Figura 29.

Resultado predicción por algoritmo de regresión. Ilustración derivada del software Kibana.



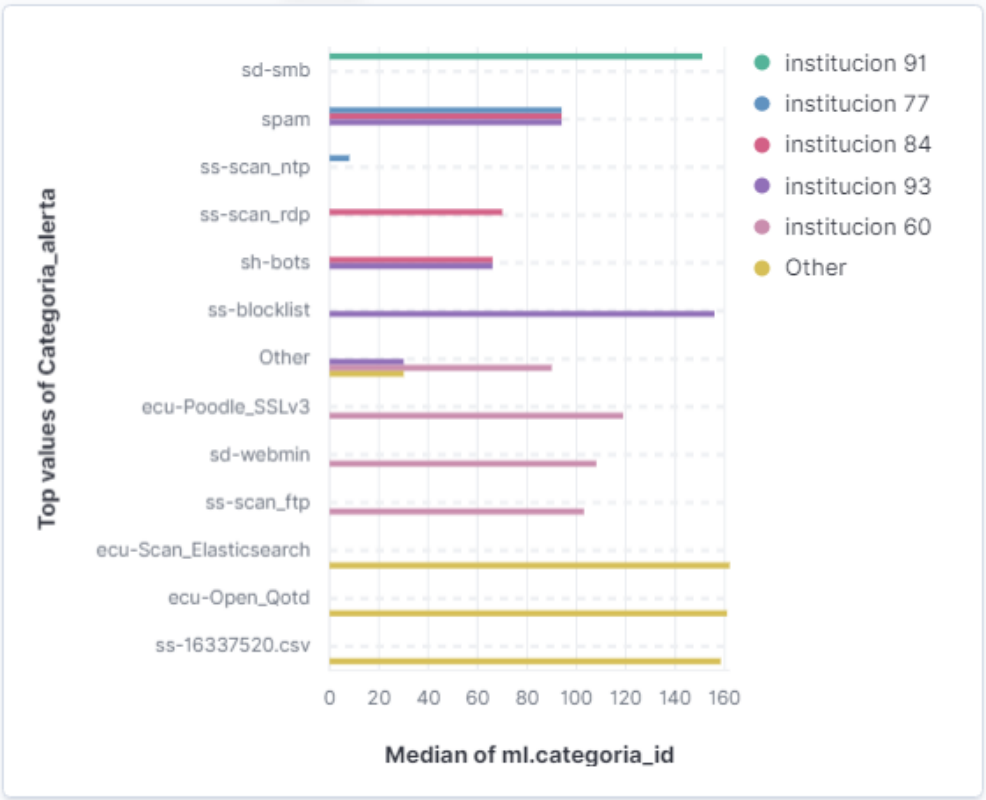
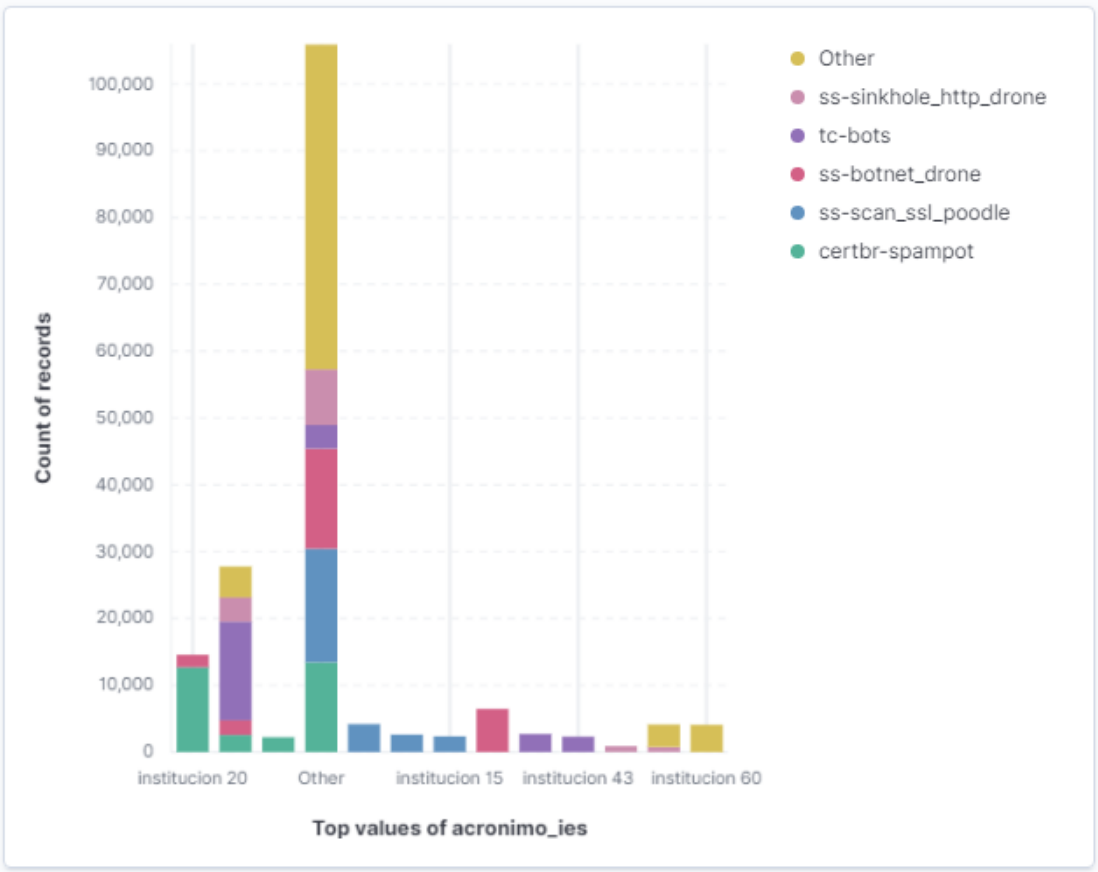


Figura 30.

Resultado predicción por algoritmo de clasificación. Ilustración derivada del software Kibana.



Capítulo V: Conclusiones y Recomendaciones

Conclusiones

En este estudio se aplicó la combinación de las metodologías de investigación acción, bibliográfica y descriptiva. A ella se le sumo CRISP-DM como la principal metodología para realizar minería de datos. Así mismo se añadieron técnicas de Machine Learning, que facilitaron la analítica de datos. Esto permite concluir que este proyecto fue desarrollado metódicamente y reúne la calidad técnica exigida.

Al realizar la revisión de literatura SLR, se concluye que existen diversas propuestas sobre la protección de los sistemas de información, el uso de minería de datos para realizar predicciones sobre un ataque a los sistemas. Los autores utilizan algoritmos para explorar el conocimiento de los patrones de ataque frecuentes, que permita la predicción precisa de futuros ataques. Los estudios hacen referencia a sistemas de aprendizaje automático que aprovecha grandes volúmenes de datos de diversos registros de seguridad, información de alertas y conocimientos de analistas para la identificación de los riesgos. Los estudios analizados no hacen referencia al sistema de soporte a la toma de decisiones.

CRISP-DM y el proceso de minería de datos fue útil en el proceso de exploración de datos, mediante las tecnologías analíticas y procesos estadísticos que permitió generar reglas a partir de los datos históricos para generar patrones que permitieron predecir ataques.

La arquitectura del DSS diseñado, contiene componentes, que permiten realizar procesos para explorar y analizar la información y así poder descubrir tendencias o patrones a partir de los cuales se tomen decisiones. Además, permite aplicar técnicas de Machine Learning y minería de datos para desplegar la información utilizando software especializados. En nuestro caso, facilitar la gestión de las alertas de seguridad de la información.

Se aplicó la técnica de aprendizaje automático no supervisado para anomalías basadas en categoría alertas, sobre los que están considerados los influyentes y los resultados para el tráfico en tiempo real, y que son satisfactorios. Machine Learning es tan diverso como la ciberseguridad y hay mucho por hacer en Machine Learning para la seguridad cibernética.

El modelo de regresión que se evaluó en Machine Learning, dio un error cuadrático medio (MSE) aproximado de cero que significa que el modelo predice la variable dependiente en nuestro caso categoría alerta con una buena precisión. Del mismo modo, un valor R cuadrado de 1 que indica que toda la varianza en la variable dependiente puede explicarse por las variables características. Lo cual el modelo que se ejecutó en Elasticsearch y Kibana se adaptó para la gestión de alertas de seguridad de la información de las IES.

Recomendaciones

Para cualquier proceso de minería de datos es indispensable cumplir las fases de la metodología CRISP-DM. Luego contar con suficientes y diferentes fuentes de datos que tengan un nivel de confiabilidad y volumen suficiente. Posteriormente, seleccionar adecuadamente los procesos de extracción, recolección y carga de los datos, la selección acertada de variables, el disponer de herramientas informáticas de avanzada para modelarlos, evaluarlos y validar sus resultados.

En Machine Learning es recomendable comparar los resultados con diferentes algoritmos para definir cual se adapta mejor a la gestión de alertas de seguridad de la información de las IES tales como los algoritmos de clasificación y regresión.

Es recomendable entrenar el modelo seleccionado con más datos históricos para obtener un mejor rendimiento del algoritmo y obtener mejores resultados en la predicción de una amenaza que se pueda dar.

Realizar todas las fases de la metodología seleccionada, para llegar a obtener el resultado. Las partes más importantes a las que se debe llegar a tener es la base de conocimiento (la información, datos), el procesamiento de la base de conocimiento (tecnología, algoritmos, filtros), la analítica y control del negocio (medir todo, estrategia del negocio) y la interfaz de usuario.

Realizar adecuadamente la preparación y limpieza de los datos antes de importar en la herramienta Elasticsearch y Kibana, para que todos los datos se carguen y no tener perdida de datos al momento de importar. Además, evitar errores que se presentan al momento de la manipulación de los datos.

Referencias Bibliográficas

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Carniege Mellon University, 7 Diciembre 2017. [Online]. Available: http://sc.isri.cmu.edu/component/content/article?id=129:new-research-tackles-adaptive-security-decision-support.

Tejada, E. C. (2015). *Gestión de incidentes de seguridad informática. IFCT0109*. IC Editorial.

Vieites, Á. G. (2013). *Auditoría de seguridad informática*. Ediciones de la U.

Cardona, M., Durley, L., & Uribe Serna, A. E. (2015). Sistema de gestión de incidentes de seguridad informática para corbeta.

Dorofee, Audrey., Ruefle, Robin., Zajicek, Mark., McIntire, David., Perl, Samuel., Alberts, Christopher., Huth, Carly., & Walters, Pennie. (2018). *Incident Management Capability Assessment* (CMU/SEI-2018-TR-007). Retrieved January 18, 2019, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=538848

Gonzalez Diaz, J. E., & Parrado Rodríguez, V. A. (2017). *Guía de gestión de incidentes de seguridad de la información para la oficina TIC del ministerio de salud, tomando como base la norma ISO 27001-2013* (Bachelor's thesis, Universidad Piloto de Colombia).

Colmenares E, A. M. (2012). Investigación-acción participativa: una metodología integradora del conocimiento y la acción. *Voces y Silencios. Revista Latinoamericana de Educación*, *3*(1), 102-115.

Zikopoulos, P., & Eaton, C. (2011). *Understanding big data: Analytics for enterprise class hadoop and streaming data*. McGraw-Hill Osborne Media.

Sauter, V. L. (2014). *Decision support systems for business intelligence*. John Wiley & Sons.

Hernández Orallo, J., FERRI RAMIREZ, C. E. S. A. R., & RAMIREZ QUINTANA, M. J. (2004). *Introducción a la Minería de Datos*. Pearson Prentice Hall.

ISO - the International Organization for Standardization, a. I.-t. (2016). INTERNATIONAL STANDARD ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 14,15.

Larrea, O. H. (2012). Sistema de Educacion Superior del Ecuador. *Obtenido de Ministerio de Educacion*.

Fuertes, W., Reyes, F., Valladares, P., Tapia, F., Toulkeridis, T., & Pérez, E. (2017). An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. *Systems*, *5*(4), 52.

Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. Editex.

Dean, J. (2014). *Big data, data mining, and Machine Learning: value creation for business leaders and practitioners*. John Wiley & Sons.

Husák, M., & Kašpar, J. (2018, June). Towards Predicting Cyber Attacks Using Information Exchange and Data Mining. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 536-541). IEEE.

Thuraisingham, B. (2009, September). Data mining for malicious code detection and security applications. In *Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology-Volume 02* (pp. 6-7). IEEE Computer Society.

Collier, R., & Azarmi, B. (2019). *Machine Learning with the Elastic Stack: Expert techniques to integrate Machine Learning with distributed search and analytics*. Packt Publishing Ltd.

Dali, L., Mivule, K., & El-Sayed, H. (2017, September). A heuristic attack detection approach using the “least weighted” attributes for cyber security data. In *Intelligent Systems Conference (IntelliSys), 2017* (pp. 1067-1073). IEEE.

Amin, A., Anwar, S., Adnan, A., Khan, M. A., & Iqbal, Z. (2015, November). Classification of cyber attacks based on rough set theory. In *Anti-Cybercrime (ICACC), 2015 First International Conference on* (pp. 1-6). IEEE.

Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. *IEEE Communications Surveys & Tutorials*.

Ban, T., Eto, M., Guo, S., Inoue, D., Nakao, K., & Huang, R. (2015, July). A study on association rule mining of darknet big data. In *Neural Networks (IJCNN), 2015 International Joint Conference on* (pp. 1-7). IEEE.

Colbaugh, R., & Glass, K. (2012, October). Predictability-oriented defense against adaptive adversaries. In *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*(pp. 2721-2727). IEEE.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

Aguilar, L. J. (2016). *Big Data, Análisis de grandes volúmenes de datos en organizaciones*. Alfaomega Grupo Editor.

Feng, C., Wu, S., & Liu, N. (2017, July). A user-centric Machine Learning framework for cyber security operations center. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 173-175). IEEE.

Sinoara, R. A., Antunes, J., & Rezende, S. O. (2017). Text mining and semantics: a systematic mapping study. Journal of the Brazilian Computer Society, 23(1), 9.

Kawakani, C. T., Junior, S. B., Miani, R. S., Cukier, M., & Zarpelão, B. B. (2016, May). Intrusion alert correlation to support security management. In Anais Principais do XII Simpósio Brasileiro de Sistemas de Informação (pp. 313-320). SBC.

Stroeh, K., Madeira, E. R. M., & Goldenstein, S. K. (2013). An approach to the correlation of security events based on Machine Learning techniques. Journal of Internet Services and Applications, 4(1), 7.

Franklin, L., Pirrung, M., Blaha, L., Dowling, M., & Feng, M. (2017, October). Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. In 2017 IEEE Symposium on Visualization for Cyber Security (VizSec) (pp. 1-8). IEEE.

Hachmi, F., Boujenfa, K., & Limam, M. (2019). Enhancing the accuracy of intrusion detection systems by reducing the rates of false positives and false negatives through multi-objective optimization. Journal of Network and Systems Management, 27(1), 93-120.

Granadillo, G. G., El-Barbori, M., & Debar, H. (2016, November). New types of alert correlation for security information and event management systems. In 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-7). IEEE.

Garae, J., & Ko, R. K. (2017). Visualization and data provenance trends in decision support for cybersecurity. In Data Analytics and Decision Support for Cybersecurity (pp. 243-270). Springer, Cham.

Mikut, R., & Reischl, M. (2011). Data mining tools. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 1(5), 431-443.

Hoffmann, F., Bertram, T., Mikut, R., Reischl, M., & Nelles, O. (2019). Benchmarking in classification and regression. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(5), e1318.

De Cnudde, S., Martens, D., Evgeniou, T., & Provost, F. (2020). A benchmarking study of classification techniques for behavioral data. International Journal of Data Science and Analytics, 9(2), 131-173.

Hassan, A., Tahir, S., & Baig, A. I. (2019, August). Unsupervised Machine Learning for malicious network activities. In *2019 International Conference on Applied and Engineering Mathematics (ICAEM)* (pp. 151-156). IEEE.

Galán Cortina, V. (2016). *Aplicación de la metodología CRISP-DM a un proyecto de minería de datos en el entorno universitario* (Bachelor's thesis).

Roldán, M. C. (2013). *Pentaho Data Integration Beginner's Guide*. Packt Publishing Ltd.

Shmueli, G., Bruce, P. C., Gedeck, P., & Patel, N. R. (2019). *Data mining for business analytics: concepts, techniques and applications in Python*. John Wiley & Sons.

Reyes, F., Fuertes, W., Tapia, F., Toulkeridis, T., Aules, H., & Pérez, E. (2018, July). A BI Solution to Identify Vulnerabilities and Detect Real-Time Cyber-Attacks for an Academic CSIRT. In *Science and Information Conference* (pp. 1135-1153). Springer, Cham.

Reyes-Mena, F. X., Fuertes-Díaz, W. M., Guzmán-Jaramillo, C. E., Pérez-Estévez, E., Bernal-Barzallo, P. F., & Villacís-Silva, C. J. (2018). Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT. *Revista Facultad de Ingeniería*, *27*(47), 21-29.

Valladares, P., Fuertes, W., Tapia, F., Toulkeridis, T., & Pérez, E. (2017, July). Dimensional data model for early alerts of malicious activities in a CSIRT. In *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)* (pp. 1-8). IEEE.