# UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERIA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistema


**Controles y mecanismo en la gestión de seguridad de red basado en Sistemas de Detección de intrusos: Una revisión sistemática de la literatura**

Trabajo para obtener el Grado Académico de Bachiller en Ingeniería de Sistemas

**Autor:**

Nick Brayan Mostacero Gamboa

**Asesor:**

Mg. Fernando Manuel Asin Gómez

Lima, Setiembre del 2020

# DECLARACIÓN JURADA DE AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

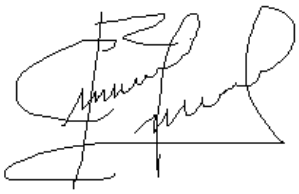
Mg. Fernando Manuel Asin Gómez, de la Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que la presente investigación titulada: "**Controles y mecanismo en la gestión de seguridad de red basado en Sistemas de Detección de intrusos: Una revisión sistemática de la literatura"** constituye la memoria que presenta el estudiante Nick Brayan Mostacero Gamboa para aspirar al Grado Académico de Bachiller en Ingeniería de Sistemas, cuyo trabajo de investigación ha sido realizado en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente declaración en la ciudad de Lima, a los 11 días del mes de octubre del año 2020.



Mg. Fernando Manuel Asin Gómez

## ACTA DE SUSTENTACIÓN DE TRABAJO DE INVESTIGACIÓN

En Lima, Ñaña, Villa Unión, a……..los.....18.....día(s) del mes de…..septiembre.....del año 2020.... siendo las.....09:45.....horas, se reunieron los miembros del jurado en la Universidad Peruana Unión campus Lima, bajo la dirección del (de la) presidente(a): ..... Dra. Erika Inés Acuña Salinas....., el (la) secretario(a): ..... M.Sc. Fredy Abel Huanca Torres..... y los demás miembros: ..… Ing. Carlos Eduardo Saavedra Vasconez …..y el (la) asesor(a): Mg. Fernando Manuel Asin Gomez……con el propósito de administrar el acto académico de sustentación del trabajo de investigación titulado: "Revisión sistemática de la literatura: Controles y mecanismo en la gestión de seguridad de red basado en Sistemas de Detección de intrusos en la red".

…….....….de los (las) egresados (as): a)……..... Nick Brayan Mostacero Gamboa …….....

……b)……

…… conducente a la obtención del grado académico de Bachiller en

……..……Ingeniería de Sistemas……..
*(Denominación del Grado Académico de Bachiller)*

El Presidente inició el acto académico de sustentación invitando …al… candidato(a)/s hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del jurado a efectuar las preguntas, y aclaraciones pertinentes, las cuales fueron absueltas por …el.. candidato(a)/s. Luego, se produjo un receso para las deliberaciones y la emisión del dictamen del jurado.

Posteriormente, el jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Candidato/a (a): …… Nick Brayan Mostacero Gamboa …….

| CALIFICACIÓN | ESCALAS | | | Mérito |
|---|---|---|---|---|
| | Vigesimal | Literal | Cualitativa | |
| Aprobado | **17** | **B+** | **Con nominación de muy bueno** | Sobresaliente |

Candidato/a (b): ……...

| CALIFICACIÓN | ESCALAS | | | Mérito |
|---|---|---|---|---|
| | Vigesimal | Literal | Cualitativa | |
| | | | | |

*(*) Ver parte posterior*

Finalmente, el Presidente del jurado invito …al… candidato(a)/s a ponerse de pie, para recibir la evaluación final y concluir el acto académico de sustentación procediéndose a registrar las firmas respectivas.

| | | |
|---|---|---|
| Presidente<br>Dra. Erika Inés Acuña Salinas | | Secretario<br>M.Sc. Fredy Abel Huanca Torres |
| Asesor<br>Mg. Fernando Manuel Asin Gomez | Miembro | Miembro<br>Ing. Carlos Eduardo Saavedra Vasconez |
| Candidato/a (a)<br>Nick Brayan Mostacero Gamboa | | Candidato/a (b) |

# INDICE


1. Introducción ..... 4
2. Marco Conceptual ..... 5

Sistema de Detección de Intrusos ..... 5

Tipos de IDS ..... 5

Falso positivos ..... 5

Machine Learning ..... 6

3. Método del artículo de revisión ..... 6

Revisión Sistemática de la Literatura (RSL) ..... 6

Preguntas para la revisión sistemática ..... 7

Estrategia de búsqueda ..... 8

Criterios de inclusión y exclusión. ..... 9

Evaluar la calidad de los datos ..... 11

4. Resultados ..... 11

Resultados de la búsqueda ..... 12

Resultados de los filtros ..... 13

5. Análisis bibliométrico ..... 15
6. Preguntas de investigación ..... 18
7. Conclusiones ..... 21
8. References ..... 22

# Controles y mecanismo en la gestión de seguridad de red basado en Sistemas de Detección de intrusos: Una revisión sistemática de la literatura

Nick Mostacero [1]

[1] Universidad Peruana Unión, Km 19 Carretera Central, Ñaña, Lurigancho, Lima, Perú
nickmostacero@upeu.edu.pe

**Resumen.** El rápido crecimiento de las tecnologías no solo formula la vida más fácilmente, sino que también expone muchos problemas de seguridad. Con el avance de Internet a lo largo de los años, se ha incrementado el número de ataques a través de Internet. El Sistema de detección de intrusiones (IDS) es una de las herramientas de soporte aplicables a la seguridad de la información. IDS proporciona un entorno fiable para los negocios, los mantiene alejado de las actividades sospechosas de la red. El presente artículo busca identificar el estado en que se encuentran las investigaciones sobre los controles y mecanismos relacionados con la gestión de seguridad de red basándose en IDS. Para la identificación de dichos elementos mencionados realizo una revisión sistemática de la literatura en las bases de datos reconocidas. De un aproximado de 376 artículos se realizó una revisión, y se identificaron 35 artículos que hacen referencia al tema de estudio propuesto con anterioridad. Luego de realizar una revisión sistemática de la literatura se encontró que entre los controles más usados es el tráfico de red en su totalidad, y se pudo encontrar un sinfín de herramientas provenientes de Machine Learning.

**Palabras claves:** Sistema de detección de intrusos, Machine Learning, Trafico de red, Falso positivos.

# Controls and mechanism in network security management based on Intrusion Detection Systems: A systematic review of the literature

Nick Mostacero [1]

[1] Universidad Peruana Unión, Km 19 Carretera Central, Ñaña, Lurigancho, Lima, Perú
nickmostacero@upeu.edu.pe

**Abstract.** The rapid growth of technologies not only makes life easier, but also exposes many security issues. With the advance of the Internet over the years, the number of attacks over the Internet has increased. Intrusion Detection System (IDS) is one of the support tools applicable to information security. IDs provides a reliable environment for businesses, keeping them away from suspicious network activities. This article seeks to identify the status of investigations into controls and mechanisms related to managing network security based on IDS. For the identification of these elements I carried out a systematic review of the literature in the recognized databases. A review was carried out of an estimated 376 articles, and 35 articles were identified that refer to the subject of study proposed above. After a systematic review of the literature it was found that among the most used controls is network traffic in its entirety, and a host of tools from Machine Learning could be found.

**key words:** Intruder Detection System, Machine Learning, Network Traffic, False Positives.

# 1. **Introducción**

En el mundo de la tecnología de rápido desarrollo, las redes enfrentan amenazas como virus, gusanos, troyanos, spyware, adware, etc. Estas intromisiones deben identificarse antes de cualquier tipo de pérdida para las organizaciones. Incluso la red de área local (LAN) interna también está luchando seriamente con las intromisiones. Esto está afectando la productividad de las redes de computadoras en términos de ancho de banda y otros recursos. Los hackers usan funciones avanzadas como puertos dinámicos, suplantación de direcciones IP, carga útil cifrada, etc., para evitar la detección.[1]

El Sistema de detección de intrusiones (IDS) es el proceso de monitorear los eventos que ocurren en el sistema o la red y analizar si una actividad en la red es normal o una intrusión. Para detectar la intrusión se puede hacer mediante dos enfoques, a saber, la detección de anomalías y la detección de mal uso. La detección de uso indebido utiliza un enfoque basado en antivirus que coincide con patrones de intrusión o ataques al tráfico de red que ya está almacenado en la base de datos, por lo que la base de datos siempre debe actualizarse para detectar patrones de infiltración o nuevos ataques.[2]

Según el tipo de técnica de detección de intrusos, los IDS pueden ser categorizados como IDS basados en firma (S-IDS) e IDS basados en anomalías (A-IDS). Los S-IDS identifican intrusiones por hacer coincidir el tráfico de red entrante con patrones de intrusión conocidos previamente. Este tipo de IDS es capaz de detectar ataques conocidos, pero no pueden identificar nuevos tipos de ataques. Por el contrario, los A-IDS crean un modelo de comportamiento normal de la red y generar una alerta por cada actividad de la red que se desvía del normal establecido perfil. Esto hace que los A-IDS sean sensibles a intrusiones previamente conocidas y desconocidas. En este artículo, nuestro objetivo es Mejorar la capacidad de detección de intrusos de los A-IDS.[3]

El objetivo artículo busca identificar los controles y mecanismos relacionados con la gestión de seguridad de red basándose en IDS.
El articulo se distribuye de la siguiente manera: Sección 2 presenta el marco teórico, la sección 3 presenta la metodología utilizada, la sección 4 muestra los resultados obtenidos y por último la sección 5 las conclusiones.

# 2. Marco Conceptual

### Sistema de Detección de Intrusos

Los Sistema de Detección de Intrusos (IDS) es un módulo importante en la red. El sistema de seguridad se utiliza para descubrir, determinar e identificar uso no autorizado, duplicación, alteración y destrucción de sistemas de información.[4]

El concepto no da a entender que cualquier ataque o intrusión se puede definir como un esfuerzo para comprometer la confidencialidad, integridad, disponibilidad de la información que se tiene.

### Tipos de IDS

Básicamente se dividen en 3 tipos de IDS

a) Sistema de Detección de Intrusos de Host (HIDS): HIDS se usa para monitorear datos de tráfico encriptados a un host específico. Funciona en información recopilada desde una computadora individual sistema. Este enfoque se basa en estadísticas y probabilidad La teoría y todos los ataques se toman como un espacio muestral.[5]

b) Sistemas de Detección de Intrusos de Red (NIDS): Detectan actividad maliciosa monitoreando todo el tráfico de la red. Los sistemas IDS son instalado en general colocando la tarjeta de interfaz de red en modo promiscuo para capturar todos los segmentos de tráfico de redes.[5]

c) Sistemas de Detección de Intrusos Distribuidos (DIDS): Los DIDS son desarrolla generalmente usando una combinación de sistemas basados tanto en host como en red, aparte de esto todavía muchos de los IDS se consideran más fuertes en un campo o el otro.[5]

### Falso positivos

Un falso positivo es un término aplicado a un fallo de detección en un sistema de alertas. Sucede cuando se detecta la presencia de una intrusión en el sistema que realmente no existe.[6]

**Machine Learning**

> El aprendizaje automático requiere un sistema capaz de la adquisición autónoma y la integración del conocimiento. Esta capacidad incluye el aprendizaje a partir de la experiencia, la observación analítica, etc. El resultado es un sistema que puede mejorarse continuamente y, por lo tanto, ofrece una mayor eficiencia y eficacia. El objetivo principal del estudio del aprendizaje automático es diseñar y desarrollar algoritmos y técnicas que permitan que las computadoras aprendan. En general, hay dos tipos de técnicas de aprendizaje automático, supervisadas y no supervisadas.[7]

## 3. Método del artículo de revisión

**Revisión Sistemática de la Literatura (RSL)**

La revisión sistemática de la literatura nos ayuda a recolectar información de las diferentes bases de datos y librerías digitales que tengan relación con el objetivo [1]. A partir de este concepto nace la necesidad de conocer los controles y mecanismos en la gestión de seguridad de red basado en Sistemas de Detección de intrusos (IDS).

Tabla 1. Elaboración del objetivo de la investigación

| Campo | Valor |
|---|---|
| Objetivo de estudio | Controles y Mecanismos |
| Propósito | Identificar |
| Foco | Métodos o herramientas |
| Involucrados | Seguridad de red, IDS |
| Factor de contexto | Ninguno |

**Preguntas para la revisión sistemática**

A continuación, se describirán las preguntas de investigación y bibliometría propuestas para la evaluación de los artículos encontrados en los diferentes gestores de base de datos utilizados para la revisión sistemática de la literatura. Tabla 2 – Tabla 3.

Tabla 2. Preguntas de Investigación

| ID | Preguntas | Motivación |
|---|---|---|
| PI-01 | ¿Qué controles se utilizan para la gestión de seguridad de red según IDS? | Determinar los controles que se utilizan para la gestión de seguridad de red según IDS |
| PI-02 | ¿Qué tipos mecanismos se implementan en la gestión de seguridad de red? | Determinar los tipos de mecanismos que se utilizan para la gestión de seguridad de red |
| PI-03 | ¿Qué herramientas IDS se utilizan para seguridad de red? | Determinar las herramientas que se utilizan para la gestión de seguridad de red según IDS |
| PI-04 | ¿Métodos o herramientas que utilizan para la gestión de seguridad de red? | Determinar los métodos o herramientas que se utilizan para la gestión de seguridad de red según IDS |

Tabla 3. Preguntas bibliométricas

| ID | Pregunta | Motivación |
|---|---|---|
| PB-01 | ¿Cuál es la cantidad de publicaciones por tipo de fuente en el artículo? | Determinar la cantidad de estudios publicados por tipo de artículo para identificar la concentración de los mismos. |
| PB-02 | ¿Cuáles son las publicaciones en las que se han encontrado estudios relacionados al tema? | Identificar la cantidad de publicaciones sobre este tema. |
| PB-03 | ¿Cuál es la cantidad de publicación por año? | Identificar la frecuencia de las publicaciones para poder establecer la relevancia del tema |

| | | |
|---|---|---|
| | | en el tiempo. |

**Estrategia de búsqueda**

La estrategia para la elaboración de la cadena de búsqueda fue, la estrategia PICOC , priorizando la búsqueda en librerías indexadas y bases de datos. Dicha estrategia tiene la siguiente estructura:

**Población:**

- Término principal: Intrusion Detection System
- Términos alternos: IDS
- Justificante: Seguridad de red

**Intervención:**

- Entidad: No aplica
- Término principal: No aplica
- Términos alternos: No aplica
- Justificación: No aplica

**Comparación:**

No aplica, ya que en la RSL no se hace contraste alguno con algún patrón de referencia

**Resultado:**

- Entidad: Controles y mecanismo
- Término principal: controls
- Términos alternos: mechanisms
- Justificante: copia y pegar

**Contexto**: Seguridad de la red

**Idioma:**

El idioma seleccionado para definir la cadena de búsqueda fue el inglés, esto se debe a que es el más utilizados en la elaboración de artículos en las librerías seleccionadas. Basados en la estrategia PICOC, se definió la siguiente cadena de búsqueda:

Tabla 4.

| Concepto | Términos |
|---|---|
| Población | ("Intrusion Detection System" AND " IDS ") |
| Intervención | No aplica |
| Comparación | no aplica |
| Resultado | ("controls" AND "mechanisms") |
| Contexto | No aplica |

**Criterios de inclusión y exclusión.**

De acuerdo a lo establecido por Kitchenham[8]. Luego de realizar la ejecución de las cadenas de búsquedas en las librerías digitales definidas posteriormente, los resultados encontrados deben ser previamente evaluados con la finalidad de responder las preguntas de la Tabla 2 - 3. Teniendo en cuenta ello, se ha establecido los siguientes criterios:

Tabla 5.

| ID | Criterios de Inclusión |
|---|---|
| CI-01 | Los que contengan Controles y/o mecanismo para IDS |
| CI-02 | Artículos que contengan herramientas y/o modelos en IDS |
| CI-03 | Artículos provenientes de librerías digitales indexadas y bases de datos |
| CI-04 | Artículos cuyo rango de años esté conformado desde el año 2015 hasta la actualidad. |
| CI-05 | Se aceptarán artículos provenientes de conferencias y artículos. |

Tabla 6.

| ID | Criterios de Exclusión |
|---|---|
| CE-01 | Artículos de años inferiores a 2015 |
| CE-02 | Artículos cuyo resumen no contenga un contenido similar al objetivo |
| CE-03 | Todos los artículos duplicados |
| CE-04 | Serán excluidos los artículos cuyo título no tenga relación con el objeto de estudio |
| CE-05 | Serán rechazados los artículos cuyas conclusiones y resúmenes sean de bajo nivel |

**Fuentes de datos.** Las fuentes científicas utilizadas para la obtención de los artículos fueron las siguientes:

- ScienceDirect (http://www.sciencedirect.com)
- IEEE Xplore: (http://ieeexplore.ieee.org)
- ACM Digital Library (http://portal.acm.org)
- Springer Link(http://link.springer.com)
- Web of Science (webofknowledge.com)

**Procedimientos para la selección de estudios.** Se considera el siguiente procedimiento para la selección de artículos de la RSL:

- **Paso 1:** Se procedió a ejecutar la cadena de búsqueda PICO, en las bases de datos indexadas previamente seleccionadas, aplicando los criterios de inclusión y exclusión de acuerdo a la tabla 6.
- **Paso 2:** Se aplico una revisión rápida a los títulos de los artículos resultantes de la ejecución del Paso 1 para descargar artículos que no sean relevantes con el objetivo de estudio de la RSL.
- **Paso 3:** Se revisaron los resúmenes de los artículos previamente seleccionados en el Paso 2 para proceder con la exclusión de todos los estudios según los criterios definidos en la tabla 6.
- **Paso 4:** Se procedió con la realización de una revisión preliminar del contenido de los artículos seleccionados luego del Paso 3, con un enfoque en la introducción y conclusiones obtenidas, descartando artículos con una relevancia bajo respecto a su introducción y conclusiones.

TABLA 7. PROCEDIMIENTOS Y CRITERIOS DE INCLUSIÓN

| **Procedimiento** | **Criterio de selección** |
|---|---|
| Paso 1 | CI-01, CI-02, CI-03, CI-04, CI-05 |
| Paso 2 | CE-01, CE-02 |
| Paso 3 | CE-03, CE-04 |
| Paso 4 | CE-05 |

**Evaluar la calidad de los datos**

Tabla 8. Criterios de evaluación de calidad

| ID | Criterios de evaluación de calidad |
|---|---|
| CE-01 | ¿Qué método utilizaron para la gestión de seguridad de red basado en IDS?<br>S: El método seleccionado ha sido documentado apropiadamente<br>P: El método seleccionado ha sido documentado parcialmente<br>N: No se ha documentado el método mencionado |
| CE-02 | ¿Qué porcentaje de mejora tuvieron?<br>S: El porcentaje de mejora ha sido documentado apropiadamente<br>P: El porcentaje de mejora ha sido documentado parcialmente<br>N: No se ha documentado el porcentaje de mejora mencionado |
| CE-03 | ¿Qué controles utilizaron para la gestión de seguridad de red basado en IDS?<br>S: Los controles se han documentado apropiadamente<br>P: Los controles se han documentado parcialmente<br>N: No se ha documentado los controles mencionados |
| CE-04 | ¿Qué mecanismos utilizaron para la gestión de seguridad de red basado en IDS?<br>S: Los mecanismos se han documentado apropiadamente<br>P: Los mecanismos se han documentado parcialmente<br>N: No se ha documentado los mecanismos mencionados |
| CE-05 | ¿Qué herramientas utilizaron para la gestión de seguridad de red basado en IDS?<br>S: Las herramientas se han documentado apropiadamente<br>P: Las herramientas se han documentado parcialmente<br>N: No se ha documentado las herramientas mencionados |

## 4. **Resultados**

De acuerdo a las pautas de la guía de Kitchenham para la Revisión Sistemática de la Literatura (RSL) [1] en esta sesión se procede con el detallado de todos los pasos ejecutados.

**Resultados de la búsqueda**

De acuerdo con los pasos definidos en la sección 3, el paso inicial para este trabajo es la ejecución de la cadena de búsqueda en las librerías digitales ya mencionadas anteriormente. En siguiente Tabla se muestra los resultados y las cadenas de búsquedas utilizadas de acuerdo a cada librería digital.

Tabla 10. Resultados de Búsqueda

| Base de Datos | Fecha | Total |
|---|---|---|
| Cadena de Búsqueda | | |
| Web of Science | Mayo 2020 | 9 |
| (('Intrusion Detection System AND "ids") AND (protocol) AND (process)) | | |
| Springer Link | Mayo 2020 | 106 |
| 'Intrusion AND Detection AND System AND "ids" AND (protocol) AND NOT (process)' | | |
| Science Direct | mayo 2020 | 208 |
| ((Intrusion Detection System) AND (ids)) | | |
| IEEE Explorer | mayo 2020 | 49 |
| (("Document Title":Intrusion Detection System) AND "Document Title":*ids) | | |
| ACM Digital Library | mayo 2020 | 56 |

[[Publication Title: "intrusion detection system"] OR [Publication Title: "ids"]] AND [Abstract: ids] AND [Publication Date: (01/01/2015 TO 12/31/2020)]

**Resultados de los filtros**

- **Paso 1:**
  En el paso 1 se aplicó los criterios de inclusión y exclusión que fueron definidos anteriormente, con la finalidad que disminuir y seleccionar los artículos más relevantes sobre el tema a investigar.

- **Paso 2:**
  En el paso 2 se llevó acabo la revisión de los títulos sobre los artículos que provenían del resultado de la aplicación del paso 1, con el fin de descartar los artículos que no tengan correlación con el tema de estudio.

- **Paso 3:**
  Los artículos resultantes del paso 2, fueron revisados de acuerdo a lo definido en el paso 3, el lo cual se realizo la lectura de los resúmenes con el fin de seleccionar los artículos que tengas mas afinidad con el tema de estudio.

- **Paso 4:**
  En este paso, se filtró los artículos restantes, se aplicó una revisión más detallada, que consistió en realizar la lectura de la introducción como de la conclusión de cada uno de los artículos para descartar los que cuyo impacto sean bajos para nuestro tema de estudio.
  En la siguiente Tabla 11 se muestra un resumen de la cantidad de artículos resultantes luego de la aplicación de los pasos ya revisados.

Tabla 11. Resultados del proceso de selección

| Base de datos | Artículos descubiertos | Paso 1 | Paso 2 | Paso 3 | Paso 4 |
|---|---|---|---|---|---|
| ACM Digital Library | 56 | 44 | 35 | 29 | 8 |
| IEEE Explorer | 47 | 29 | 20 | 16 | 8 |
| Science Direct | 208 | 106 | 76 | 41 | 13 |
| Springer Link | 56 | 35 | 20 | 13 | 5 |
| Web of science | 9 | 8 | 7 | 6 | 1 |
| **Total** | 376 | 222 | 158 | 105 | 35 |

**Evaluar la calidad del contenido de los artículos:**

Se evaluó la calidad de cada uno de los artículos que finales que fueron 35, cada uno de ellos fue almacenado en la herramienta Mendeley y con la herramienta Parsifal se aplicó cada uno de los criterios de inclusión y exclusión definidos en la sesión 3.4:

Tabla 12. Evaluación de calidad

| ID | C1 | C2 | C3 | C4 | C5 | Total |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 4.0 |
| 2 | 1 | 1 | 0 | 1 | 0 | 3.0 |
| 3 | 1 | 1 | 1 | 1 | 0 | 4.0 |
| 4 | 1 | 0 | 1 | 1 | 0 | 3.0 |
| 5 | 1 | 0 | 1 | 1 | 0.5 | 3.5 |
| 6 | 1 | 0 | 1 | 1 | 1 | 4.0 |
| 7 | 1 | 0 | 1 | 0.5 | 0 | 2.5 |
| 8 | 1 | 0 | 0.5 | 0.5 | 0 | 2.0 |
| 9 | 0 | 0 | 0.5 | 1 | 0 | 1.5 |
| 10 | 0.5 | 0 | 0.5 | 1 | 0 | 2.0 |
| 11 | 1 | 0 | 1 | 1 | 0 | 3.0 |
| 12 | 1 | 1 | 1 | 1 | 0 | 4.0 |
| 13 | 1 | 0 | 1 | 1 | 0 | 3.0 |
| 14 | 1 | 1 | 1 | 0.5 | 0.5 | 4.0 |
| 15 | 0.5 | 0 | 1 | 0.5 | 1 | 3.0 |
| 16 | 1 | 0 | 1 | 1 | 0 | 3.0 |
| 17 | 1 | 0 | 1 | 0.5 | 0 | 2.5 |
| 18 | 0.5 | 0 | 1 | 1 | 1 | 3.5 |
| 19 | 1 | 0 | 0.5 | 1 | 0 | 2.5 |
| 20 | 1 | 0 | 0.5 | 0.5 | 0 | 2.0 |
| 21 | 1 | 1 | 1 | 1 | 0.5 | 4.5 |
| 22 | 0.5 | 1 | 1 | 1 | 0.5 | 4.0 |
| 23 | 1 | 1 | 1 | 1 | 0 | 4.0 |
| 24 | 1 | 0 | 1 | 1 | 1 | 4.0 |
| 25 | 0.5 | 0 | 1 | 1 | 0 | 2.5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 26 | 1 | 1 | 0 | 0 | 1 | 3.0 |
| 27 | 0.5 | 1 | 1 | 1 | 0 | 3.5 |
| 28 | 0.5 | 0.5 | 1 | 0 | 0.5 | 2.5 |
| 29 | 1 | 1 | 1 | 1 | 0.5 | 4.5 |
| 30 | 0.5 | 1 | 1 | 0.5 | 1 | 4.0 |
| 31 | 0.5 | 0 | 0.5 | 0 | 0 | 1.0 |
| 32 | 0.5 | 1 | 1 | 1 | 0 | 3.5 |
| 33 | 0.5 | 1 | 1 | 1 | 0 | 3.5 |
| 34 | 0.5 | 0 | 1 | 1 | 1 | 3.5 |
| 35 | 0.5 | 1 | 0.5 | 1 | 0 | 3.0 |

## 5. Análisis bibliométrico

**PB-01 ¿Cuál es la cantidad de publicaciones por tipo de fuente en el artículo?**

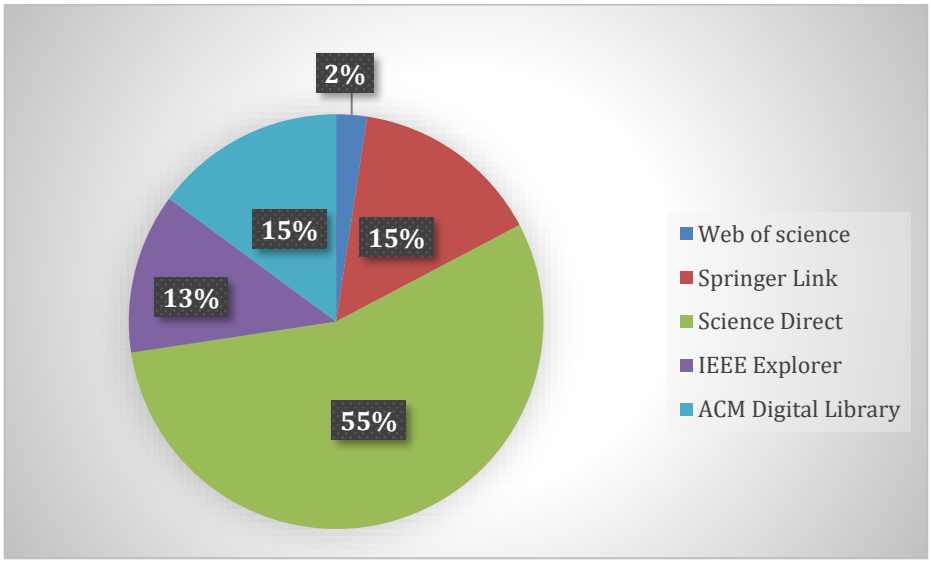



*Gráfico 1. Cantidad de publicaciones*

En el gráfico se observa el porcentaje que corresponde a cada librería digital de la siguiente manera:

208 artículos son de la librería “Science Direct” y representa un 55% de la cantidad total, en segundo lugar, tenemos “ACM Digital Library” y “Springer Link” cada una

con 56 artículos, la cual representando el 15% individualmente, luego se tiene 47 artículos son de la librería “IEEE Explorer” con un 13% y por último 9 artículos de la librería “Web of Science” la cual representa el 2% del total.

Se observa que Science Direct tiene una gran cantidad de artículos relacionados al tema a investigar.

**PB-02 ¿Cuáles son las publicaciones en las que se han encontrado estudios relacionados al tema?**

En el siguiente grafico se observa el porcentaje de artículos relacionado con el estudió ya mencionado:

Del total de artículos que pasaron el proceso de calidad fueron 13 de Science Directe que representan 37%, 8 de ACM Digital Library y IEEE Explore respectivamente, la cual representan 23% cada una de ella, 5 de Spring Link que representa 14%, por ultimo y no la menos importante Web of Science con 1 articulo el cual representa el 3% del total.

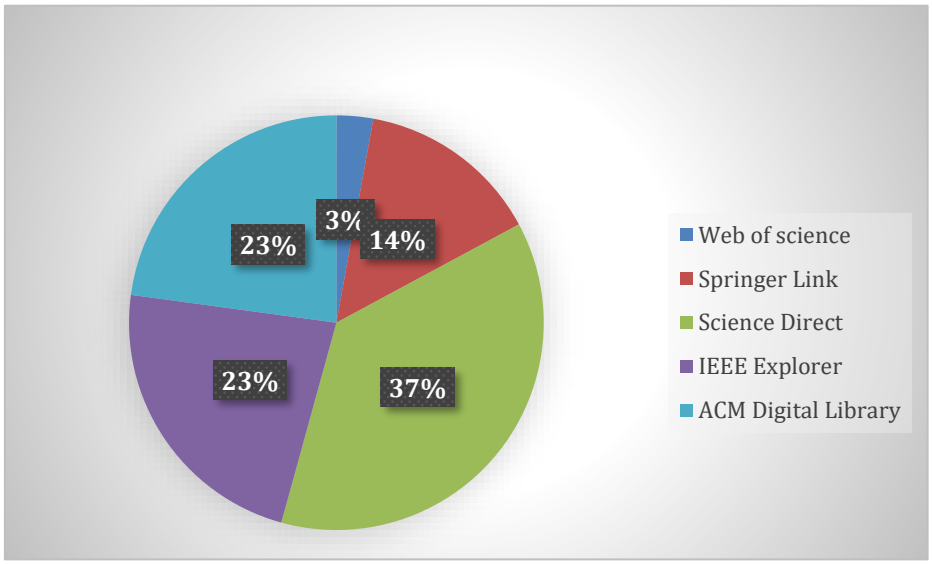



*Gráfico 2. Cantidad de relacionados con el estudio*

**PB-03 ¿Cuál es la cantidad de publicación por año?**

Luego de realizar la cadena de búsqueda ya definida con anterioridad, se puede observar en el grafico 3 los artículos que fueron publicados en los siguientes años. En total se tiene 376 d las cuales 44 fueron publicadas en el año 2015, 47 en el año 2016, 51 en el año 2017, 85 en el año 2018, 81 en el año 2019 y, por último, 68 en el año 2020.

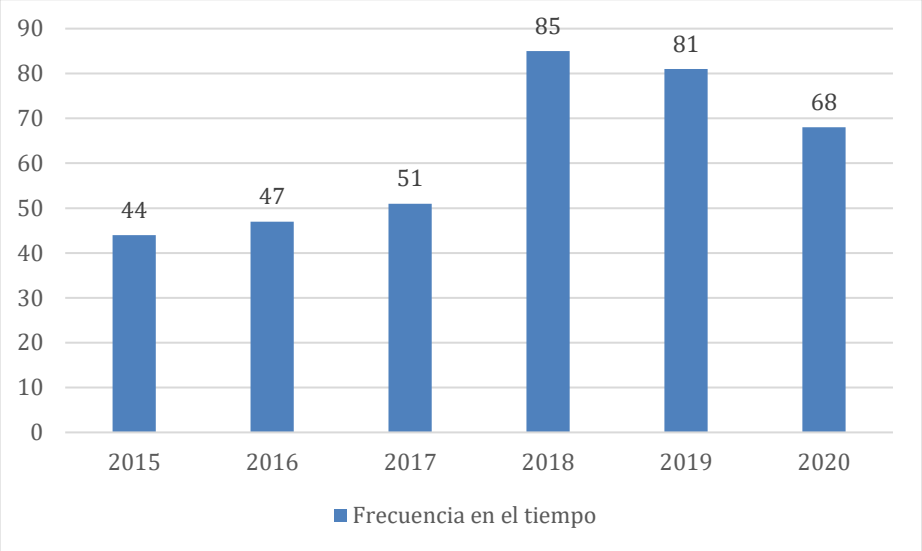



*Gráfico 3. Año de publicación*

## 6. Preguntas de investigación

**PI-01 ¿Qué controles se utilizan para la gestión de seguridad de red según IDS?**

En el siguiente grafico se muestra los controles encontrados en la revisión de los artículos que tiene relación con el tema de estudio:

De los 35 artículos que pasaron los criterios de calidad, 29 (83%) utilizaron el "tráfico de red" como control para la gestión de seguridad de red, 4 utilizaron Características de datos, y por último, 2 (6%) de ellos utilizaron "Lista negra de IP".

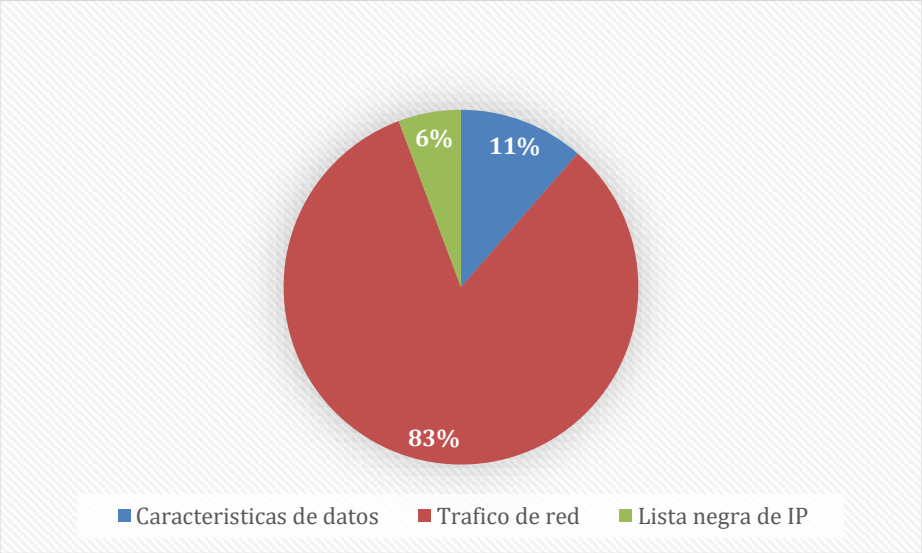



*Gráfico 4. Controles para seguridad de red según IDS*

**PI-02 ¿Qué tipos mecanismos se implementan en la gestión de seguridad de red?**

Los mecanismos para los IDS encontrados fueron 3. Entre estos mecanismos se encuentra los siguientes:

Tabla 13. Tipo de herramientas

| Tipo | Características | Relacionados |
|---|---|---|
| Anomalías | generar una alerta por cada actividad de la red que se desvía del normal establecido perfil | 32 |
| Firma | supervisan todos los paquetes de la red y los comparan con la base de datos de firmas | 12 |
| Comité de expertos | Supervisa las características definidas de acuerdo a la experiencia del comité | 1 |

**PI-03 ¿Qué herramientas IDS se utilizan para seguridad de red?**

**Las herramientas IDS:** Son las plataformas que nos ayudaran a contener y evitar ataques que puedan poner en peligro la información confidencial de cada entidad.

- **Snort:**
  Snort es un sistema ligero de detección de intrusos de red de código abierto basado en Libpcap. Snort se puede configurar para ejecutarse en tres modos: (1) modo Sniffer, que simplemente lee los paquetes fuera de la red y los muestra en una secuencia continua en la pantalla. (2) Modo de registro de paquetes, que registra los paquetes en el disco. (3) Modo de sistema de detección de intrusiones de red (NIDS), que realiza la detección y el análisis del tráfico de red.[9]

- **Kismet:**

Kismet es un detector de red inalámbrica 802.11, sniffer y sistema de detección de intrusiones. Kismet funciona con cualquier tarjeta de interfaz de red inalámbrica que admita monitoreo en bruto y puede detectar cualquier forma de tráfico.[10]

**PI-04 ¿Métodos o herramientas que utilizan para la gestión de seguridad de red?**

Tabla 13. Herramientas y modelos

| Trabajo | Mecanismo | Dataset | Ataques | Método de Evaluación | % de mejora |
|---|---|---|---|---|---|
| Puma Bedi et al.[3] | anomalías | NSL-KDD | R2L - U2R | Backpropagation | 80,00% |
| Ngoc Tu Pham et al.[11] | anomalías | NSL-KDD / KDD-Cup 99 | | Tree – Random Forst | 84,25% |
| Krishnan Subramanian et al.[12] | Comité de expertos | NSL-KDD | R2L - U2R | RNN - Bayesian network fuzzy neural network | 96,14% |
| Aditya Chellam et al.[13] | anomalías | NSL-KDD | | Lazy Learning Algorithms | 97,59% |
| Zohreh Abtahi et al.[14] | anomalías | NSL-KDD | DoS, U2R, R2L y Probe | Decision Tree y knn | 99,60% |
| Aniruddha Parvat et al.[15] | anomalías | NSL-KDD | DoS, U2R, R2L y Probe | Gaussian nb<br>logistic regression<br>Decision tree | 96,52%<br>98,14%<br>99,89% |
| Bisyron Wahyudi et al.[16] | anomalías / firmas | KDD-Cup 99 | DoS, U2R, R2L y Probe | Support Vector Machine (SVM) | 95,73% |
| Sinh-Ngoc Nguyen et al.[4] | anomalías / firmas | KDD-Cup 99 | DoS | KNN / Random Forest | 99,87% |
| Lekhraj Mehra et al.[5] | Firma | | | Reglas modificadas | 89,56% |
| Raman Singh et al.[1] | anomalías | NSL-KDD | DoS, U2R, R2L y Probe | Fuzzy | 96,30% |
| Muhammad Salman et al.[17] | anomalías | KDD-1999 | | LVQ - PCA | 96,52% |
| Jabbar, Rajanikanth et al.[18] | anomalías | NSL-KDD | DoS | K-means / Tree y KNN | 99,80% |

| | | | | | |
|---|---|---|---|---|---|
| Wisesty, Adiwijaya [2] | anomalías / firmas | KDD-Cup 99 | DoS, R2L y Probe | Algoritmo de retro propagación/Gradiente conjugado | 93,20% |
| J. Huassain et al.[19] | anomalías | NSL-KDD | | SVM | 99,98% |

## 7. Conclusiones

En el presente estudio se busca identificar el estado en que se encuentran las investigaciones sobre los métodos y herramientas para la gestión de red basado en IDS, los resultados obtenidos de una revisión sistémica aplicada a 35 artículos seleccionados de librerías digitales indexadas. Estos artículos fueron escogidos luego de pasar por un análisis bibliométrico en el cual se busca encontrar aquellos estudios que apoyan al objetivo de esta investigación y hayan sido publicados desde 2015 hacia adelante.

Como se demuestra en los resultados de la presente investigación, los métodos más utilizadas para un IDS son los algoritmos supervisados como se muestran en la tabla 13, la cual ayuda a disminuir los falsos positivos que se dan al implementar los IDS; también se encontró que los mecanismos utilizados en la implementación de IDS es por anomalías debido a que permite reconocer un ataque desde el día cero. Esto nos muestra que los nuevos IDS para una implementación deben utilizar un algoritmo supervisado con el fin de mejorar su eficiencia.

Se puede observar la gráfica 5 que 11(79%) de los artículos seleccionados tiene más del 91% de mayor detección de intrusión, y 3 (21%) de los artículos tienen entre un 80% a 90% de mejora en la detección de intrusos, la cual reduce considerablemente el hallazgo de falso positivos.

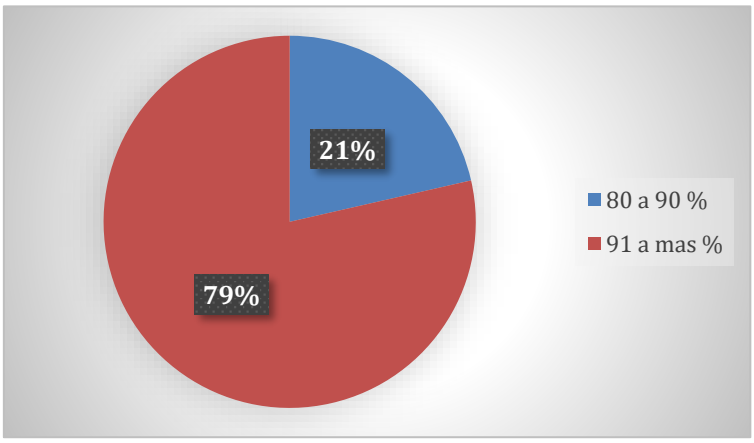



*Gráfico 5. Porcentaje de mejora de los IDS con algoritmos*

# 8. References


[1] R. Singh, H. Kumar, and R. K. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine," *Expert Syst. Appl.*, vol. 42, no. 22, pp. 8609–8624, 2015, doi: 10.1016/j.eswa.2015.07.015.

[2] U. N. Wisesty and Adiwijaya, "Comparative study of conjugate gradient to optimize learning process of neural network for Intrusion Detection System (IDS)," *Proceeding - 2017 3rd Int. Conf. Sci. Inf. Technol. Theory Appl. IT Educ. Ind. Soc. Big Data Era, ICSITech 2017*, vol. 2018-Janua, pp. 459–464, 2017, doi: 10.1109/ICSITech.2017.8257156.

[3] P. Bedi, N. Gupta, and V. Jindal, "Siam-IDS: Handling class imbalance problem in Intrusion Detection Systems using Siamese Neural Network," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 780–789, 2020, doi: 10.1016/j.procs.2020.04.085.

[4] S. N. Nguyen, V. Q. Nguyen, J. Choi, and K. Kim, "Design and implementation of intrusion detection system using convolutional neural network for DoS detection," *ACM Int. Conf. Proceeding Ser.*, pp. 34–38, 2018, doi: 10.1145/3184066.3184089.

[5] L. Mehra, M. K. Gupta, and H. S. Gill, "An effectual & secure approach for the detection and efficient searching of Network Intrusion Detection System (NIDS)," *IEEE Int. Conf. Comput. Commun. Control. IC4 2015*, pp. 4–8, 2016, doi: 10.1109/IC4.2015.7375615.

[6] A. Gramajo, "Introducci ´ on a conceptos de IDS y t ´ ecnicas avanzadas con Snort," *Networks*, 2005.

[7] W. C. Lin, S. W. Ke, and C. F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowledge-Based Syst.*, vol. 78, no. 1, pp. 13–21, 2015, doi: 10.1016/j.knosys.2015.01.009.

[8] D. Budgen and P. Brereton, "Performing systematic literature reviews in software engineering," *Proc. - Int. Conf. Softw. Eng.*, vol. 2006, pp. 1051–1052, 2006, doi: 10.1145/1134285.1134500.

[9] "Snort Improvement on Profnet RT for Industrial Control System Intrusion," no. 2, pp. 942–946, 2016.

[10] G. Thejdeep, S. B. Sagar, L. K. Siddartha, and B. R. Chandavarkar, "Detecting Rogue Access Points using Kismet," *2015 Int. Conf. Commun. Signal Process. ICCSP 2015*, pp. 172–175, 2015, doi: 10.1109/ICCSP.2015.7322813.

[11] N. T. Pham, E. Foo, S. Suriadi, H. Jeffrey, and H. F. M. Lahza, "Improving performance of intrusion detection system using ensemble methods and feature selection," *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3167918.3167951.

[12] N. Kaja, A. Shaout, and D. Ma, "An intelligent intrusion detection system," *Appl. Intell.*, vol. 49, no. 9, pp. 3235–3247, 2019, doi: 10.1007/s10489-019-01436-1.

[13] A. Chellam, L. Ramanathan, and S. Ramani, "Intrusion Detection in Computer Networks using Lazy Learning Algorithm," *Procedia Comput. Sci.*, vol. 132, pp. 928–936, 2018, doi: 10.1016/j.procs.2018.05.108.

[14] Z. A. Foroushani and Y. Li, "Intrusion detection system by using hybrid algorithm of data mining technique," *ACM Int. Conf. Proceeding Ser.*, pp. 119–123, 2018, doi: 10.1145/3185089.3185114.

[15] A. Gosain and J. Singh, *Smart Trends in Information Technology and Computer Communications*, vol. 876. Springer Singapore, 2018.

[16] B. W. Masduki, K. Ramli, F. A. Saputra, and D. Sugiarto, "Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS)," *14th Int. Conf. QiR (Quality Res. QiR 2015 - conjunction with 4th Asian Symp. Mater. Process. ASMP 2015 Int. Conf. Sav. Energy Refrig. Air Cond. ICSERA 2015*, pp. 56–64, 2016, doi: 10.1109/QiR.2015.7374895.

[17] M. Salman, D. Husna, S. G. Apriliani, and J. G. Pinem, "Anomaly based detection analysis for intrusion detection system using big data technique with Learning Vector

Quantization (LVQ) and Principal Component Analysis (PCA)," *ACM Int. Conf. Proceeding Ser.*, pp. 20–23, 2018, doi: 10.1145/3293663.3293683.

[18] M. A. Jabbar, R. Aluvalu, and S. Sai Satyanarayana Reddy, "Cluster based ensemble classification for intrusion detection system," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1283, pp. 253–257, 2017, doi: 10.1145/3055635.3056595.

[19] J. Hussain and S. Lalmuanawma, "Fusion of misuse detection with anomaly detection technique for novel hybrid network intrusion detection system," *Adv. Intell. Syst. Comput.*, vol. 555, pp. 73–87, 2017, doi: 10.1007/978-981-10-3779-5_10.