SISTEMA DE DETECCIÓN DE INTRUSOS APLICADO A REDES DE PYMES

ANDERSON DAVID SOLARTE CAICEDO
YEHISON HAMMER ESPAÑA MONTAÑO

UNIVERSIDAD CESMAG
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2021

SISTEMA DE DETECCIÓN DE INTRUSOS APLICADO A REDES DE PYMES

ANDERSON DAVID SOLARTE CAICEDO
YEHISON HAMMER ESPAÑA MONTAÑO

Proyecto de investigación como requisito para obtener el titulo de INGENIERO DE SISTEMAS

ASESOR:
ARTURO ERASO TORRES
Mg. Software Libre

UNIVERSIDAD CESMAG
FACULTAD DE INGENIERÍA
PROGAMA INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2021

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

INTRODUCCIÓN

El avance de la tecnología y el aumento del uso de dispositivos móviles y plataformas web, ha conducido a las PYMES a digitalizar sus negocios, esto ocasiona algunos inconvenientes de seguridad debido a que las PYMES no cuentan con los recursos necesarios en materia de seguridad. Los responsables de seguridad de ACENS han realizado un análisis de la situación actual de las PYMES frente a la protección de datos y que medidas son claves para afrontar un 2020 de forma segura, en donde encontraron que una de cada cinco PYMES ha sufrido un ataque, además de que un 90% de las PYMES no cuenta con un responsable de seguridad y el 40% apenas implementa protocolos básicos de seguridad como la verificación de dos pasos para el correo electrónico.

Por lo cual, es necesario analizar los niveles de seguridad con los que cuentan las PYMES a nivel regional y de acuerdo a este análisis llevar a cabo el sistema de detección de intrusos alineándolo a las necesidades de las PYMES y asegurando que se gestione eficazmente.

Con el fin de mejorar la seguridad en las PYMES, se implementará un sistema de detección de intrusos de fácil configuración, dinámico y amigable con el usuario, el cual mejorará la disponibilidad, integridad y confidencialidad de la información en las PYMES.

1. PROBLEMA DE INVESTIGACIÓN

1.1 TEMA DE INVESTIGACIÓN

Detección de intrusos en redes.

1.2 ÁREA DE INVESTIGACIÓN

Seguridad Informática.

1.3 LÍNEA DE INVESTIGACIÓN

Seguridad de la Información, el programa de ingeniería de sistemas la define como:

> La disciplina que, enmarca todos los métodos y controles tecnológicos que se pueden implementar con el fin de mitigar el riesgo relacionado a las amenazas cibernéticas que pueden comprometer la privacidad, integridad o confidencialidad de los sistemas de información, incluyendo la transmisión y almacenamiento de la información tratada por los mismos, entre las principales amenazas se encuentran: infección por malware, ataque de denegación de servicio, suplantación de identidades, errores de los usuarios, interceptación de las comunicaciones, entre otros[1] .

1.4 PLANTEAMIENTO DEL PROBLEMA

Según la revista de seguridad informática, it Digital Security en su artículo publicado el 29 de enero del año 2020 cuyo nombre “Los ataque contra pymes están creciendo en frecuencia y sofisticación”[2], el 63% de las empresas alrededor del mundo reportaron un incidente, este tipo de incidente estuvo relacionado con pérdida de información tanto de los clientes como de los propios empleados.

Teniendo en cuenta el proceso de investigación que se está llevando a cabo, se fundamenta con el fin, de reconocer que la migración de los sistemas tradicionales a uno de innovación el cual es controlado atreves de un software, conlleva a que se debe salvaguardar la información, que se obtenga atreves de los procesos de control de la PYME y donde prime los pilares fundamentales de la seguridad informática tales como la confiabilidad, integridad y disponibilidad de la información.

---

[1] HERTZOG Raphael, MAS, Roland. Líneas de investigación del programa de ingeniería de sistemas universidad CESMAG. 2020.

[2] YERRO Ster, Articulo por it Digital Security, Los ataques contra pymes están creciendo en frecuencia y sofisticación,2020 disponible en: https://www.itdigitalsecurity.es/endpoint/2020/01/los-ataques-contra-pymes-estan-creciendo-en-frecuencia-y-sofisticacion

Entre las posibles causas del aumento de ataques alrededor del mundo hacia las PYMES, es que las PYMES no cuentan con buenas bases tecnológicas, las cuales les puedan ayudar a proteger su red, esto debido a su elevado costo y que para la configuración se debe contar con conocimientos técnicos para su implementación y correcto funcionamiento.

Generalmente los recursos disponibles con los que cuentan las PYMES para seguridad Informática son muy limitados, en algunos casos prácticamente nulos, con lo cual puede dejar expuesta toda la seguridad y la información que se encuentra resguardada en las PYMES.

Por otra parte, como posibles consecuencias se tiene, la perdida de información de las PYMES. Con lo cual se verá afectado en su credibilidad y prestigio, como otras posibles causas también están las intrusiones de personas con ánimo de penetrar el sistema de información. Lo cual tiene como único fin apoderarse de información valiosa, de tal manera que al ser vulnerada se verá afectada en el desarrollo de la misma.

1.5 FORMULACIÓN DEL PROBLEMA

¿Cómo los intrusos pueden penetrar la seguridad de las redes de datos pertenecientes a PYMES?

1.6 OBJETIVOS

1.6.1 Objetivo general

Disminuir el nivel de penetración de intrusos en las redes PYMES en San Juan de Pasto, a través de un sistema de defensa para mejorar la seguridad.

1.6.2 Objetivos específicos

- Analizar los niveles de seguridad y los tipos de ataques que se presentan en las PYMES.

- Desarrollar un sistema de aislamiento que permita la caracterización de los ataques y mejorar la seguridad de la red.

- Evaluar el sistema de detección de ataques en PYMES para determinar su eficiencia en cuanto a seguridad de la información.

1.7 JUSTIFICACIÓN

La seguridad informática se ha convertido en uno de los pilares fundamentales en la lucha de la protección de la información. Según el estudio denominado, informe tendencias del cibercrimen primer trimestre 2020, el cual está respaldado por la Policía Nacional de Colombia, la Dirección de investigación criminal e interpol (DIJIN), la Cámara colombiana de informática y telecomunicaciones (CCIT), el tanque de análisis y creatividad de las TIC (TicTac) y su programa de seguridad aplicada para el fortalecimiento empresarial (SAFE) "concluye que en el primer trimestre del año 2020, se presentaron 6.082 ataques cibernéticos, es decir un incremento del 8% con respecto al año 2019. Sin embargo, con la nueva forma de trabajo que se adoptó debido a la pandemia el incremento de ciberataques fue de un 37%. Otra estadística del estudio es que el 65.5% aun no implementan medidas de seguridad para la protección de su información, como también el 63% no hacen uso de herramientas de gestión de riesgos que les ayude a cuidar los datos personales"[3].

Este proyecto se desarrolla con el fin de detectar los ataques, implementando un sistema que mejorar la seguridad de las PYMES. Además, este sistema refuerza la confidencialidad, integridad de los datos y mantiene la disponibilidad de los servicios que presten las PYMES.

Con lo cual, se considera implementar un sistema de detección de intrusos, adicional a esto el sistema facilitara la configuración y la administración haciéndolo más amigable y accesible para la implementación en las PYMES.

1.8 VIABILIDAD

1.8.1 Viabilidad operativa

El presente proyecto de investigación es viable operativamente ya que cuenta con los recursos humanos y recursos físicos necesarios para poder cumplir con el proyecto de investigación el cual será realizado bajo los conocimientos de los estudiantes Yehison Hammer España Montaño y Anderson David Solarte Caicedo pertenecientes al programa de ingeniería de sistemas de séptimo semestre de la jornada nocturna, quienes tendrán la asesoría del Mg Arturo Eraso docente tiempo completo del programa de ingeniería de sistemas de la Universidad CESMAG.

1.8.2 Viabilidad técnica

Con el fin de llevar a cabo el proyecto de investigación es necesario tener en cuenta los siguientes recursos:

[3] ESTUDIO, Informe Tendencias del Cibercrimen Primer Trimestre 2020

- A nivel de software se utilizará un sistema operativo libre (Kali Linux), además se utilizará herramientas de uso libre como SNORT.

- En cuanto a Hardware será necesario dos computadoras una con un procesador AMD Ryzen 5 3500u, memoria ram 16Gb y disco duro de 1tb + 128 gb SSD, otra con un procesador Intel Core i5, memoria ram de 8gb y disco duro de 1tb

- Computador de escritorio con procesador Core i7 de cuarta generación, memoria ram 12gb y disco duro de 500gb.

1.8.3 Viabilidad económica

Para la realización de este proyecto de investigación denominado “SISTEMA DE DETECCIÓN DE INTRUSOS APLICADA A REDES DE PYMES” los estudiantes Yehison Hammer España Montaño y Anderson David Solarte Caicedo, seran los encargados de asumir los costos econónmicos, teniendo en cuenta los recursos humanos, recursos físicos, recursos de software y servicio de internet, que se requieran para la realización del proyecto.

1.9 DELIMITACIÓN

El presente proyecto de investigación se desarrollará durante 9 meses en el departamento de Nariño, en la ciudad de San Juan de Pasto. El cual será implementado en un ambiente virtual en el que se realizaran pruebas que llevaran a la detección de intrusos y garantizar el fácil manejo del sistema.

2. MARCO TEÓRICO

2.1 ANTECEDENTES

2.1.1 Antecedentes Internacionales

A nivel internacional se han realizado varios estudios entre estos se encuentra a Antonio Inoguchi y Erika Macha [4] quienes, con su proyecto titulado **Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú. 2016,** con el que pretenden fomentar una cultura de prevención y detección de riesgos cibernéticos en las PYMES del Perú, concientizar sobre el peligro que representa no estar preparado para los diferentes ataques cibernéticos que existen actualmente y elaborar planes de acción y estrategias basadas en minimizar los riesgos. Este proyecto aporta con información para elaborar planes de acción y estrategias para minimizar los riesgos.

Otro proyecto relacionado es el Javier De la Rosa[5] titulado **Ciberseguridad para PYMES. 2019,** en la ciudad de Valladolid, en donde se quiere exponer el concepto de ciberseguridad de un modo que sea comprensible, también expone las diferentes vulnerabilidades a las que se puede estar expuesto, y muestran algunas herramientas de software libre a las cuales pueden acceder las PYMES, con el fin de tener unos altos estándares de seguridad. Este proyecto aporta información sobre algunos de los riesgos que pueden estar expuestas las PYMES.

En el proyecto de Adán Hernández[6] titulado, **Implementación de un sistema de detección de intrusos basado en la herramienta SNORT. 2018,** en el cual por medio de la herramienta SNORT y con conocimientos previos de Seguridad Informática, se enfoca en conocer los tipos de ataques y su funcionamiento, con el fin de configurar el sistema de detección de intrusos, en conjunto de varias herramientas como son SNORT, Snorby, Barnyard2, las cuales garantizan un sistema más confiable y con menores probabilidades de ser vulnerado. El aporte de este proyecto es la utilización de Herramientas por medio de las cuales se puede conocer los tipos de ataques, mejorando las posibilidades de NO ser vulnerado.

[4] INOGUCHI, Antonio y MACHA, Erika. Gestión de la Ciberseguridad y Prevención de los Ataques Cibernéticos en las PYMES del Perú. 2016
[5] DE LA ROSA, Javier. Ciberseguridad para PYMES. 2019
[6] HERNANDEZ, Adan. Implementación de un Sistemas de Detección de Intrusos Basado en la Herramienta SNORT. 2018

2.1.2 Antecedentes Nacionales

A nivel nacional se han desarrollado proyectos como Blanca Rosety[7], con su proyecto titulado **Diseño de prototipo de defensa para mitigación de ataques DDoS para PYMES. 2016,** este proyecto fue presentado en la ciudad de Cartagena. Pretende mejorar la seguridad de la información en las PYMES por medio de software libre, el cual se implementará y se configurará de acuerdo a los resultados de las pruebas realizadas, dejando abierta la posibilidad de continuar con un estudio posterior, poder mejorar y ampliar los repositorios. Este proyecto aporta conocimientos del uso de software libre y como se puede mejorar la seguridad de la información en las PYMES.

Otro proyecto es el de Iván Flores y Jesús Quintana[8] S**istema de detección de ataques informáticos a redes de datos empresariales soportado en Honeypots. 2018,** en este proyecto se utiliza el principio por la cual fueron creados los Honeypots expresando la frase "CONOCE A TU ENEMIGO", ya que, al identificarlo, estudiarlo conocer los servicios que más ataca, o los más vulnerables, es posible tomar medidas que permitan mitigar en cierto modo las vulnerabilidades existentes en cualquier entorno de red. Todo esto con el fin de apoyar la labor de los administradores de infraestructura de las Tecnologías de la Información en la identificación de amenazas a la seguridad del sistema. Este proyecto enseña a conocer los tipos de vulnerabilidades que pueden tener las PYMES con el fin de mejorar la seguridad en estos puntos críticos.

En este proyecto es de Yamith Niño[9] el cual fue realizado en la ciudad de Bogotá, bajo el nombre de, **Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo pymes. 2015,** el objetivo de esta investigación es analizar la necesidad de implementar el concepto de ciberseguridad organizacional en las Pymes, como componente para garantizar su normal funcionamiento. Esto debe ser motivo de reflexión colectiva dentro del contexto de las PYMES, porque la situación de vulnerabilidad en la que se encuentra la infraestructura en Colombia con respecto a los ataques cibernéticos, constituye amenazas a sus propios bienes, los cuales afectan de una u otra manera la seguridad de las mismas. Este proyecto proporciona un aprendizaje del concepto de ciberseguridad organizacional en las PYMES.

[7] ROSETY, Blanca. Diseño de Prototipo de defensa para mitigación de ataques DDoS para PYMES. 2016

[8] FLOREZ, Iván y QUINTANA, Jesús. Sistema de Detección de Ataques Informáticos a Redes de Datos Empresariales Soportado en Honeypots. 2018

[9] NIÑO Yamith, Importancia De La Implementación Del Concepto De Ciberseguridad Organizacional En Las Organizaciones Tipo Pymes. 2015

2.1.3 Antecedentes Regionales

A nivel regional se encontraron algunos estudios relacionados con diseños de Sistemas de Gestión de la Seguridad Informática como el de Alba Córdoba[10] **Diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de Pasto bajo la norma ISO/IEC 27001. 2015,** en el cual su objetivo fundamental es de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática, y con base en estas vulnerabilidades definir las políticas y controles de seguridad que se deben seguir, todo esto aplicando el modelo PHVA (Planificar, Hacer, Verificar y Actuar). Con este proyecto se puede precisar las políticas y controles de seguridad que se deben seguir en un área definida.

Otro proyecto es el de Yesid Guerrero[11] **Diseño del sistema de gestión de seguridad de la información para la unidad de informática, ingeniería de sistemas y telemática de la universidad de Nariño soportada en los estándares MAGERIT e ISO/IEC 27001 y 27002/2013. 2020** con el fin de mejorar la gestión de la seguridad de la información en la unidad de Informática y Telecomunicaciones de la Universidad de Nariño, se diseña el SGSI con el cual se planea mejorar los niveles de acceso a la información y mejorar los controles de usuarios del sistema, todo esto soportado bajo la norma ISO 27001 e ISO 27002/2013. En este proyecto aporta información, conocimiento y unas bases de cómo aplicar las normas internacionales.

En este proyecto realizado por Carlos Pulido[12] **Diseño de un sistema de gestión de seguridad de la información para las áreas administrativa y académica de la institución system plus Pasto Ltda., basado en el estándar internacional ISO/IEC 27001:2013. 2015.** En el desarrollo de este proyecto se pretende diseñar e implementar medidas de seguridad en la Institución system plus pasto Ltda., y más específicamente las áreas Administrativa y Académica de la Institución, para tratar de ofrecer una adecuada protección a los activos de información, los cuales se ven expuestos a una gran cantidad de amenazas y vulnerabilidades que ponen en riesgo la disponibilidad, integridad y confidencialidad de la información, buscando alcanzar un nivel aceptable de los riesgos que actualmente se presentan y que se espera sea un modelo a seguir para todos los miembros de la Institución. Este proyecto contribuye con la importancia de la implementación de las normas internacionales

[10] CORDOBA, Alba. Diseño e Implementación de un SGSI Para el Área de Informática de la Curaduría Urbana Segunda de Pasto Bajo la Norma ISO/IEC 27001. 2015

[11] GUERRERO, Yesid. Diseño del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño Soportada en los Estándares MAGERIT e ISO/IEC 27001 y 27002/2013. 2020

[12] PULIDO Carlos, Diseño de Un Sistema de Gestión de Seguridad de la Información Para Las Áreas Administrativa Y Académica De La Institución System Plus Pasto Ltda., Basado En El Estándar Internacional ISO/IEC 27001:2013. 2015

2.2 SUPUESTOS TEÓRICOS DE LA INVESTIGACIÓN

2.2.1 Modelo OSI

El Open Systems Interconnection Model, conocido como modelo OSI por su abreviatura, fue creado por la Organización Internacional para la Normalización (ISO) como modelo de referencia para el establecimiento de una comunicación abierta en diferentes sistemas técnicos[13].

- **Capas OSI**

  Es considerada como el proceso que desarrolla diversas actividades en las cuales debe cumplir cierto tipo de requisitos, rigiéndose por el cuidado de la seguridad informática basada en la disponibilidad, confidencialidad y disponibilidad de la información, por tanto, se ha llegado a la necesidad de redistribuir las denominas capas de red y transporte

  Como dice Tolosa "cada una de ellas está orientada a una tarea diferente, por lo que los estándares solo cubren una parte del modelo de capas"[14].

- **Capa 7**

  Capa de aplicación: En este proceso de la capa 7 del modelo OSI es el encargado de recepcionar las entradas y salidas de datos recibidos de diversos flujos de la red tales como aplicativos interactivos entre otros, esta capa proporciona conectividad con los demás niveles del protocolo OSI preparando consigo todo tipo de procesamiento de función y aplicación y dándole uso a la transmisión de los datos a la capa de aplicación "Este proceso se puede explicar mediante el **ejemplo de la transmisión por correo electrónico**: un usuario escribe un mensaje en el programa de correo electrónico en su terminal y la capa de aplicación lo acepta en forma de paquete de datos. A los datos del correo electrónico se le adjuntan datos adicionales en forma de encabezado de la aplicación: a esto se le llama también "encapsulamiento". Este encabezado indica, entre otras cosas, que los datos proceden de un programa de correo electrónico. Aquí también se define el protocolo que se usa en la transmisión del correo electrónico en la capa de aplicación (normalmente el protocolo SMTP)"[15].

---

[13] Digital Guide IONOS, "¿Qué es el modelo OSI?" {En línea}. {25 03 2020} disponible en https://www.ionos.es/digitalguide/servidores/know-how/el-modelo-osi-un-referente-para-normas-y-protocolos/

[14] TOLOSA, Gabriel, Protocolos y Modelos OSI, disponible en https://sistemamid.com/panel/uploads/biblioteca/2017-08-04_09-52-51141670.pdf

[15] Digital Guide IONOS, "¿Qué es el modelo OSI?" {En línea}. {25 03 2020} disponible en https://www.ionos.es/digitalguide/servidores/know-how/el-modelo-osi-un-referente-para-normas-y-protocolos/

- **Capa 6**

Capa de presentación: es la encargada de garantizar la codificación de los datos enviados en un formato estándar, esto con el fin de que puedan ser comprendidos tanto como el emisor, como por el receptor, además esta capa cuenta con servicios de transformación de datos, de este modo garantiza él envió de datos en formatos estándares[16].

- **Capa 5**

Capa de sesión: se encarga de controlar el intercambio de datos, también proporciona los mecanismos necesarios para que la comunicación entre el emisor y el receptor se lleve a cabo sin interrupción gestionando su mantenimiento[17].

- **Capa 4**

Capa de transporte: Es la encargada de establecer, mantener y garantizar la conexión lógica entre los hosts, además puede realizar verificaciones a medida que se reciben los paquetes[18].

- **Capa 3**

Capa de red: Se encarga del enrutamiento del paquete a una dirección lógica, también puede fragmentar y volver a ensamblar los paquetes si así lo necesita, esta puede mover los paquetes desde el emisor hacia el receptor y a través de redes si es necesario[19].

- **Capa 2**

Capa de vínculo de datos: es la encargada de preparar los datos para la entrega final hacia la capa física, esto lo hace asignando un encabezado a cada una de las piezas con el fin de identificar errores y evitarlos al momento de la transferencia[20].

---

[16] ROMERO TERNERO, María del Carmen, BENJUMEA MONDEJAR, Jaime, El modelo de referencia OSI (ISO 7498) Arquitecturas y modelos de referencia {En línea}.{20 octubre de 2020} disponible en http://itisolaris.upaep.mx/electronica/docs/telemetria/ModeloOSI.pdf

[17] Ibid., p. 25

[18] BLANK, Andrew G, TCP/IP Foundations, John Wiley & Sons 20/02/2006 304P.

[19] Ibid., p. 21

[20] MARIN MORENO, William, Modelo OSI {En línea}. {25 octubre de 2020} disponible en http://www.academia.edu/download/35756801/01_modelo_OSI_v2.pdf

- **Capa 1**

  Capa física: esta capa es la encargada de convertir los bits en señales, que viajan a través de los elementos físicos como son cables, tarjetas de red y demás componentes hasta llegar a su destinatario[21].

2.2.2 Modelo TCP/IP

Para poder comprender los sistemas de comunicación es de vital importancia conocer la estructura de los modelos TCP/IP OSI, de este modo conocer las funcionalidades de cada capa y sus protocolos, los cuales permiten la conexión de los terminales y aplicaciones a través de internet o una red privada.[22]

TCP/IP integra funciones de la capa de presentación y sesión en una sola capa de aplicación, lo cual lo hace más simple al unificar en una sola capa, aunque normalmente las redes utilizan el modelo OSI como una guía[23].

2.2.3 Capas Modelo TCP/IP

- **Aplicación**

  Esta capa es la encargada de gestionar las comunicaciones, a través de los protocolos HTTP, SMTP, Telnet, entre otros[24].

- **Transporte**

  En esta capa se puede encontrar dos protocolos como son el TCP y UDP, los cuales cumplen la función de brindar una conexión estable y confiable y que garantizan la transferencia de datos entre equipos[25].

---

[21] Ibid., p. 18

[22] ESTRADA CORONA, Adrián, Protocolos TCP/IP de Internet, Revista Digital Universitaria, 2004, Disponible en: http://www.ru.tic.unam.mx/bitstream/handle/123456789/791/220.pdf?sequence=1&isAllowed=y

[23] COMER, Douglas, Libro, Interligacao de Redes com TCP/IP: Principios, Protocolos e Arquitectura, Volumen1, Editorial Elsevier Brasil, 2016

[24] PELÁEZ SILES, Raúl, Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados, Análisis de seguridad de TCP/IP Edición 1 junio 2002 {En línea} Disponible en: http://ftp.nluug.nl/ftp/pub/os/Linux/doc/LuCaS/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf

[25] Ibid., p. 18

- **Internet**

  Esta capa es la encargada de conducir y guiar a los paquetes para que estos puedan llegar a su destino sin ningún tipo de retraso[26].

- **Red**

  Se encarga del enrutamiento, de los paquetes por las diferentes rutas hasta llegar a su destino [27].

- **Físico**

  Se encarga de conectar los hosts a la red por medio de algún protocolo el cual permita enviar y recibir paquetes IP [28].

2.2.4 Protocolos de comunicación

Un protocolo es un conjunto de normas estandarizadas por medio de las cuales las máquinas y los programas pueden intercambiar información. Para garantizar la comunicación entre el emisor y el receptor ambos deben manejar el mismo protocolo, esto con el fin de que la información puede viajar sin ningún inconveniente[29].

"La Internet es vista como un medio para enviar y acumular información, una mega red, una red de redes o una red global de redes de computadoras, pero también es un conjunto de tecnologías que ha originado un nivel de comunicación y un acceso a la información sin antecedente alguno en la historia de la humanidad" [30].

2.2.5 Seguridad informática

Según Álvaro Gómez, en su libro, Enciclopedia de la seguridad informática afirma que "Podemos definir la Seguridad Informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su

[26] FERNÁNDEZ BARCELL, Manuel, Protocolo TCP/IIP, Grado en gestión y administración pública, Redes de datos, Departamento de Ingeniería Informática, Facultad de Ciencias sociales y de la comunicación, Universidad de Cádiz. {En línea}. Disponible en: https://rodin.uca.es/xmlui/bitstream/handle/10498/16833/temaIII_tcpip.pdf
[27] PELÁEZ SILES, Raúl. Op. Cit., p.12
[28] Ibid., p. 3.
[29] ESTRADA CORONA, Adrián, Protocolos TCP/IP de Internet, Revista Digital Universitaria, Volumen 5, 10 de septiembre de 2004, Disponible en: http://www.ru.tic.unam.mx/bitstream/handle/123456789/791/220.pdf?sequence=1&isAllowed=y
[30] Ibid., p. 2.

confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios no autorizados al sistema" [31].

La seguridad informática comprende una serie de medidas de seguridad como son, programas de software antivirus, firewalls y otras medidas que dependen del usuario, el uso correcto de los recursos de la red, cuidar el uso de las computadoras, y activación y desactivación de funciones de software determinado.

La seguridad informática se enfoca cubrir unas áreas específicas, esto con el único fin de garantizar la seguridad y buen manejo de la información:

- **Integridad**

  Este principio garantiza la autenticidad y precisión de la información, sin importar el momento en la que esta se solicita, comprobando que los datos no han sido alterados o destruidos de modo no autorizado[32].

- **Confidencialidad**

  Según Ángel Ortiz en su artículo sobre los pilares de la seguridad informática afirma que "Garantizar la confidencialidad significa que la información está organizada en términos de quién necesita tener acceso, así como la sensibilidad de los datos. Una violación de la confidencialidad puede tener lugar a través de diferentes medios, por ejemplo, piratería o ingeniería social." [33].

- **Disponibilidad**

  Este componente de la seguridad informática se encarga de garantizar el acceso a la información para los usuarios autorizados, en el momento que sea necesario, de esta manera se garantiza que usuarios sin autorización puedan tener acceso a información sensible[34].

2.2.6 Tipos de seguridad

En este punto se tratará algunos de los tipos de seguridad informática, los cuales desde el punto de vista de la investigación son los más críticos para garantizar un buen nivel de seguridad en las PYMES.

---

[31] GOMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática 2da Edición. 2017
[32] Ibid., p. 50.
[33] ORTIZ, Ángel Eulises, ¿Cuáles son los tres pilares de la seguridad informática?, Seguridad Web, HostDimeBlog Premier Global Data Centers {En línea}, {14 de julio 2020} Disponible en: https://www.hostdime.com.pe/blog/cuales-son-los-tres-pilares-de-la-seguridad-informatica/
[34] JUÁREZ, Jaime, Seguridad Informática, Principios de Seguridad Informática {En línea}, {11 de enero 2021} Disponible en: https://sites.google.com/site/seguridadinformatica052015/principios-de-seguridad-informatica.

- **Seguridad de Hardware**

La seguridad informática de hardware se encarga de velar por todos los equipos físicos que se encuentran en una PYME, así de este modo se puede incluir a los firewalls, servidores y demás dispositivos que se encuentren conectados a la red y puedan ser vulnerables tanto como a un evento catastrófico o a un ataque [35].

- **Seguridad de Software**

En cuanto a seguridad en software se trata tenemos que tener en cuenta varios aspectos como son corrección de errores, proteger nuestros equipos de software maligno, mantener actualizado el software, esto con el fin de corregir posibles errores [36].

- **Seguridad de Red**

Es de vital importancia proteger las redes ante algún tipo de ataque ya que es por medio de estas en donde circula toda la información de nuestra PYME, también es importante entender que existen diversas modalidades de infección y ataque que puedan sufrir nuestras redes, por este motivo también debemos tener varias soluciones que puedan proteger nuestra red, algunas de las cuales pueden ser, Antivirus y antispyware, cortafuegos, se encarga de bloquear los accesos no autorizados a la red, VPN para garantizar un acceso remoto seguro, IPS ayuda a identificar las amenazas de rápida propagación[37].

2.2.7 Seguridad ofensiva

Según un artículo publicado por Auditech, una empresa reconocida por prestar servicios Consultorías, ciberseguridad y derecho tecnológico nos dice que “la mejor defensa es un buen ataque”, considerando estas palabras consideramos que la seguridad Ofensiva hace uso de herramientas, técnicas y metodologías las cuales también pueden ser utilizadas por un cibercriminal, esto con el fin de detectar vulnerabilidades antes de que los cibercriminales las encuentren y en caso de sufrir un ataque poder tener un plan de contingencia[38].

---

[35] UNIVERSIDAD Internacional de Valencia, Ciencia y Tecnología, Tres tipos de seguridad informática que debes conocer, {En línea} {28 de diciembre 2020} Disponible en: https://www.universidadviu.com/int/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer

[36] Tecno Mental, Seguridad Informática, Tipos de seguridad informática, {En línea}, {5 de Enero 2021} Disponible en: https://www.tecnomental.com/seguridad-informatica/tipos-de-seguridad-informatica/

[37] Universidad Internacional de Valencia. Op. Cit., p.1

[38] AUDITECH, Seguridad Ofensiva, {En línea} {14 de noviembre 2020} disponible en https://auditech.es/seguridad-ofensiva/#:~:text=La%20Seguridad%20Ofensiva%2C%20toma%20como,previas%20a%20un%20ciberataque%20real

2.2.8 Seguridad defensiva

La seguridad defensiva se basa en la Configuración de interfaces, usuarios, servicios, enrutamientos y políticas de seguridad en la empresa para tener el máximo control de lo que ocurre en la red y tomar las medidas necesarias ante posibles ataques[39].

2.2.9 Análisis forense

El análisis forense utiliza una serie de herramientas y técnicas por medio de las cuales se puede buscar, identificar y reconstruir información de algún equipo afectado, esto con el fin de que sean validados en un proceso legal, también permite analizar las consecuencias producidas en el ataque o suceso que produjo un daño a la información almacenada en los equipos tecnológicos, además de poder identificar al posible autor de ese ataque[40].

2.2.10 Ataque

Un ataque informático consiste en que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, ya sea el caso de un host, una red privada o un servidor, lo cual tendrá como consecuencia perdida de información y/o pérdidas económicas en alguna organización[41].

2.2.11 Tipos de ataques

En la actualidad existe gran variedad de ataques que pueden afectar a las PYMES, por este motivo se da a conocer los tipos de ataques que son usados con más frecuencia:

[39] AUDITECH, Seguridad Defensiva, {En línea},{14 de noviembre 2020} disponible en: https://auditech.es/seguridad-defensiva/

[40] GERVILLA RIVAS, Carles, Metodología para un análisis forense, Trabajo de Final de Máster, Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones(MISTIC), Universitat Oberta de Catalunya INCIBE (Instituto Nacional de Ciberseguridad) (INTECO) {En línea} {5 de enero 2021} Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

[41] MEDINA ROJAS, Jhonatan Deyvi, RIVAS MONTALVO, Yonathan Yajanovic, Evaluacion delRendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos, 2019, {En línea} {16 de noviembre 2020} Disponible en http://repositorio.unprg.edu.pe/handle/UNPRG/8074

- **Ataques pasivos**

Este tipo de ataques es conocido por que el atacante tiene una forma particular en la cual no se ve alterada la comunicación, y solo está monitorizando a la víctima, esto con el fin de obtener la información que está siendo transmitida.[42]

  - **Sniffing**

    En el tipo de ataque de Sniffing el cual consiste en la captura de paquetes que están transitando por la red, esto con el fin de poder obtener datos como son la direcciones MAC, direcciones IP, direcciones de email, usuarios y contraseñas entre otros tipos de información que transita por la red.[43]

  - **Análisis de trafico**

    Este tipo de ataque se centra en la obtención de la mayor cantidad de información de la red de una víctima, algunos de los resultados que se puede obtener con este tipo de ataque son: a qué hora se inician o prenden algunos dispositivos, a qué hora hay más tráfico en la red, todo el tráfico que se envía a través de la red entre otras más.[44]

- **Ataques activos**

  - **Suplantación**

    En este tipo de ataque se puede hacer pasar por un dispositivo que si se encuentra correctamente autentificado en la red y así poder recibir paquetes que fueron enviados a ese destino[45].

[42] Ibid., p. 29.
[43] GOMEZ VIEITES, Álvaro, Tipos de ataques e intrusos en las redes informáticas, Resumen de la ponencia. {En línea} {6 de enero de 2021} Disponible en: https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf
[44] Ibid., p. 50.
[45] ASTUDIILLO PIZARRO, Luis Alberto, Análisis de vulnerabilidades de suplantación en el protocolo TCP/IP e implementación de controles de mitigación, Unidad Académica de Ingeniería Civil, Universidad Técnica de Machala, {En línea} {6 de enero de 2021} Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/12569/1/E-9449_ASTUDILLO%20PIZARRO%20LUIS%20ALBERTO.pdf

- **Modificación**

  Según Álvaro Gómez en este tipo de ataque se compromete el contenido de los paquetes, en el cual se modifican y reenviar sin que el usuario se entere de las alteraciones que se les realizaron a los paquetes[46].

- **DoS**

Este tipo de ataque DoS conocido como Denegación de Servicios, consiste en aumentar el consumo del ancho de banda de una red o sobrecargar los recursos que tiene disponible un servidor o un sistema, esto con el fin de dejarlo fuera de línea o inaccesible a sus usuarios[47].

- **Ataque AP Spoofing**

En el tipo de ataque AP, el atacante copia la configuración legitima de redes cercanas esto con el fin de engañar a clientes cercanos y poder obtener la información de estos usuarios[48].

- **Mac Spoofing**

Este tipo de ataques el atacante oculta la dirección MAC original, y la remplaza con una legítima que se encuentra en la misma red, esto con el fin de no ser detectado[49].

2.2.12 Riesgos

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información combatiendo la probabilidad de que un evento nocivo ocurra y con ello activar impacto que perjudique la organización[50].

---

[46] GOMEZ VIEITES, Álvaro. Op. Cit., p.1

[47] AVALOS, Héctor, GÓMEZ, Esteban, Seguridad de la información, generación y mitigación de un ataque de denegación de servicios, Instituto de informática y computación, Universidad Tecnológica Equinoccial. {En línea} Disponible en http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/425/292

[48] CALLES, Juan Antonio, Wi-Fis: Tipos de ataque y recomendaciones de seguridad, Fujoproject, Artículo, {En línea}. {6 de enero 2020} Disponible en: https://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html

[49] DIGITAL GUIDE IONOS, MAC Spoofing: qué es y cuándo se utiliza, {En línea}. {6 de enero 2021}. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-mac-spoofing/

[50] QUIROZ Silvia, MACIAS David. Seguridad informática: condiciones Articulo {En línea}, Publicado [26 agosto 2017], p. 25. Disponible en internet: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

El riesgo de seguridad digital es denominado también como “una combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas"[51].

En el análisis de riesgos se infiere a que “el riesgo se define como la posibilidad de que no se obtengan los resultados deseados, en informática, las empresas nunca desean sufren un ataque externo o interno a sus sistemas de información, por tanto, la empresa siempre será uno de los principales focos para sufrir un ataque cibernético lo cual puede provocar daño en su sistema de información”[52].

2.2.13 Vulnerabilidades

> Constituye un hecho o una actividad que permite concretar una amenaza, se es vulnerable en la medida en que no hay suficiente protección para evitar que llegue a suceder una amenaza, teniendo en cuenta que en la actualidad se determina a las amenazas como intencionadas y no intencionados, cuando existe una vulnerabilidad en la seguridad de una PYME, por lo generar es por qué hay problemas de diseño en la implementación del sistema. La primera amenaza es en que los diseñadores del sistema no puedan proveer y no ser vulnerados por las amenazas que pueden existir en el futuro, otra posible consecuencia de vulnerabilidad es el mal diseño del protocolo[53].

---

[51] COSTAIN Sylvia y ROSO Carlos, Ministerio de las Tecnologías de la Información y las Comunicaciones Articulo {En línea}, Bogotá D.C publicado {octubre 2018}, p. 2, Disponible en internet: https://www.mincit.gov.co/temas-interes/documentos/guia-para-la-administracion-del-riesgo-y-el-diseno.aspx

[52] BACA Gabriel. Introducción a la seguridad informática Libro [EN LINEA], Primera edición MEXICO, Publicado [2016], p, 23. Disponible en internet: https://books.google.com.co/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=que+es+vulnerabilidad+informatica&ots=0XLu2AtgDs&sig=j9zKGlKwJI7-kF4X-mv_Sdy3G0U&redir_esc=y#v=onepage&q&f=false

[53] BACA Gabriel. Introducción a la seguridad informática LIBRO [EN LINEA], Primera edición MEXICO, Publicado [2016], p, 31. Disponible en internet: https://books.google.com.co/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=que+es+vulnerabilidad+informatica&ots=0XLu2AtgDs&sig=j9zKGlKwJI7-kF4X-mv_Sdy3G0U&redir_esc=y#v=onepage&q&f=false

2.2.14 Amenazas

Las amenazas son consideradas alertas de detección, por tanto “una amenaza se refiere a un incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o su empresa en general. Una amenaza es un evento hipotético en el que un atacante usa la vulnerabilidad”[54].

> Las amenazas cibernéticas a veces se confunden incorrectamente con vulnerabilidades. Mirando las definiciones, la palabra clave es “potencial”. La amenaza no es un problema de seguridad que existe en una implementación u organización. En cambio, es algo que puede violar la seguridad. Esto se puede comparar con una vulnerabilidad que es una debilidad real que se puede explotar. La amenaza siempre existe, independientemente de cualquier contramedida. Sin embargo, se pueden utilizar contramedidas para minimizar la probabilidad de que se realice[55].
>
> Las amenazas son un factor de riesgo externo de un sujeto o sistema, representado por un peligro latente asociado con un fenómeno físico de origen natural o tecnológico que puede presentarse en un sitio especifico y en un tiempo determinado produciendo efectos adversos en las personas, los bienes y/o el medio ambiente, matemáticamente expresado como la probabilidad de envere un nivel de ocurrencia de un evento con una cierta intensidad en un cierto sitio y en vierto periodo de tiempo. Técnicamente, se expresa como la probabilidad de exceder un nivel de ocurrencia de un evento con un nivel de severidad, en un sitio específico y durante un periodo de tiempo[56].

2.2.15 Firewalls

Conocidos como “cortafuegos (FIREWALLS), Es un sistema empleado para proteger una de del resto de las demás redes, este es una puerta que controla la entrada y salida de paquetes considerado un guardián el cual decide que deja pasar y que no, su actividad es monitoreada y realizada por el bloqueo de puertos”[57].

---

[54] ORTIZ Ángel. Amenaza informática ¿Qué es? ¿Cómo contenerla? Articulo [Online], Publicado [13 julio 2020], p. 1, Disponible en internet: https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/

[55] Ibid., p. 1

[56] CARDONA Omar. Evaluación de la amenaza, la vulnerabilidad y el riesgo. Articulo [Online], Publicado [2020], p. 1, Disponible en internet: https://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

[57] MONTAÑO Erika, Evaluación de las vulnerabilidades que presentan los firewalls en la empresa datasolution s.a. Tesis [En línea], Ecuador-Guayaquil: , Universidad De Guayaquil, Publicado [2011], p. 45. Disponible en internet: http://repositorio.ug.edu.ec/bitstream/redug/6743/1/Tesis%20Completa%20-342-2011.pdf

> Los firewalls son dispositivos que buscan proteger la información, por lo que son una de las herramientas principales de seguridad informática. Las organizaciones mantienen un flujo constante de información con su entorno y a través de este flujo puede entrar en riesgo el propio negocio por diversas amenazas, tanto internas (fuga de información) como externas (suplantación, estafas, malware). Estas amenazas están en constante evolución, por lo que el firewall (principal mecanismo de defensa y protección en el flujo de información) también debe adaptarse a las cambiantes condiciones del entorno. Esto hace que el firewall tradicional evolucione a través de retos como el descifrado e inspección de SSL, IPS con tecnología anti evasión, el control de aplicaciones basado en contexto y la protección contra malware basada en red. Estos retos han creado un nuevo mercado, donde los proveedores se diversifican y compiten para satisfacer las necesidades de sus clientes[58].

Se dice que "este mecanismo de seguridad continúa siendo altamente utilizado en el entorno corporativo. Según un estudio de seguridad informática en Latinoamérica, el 76% de los ejecutivos de 14 países de esta región cuentan con una solución de este tipo; lo que ubica al firewall en el segundo lugar de los controles de seguridad más utilizados, después de los antivirus"[59].

2.2.16 Servidores

En los procesos informáticos "un servidor es un ordenador o equipo informático que se encarga de transmitir información a otros ordenadores que estén conectados a él. Además, esta transmisión de información también puede ser de ordenador a personas"[60].

> Los ordenadores son una herramienta fundamental en la sociedad de la información. Estamos rodeados de ordenadores y un gran número de las tareas que realizamos en nuestra vida cotidiana involucran a algún tipo de ordenador. Básicamente, un ordenador es una máquina que es capaz de transformar datos a través de un programa que tiene almacenado en la memoria. Siguen el mismo esquema desde su creación en los años 40, conocido como la arquitectura de Von Neumann, independientemente de la tecnología empleada o de su tamaño. En función de su potencia de cálculo, podemos encontrar desde los grandes mainframes a pequeños ordenadores de mano. Básicamente, encontramos dos grandes categorías: los ordenadores multi-usuario, que dan servicio a varios usuarios

[58] CORTES David, Firewalls de nueva generación: la seguridad informática vanguardista. Trabajo de grado [En línea], Colombia, Universidad Piloto De Colombia, publicado en [2016 09 06], p. 1. Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2719/Trabajo%20de%20grado3329.pdf?sequence=1&isAllowed=y

[59] Ibid., p. 3

[60] CABRERA Robert. ¿Qué es un servidor? Articulo [Online], España, Publicado [junio 27 2019], p. 1. Disponible en internet: https://desafiohosting.com/que-es-un-servidor/

simultáneamente, y las máquinas mono-usuario, pensadas como puestos de trabajo personales. La técnica de tiempo compartido es la que va a permitir a los sistemas multi-usuario atender adecuadamente a las tareas que cada uno de los usuarios lanza en el ordenador, de forma que cada uno de ellos tiene la ilusión de que la máquina le está atendiendo de forma exclusiva[61].

2.2.17 Tipos de servidores

Existen diferentes tipos de servidores, esto dependiendo de la información que se requiera transmitir, a continuación, se lista los servidores más comunes con una breve descripción de su función.

- **Servidor web**

  Un servidor web es un ordenador de gran potencia que se encarga de "prestar el servicio" de transmitir la información pedida por sus clientes, otros ordenadores, dispositivos móviles, impresoras, personas, etc. Los servidores web (web server) son un componente de los servidores que tienen como principal función almacenar, en web hosting, todos los archivos propios de una página web (imágenes, textos, videos, etc.) y transmitirlos a los usuarios a través de los navegadores mediante el protocolo HTTP, el rol principal de un servidor web es **almacenar y transmitir el contenido solicitado de un sitio web al navegador del usuario**, este proceso, para los internautas no dura más que un segundo, sin embargo, a nivel del web server es una secuencia más complicada de lo que parece, ara cumplir con sus funciones el servidor deberá tener la capacidad de estar siempre encendido para evitar interrumpir el servicio que le ofrece a sus clientes. Si dicho servidor falla o se apaga, los internautas tendrán problemas al ingresar al sitio web[62].

- **Servidor dedicado**

Existen variedad de servidores entré los que encontramos "este tipo de servidores, se caracterizan por recibir peticiones de un único cliente**,** Son servidores exclusivos y que, por tanto, suelen ofrecer mayor cantidad de almacenamiento. Este tipo de servidores son los que ofrecen algunas empresas de hosting para aquellos clientes que tienen una página web que requieren un volumen de transferencia de datos muy elevado"[63].

---

[61] REBOLLEDO Miguel, Definición y tipo de ordenadores. Articulo [Online], España: Universidad Politécnica De Valencia, Publicado [2011], p. 3. Disponible en internet: https://riunet.upv.es/handle/10251/10787

[62] DE SOUSA Iván, ¿Para qué sirve un servidor web y para qué sirve internet? Articulo [Online], Publicado [14 junio 2019], p. 1. Disponible en internet: https://rockcontent.com/es/blog/que-es-un-servidor/

[63] CABRERA Robert. ¿Qué es un servidor? Articulo [Online], España, Publicado [junio 27 2019], p. 1. Disponible en internet: https://desafiohosting.com/que-es-un-servidor/

- **Servidor compartido**

Por otra parte, encontramos el servidor compartido que sería “lo opuesto al servidor dedicado. Los servidores compartidos se encargan de recibir peticiones de muchos clientes. Por normal general, los clientes de este tipo de servidores son aquellos que no realizan muchas peticiones al servidor ya que, de no ser así, éste no sería lo suficiente rápido para adaptarse a las necesidades de todos sus clientes”[64].

- **Servidores de audio y video**

Este tipo de servidores es muy importante para la visualización de datos por tanto” el streaming es la transmisión de video o de audio en tiempo real, es decir, es la forma de ver o escuchar algún tipo de contenido multimedia (muchas veces en vivo) y sin la necesidad de descargar archivos de audio o de video a nuestro dispositivo o computadora”[65].

- **Servidor de correo electrónico**

> Un servidor de correo es una aplicación informática que permite gestionar el correo electrónico en un ordenador o computadora. Lo que para cualquier persona es el acto rutinario de acceder a una aplicación de un dispositivo, es un software cliente de correo o un webmail (como Gmail, en cualquier navegador web), redactar un mensaje, dar clic en “Enviar” y esperar la respuesta, es posible gracias al llamado Protocolo Simple de Transferencia de Correo (SMTP), Piensa en el servidor de correo como una “oficina postal virtual”. Su función es recibir las “cartas” (emails) de los usuarios, identificar al remitente y al destinatario (dirección email), asignarle la “ruta” correcta (servidor DNS, lo que está después del @), finalmente, elegir al “cartero” (protocolo del servidor de entrada, IMAP, POP3)[66].

- **Servidor FTP**

> En inglés, las siglas **FTP** significan “File Transfer Protocol”, que se traduciría como “Protocolo de Transferencia de Archivos”. El servicio FTP es un servicio utilizado para el envío y obtención de archivos entre dos equipos remotos. Los casos más usuales son transferencias entre el equipo local de un cliente y el servidor del proveedor, aunque también se pueden establecer conexiones FTP entre dos servidores. Los puertos típicos utilizados para conectarse al FTP son el 20 y el 21 para la gran mayoría de los casos, aunque en algunos proveedores esto puede variar. Por lo general se usan dos tipos de

[64] Ibid., p.1
[65] BORGES Santiago, Servidor de Streaming: ¿Qué es y cómo funciona? Articulo [Online], Publicado [21 mayo 2020], p. 1. Disponible en: https://blog.infranetworking.com/servidor-streaming/
[66] LARA GALICIA Fernando, Servidor de correo electrónico, ¿cómo funciona? Articulo [Online], Publicado [12 junio 2020], p. 1. Disponible en internet: https://co.godaddy.com/blog/servidor-de-correo-electronico-como-funciona/

transferencia: una es la ASCII y la otra es la de tipo Binario. La primera de estas solamente transfiere texto plano del tipo ASCII, como serían por ejemplo páginas HTML sin imágenes, mientras que la segunda clase se usa para transferir archivos como imágenes, audios, videos, etc.[67].

- **Servidor de impresión**

Son dispositivos muy útiles en las labores cotidianas sin embargo se dice que "un servidor de impresión puede ser una herramienta extremadamente útil en la oficina, ya que nos permitirá utilizar una impresora en forma remota, evitándonos la ardua tarea de transportar el archivo a imprimir en un pendrive o similar hacia la computadora que tiene la impresora conectada. Además, nos ahorra la necesidad de tener instalada la aplicación con que desarrollamos el trabajo en dicha PC"[68].

- **Servidor en la nube**

Por tanto, también están los "servidores de la nube es una potente infraestructura física o virtual que lleva a cabo el almacenamiento de procesamiento de aplicaciones e información. Los servidores en la nube se crean utilizando software de virtualización para dividir un servidor físico en varios servidores virtuales"[69]. Facilitando consigo el trabajo de las transiciones de los datos.

- **Servidor de base de datos**

Un servidor de base de datos, también conocido como database server o RDBMS (Relational DataBase Management Systems) en caso de bases de datos relacionales, es un tipo de software de servidor que permiten la organización de la información en el uso de tablas, índices y registros. A nivel de hardware, un servidor de base de datos es un equipo informático especializado en servir consultas a clientes remotos o locales que solicitan información o realizan modificaciones a los registros y tablas que existen dentro de las bases de datos del sistema (en muchos casos desde un servidor web o de aplicaciones)[70].

---

[67] BORGES Esteban, Servidor FTP, Articulo [Online], Publicado [12 febrero 2019], p. 1. Disponible en: https://blog.infranetworking.com/servidor-ftp/

[68] MARKER Graciela, Servidor de impresión ¿Qué es? ¿para que sirve?, Articulo [Online], Publicado [17 julio 2020], p. 1. Disponible en internet: https://www.tecnologia-informatica.com/servidor-impresion/

[69] HAZARD Kevin, IBM, Servidores en la nube, Articulo [Online], Publicado [2020], p. 1. Disponible en https://www.ibm.com/co-es/cloud/learn/what-is-a-cloud-server#:~:text=Un%20servidor%20de%20la%20nube,metal)%20en%20varios%20servidores%20virtuales.

[70] BORGES Esteban, Servidor base de datos, Articulo [Online], Publicado [17 marzo 2019], p. 1. Disponible en internet: https://blog.infranetworking.com/servidor-base-de-datos/

- **Clúster de servidores**

Por otro lado, “el clúster de servidores, es denominado un conjunto de diversos servidores que trabajan acoplados realizando como finalidad una única tarea, es decir una red de ordenadores que trabajan agrupados y se unen en redes de alta velocidad de tal forma que su resultado sea unificado. Alcanzando así un gran rango de ordenadores trabajando de manera sincronizada y llevando a cabo a poner en marcha múltiples portales en ejecución”[71].

- **Servidor Proxy**

Sin embargo, también encontramos “Los servidores proxy generalmente se usan como un puente entre el origen y el destino de una solicitud. En nuestra imagen, puedes ver que la computadora necesita pasar por el servidor proxy para acceder a Internet, y este es uno de los usos comunes de los servidores proxy”[72].

- **Servidor de archivos**

Uno de los más importantes servers es “El servidor de archivos ha venido siendo el modelo de gestión de documentos más implantado en las empresas. Ha cubierto la necesidad de disponer de un almacenamiento de ficheros centralizado al que los empleados pueden acceder para compartir carpetas y ficheros”[73].

- **Servidores DNS**

> DNS es el acrónimo de *Domain Name System* o **Sistema de Nombres de Dominio**, que es el método utilizado por Internet para traducir de forma fácil de recordar los nombres de dominio como *wpseguro.com* en lugar de su IP 178.33.117.45 de manera que sean entendibles por las personas y más fácil que si se trata de recordar secuencias numéricas, como es el caso de las IPs. Todo equipo o dispositivo conectado a Internet necesita de una dirección IP y que esta sea única de forma que pueda ser accesible desde cualquier punto de la red. Recordar números de IPs para acceder a sitios web es una tarea compleja que nos limitaría bastante la cantidad que podríamos memorizar, por este motivo los DNS nos ayudan a convertir estas secuencias numéricas

[71] RIBERA Op cit, p. 3

[72] CUNHA BARBOSA Daniel, Que es un servidor proxy y para sirve, Articulo [En línea], Publicado [enero 2 2020], p. 1. Disponible en internet: https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

[73] RUIZ Francisco, Servidor de archivos en la empresa, alternativas actuales, Articulo [Online] Publicado [20 noviembre 2019], p. 1. Disponible en internet: https://blog.dataprius.com/index.php/2019/11/20/servidor-de-archivos-en-la-empresa-alternativas-actuales/

en nombres entendibles, y en la mayoría de casos asociados a la marca, entidad, persona o servicio al que sirven[74].

2.2.18 Sistemas de detección de intrusos

Un IDS está definido como un sistema de seguridad que actúa para la protección de la infraestructura. Tecnologías de Información permite la gestión de acceso tanto internamente como externamente, permitiendo así la negación de peticiones o conexiones no autorizadas dentro del margen establecido en la implementación de un IDS. Existen definiciones similares en cuanto a IDS se menciona, la mayoría dando referencia a la virtud del acceso no autorizado a la infraestructura por parte de agentes externos, además de esto, existen definiciones como en el artículo que hacen referencia a la capacidad que poseen los IDS para monitorizar y analizar el flujo de datos de la infraestructura de red en la que se encuentre, es decir pueden verificar el tráfico de red conforme los ajustes o previas configuraciones que estos posean[75].

Un Sistema de Detección de Intrusos (IDS: *Intrusion Detection System*) es un componente dentro del modelo de seguridad informática de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas, desde el exterior o interior de un dispositivo o una infraestructura de red. el IDS se basa en la hipótesis de que el patrón de comportamiento de un intruso es diferente al de un usuario legítimo, lo que se emplea para su detección por análisis de estadísticas de uso. un modelo IDS intenta crear patrones de comportamiento de usuarios respecto al uso de programas, archivos y dispositivos, tanto a corto como a mediano y largo plazo, para hacer la detección efectiva; además, utiliza un sistema de reglas predefinidas (“firmas o signaturas”) para la representación de violaciones conocidas[76].

Existen diversos tipos de IDS tales como los que se mencionan a continuación.

- **IDS basados en Red**

  Uno de los IDS más comunes son los IDS basado en red (NIDS por sus siglas en inglés) usa sensores, los cuales están distribuidos por todos los hosts de la red. Cada uno de ellos posee su tarjeta de interfaz de red (NIC) en modo promiscuo, lo que permite que cada NIC vigila el tráfico que tiene la dirección

[74] MENDEZ Luis, Que es un servidor DNS y como solucionar problemas habituales Articulo [Online], Publicado [22 febrero 2019], p. 1. Disponible en internet: https://www.webempresa.com/blog/servidor-dns-como-solucionar-problemas-habituales.html

[75] PANTOJA Nelson, DONADO Siler y MARCELES Katerine, Selección de indicadores para la implementación de un IDS en PYMES. Libro [Online], Ecuador, 2020, p. 778,779. Disponible en internet: https://search.proquest.com/openview/ddddee94d23b4c4a6d43646933893d01/1?pq-origsite=gscholar&cbl=1006393

[76] INFOTECS, IDS Sistema de detección de intrusos, Articulo [Online], Publicado [12 marzo 2019], p. 1. Disponible en internet: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

de red de su host, su broadcast e incluso su multicast. Los NIC capturan todo el tráfico en modo promiscuo, hacen una copia de todos los paquetes, y pasan una copia al TCP sack y otra al analizador para buscar tipos específicos de patrones[77].

- **IDS basados en Host**

  Como también tenemos los IDS basados en host los cuales son denominados (NIDS por sus siglas en inglés) usa sensores, los cuales están distribuidos por todos los hosts de la red. Cada uno de ellos posee su tarjeta de interfaz de red (NIC) en modo promiscuo, lo que permite que cada NIC vigila el tráfico que tiene la dirección de red de su host, su broadcast e incluso su multicast. Los NIC capturan todo el tráfico en modo promiscuo, hacen una copia de todos los paquetes, y pasan una copia al TCP sack y otra al analizador para buscar tipos específicos de patrones[78.]

- **IDS basado en conocimiento**

Un IDS muy típico y de gran ayuda el cuál "hace referencia a una base de datos de perfiles de vulnerabilidades de sistemas ya conocidos para identificar intentos de intrusión activos. En este caso, es de suma importancia que la estructura tenga una política de actualización continua de la base de datos (firmas) para garantizar la continuidad de la seguridad del ambiente, teniendo en cuenta que lo que no se conoce, literalmente, no será protegido"[79].

- **IDS basado en comportamiento**

Se define "como activo, desde el momento en que se determina que bloqueará automáticamente ataques o actividades sospechosas que sean de su conocimiento, sin necesidad de intervención humana. Aunque potencialmente es un modelo extremadamente interesante, es importante un ajuste de parámetros adecuado a los ambientes protegidos, para minimizar falsos positivos, y que se bloqueen conexiones legítimas que causen trastornos para las organizaciones"[80].

[77] PEÑA Rodrigo, RODRIGUEZ Álvaro, Implementación en un dispositivo hardware de un sistema de detección de intrusos basados en red, Trabajo de grado [En línea], 2019, Madrid: , Universidad Complutense De Madrid, p. 19. Disponible en internet: https://eprints.ucm.es/56504/1/1138534699-355685_RODRIGO_LAGARTERA_PE%C3%91A_Implementaci%C3%B3n_en_un_dispositivo_hardware_de_un_sistema_de_detecci%C3%B3n_de_intrusos_basado_en_red_3940146_794802335.pdf

[78] Ibid., P. 19

[79] INFOTECS, IDS Sistema de detección de intrusos, Articulo [Online], Publicado [12 marzo 2019], p. 1. Disponible en internet: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

[80] Ibid., p. 1

- **IDS activo**

Se define un "IDS como activo desde el momento en que se define para bloquear automáticamente ataques o actividades sospechosas que sean de su conocimiento, sin necesidad de intervención humana. Aunque potencialmente es un modelo extremadamente interesante, es importante un ajuste de parámetros adecuado a los ambientes protegidos para minimizar falsos positivos, bloqueando conexiones legítimas y causando trastornos para las empresas"[81].

- **IDS pasivo**

> Un IDS pasivo, por otro lado, actúa de manera a monitorear el tráfico que pasa a través de él, identificando potenciales ataques o anormalidades y, con base en ello, generando alertas para administradores y equipos de seguridad; sin embargo, no interfiere en absolutamente nada en la comunicación. Se trata de un modelo bastante interesante en una arquitectura de seguridad, independientemente de no actuar directamente en la prevención, sirve como un excelente termómetro de ataques e intentos de acceso no autorizados a la infraestructura de una empresa[82].

2.2.19 Sistemas de prevención de intrusos

Un sistema de prevención de intrusos se encarga de ejecutar "el sistema de prevención contra intrusiones, permite detectar los intentos de intrusión por medio de un fichero de identificadores de intrusiones analizando el flujo de los protocolos IP, ICMP, TCP y UDP; y el administrador puede configurar el bloqueo automático de las intrusiones detectadas, además de especificar unos valores límite y umbral para cada regla, que reducirán los falsos positivos"[83].

> Un Sistema de Prevención de Intrusos es un dispositivo de seguridad, fundamentalmente para redes, que se encarga de monitorear actividades a nivel de la capa 3 (red) y/o a nivel de la capa 7 (aplicación) del Modelo OSI, con el fin de identificar comportamientos maliciosos, sospechosos e indebidos, a fin de reaccionar ante ellos en tiempo real mediante una acción de contingencia. El IPS fue creado con la intensión de ser una alternativa complementaria a otras herramientas de seguridad en redes, tales como un *firewall* o un IDS, por lo que muchas de sus características son heredadas de estos dos elementos, complementadas con un comportamiento proactivo ante ataques y amenazas. Los Sistemas de Detección de Intrusos tienen

[81] CECHINEL Eduardo, IDS activo y pasivo, Articulo [Online], Publicado [2020], Brasil, p. 1. Disponible en internet: https://ostec.blog/es/seguridad-perimetral/ids-conceptos/#:~:text=Se%20define%20un%20IDS%20como,sin%20necesidad%20de%20intervenci%C3%B3n%20humana.

[82] Ibid., p. 1

[83] PANDA, IPS prevenga su red contra ataques inesperados, evitando intrusiones, Articulo [Online], Publicado [2020], p. 1. Disponible en internet: https://www.pandasecurity.com/es/enterprise/solutions/security-appliances/ips/

como ventaja respecto de los *firewalls* tradicionales, el que toman decisiones de control de acceso basados en los contenidos del tráfico, en lugar de hacerlo basados en direcciones o puertos IP[84].

- **¿Qué es un Sistema de Detección de Intrusos?**

Principalmente "Un IDS (Intrusión Detección System) es una herramienta de seguridad, que se encarga de monitorizar los sucesos que resultan en un sistema informático en busca de intentos de intrusión. Los IDS están compuestos por tres elementos fundamentales: Una fuente de información que proporciona eventos del sistema, un motor de análisis que busca evidencias de intrusiones y un mecanismo de respuesta que actúa según los resultados del motor de análisis"[85].
Como se comporta:

> La idea central del funcionamiento de un IDS se basa en el hecho de que la actividad intrusiva constituye un conjunto de anomalías (acciones extrañas o sospechosas). Si alguien consigue entrar de forma ilegal a un sistema, no actuará como un usuario comprometido, sino que su comportamiento se alejará del de un usuario normal. De forma general, la mayoría de las actividades intrusivas resultan de la suma de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo[86].

- **Como se clasifican:**

> Intrusivas, pero no anómalas: denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema.
> No intrusivas pero anómalas: denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados.
> No intrusiva ni anómala: son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
> Intrusiva y anómala: se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada. Los detectores de intrusiones anómalas requieren realizar muchas estimaciones de varias métricas estadísticas, para

[84] INFOTEC, IPS: Sistemas de prevención de intrusos, Articulo [Online], Publicado [13 marzo de 2019], p. 1. Disponible en internet: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html
[85] MIRA ALFARO Emilio, Implantación de un sistema de detección de intrusos, Trabajo de grado. [En línea]. Universidad de Valencia. Ingeniería Informática.
[86] Ibid., p. 1

determinar cuánto se aleja el usuario de lo que se considera comportamiento normal[87].

- **Funciones de un IDS**

  En el momento que el ataque está sucediendo o después, los IDS detectan esta intrusión. Automatización de la búsqueda de nuevos patrones de ataque, gracias a herramientas estadísticas de búsqueda y al análisis de tráfico anómalo, realizando una función de monitorización y análisis de las actividades de los usuarios, de este modo se pueden conocer los servicios que usan los usuarios y estudiar el contenido del tráfico, en busca de elementos anómalos., utilizando como ayuda la auditoría de configuraciones y vulnerabilidades de determinados sistemas descubriendo sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs con el fin de analizar el comportamiento que no es usual. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs pueden revelar una máquina comprometida o un usuario con su contraseña al descubierto, Automatizando tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos y otros[88].

- **Como detectan tráfico malicioso**

En este proceso se realiza con "los IDS los cuales detectan tráfico ilegítimo haciendo uso de patrones, que, de cumplirse, harían saltar las alarmas. Esto es lo que se conoce como una 'firma'. Estas firmas pueden ser atómicas (constituidas por un paquete individual determinado) o compuestas (paquetes múltiples). Se configuran un conjunto de reglas de variada complejidad que, al coincidir, generarán las alertas correspondientes"[89].

[87] INFOTEC, IPS: Sistemas de prevención de intrusos, Articulo [Online], Publicado [13 marzo de 2019], p. 1. Disponible en internet: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

[88] GARZON PADILLA Gilberzon, Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la dirección general sede central del instituto nacional penitenciario y carcelario INPEC "PIDSINPEC", Tesis [En línea], Colombia, Tunja, 2015,
universidad nacional abierta y a distancia- UNAD escuela de ciencias básicas tecnología e ingeniería- ECBTI especialización en seguridad informática Tunja, p. 29. Disponible en internet: https://repository.unad.edu.co/bitstream/handle/10596/3494/86057594.pdf?sequence=3&isAllowed=y

[89] FERNADEZ ARNAL Adrián y TRUJILLO LONDOÑO Mauricio, ¿Qué es un IDS? Tipos, técnicas evasión y como evitarla, Articulo [Online], Publicado [16 abril 2018], p.1. Disponible en: https://siemlab.com/que-es-un-ids-intrusion-detection-system/

- **Tipos de IPS**

    - **IPS basado en firmas**

Por otra parte, encontramos “IPS realice la detección basada en firmas, se debe contar con una base de datos, en la cual se contengan todos los patrones conocidos de un ataque particular. Esta información se adhiere al dispositivo que realizará la detección para que así, mediante una búsqueda de coincidencias, se pueda establecer si existe o no un ataque”[90].

    - **IPS basado en anomalías**

También conocido como, “basado en perfil, Este tipo de IPS intenta identificar un comportamiento diferente o que se desvíe de lo que, de alguna forma, se ha predefinido como un “comportamiento normal” de la red. Un IPS basado en anomalías es también basado en estadísticas”[91].

    - **IPS basado en políticas**

> Una de las exigencias más imponentes es que se requiere que se declaren muy específicamente las políticas de seguridad. El IPS reconoce el tráfico definido por el perfil establecido, permitiendo o descartando paquetes de datos, por lo que su manera de actuar ocurre de forma muy similar al funcionamiento de un firewall, en donde se evidencie el protocolo de seguridad y según su varianza se argumente que en este proceso se esté desarrollando de la manera más pertinente con el fin de cumplir cada una de las políticas establecidas en este paso a paso de ejecución[92].

    - **IPS basado en detección por Honey Pot**

> los hackers siempre están ansiosos por encontrar servidores que no estén lo suficientemente protegidos. Tanto es así que la metáfora del bote de miel sirve para describir el afán de unos y otros. En términos informáticos, un honeypot es un mecanismo de seguridad con el que los administradores engañan a los hackers y los ciberataques se realizan en vano. Un bote de miel de tales

[90] CAMACHO CACERES Nicolas, Sistema de prevención de intrusos (IPS) para un entorno de red SDN, Trabajo de grado [En línea], Publicado [2016] Colombia-Bogotá Pontificia universidad javeriana, p. 19. Disponible en internet: https://repository.javeriana.edu.co/bitstream/handle/10554/21421/CamachoCaceresNicolasAlfonso2016.pdf?sequence=1

[91] Ibid., p.16

[92] Ibid., P.1

características simula servicios de red o programas de aplicación que permiten atraer a los atacantes y proteger el sistema productivo ante posibles daños. En la práctica, los usuarios hacen acopio de tecnologías del lado del servidor o del cliente para crear honeypots[93].

- **IPS basado en host**

Los IPS basados en host se los denomina "Host que requieren de la instalación de un software en cada equipo que se desea monitorear. Esto origina que su mantenimiento sea más complejo ya que es indispensable que el software de cada equipo se mantenga actualizado para garantizar su efectividad"[94].

- **IPS basado en la red**

Con esta tecnología de "IPS, se realiza monitoreo sobre el tráfico de red que fluye a través de segmentos particulares, y analizan protocolos de red, de transporte y de aplicación para identificar actividades sospechosas. La principal diferencia entre esta tecnología, y la anterior, es la ubicación de sus sensores. Este, los distribuye a lo largo de varios segmentos de red"[95].

2.2.20 Pymes

De acuerdo con la Ley 905 de 2004, para clasificar a las micro y las pymes se tienen en cuenta dos criterios, su valor en activos y el número de empleados que la componen, por tanto, Estos criterios se mantienen vigentes dado que no se ha reglamentado el criterio de ventas, que estableció el artículo 43 de la ley 1450 de 2011. Según los datos de Confecámaras, que agrupa a todas las cámaras de comercio del país, existen aproximadamente 1.500.000 micro, pequeñas y medianas empresas en el Registro Único Empresarial -RUES-. Esta cifra incluye a personas

[93]IONOS GIGITAL, Que es un honeypot, Articulo [Online], Publicado [08 agosto 2017], p. 1. Disponible en internet: https://www.ionos.es/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/

[94] MARIDUEÑA CARRION Nora, La importancia de los IPS y BYOD en las organizaciones: Caso de estudio CONFIDENCIAL S.A, Articulo [Online], Publicado [2016], Ecuador-Samborondón, UEES Universidad espíritu santo, p. 5. Disponible en internet: http://201.159.223.2/bitstream/123456789/1436/1/Tesis%20Nora%20Mariduena_Final.pdf

[95] CAMACHO CACERES Nicolas, Sistema de prevención de intrusos (IPS) para un entorno de red SDN, Trabajo de grado [En línea], Publicado [2016] Colombia-Bogotá Pontificia universidad javeriana, p. 19. Disponible en internet: https://repository.javeriana.edu.co/bitstream/handle/10554/21421/CamachoCaceresNicolasAlfonso2016.pdf?sequence=1

naturales y a personas jurídicas. Esta clasificación se realiza, por lo general, con base en el valor de los activos reportados por las empresas[96].

- **Su clasificación:**

Imagen 1 Clasificación

Autor 1 Bancolombia

En Colombia, según la Ley para el Fomento de la Micro, Pequeña y Mediana Empresa, Ley 590, las PYMES se clasifican así:
Microempresa: Personal no superior a 10 trabajadores. Activos totales inferiores a 501 salarios mínimos mensuales legales vigentes.
Pequeña Empresa: Personal entre 11 y 50 trabajadores. Activos totales mayores a 501 y menores a 5.001 salarios mínimos mensuales legales vigentes.
Mediana: Personal entre 51 y 200 trabajadores. Activos totales entre 5.001 y 15.000 salarios mínimos mensuales legales vigentes.
El aporte de la micro, pequeña y mediana empresa industrial se refleja en estos indicadores, La Encuesta Anual Manufacturera nos permite valorar la incidencia de la MIPYME en el panorama empresarial colombiano. Representan el 96.4% de los establecimientos, aproximadamente el 63% del empleo; el 45% de la producción manufacturera, el 40% de los salarios y el

[96] BANCOLOMBIA, Conoce todo sobre las pymes en Colombia, Articulo [Online], Publicado [12 julio 2018], Colombia, p. 1. Disponible en internet: https://www.grupobancolombia.com/wps/portal/negocios/actualizate/legal-y-tributario/todo-sobre-las-pymes-en-colombia

37% del valor agregado. Son más de 650.000 empresarios cotizando en el sistema de seguridad social[97].

2.2.21 Modelo de seguridad para Pymes

Es esencial potenciar la seguridad a pymes por tanto" el objetivo principal del modelo de seguridad para redes de empresas es ofrecer información sobre las mejores prácticas a las partes interesadas en el diseño e implementación de redes seguras"[98].

2.2.22 Protocolos de seguridad

Los protocolos de seguridad se caracterizan por ser "un conjunto de reglas que gobiernan las comunicaciones, la cuales están diseñadas para que puedan soportar los diferentes tipos de ataques, lo cual puede llegar a ser muy costoso protegerse de todo tipo de ataque, por este motivo los protocolos están diseñados bajo ciertas premisas con respecto a los riesgos que puede estar expuesto un sistema"[99].

2.2.23 Detección de intrusos

> Cunando se hace alusión a un sistema de detección de intrusiones, generalmente los asocia a "alarmas de ladrones para ordenadores o redes". Es fácil entender el concepto como este usando comparaciones sencillas. En realidad, la explicación es bastante aproximada y los usuarios que no se dedican a seguridad informática no necesitan ser expertos, sin embargo, la seguridad no puede cometer errores ni estar expuesta ante un suceso de esta índole y no llevarse de lago trivial, sin tener conocimiento alguno sobre la trascendencia que ha tenido este tipo de ataques[100].
>
> Todos están propensos a sufrir un ataque se han observado a través de los diferentes medios de comunicación (televisión, radio, etc...), noticias importantes sobre ataques informáticos a entidades como Yahoo, Microsoft entre otras entidades, pero eso significa que ¿Solo las Grandes Empresas son las que están propensas a recibir dichos ataques?, pues lastimosamente

---

[97] BUSINESSCOL, Sección pymes, Articulo [Online], Publicado [2020], Colombia P. 1. Disponible en internet: https://www.businesscol.com/empresarial/pymes/#:~:text=En%20Colombia%2C%20seg%C3%BAn%20la%20Ley,no%20superior%20a%2010%20trabajadores.&text=Peque%C3%B1a%20Empresa%3A%20Personal%20entre%2011,salarios%20m%C3%ADnimos%20mensuales%20legales%20vigentes.

[98] CONVERY, Sean y TRUDEL, Bernia, Cisco SAFE Un modelo de Seguridad para las Redes de las Empresas, Articulo [Online], P.26,29. Disponible en internet: https://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf

[99] CISCO SAFE, Un modelo de seguridad para las redes de las empresas, Articulo [Online], p. 28. Disponible en internet: https://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf

[100] GONZALES GOMEZ Diego, Historia de sistemas de detección de intrusiones, Articulo [Online] Publicado 2003, p.19. Disponible en internet: https://dgonzalez.net/papers/ids/ids_v1.0.pdf

no es así, cualquier persona que posea un computador está en riesgo de sufrir un ataque por un hacker, aunque la información que se obtenga de este computador puede no tener mucho significado para el hacker, este puede hacer uso de su computador para realizar ataques a terceras personas, quedando así incognito, de tal forma que puede desaparecer fácilmente sin que su verdadera identidad se dé a conocer[101].

Conocer más de los sistemas de detección de intrusos se deben tener concepto claro sobre la historia de estos sistemas, la seguridad empieza desde nuestras viviendas como por ejemplo una buena seguridad de nuestra casa debe tener puertas, ventanas, cerraduras y cerras, además de contar con un sistema de alamar instalado, existe otro sistemas un poco más sofisticados como cámaras de vigilancia que utiliza diferentes tipos dispositivos como sensores , infrarrojos y sensores de o temperatura para la detección de un intruso , otras forma de seguridad es la contratación de empresas de seguridad. Hoy en día se puede contar con diversos tipos de sistemas de detección de intrusos que son adaptable a diferentes tipos de entornos, como por ejemplo están Sistemas de Detección diseñados para monitorizar redes completas mientras otros se implementan a nivel de host. Una de las estrategias más utilizadas en control de espacio perimetral son los cortafuegos, los cortafuegos actúan como las rejas con puntas afiladas y las puertas con una docena de cerraduras. Sirven para mantener fuera a los bandidos, es decir, sirven al propósito de prevenir ataques o intrusiones en la red interna por ellos protegida, pero todo esto no garantiza que algún intruso puede acceder por otro lado o través de tipos de dispositivo, sin embargo, el cortafuego garantiza una poderosa línea de defensa frente amenazas externas, pero en algunos casos puede generar falsa sensación de seguridad[102].

Bajo el enfoque de detección de intrusos y partir del mal uso que le se le da al equipo de cómputo, las intrusiones se detectan comparando el comportamiento real registrado con patrones conocidos como sospechosos. Este enfoque resulta eficaz en el descubrimiento de ataques conocidos, pero es inútil cuando se enfrentan a variantes de ataques desconocidas, es decir, variantes de ataques de los cuales no se tiene firmas. Cualquier error en la definición de estas firmas aumenta la tasa de falsas alarmas y disminuye la eficacia de la técnica de detección. El mismo consta de cuatro componentes: la colección de datos, el perfil del sistema, detección de uso indebido y la respuesta. Los datos se recogen de una o varias fuentes de datos, incluyendo, el tráfico de red, las trazas de llamadas al sistema, etc., esos datos recogidos se estandarizan a un formato comprensible por los demás

[101] OCAMPO Carlos, CASTRO BERMUDEZ Yanci y SOLARTE MARTINEZ Guillermo, Intrusión detection system in corporate networks, Articulo [Online], Colombia- Pereira, Publicado [2017], Vol. 22, Universidad tecnológica de Pereira, p. 60. Disponible en internet: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/9105
[102] Ibid., p. 61.

componentes del sistema. Por otra parte, el perfil de sistema se utiliza para caracterizar los comportamientos normales y anormales[103].

2.2.24 Snorby

Se caracteriza por ser una aplicación web (front-end) basada en Ruby on Rails, que interactúa con un IDS para monitorizar gráficamente la seguridad de la red. Se comunica con sistemas como Snort, Sagan, Suricata y cualquier otro que genere eventos de log en el formato binario Unified2.Tambien permite monitorizar y administrar, mediante una interfaz gráfica, diversos aspectos del sistema IDPS, realizando la sincronización de los datos mediante un script (Snorby Worker).Posee un tablero de reportes que muestra la cantidad de eventos registrados en un lapso de tiempo, permitiendo filtrar estos eventos por su grado de severidad, sensor donde se originan, protocolo empleado, reglas asociadas y el origen o destino del ataque[104].

2.2.25 Snort

Snort es un Sistema de Detección de Intrusos (IDS) basado en red (IDSN) open source. Cuenta con un lenguaje de creación de reglas en el que se pueden definir los patrones que se utilizarán a la hora de monitorizar el sistema. Además, ofrece una serie de reglas y filtros ya predefinidos que se pueden ajustar durante su instalación y configuración para que se adapte lo máximo posible a lo que deseamos. Una de las ventajas de este sistema es que puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se loguea. Así se sabe cuándo, de dónde y cómo se produjo el ataque[105].

El desarrollo de reglas para Snort, que es uno de los sistemas de detección de intrusiones de red más populares, es una habilidad fundamental para detectar nuevos ciberataques cada vez más emergentes. Tan emergente, que gran parte de empresas más relevantes, ya lo están empezando a usar. SNORT es un software NIDS de código abierto. Combinando los beneficios de la inspección basada en firmas, protocolos y anomalías, SNORT es la

---

[103] RIVERO PEREZ Jorge y RODRIGUEZ Carlos, Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras, Articulo [Online], Publicado [2014], Cuba, Universidad de Cienfuegos, p. 1. Disponible en internet: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992014000400003

[104] LEACOCK Sheyla, Analizando la seguridad de la red con SNORBY, Articulo [Online], Chile, Publicado [26 noviembre 2018], p. 1. Disponible en internet: https://backtrackacademy.com/articulo/analizando-la-seguridad-de-la-red-con-snorby

[105] ORTEGO DELGADO Daniel, Qué es Snort: Primeros pasos, Articulo [Online], Publicado [21 marzo 2017], p. 1 Disponible en internet: https://openwebinars.net/blog/que-es-snort/

tecnología IDS / IPS más utilizada en todo el mundo. Es capaz de realizar un "análisis de alto nivel" en todo el tráfico que fluye a través de su sensor. La ubicación del sensor es importante. Normalmente, un buen punto de entrada se encuentra en el límite entre la LAN e Internet. Situar SNORT o aplicarlos un punto como los firewalls perimetrales o similar, en un sitio estratégico, permite analizar todo el tráfico que entra y sale de la red local. También es importante definir qué detectar con SNORT[106].

2.2.26 Sistema de Gestión Base de Datos

Un SGBD es un programa de ordenador que facilita una serie de herramientas para manejar bases de datos y obtener resultados (información) de ellas. Además de almacenar la información, se le pueden hacer preguntas sobre esos datos, obtener listados impresos, generar pequeños programas de mantenimiento de la BD, o ser utilizado como servidor de datos para programas más complejos realizados en cualquier lenguaje de programación. Además, ofrece otras herramientas más propias de la gestión de BD como sistemas de permisos para autorización de accesos, volcados de seguridad, transferencia de ficheros, recuperación de información dañada e indización[107].

2.2.27 Tipos De Bases De Datos

Las bases de datos pueden clasificarse de varias maneras, de acuerdo con el criterio elegido para su clasificación:

- **Bases de Datos Estática**

  Es una base de datos en las cuales los archivos contenidos solo son de lectura utilizadas primordialmente para almacenar datos históricos, que después pueden ser utilizados, se las conoce como bases de datos únicamente de lectura sirven para almacenar datos históricos que posteriormente pueden ser utilizados. se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, Un ejemplo de este sería bibliotecas, periódicos (para almacenar información y si se

[106] RAMIRO Ruben, Reglas SNORT, detección de intrusos y uso no autorizado, Articulo [Online], Publicado [22 noviembre 2020], p. 1, Disponible en internet: https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/

[107] GOMEZ Eva, MARTINEZ Patricio, MOREDA Paloma, ARMANDO Suares, MONTOYA Andrés y SAQUETE Estela, Bases de datos 1, Trabajo investigación [En línea], Publicado [2007], España, Universidad de alicate,
p. 14. Disponible en internet: https://rua.ua.es/dspace/bitstream/10045/2990/1/ApuntesBD1.pdf

requiere consultarla tiempo después). Se puede realizar proyecciones, tomar decisiones y realizar análisis de datos para inteligencia empresarial[108].

- **Bases de Datos Dinámicas**

Se las denomina bases de datos dinámicas a "aquellas donde los **datos pueden actualizarse** o incluso modificarse. La mayoría puede ser actualizada en tiempo real"[109].

2.2.28 Postgresql

PostgreSQL, o simplemente Postgres para darle un nombre más pintoresco, es un sistema de código abierto de administración de bases de datos del tipo relacional, aunque también es posible ejecutar consultas que sean no relaciones. En este sistema, las consultas relacionales se basan en SQL, mientras que las no relacionales hacen uso de JSON. Como decíamos, se trata de un sistema de código abierto y además gratuito, y su desarrollo es llevado adelante por una gran comunidad de colaboradores de todo el mundo que día a día ponen su granito de arena para hacer de este sistema una de las opciones más sólidas a nivel de bases de datos. Dos detalles a destacar de PostgreSQL es que posee data types (tipos de datos) avanzados y permite ejecutar optimizaciones de rendimiento avanzadas, que son características que por lo general solo se ven en sistemas de bases de datos comerciales, como por ejemplo SQL Server de Microsoft u Oracle de la compañía homónima[110].

2.2.29 Kali Linux

Más conocido como hacking ético más populares y utilizadas en todo el mundo, está basada en Debian y mantenida por Offensive Security Ltd. Aunque no es una de las más completas en cuanto a número de programas, sus desarrolladores se encargan de que no haya herramientas repetidas. Esto significa que los usuarios que opten por ella tendrán una base conocida y con excelente soporte y mantenimiento. La personalización es también uno de los puntos fuertes de esta alternativa, así como la posibilidad de usarla en el idioma que se necesite. Dentro de Kali se puede encontrar un total de 600 aplicaciones de hacking y seguridad, Una de las principales características que nos ofrece Kali Linux es que podemos usar esta distro tanto en un ordenador como en un smartphone. Para ordenador, basta con

[108] PINEDA Angelica y PEÑARANDA Carlos, Bases de datos estáticas, Presentación [Online], Publicado [3 octubre 2016], p. 3. Disponible en internet: https://prezi.com/rhdgiuon8_rq/base-de-datos-estatica/

[109] REDATOR, Tipos de bases de datos, Articulo [En línea], Publicado [25 enero 2019], p.1. Disponible en internet: https://rockcontent.com/es/blog/tipos-de-base-de-datos/

[110] BORGES Santiago, Servidor PostgreSQL, Articulo [Online], Publicado [19 noviembre 2019], p. 1. Disponible en internet: https://blog.infranetworking.com/servidor-postgresql/

tener un equipo con arquitectura i386 o AMD64 para poder cargarla e instalarla sin problemas. También podemos encontrar imágenes para sistemas ARM, lo que nos permite convertir un micro-ordenador, como el Raspberry Pi, en una completa herramienta de hacking. Y, además, podemos encontrar imágenes para equipos especiales, como varios modelos de Chromebook, CuBox, Odroid y Samsung Galaxy Note. Los desarrolladores de Kali Linux también ofrecen imágenes de un sistema alternativo llamado Kali NetHunter. Esta versión está diseñada especialmente para smartphones, aunque la compatibilidad es mucho más limitada[111].

2.2.30 Virtual Box

Se la denomina una" aplicación que sirve para hacer máquinas virtuales con instalaciones de sistemas operativos. Esto quiere decir que, si tienes un ordenador con Windows, GNU/Linux o incluso macOS, puedes crear una máquina virtual con cualquier otro sistema operativo para utilizarlo dentro del que estés usando"[112].

2.2.31 Metodologías de Desarrollo

Existen dos tipos de metodologías de desarrollo:

- **Tradicional**

  Las metodologías tradicionales imponen una disciplina de trabajo sobre el proceso de desarrollo del software, para ello, se hace énfasis en la planificación total de todo el trabajo a realizar y una vez que está todo detallado, comienza el ciclo de desarrollo del producto software. Se centran especialmente en el control del proceso, mediante una rigurosa definición de roles, actividades, artefactos, herramientas y notaciones para el modelado y documentación detallada. Además, las metodologías tradicionales no se adaptan adecuadamente a los cambios, por lo que no son métodos adecuados cuando se trabaja en un entorno, donde los requisitos no pueden predecirse o bien pueden variar[113].

[111] VELAZCO Ruben, Conviértete en un hacker ético con Kali Linux, Articulo [Online], publicado [3 marzo 2020], p. 1. Disponible en internet: https://www.softzone.es/programas/linux/kali-linux/

[112] FERNANDEZ Yúbal, VirtualBox: Qué es y como usarlo para crear una maquina virtual con Windows u otro sistema operativo, Articulo [Online], Publicado [1 junio 2020], p. 1. Disponible en internet: https://www.xataka.com/basics/virtualbox-que-como-usarlo-para-crear-maquina-virtual-windows-u-otro-sistema-operativo

[113] GRUPO PTM, Metodología tradicional, Articulo [Online], Publicado [30 mayo 2019], P. 1. Disponible en internet: https://pmtgrupoeafit.wixsite.com/gestion-proyectos/post/metodolog%C3%ADa-tradicional

- **Tipos de metodología tradicional**

    - **Metodología en Cascada**

Hay diversos modelos tradicionales entre los que se encuentran “el modelo en cascada es un proceso de desarrollo secuencial, en el que el desarrollo de software se concibe como un conjunto de etapas que se ejecutan una tras otra. Se le denomina así por las posiciones que ocupan las diferentes fases que componen el proyecto”[114].

    - **Metodología en Espiral**

Otro de los modelos de metodología tradicional es “el modelo espiral en el desarrollo del software es un modelo meta del ciclo de vida del software donde el esfuerzo del desarrollo es iterativo, tan pronto culmina un esfuerzo del desarrollo por ahí mismo comienza otro; además en cada ejecución del desarrollo se sigue cuatro pasos principales, Determinar o fijar los objetivos, Análisis del riesgo, Desarrollar, verificar y validar Y Planificar”[115].

    - **Modelo prototipo**

> El modelo de prototipos es un método para obtener una retroalimentación rápida respecto de los requisitos, proporcionando un modelo operativo del producto esperando antes de construirlo realmente. Puesto que los prototipos son tangibles, permiten a los interesados experimentar con un modelo de su producto final, en lugar de sólo debatir en forma abstracta sobre sus requisitos. El modelo de prototipos, también conocido como modelo de desarrollo evolutivo, es usado principalmente en proyectos de desarrollo de software. Este modelo se utiliza para dar al usuario una vista preliminar de lo que será el sistema. Dentro de los recursos que se buscan reducir al utilizar este modelo son el tiempo, pues el prototipo debe ser construido a la brevedad posible, y dinero ya que en el prototipo no se deben invertir muchos recursos[116].

[114] OPENCLASSROOMS, En qué consiste el modelo en cascada, Articulo [Online], Publicado [2 junio 2020], p. Disponible en internet: https://openclassrooms.com/en/courses/4309151-gestiona-tu-proyecto-de-desarrollo/4538221-en-que-consiste-el-modelo-en-cascada

[115] FARIÑO Galo, Modelo espiral de un proyecto de desarrollo de software, Articulo [Online], 2011, Ecuador, Universidad estatal de milagro, p. 3. Disponible en internet: http://www.ojovisual.net/galofarino/modeloespiral.pdf

[116] GARCIA Omar, Modelo de prototipos, Articulo [Online], Publicado [2 septiembre 2013], p. 1. Disponible en internet: https://www.proyectum.com/sistema/blog/modelo-de-prototipos/

- **Modelo en V**

El modelo V o modelo en cuatro niveles es un modelo empleado en diversos procesos de desarrollo, por ejemplo, en el desarrollo de software. En los años 90 apareció su primera versión, pero con el tiempo se ha ido perfeccionando y adaptando a los métodos modernos de desarrollo. La idea básica, sin embargo, se remonta a los años 70 y fue concebida como una especie de desarrollo posterior del modelo de cascada, Además de las fases de desarrollo de un proyecto, el modelo V también define los procedimientos de gestión de la calidad que lo acompañan y describe cómo pueden interactuar estas fases individuales entre sí. Su nombre se debe a su estructura, que se asemeja a la letra V. Iniciando con pruebas de unidad, siguiendo con pruebas de integración, posteriormente Integración del sistema y secuencialmente con la validación[117].

- **Agiles**

Las metodologías ágiles son flexibles, pueden ser modificadas para que se ajusten a la realidad de cada equipo y proyecto. Los proyectos ágiles se subdividen en proyectos más pequeños mediante una lista ordenada de características. Cada proyecto es tratado de manera independiente y desarrolla un subconjunto de características durante un periodo de tiempo corto, de entre dos y seis semanas. La comunicación con el cliente es constante al punto de requerir un representante de él durante el desarrollo. Los proyectos son altamente colaborativos y se adaptan mejor a los cambios; de hecho, el cambio en los requerimientos es una característica esperada y deseada, al igual que las entregas constantes al cliente y la retroalimentación por parte de él. Tanto el producto como el proceso son mejorados frecuentemente[118].

[117] DIGITAL Guide, ¿Qué es el modelo en V?, Articulo [Online], publicado [23 junio 2020], p.1. Disponible en internet: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/modelo-v/#:~:text=La%20%E2%80%9CV%E2%80%9D%20del%20nombre%20del,de%20calidad%20de%20cada%20fase.

[118] CADAVID NAVARRO Andrés, MARTINEZ FERNANDEZ Juan, VELEZ MORALES Jonathan, Revisión de metodologías agiles para el desarrollo de software, Articulo [Online], Colombia, 2013, Universidad autónoma del caribe, Prospectiva, Vol. 11. P. 3. Disponible en internet: https://www.redalyc.org/pdf/4962/496250736004.pdf

- **Tipos de metodología ágil**

  - **Modelo XP**

La Metodología XP “Extreme Programming” o “Programación Extrema” es una de las llamadas metodologías Ágiles de desarrollo de software más exitosas. Es habitual relacionarla con scrum, y la combinación de ambas asegura un mayor control sobre el proyecto, y una implementación más efectiva y eficiente. La metodología XP define cuatro variables para cualquier proyecto de software: costo, tiempo, calidad y alcance. El método especifica que, de estas cuatro variables, tres de ellas podrán ser fijadas arbitrariamente por actores externos al grupo de desarrolladores (clientes y jefes de proyecto), y el valor de la restante deberá será establecida por el equipo de desarrollo, quien establecerá su valor en función de las otras tres. Al igual que otras metodologías de gestión de proyectos, tanto Ágiles como tradicionales, el ciclo de vida XP incluye, entender lo que el cliente necesita en una llamada fase de exploración, como también lo es estimar el esfuerzo el cual está en la fase de Planificación, para poder crear la solución y llevándola a una fase de Iteraciones, para poder hacer la entregar del producto final al cliente terminando con la fase de puesta en producción[119].

  - **Modelo SCRUM**

La metodología Scrum es un marco de trabajo o framework que se utiliza dentro de equipos que manejan proyectos complejos. Es decir, se trata de una metodología de trabajo ágil que tiene como finalidad la entrega de valor en períodos cortos de tiempo y para ello se basa en tres pilares: la transparencia, inspección y adaptación. Esto permite al cliente, junto con su equipo comercial, insertar el producto en el mercado pronto, rápido y empezar a obtener ventas. La flexibilidad en la adopción de cambios y nuevos requisitos durante un proyecto complejo, teniendo como prioridad principal el factor humano, y en secuencia la colaboración e interacción con el cliente para el desarrollo iterativo como forma de asegurar buenos resultados[120].

[119] VILA Juan, La metodología XP: la metodología de desarrollo de software más exitosa, Articulo [Online], Publicado [8 julio 2016], p. 1. Disponible en internet: https://proagilist.es/blog/agilidad-y-gestion-agil/agile-scrum/la-metodologia-xp/

[120] ABELLÁN Encarna, Metodología Scrum: que es y cómo funciona, Articulo [Online], Publicado [05 marzo 2020], p. 1. Disponible en internet: https://www.wearemarketing.com/es/blog/metodologia-scrum-que-es-ycomofunciona.html#:~:text=La%20metodolog%C3%ADa%20Scrum%20es%20un,equipos%20que%20manejan%20proyectos%20complejos.&text=Esto%20permite%20al%20cliente%2C%20junto,obtener%20ventas%20(Sales%20enablement).

- **RUP**

La metodología de desarrollo RUP por sus siglas en inglés o Proceso de Desarrollo Unificado es un proceso de desarrollo de software y junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización[121].

2.3 VARIABLES DE ESTUDIO

En el transcurso del proceso de investigación se tendrá en cuenta las siguientes variables:

2.3.1 Variable Independiente

- ✓ Sistema de detección de intrusos

2.3.2 Variable Dependiente

- Eficiencia
  - Verdadero positivo (VP)
  - Verdadero negativo (VN)
  - Falso positivo (FP)
  - Falso negativo (FN)
- Usabilidad
  - Comprensibilidad del sitio
  - Mecanismos de ayuda

[121] PABÓN Elías, Metodología de desarrollo tradicional RUP, Articulo [Online], Publicado [31 julio 2018], p. Disponible en internet: https://smartsoftcolombia.com/portal/index.php/blog/49-rup#:~:text=La%20metodolog%C3%ADa%20de%20desarrollo%20RUP,de%20sistemas%20orientados%20a%20objetos.

2.4 DEFINICIÓN NOMINAL DE LAS VARIABLES

A continuación, se realizará la definición nominal de las variables elegidas para el proyecto de investigación, se formulan según la finalidad o lo esperado en el proceso de ejecución y las cuales se definirán a continuación:

- **Sistema de detección de intrusos**

  El sistema reúne determinadas funcionalidades y características en pro de mejorar la protección en las PYMES siempre teniendo en cuenta los pilares de la seguridad que son la Integridad, Disponibilidad y Confidencialidad de la información. Para esto se llevará a cabo mediante la utilización un equipo de cómputo correctamente configurado con software libre.

  Estas herramientas de software que se implementaran tienen como fin, mejorar la seguridad de la información que manejan las PYMES, logrando así que las mismas puedan prestar un mejor servicio.

El cálculo de las variables independientes se obtiene directamente de las pruebas realizadas, con el fin de realizar un conteo y obtener la clasificación de cada una de ellas, para lo cual se dará uso de las siguientes formulas.

Falsos Negativos + Verdaderos negativos=Total de análisis de trafico

Verdaderos positivos + Falsos negativos = Total de análisis de intrusos

Para identificar las intrusiones a sistemas de seguridad (expresa en Porcentaje%) y se llevara a cabo con la siguiente formula.

$$X = \frac{\text{(Prueba de intrusos detectados)}}{\text{(Prueba de intrusiones realizada)}} * 100\%$$

Como también se estudiará el análisis de tráfico que no tenga ningún tipo de inconvenientes y se lo representará de la siguiente manera.

$$X1 = \frac{\text{(Análisis de tráfico sin anomalías)}}{\text{(Análisis de tráfico realizado)}} X\ 100\%$$

2.5 DEFINICIÓN OPERATIVA DE LAS VARIABLES

A continuación, se realizará la definición operativa de las variables elegidas para el proyecto de investigación, en donde se describirá las acciones u operaciones para medir las variables.

- Eficiencia

Es el proceso mediante el cual se puede medir la ejecución de un proyecto o las variables con un fin de poder llegar a los resultados esperados de dicha investigación con un menor número de errores y tomando el camino más adecuado para llevar a cabo la investigación

- Verdadero positivo (VP)

Este proceso se lo determina cuando en el análisis del tráfico de la red se detecta un intruso en la misma, y se lo determina finalmente como un intruso intentando captar información en el sistema de la PYME.

- Verdadero negativo (VN)

Se lo considera un resultado en el que el detector de intrusos predice correctamente la clase negativa.

Tráfico en la red monitoreado y detectado como posibles amenazas de intrusión se lo (expresa en porcentaje%).

En esta variable se realizará el registro total de el escaneo del tráfico de red de la PYME, con el fin de considerar las posibles intrusiones y se expresaran en un rango de 0% a 100%.

Tráfico en la red monitoreado y detectado sin amenazas de intrusión se lo (expresa en porcentaje %)

En esta variable se medirá los casos confirmados los cuales presentan todas las características del caso identificándolos como intrusos en la red los cuales se los expresan en un porcentaje de rango de 0% a 100%.

- Falsos positivos (FP)

Se le denomina falso positivo al análisis y detección de intrusos en la red, con el fin de hacer el escaneo necesario para la penetración de intrusos sospechosos al tráfico de red, escaneando características fundamentales que ayuden a reconocer

al atacante o intruso, con la intención de que la PYME evite tener pérdidas en el desarrollo de su labor.

- Falso negativo (FN)

Sin embargo, el falso negativo, se los denomina a las intrusiones no detectadas pero que ya han vulnerado la seguridad de la PYME, lo cual conlleva a tener un impacto mayor por el hecho de ingresar inadvertido a burlar a los administradores de los recursos de red, con el fin de que el ciberdelincuente se aproveche para arrebatar información importante de dicha organización y en consecuencia realizar algún tipo de daño a la PYME.

- Usabilidad

Como dice la norma ISO 9126 en su primer módulo la usabilidad se define como la capacidad de poder medir un producto de software ejecutado y funcional, el cual debe ser comprendido, aprendido, usado y atractivo para el usuario

- Comprensibilidad del sitio

Principalmente debe ser una interfaz intuitiva, en donde el usuario pueda realizar la configuración de una forma fácil, sin necesidad de conocimientos técnicos.

- Mecanismos de ayuda

En este proceso se le brindara toda la documentación necesaria para el manejo del aplicativo.

2.6 FORMULACIÓN DE HIPOTESIS

2.6.1 Hipótesis De Investigación

Hi: Disminuir los intentos de acceso no autorizado a través de un sistema de detección de intrusos con el fin de mejorar la seguridad en las redes de las PYMES.

2.6.2 Hipótesis Nula

Ho: Al no disminuir los intentos de acceso no autorizado y sin hacer uso de un sistema de detección de intrusos, aumentara la inseguridad en las redes de las PYMES.

2.6.3 Hipótesis Alterna

Ha: Disminuir los intentos de penetración al servidor web aplicando un sistema de defensa, para mejorar la seguridad de la información de las PYMES.

3. METODOLOGÍA

3.1 PARADIGMA

Este proyecto es de tipo positivista porque tiene un enfoque metodológico predominantemente cuantitativo, en donde gracias al uso de las escalas de medición se puede determinar el grado de confidencialidad, integridad y disponibilidad de la información para poder reconocer de manera más objetiva el estado de la seguridad de la información en las PYMES que cuentan con base tecnológica en la región.

3.2 ENFOQUE

Este proyecto estará enfocado de manera cuantitativa debido a que es posible realizar la recopilación de información desde fuentes reales, desde los entornos en los que se desarrollan generando mediciones más exactas de las variables que se tendrán en cuenta.

3.3 MÉTODO

El método de la investigación es científico, puesto que se basa en la búsqueda de la verdad mediante la medición de unos datos cuantificables para tratar y analizar el nivel de amenazas, riesgos y vulnerabilidades que afectan a la seguridad de la información en las PYMES que cuentan con base tecnológica en la región.

3.4 TIPO DE INVESTIGACIÓN

El tipo de investigación es correlacional puesto que la causa del estudio es conocer el comportamiento de la seguridad de la información a causa de las amenazas, riesgos y vulnerabilidades, midiendo el grado de relación que existe entre estas variables.

3.5 DISEÑO DE INVESTIGACIÓN

En la presente investigación se desarrollará un diseño cuasi-experimental dado que, se utiliza un sistema de seguridad de la información para ver el efecto que tienen las amenazas y vulnerabilidades sobre los activos de la información y conocer el nivel de riesgo a los que se ven afectados los activos de información en las PYMES que cuentan con base tecnológica en la región.

GE = P1 X P2
GC = P3 – P2
DONDE:
GE: Grupo experimental (PYMES)
GC: Grupo de control (PYMES)
P1: Pre-prueba (GE)
P2: Pos-prueba (GE)
P3: Pre-prueba (GC)
P4: Pos-prueba (GC)
X: Tratamiento experimental
-: Ausencia de tratamiento

3.6 POBLACIÓN

La población con la que se trabajará en esta investigación estará constituida por las PYMES que cuentan con una base tecnológica, y que se encuentran en el municipio de San Juan de Pasto.

Cabe resaltar que la elección dicha población también se basó en diversos aspectos en pro del alcance del proyecto y el enfoque tecnológico que tiene el mismo. Es por eso por lo que la segmentación de la población se limitó al entorno urbano y posteriormente se escogió las PYMES que cuentan con una base tecnológica.

3.7 MUESTRA

La muestra será de carácter no probabilística por lo que estará integrada por 30 PYMES del municipio de San Juan de Pasto las cuales deberán contar con bases tecnológicas. Esto con el fin de obtener los mejores resultados y poder garantizar la funcionalidad del proyecto.

3.8 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Los procedimientos empleados por el grupo de investigación para la recolección de la información necesaria para la cuantificación de las variables de estudio serán métodos convencionales, entre ellos están: La observación directa, una lista de chequeo y encuestas. Las encuestas estarán dirigidas principalmente a los administradores de tecnología de la PYMES, los cuales podrán su opinión sobre las características y detalles que consideran necesarios a tener en cuenta para ser implementados en la mejora de la seguridad de la PYMES.

3.9 VALIDEZ DE LAS TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

La técnica de recolección de la información es vital en el ámbito cuantitativo, ya que por medio de esta se podrá llegar a un estudio puntual sobre lo que se está desarrollando, por ende se desarrollara un cuestionario con diversos ítems que ayudan a tecnificar el proceso para la implementación, en lo cual también junto al equipo de trabajo se desarrollara la recolección de datos de forma visual en donde se medirá a las PYMES que si cumplan con los requerimientos logísticos y tecnológicos para el desarrollo y ejecución del proyecto.

La técnica de recolección de la información es válida ya que se realiza un juicio de un experto, el cual hará una valoración sobre los ítems que componen dicho cuestionario, así como una valoración global del mismo. El cuestionario contara con el juicio del experto procedente de la Universidad Cesmag: Magister Arturo Eraso Torres.

3.10 CONFIABILIDAD DE LAS TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Los diferentes procesos llevados a cabo para la recolección de la información son confiables puesto que los datos que se obtengan se harán de forma directa con las personas que utilizarán los aplicativos desarrollados en el proyecto. La información que se obtenga no será alterada en ningún momento y se trabajara con ella basados en los lineamientos estipulados en la metodología de desarrollo de software que, seleccionada, apoyados en las correcciones y recomendaciones del asesor y los jurados.

3.11 INTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Los instrumentos de recolección de información como ya se ha descrito en los anteriores apartados serán las encuestas. Se iniciará con una prueba piloto, esto con el fin de evaluar los niveles de seguridad en los que se encuentran las PYMES. Este instrumento se utilizará bajo las condiciones y formatos generados por el equipo de trabajo, para el caso de las encuestas serán diligenciadas por los usuarios administradores de las PYMES y se muestra en la sección de Anexos de este mismo documento. (Ver Anexo 2)

4. RECURSOS DE LA INVESTIGACIÓN

4.1 TALENTO HUMANO

Tabla 1. Talento humano

Tipo	Nombre	Estudios Realizados	Cargo ocupación
Investigadores	Yehison Hammer España Montaño Anderson David Solarte Caicedo	Estudiante de Ingeniería de Sistemas que pertenece a la Universidad CESMAG	Estudiante
Asesor proyecto de Grado	Arturo Eraso Torres	Ingeniero de Sistemas. Mg. Software Libre	Docente Tiempo Completo de la U. CESMAG

Fuente: Propia.

4.2 RECURSOS FÍSICOS

Tabla 2. Recursos Físicos

No.	Detalle	Cantidad
1	Computadores portátiles	2
2	Smartphone	2
3	Impresora	1
4	Memoria USB de 16GB	2
5	Libretas	2
6	Computadora de mesa	1
7	Resma de papel	1
8	Esferos	3

Fuente: Propia.

4.3 PRESUPUESTO

Tabla 3. Presupuesto

Costo Directo				
No.	**Descripción**	**Cantidad**	**Valor Unitario**	**Valor Total**
1	Computadores Portátiles	2	$ 1.800.000	$ 3.600.000
2	Impresora	1	$ 450.000	$ 450.000
2	Tintas	1	$ 30.000	$ 30.000
3	Resma de papel	1	$ 12.000	$ 12.000

Costo Directo				
No.	**Descripción**	**Cantidad**	**Valor Unitario**	**Valor Total**
4	Memoria USB de 16GB	2	$ 24.000	$ 48.000
5	Lapiceros	6	$ 600	$ 3.600
6	Lápiz	4	$ 700	$ 2.800
7	Borrador	2	$ 400	$ 800
8	Honorarios equipo de trabajo basados en el SMLV – Tiempo estimado de trabajo 4 horas diarias por cada integrante del equipo de trabajo Tiempo Total de Desarrollo 9 Meses Valor Hora $8.615 Horario de Trabajo: lunes a sábado	2	$1.654.080	$14.886.720
Subtotal				$ 14.941.920
Costo Indirecto				
No.	**Descripción**	**Cantidad**	**Valor Unitario**	**Valor Total**
10	Internet	2	$ 137.200	$1.234.800
11	Herramienta SNORT	2	$ -	$ -
12	Sistemas GNU/LINUX	2	$ -	$ -
13	Transporte*	2	$ 50.000	$ 1.100.000
Subtotal				$ 2.334.800
Total, Costo Directo + Costo Indirecto				$ 17.276.720
Imprevisto (5%)				$ 863.836
Costo Total				$18.140.556

Fuente: Propia.

* El valor de la mano de obra de los investigadores: el tiempo de duración de la investigación es de 9 meses, cada mes tiene 24 días hábiles, de los cuales se trabajará 4 horas diarias, el valor de la hora es de $8.615.

* Los investigadores cuentan con su propio medio de transporte, el valor que cada investigador gasta mensualmente en la gasolina de sus vehículos es de $25.000 pesos mensuales.

4.4 FINANCIACIÓN

El desarrollo de la investigación será financiado bajo los recursos propios de los investigadores.

4.5 CRONOGRAMA DE GANTT

Tabla 4. Cronograma de GANTT

OBJETIVOS	CRONOGRAMA	2021																																							
		Febrero				Marzo				Abril				Mayo				Junio				Agosto				Septiembre				Noviembre				Diciembre							
	ACTIVIDAD	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
• Analizar los niveles de seguridad y los tipos de ataques que se presentan en las PYMES.	Recolección y análisis de información																																								
	Visitar algunas de las PYMES																																								
	Creacion de encuestas																																								
	Organización y reporte de la información																																								
	Analisis de la información recolectada																																								
	Analisis de la seguridad de las PYMES encuestadas																																								
	Reconocimiento de los tipo de ataques																																								
• Desarrollar un sistema de aislamiento que permita la caracterización de los ataques y mejorar la seguridad de la red.	Planeación del desarrollo del proyecto																																								
	Diseño y Desarrollo del prototipo																																								
	Configuracion del prototipo																																								
• Evaluar el sistema de detección de ataques en PYMES para determinar su eficiencia en cuanto a seguridad de la información.	Pruebas de funcionalidad																																								
	Pruebas de deteccion de los posibles ataques																																								
	Encuestas de satisfaccion																																								
	Garantizar que cumpla con los estandares de seguridad																																								
	Documentación																																								

Fuente: Propia.

BIBLIOGRAFÍA

AGUILERA, SEGURIDAD INFORMATICA, EDITEX, Pozuelo de Alarcón, 2010. Rústica. Condición: New. Estado de la sobrecubierta: Nuevo. 1. N.º de ref. del artículo: 563323[En línea], Libro, Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es&source=gbs_vpt_reviews#v=onepage&q&f=false

ASTUDIILLO PIZARRO, Luis Alberto, Análisis de vulnerabilidades de suplantación en el protocolo TCP/IP e implementación de controles de mitigación, Unidad Académica de Ingeniería Civil, Universidad Técnica de Machala, {En línea} {6 de enero de 2021} Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/12569/1/E-9449_ASTUDILLO%20PIZARRO%20LUIS%20ALBERTO.pdf

AUDITECH, Seguridad Defensiva, {En línea}, {14 de noviembre 2020} disponible en: https://auditech.es/seguridad-defensiva/

AUDITECH, Seguridad Ofensiva, {En línea} {14 de noviembre 2020} disponible en https://auditech.es/seguridad-ofensiva/#:~:text=La%20Seguridad%20Ofensiva%2C%20toma%20como,previas%20a%20un%20ciberataque%20real

AVALOS, Héctor, GÓMEZ, Esteban, Seguridad de la información, generación y mitigación de un ataque de denegación de servicios, Instituto de informática y computación, Universidad Tecnológica Equinoccial. {En línea} Disponible en http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/425/292

BACA Gabriel. Introducción a la seguridad informática. Libro [EN LINEA], Primera edición MEXICO, Publicado [2016], p, 23,31. Disponible en internet: https://books.google.com.co/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=que+es+vulnerabilidad+informatica&ots=0XLu2AtgDs&sig=j9zKGlKwJI7-kF4X-mv_Sdy3G0U&redir_esc=y#v=onepage&q&f=false

BACKTRACK ACADEMY, analizando la seguridad de las redes con Snorby, 2017 Santiago, Chile, [En línea] Articulo, Disponible en: https://backtrackacademy.com/articulo/analizando-la-seguridad-de-la-red-con-snorby

BANCOLOMBIA, Conoce todo sobre las pymes en Colombia, Articulo [Online], Publicado [12 julio 2018], Colombia, p. 1. Disponible en internet: https://www.grupobancolombia.com/wps/portal/negocios/actualizate/legal-y-tributario/todo-sobre-las-pymes-en-colombia

BORGES Esteban, Servidor FTP, Articulo [Online], Publicado [12 febrero 2019], p. 1. Disponible en: https://blog.infranetworking.com/servidor-ftp/

BORGES Santiago, Servidor de Streaming: ¿Qué es y cómo funciona? Articulo [Online], Publicado [21 mayo 2020], p. 1. Disponible en: https://blog.infranetworking.com/servidor-streaming/

BORGES, (2019) Servidores PostgreSQL [En línea] Articulo, Disponible en: https://blog.infranetworking.com/servidor-postgresql/

BUSINESSCOL, Sección pymes, Articulo [Online], Publicado [2020], Colombia P. 1. Disponible en internet: https://www.businesscol.com/empresarial/pymes/#:~:text=En%20Colombia%2C%20seg%C3%BAn%20la%20Ley,no%20superior%20a%2010%20trabajadores.&text=Peque%C3%B1a%20Empresa%3A%20Personal%20entre%2011,salarios%20m%C3%ADnimos%20mensuales%20legales%20vigentes.

CABRERA Robert. ¿Qué es un servidor? Articulo [Online], España, Publicado [junio 27 2019], p. 1. Disponible en internet: https://desafiohosting.com/que-es-un-servidor/

CADAVID NAVARRO Andrés, MARTINEZ FERNANDEZ Juan, VELEZ MORALES Jonathan, Revisión de metodologías agiles para el desarrollo de software, Articulo [Online], Colombia, 2013, Universidad autónoma del caribe, Prospectiva, Vol. 11. P. 3. Disponible en internet: https://www.redalyc.org/pdf/4962/496250736004.pdf

CALLES, Juan Antonio, Wi-Fis: Tipos de ataque y recomendaciones de seguridad, Fujoproject, Artículo, {En línea}. {6 de enero 2020} Disponible en: https://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html

CAMACHO CACERES Nicolás, Sistema de prevención de intrusos (IPS) para un entorno de red SDN, Trabajo de grado [En línea], Publicado [2016] Colombia-Bogotá Pontificia universidad javeriana, p. 19. Disponible en internet: https://repository.javeriana.edu.co/bitstream/handle/10554/21421/CamachoCaceresNicolasAlfonso2016.pdf?sequence=1

CARATE PILATUÑA Bryan, POZO MENDOZA Diego, Ingeniería de sistemas, diseño de un sistema de detección de intrusos (NIDS) para una red simulada pymes en gns3, implementada en un módulo Raspberry pi portátil en 2019, Quito, Ecuador, Universidad politécnica salesiana sede Quito [En línea] Tesis Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf

CARDONA Omar, La necesidad de repensar de manera holística los conceptos de vulnerabilidad y riesgo" una crítica revisión necesaria para la gestión" Bogotá, Colombia, 2017, Universidad de los andes [En línea]Repositorio, Disponible en https://repositorio.gestiondelriesgo.gov.co/bitstream/handle/20.500.11762/19852/VulnerabilidadRiesgoHolistico%28Cardona_2002%29.pdf?sequence=1&isAllowed=y

CARDONA, Evaluación de la amenaza la vulnerabilidad y el riesgo, cambia, 2012, [En línea] libro online, Disponible en: http://www.planesmojana.com/documentos/estudios/19.Evaluacion%20de%20la%20amenaza,%20la%20Vulnerabilidad%20y%20el%20riesgo.pdf

CARDONA, Omar Darío, disponible http://www.planesmojana.com/documentos/estudios/19.Evaluacion%20de%20la%20amenaza,%20la%20Vulnerabilidad%20y%20el%20riesgo.pdf

CARPENTIER, Jean-François, La Seguridad Informática en la PYME: Situación actual y mejores prácticas, ediciones ENI, 2016

CISCO SAFE, Un modelo de seguridad para las redes de las empresas, Articulo [Online], p. 28. Disponible en internet: https://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf

COMER, Douglas, Libro, Interligacao de Redes com TCP/IP: Principios, Protocolos e Arquitectura, Volumen1, Editorial Elsevier Brasil, 2016

COMPAÑÍA HORNETSECURITY, Seguridad informática, Madrid España, 2020 [En línea], Articulo, Disponible en: https://www.hornetsecurity.com/es/knowledge-base/seguridad-informatica/

CORDOBA SUARES Alba, Diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma iso/iec 27001, PASTO, COLOMBIA, 2015,

CORTES David, Firewalls de nueva generación: la seguridad informática vanguardista. Trabajo de grado [En línea], Colombia, publicado en [2016 09 06], Universidad piloto de Colombia, p. 1. Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2719/Trabajo%20de%20grado3329.pdf?sequence=1&isAllowed=y

COSTAIN Sylvia y ROSO Carlos, Ministerio de las Tecnologías de la Información y las Comunicaciones Articulo [Online], Bogotá D.C publicado [octubre 2018], p. 2, Disponible en internet: https://www.mincit.gov.co/temas-interes/documentos/guia-para-la-administracion-del-riesgo-y-el-diseno.aspx

CUNHA BARBOSA Daniel, Que es un servidor proxy y para sirve, Articulo [En línea], Publicado [enero 2 2020], p. 1. Disponible en internet: https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

DE LA ROSA PINEÑO Javier, Ciberseguridad en pymes, trabajo fin de grado, Valladolid, 2019, Universidad de Valladolid [En línea], Tesis, Disponible en: https://uvadoc.uva.es/bitstream/handle/10324/38735/TFG-J-108.pdf?sequence=1&isAllowed=y

DE SOUSA Iván, ¿Para qué sirve un servidor web y para qué sirve internet? Articulo [Online], Publicado [14 junio 2019], p. 1. Disponible en internet: https://rockcontent.com/es/blog/que-es-un-servidor/

DETECTION SYSTEMS EXPLAINED: 13 best ids software tools reviewed, presenta informe detección de ataques, E.E.U.U, 2020[En línea] Articulo, Disponible en: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

DIGITAL GUIDE IONOS, MAC Spoofing: qué es y cuándo se utiliza, {En línea}. {6 de enero 2021}. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-mac-spoofing/

DIGITAL Guide, ¿Qué es el modelo en V?, Articulo [Online], publicado [23 junio 2020], p.1. Disponible en internet: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/modelo-v/#:~:text=La%20%E2%80%9CV%E2%80%9D%20del%20nombre%20del,de%20calidad%20de%20cada%20fase.

ESTRADA CORONA, Adrián, Protocolos TCP/IP de Internet, Revista Digital Universitaria, Volumen 5, 10 de septiembre de 2004, Disponible en: http://www.ru.tic.unam.mx/bitstream/handle/123456789/791/220.pdf?sequence=1&isAllowed=y

FARIÑO Galo, Modelo espiral de un proyecto de desarrollo de software, Articulo [Online], 2011, Ecuador, Universidad estatal de milagro, p. 3. Disponible en internet: http://www.ojovisual.net/galofarino/modeloespiral.pdf

FERNÁNDEZ BARCELL Manuel, Protocolo TCP/IIP, Grado en gestión y administración pública, Redes de datos, Departamento de Ingeniería Informática, Facultad de Ciencias sociales y de la comunicación, Universidad de Cádiz. {En línea}. Disponible en: https://rodin.uca.es/xmlui/bitstream/handle/10498/16833/temaIII_tcpip.pdf

FERNANDEZ Yúbal, VirtualBox: Qué es y cómo usarlo para crear una máquina virtual con Windows u otro sistema operativo, Articulo [Online], Publicado [1 junio 2020], p. 1. Disponible en internet: https://www.xataka.com/basics/virtualbox-que-como-usarlo-para-crear-maquina-virtual-windows-u-otro-sistema-operativo

FLOREZ GUERRERO Iván, Sistema de Detección de Ataques Informáticos a Redes de Datos Empresariales Soportado en Honeypots, Cartagena De Indias, Colombia, 2018, Universidad de Cartagena facultad de ingeniería programa de ingeniería de sistemas, [En línea], Tesis Disponible en: http://repositorio.unicartagena.edu.co/bitstream/handle/11227/8498/TESIS%20FLOREZ-%20MANQUINTANA.pdf?sequence=1&isAllowed=y

FLOREZ Vicente, revista innovación seguridad, Análisis y tendencias seguridad informática, ciberseguridad, informática, vulnerabilidad, amenaza, Florida Argentina [En línea] Articulo, Disponible en: https://revistainnovacion.com/nota/10697/6_claves_para_garantizar_una_red_informatica_segura/

GARCIA Omar, Modelo de prototipos, Articulo [Online], Publicado [2 septiembre 2013], p. 1. Disponible en internet: https://www.proyectum.com/sistema/blog/modelo-de-prototipos/

GERVILLA RIVAS, Carles, Metodología para un análisis forense, Trabajo de Final de Máster, Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC), Universitat Oberta de Catalunya INCIBE (Instituto Nacional de Ciberseguridad) (INTECO) {En línea} {5 de enero 2021} Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

GOMES VIETES Álvaro, Enciclopedia de la Seguridad Informática. 2da Edición, Grupo editorial RA-MA, 2011

GÓMEZ BALLESTER, Eva, MARTÍNEZ BARCO, Patricio, MOREDA POZO, Paloma, SUÁREZ CUETO Armando, GUTIÉRREZ DIAZ Alejandro, Bases de datos, centro cultural ITACA S.C, Morelos México, 2017, {En línea}. {20 mayo de 2019} Disponible en: https://www.aiu.edu/cursos/base%20de%20datos/pdf%20leccion%201/lecci%C3%B3n%201.pdf

GOMEZ Eva, MARTINEZ Patricio, MOREDA Paloma, ARMANDO Suares, MONTOYA Andrés y SAQUETE Estela, Bases de datos 1, Trabajo investigación [En línea], Publicado [2007], España, Universidad de alicate, p. 14. Disponible en internet: https://rua.ua.es/dspace/bitstream/10045/2990/1/ApuntesBD1.pdf

GOMEZ VIEITES, Álvaro, Tipos de ataques e intrusos en las redes informáticas, Resumen de la ponencia. {En línea} {6 de enero de 2021} Disponible en: https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

GOMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática 2da Edición. 2017

GOMEZ,A, Enciclopedia de la Seguridad Informática. 2ª edición,, EDITORIAL Y PUBLICACION, MADRID, ESPAÑA, TRANFORMADO EN LIBRO ELECTRONICO EN 2017,[EN LINEA]LIBRO, DISPONIBLE EN: https://books.google.com.co/books?hl=es&lr=&id=Bq8-DwAAQBAJ&oi=fnd&pg=PT2&dq=seguridad+inform%C3%A1tica+&ots=dxk30kWedJ&sig=1d9KTCTUSfAGZ8yXbqDkDq0eHIY&redir_esc=y#v=onepage&q=seguridad%20inform%C3%A1tica&f=false

GONZALES GOMEZ Diego, Historia de sistemas de detección de intrusiones, Articulo [Online] Publicado 2003, p.19. Disponible en internet: https://dgonzalez.net/papers/ids/ids_v1.0.pdf

GONZALES, D, Sistemas detección de intrusos, 2003, COPYRIGHT(C) documento licenciado versión 1.2 [EN LINEA] ARTICULO Disponible en: https://dgonzalez.net/papers/ids/ids_v1.0.pdf GRUPO PTM, Metodología tradicional, Articulo [Online], Publicado [30 mayo 2019], P. 1. Disponible en internet: https://pmtgrupoeafit.wixsite.com/gestion-proyectos/post/metodolog%C3%ADa-tradicional

GUERRERO ANGULO Yesid, Ingeniería de sistemas y telemática de la universidad de Nariño soportada en los estándares materia e iso/iec 27001 y 27002/2013, PASTO, 2020, Universidad nacional abierta y a distancia especialización en seguridad informática, Diseño del Sistema de Gestión de Seguridad de la Información para la Unidad de Informática [En línea] Tesis Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31718/ycguerreroa.pdf?sequence=1&isAllowed=y

HAZARD Kevin, IBM, Servidores en la nube, Articulo [Online], Publicado [2020], p. 1. Disponible en https://www.ibm.com/co-es/cloud/learn/what-is-a-cloud-server#:~:text=Un%20servidor%20de%20la%20nube,metal)%20en%20varios%20servidores%20virtuales.

HERNANDEZ MENDOSA Adán, Implementación de un sistema de detección de intrusos basado en la herramienta snort, Ciudad de México, 2018 [En Línea]Tesis, http://dspace.utb.edu.ec/bitstream/handle/49000/7629/ARRICIAGA%20DUMES.pdf?sequence=1&isAllowed=y

Instituto politécnico nacional, escuela superior de ingeniería mecánica y eléctrica unidad profesional “Adolfo López mateos” zacatecano DISPONIBLE EN: https://148.204.103.62/bitstream/handle/123456789/28093/tesis_final.pdf?sequence=1&isAllowed=y

JUÁREZ, Jaime, Seguridad Informática, Principios de Seguridad Informática {En línea}, {11 de enero 2021} Disponible en: https://sites.google.com/site/seguridadinformatica052015/principios-de-seguridad-informatica.

LARA GALICIA Fernando, Servidor de correo electrónico, ¿cómo funciona? Articulo [Online], Publicado [12 junio 2020], p. 1. Disponible en internet: https://co.godaddy.com/blog/servidor-de-correo-electronico-como-funciona/

LARA GALICIA, Fernando Paul, ¿Que es seguridad en la Web? Manual Básico, 2020 Disponible en: https://co.godaddy.com/blog/que-es-seguridad-en-la-web-manual-basico/

LEACOCK Sheyla, Analizando la seguridad de la red con SNORBY, Articulo [Online], Chile, Publicado [26 noviembre 2018], p. 1. Disponible en internet: https://backtrackacademy.com/articulo/analizando-la-seguridad-de-la-red-con-snorby

LICENCIATURA EN RR. HH, Encuesta, tipos y procedimiento de uso en investigación de mercados, Universidad de Champagnat, 2003, Argentina, En línea. {28 de mayo de 2019} disponible en: https://www.gestiopolis.com/encuesta-tipos-y-procedimiento-de-uso-en-investigacion-de-mercados

MACHA MORENO Erika, Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del PERÚ, 2016 [En línea], Tesis, Disponible en: http://repositorio.usil.edu.pe/bitstream/USIL/2810/1/2017_Inoguchi_Gestion-de-la-ciberseguridad.pdf

MARIDUEÑA CARRION Nora, La importancia de los IPS y BYOD en las organizaciones: Caso de estudio CONFIDENCIAL S.A, Articulo [Online], Publicado [2016], Ecuador-Samborondón, UEES Universidad espíritu santo, p. 5. Disponible en internet: http://201.159.223.2/bitstream/123456789/1436/1/Tesis%20Nora%20Mariduena_Final.pdf

MARKER Graciela, Servidor de impresión ¿Qué es? ¿para qué sirve?, Articulo [Online], Publicado [17 julio 2020], p. 1. Disponible en internet: https://www.tecnologia-informatica.com/servidor-impresion/

MEDINA ROJAS Jhonatan Deyvi, RIVAS MONTALVO Yonathan Yajanovic, Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos, 2019, {En línea} {16 de noviembre 2020} Disponible en http://repositorio.unprg.edu.pe/handle/UNPRG/8074

MENDEZ Luis, Que es un servidor DNS y como solucionar problemas habituales Articulo [Online], Publicado [22 febrero 2019], p. 1. Disponible en internet: https://www.webempresa.com/blog/servidor-dns-como-solucionar-problemas-habituales.html

MONTAÑO Erika, Evaluación de las vulnerabilidades que presentan los firewalls en la empresa datasolution s.a. Tesis [En línea], Ecuador-Guayaquil, Publicado [2011], Universidad De Guayaquil, p. 45. Disponible en internet: http://repositorio.ug.edu.ec/bitstream/redug/6743/1/Tesis%20Completa%20-342-2011.pdf

MONTOYO GUIJARRO, Andrés, SAQUETE BORO, Estela, Bases de Datos 1, Alicante España, 2007, Universidad de Alicante, {En línea}. {28 agosto de 2020} disponible en: https://rua.ua.es/dspace/bitstream/10045/2990/1/ApuntesBD1.pdf

NIÑO WILCHES Yamith, Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo PYMES, Bogota,2015, Universidad militar granada facultad de ciencias económicas maestría en gestión de organizaciones, [En línea], Tesis, Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7325/Importancia%20de;jsessionid=2ACAE82957D417722656D7C2C99A80B1?sequence=1

OCAMPO Carlos, CASTRO BERMUDEZ Yanci y SOLARTE MARTINEZ Guillermo, Intrusión detection system in corporate networks, Articulo [Online], Colombia-Pereira, Publicado [2017], Vol. 22, Universidad tecnológica de Pereira, p. 60. Disponible en internet: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/9105

ORTEGA, Openwebinars, que es snort, España, 2018, [En línea] Articulo, Disponible en: https://openwebinars.net/blog/que-es-snort/

ORTEGO DELGADO Daniel, Qué es Snort: Primeros pasos, Articulo [Online], Publicado [21 marzo 2017], p. 1 Disponible en internet: https://openwebinars.net/blog/que-es-snort/

ORTIZ Ángel. Amenaza informática ¿Qué es? ¿Cómo contenerla? Articulo [Online], Publicado [13 julio 2020], p. 1, Disponible en internet: https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/

ORTIZ, Ángel Eulises, ¿Cuáles son los tres pilares de la seguridad informática?, Seguridad Web, HostDimeBlog Premier Global Data Centers {En línea}, {14 de julio 2020} Disponible en: https://www.hostdime.com.pe/blog/cuales-son-los-tres-pilares-de-la-seguridad-informatica/

PABÓN Elías, Metodología de desarrollo tradicional RUP, Articulo [Online], Publicado [31 julio 2018], p. Disponible en internet: https://smartsoftcolombia.com/portal/index.php/blog/49-rup#:~:text=La%20metodolog%C3%ADa%20de%20desarrollo%20RUP,de%20sistemas%20orientados%20a%20objetos.

PELÁEZ SILES, Raúl, Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados, Análisis de seguridad de TCP/IP Edición 1 junio 2002 {En línea} Disponible en: http://ftp.nluug.nl/ftp/pub/os/Linux/doc/LuCaS/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf

PEÑA Rodrigo, RODRIGUEZ Álvaro, Implementación en un dispositivo hardware de un sistema de detección de intrusos basados en red, Trabajo de grado [En línea], 2019, Madrid: Universidad Complutense De Madrid, p. 19. Disponible en internet: https://eprints.ucm.es/56504/1/1138534699-355685_RODRIGO_LAGARTERA_PE%C3%91A_Implementaci%C3%B3n_en_un_dispositivo_hardware_de_un_sistema_de_detecci%C3%B3n_de_intrusos_basado_en_red_3940146_794802335.pdf

PEREZ Maribel y JURADO Mario, Diseño de un sistema de gestión de seguridad de la información para la ferretería argentina de la ciudad de pasto, Pasto,2018, [EN LINEA] TESIS Disponible En https://repository.unad.edu.co/bitstream/handle/10596/18306/1087414445.pdf?sequence=1&isAllowed=y

PINEDA Angelica y PEÑARANDA Carlos, Bases de datos estáticas, Presentación [Online], Publicado [3 octubre 2016], p. 3. Disponible en internet: https://prezi.com/rhdgiuon8_rq/base-de-datos-estatica/

PULIDO RODRIGUEZ Carlos, Diseño de un sistema de gestión de seguridad de la información para las áreas administrativa y académica de la institución system plus pasto ltda., basado en el estándar internacional iso/iec 27001:2013, PASTO,2015, Universidad nacional abierta y a distancia – UNAD escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática Pasto - Colombia, [En línea] Tesis Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/6340/98396710.pdf?sequence=1&isAllowed=y

QUIJANO VODNIZA Armando José, Guía de investigación cuantitativa, Colombia, 2009, {En línea}. {27 agosto de 2020} disponible en: https://docplayer.es/93087679-Guia-de-investigacion-cuantitativa.html

QUIROZ Silvia, MACIAS David. Seguridad informática: condiciones Articulo {En línea}, Publicado [26 agosto 2017], p. 25. Disponible en internet: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

QUIROZ Silvia, MACIAS David. Seguridad informática: condiciones. Articulo [Online], Publicado [26 agosto 2017], p. 2,5. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

RAMIRO Ruben, Reglas SNORT, detección de intrusos y uso no autorizado, Articulo [Online], Publicado [22 noviembre 2020], p. 1, Disponible en internet: https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/

REBOLLEDO Miguel, Definición y tipo de ordenadores. Articulo [Online], España, Publicado [2011], Universidad Politécnica De Valencia p. 3. Disponible en internet: https://riunet.upv.es/handle/10251/10787

REDATOR, Tipos de bases de datos, Articulo [En línea], Publicado [25 enero 2019], p.1. Disponible en internet: https://rockcontent.com/es/blog/tipos-de-base-de-datos/

RIBERA Gersson, Seguridad informática, Libro [En línea], 2020, Colombia, p. 3. Disponible en internet: https://infosegur.wordpress.com/

RISTI, REVISTA IBERICASISTEMAS Y TECNOLOGIA, Selección de indicadores para la implementación de un IDS en PYMES, Cauca, Colombia,2020[En línea] Articulo, Disponible en: https://search.proquest.com/openview/ddddee94d23b4c4a6d43646933893d01/1?pq-origsite=gscholar&cbl=1006393

RIVERO PEREZ Jorge y RODRIGUEZ Carlos, Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras, Articulo [Online], Publicado [2014], Cuba, Universidad de Cienfuegos, p. 1. Disponible en internet: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992014000400003

ROSETY MOLINS Blanca, Diseño de prototipo de defensa para mitigación de ataques DDOS para PYMES, Cartagena, 2016 [En línea], Universidad internacional del rioja unir master universitario en seguridad informática, Tesis, Disponible: en: https://reunir.unir.net/bitstream/handle/123456789/4454/ROSETY%20MOLINS%2C%20BLANCA.pdf?sequence=1&isAllowed=y

RUIZ Francisco, Servidor de archivos en la empresa, alternativas actuales, Articulo [Online] Publicado [20 noviembre 2019], p. 1. Disponible en internet: https://blog.dataprius.com/index.php/2019/11/20/servidor-de-archivos-en-la-empresa-alternativas-actuales/

Tecno Mental, Seguridad Informática, Tipos de seguridad informática, {En línea}, {5 de enero 2021} Disponible en: https://www.tecnomental.com/seguridad-informatica/tipos-de-seguridad-informatica/

TELEFONICA, Claves para Proteger la Información de la PYME este 2020, COLOMBIA,2020, [En línea], Articulo Disponible en: https://blog.acens.com/notas-prensa/20-claves-proteger-informacion-pyme-2020/

TIC TAC, El TicTac presenta su informe: Tendencias del Cibercrimen en Colombia; primer trimestre de 2020, COLOMBIA, 2020 [En línea] Informe Disponible en: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

TOLOSA, Gabriel, Protocolos y Modelos OSI, Disponible en: https://sistemamid.com/panel/uploads/biblioteca/2017-08-04_09-52-51141670.pdf
UNIVERSIDAD BARCELONA," obs" tendencia & innovación, tipos de seguridad informática más importante a conocer y tener en cuenta, Barcelona, España, 2020
Universidad cesmag facultad de ingeniería de sistemas línea de investigación, Seguridad de la Información, Pasto, Colombia, 2020, [En línea] Informe Disponible en: https://www.unicesmag.edu.co/

UNIVERSIDAD Internacional de Valencia, Ciencia y Tecnología, Tres tipos de seguridad informática que debes conocer, {En línea} {28 de diciembre 2020} Disponible en: https://www.universidadviu.com/int/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer

UNIVERSIDAD INTERNACIONAL DE VALENCIA, Que es la seguridad informática y como puede ayudarme, Valencia, España, 2018 ciencia y tecnología, Articulo [En línea] Disponible en: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Universidad nacional abierta y distancia "UNAD" facultad de ciencias básicas e ingeniería especialización en seguridad informática, [En línea], Tesis Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3627/1/59650050.pdf

UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO, Diseño de un sistema de detección de intrusos (NIDS)para una red simulada pymes en hns3, implementada en un módulo Raspberry Pi Portátil, Quito Ecuador,2019[En línea] Trabajo de grado, Disponible En: HTTPS://DSPACE.UPS.EDU.EC/BITSTREAM/123456789/17546/1/UPS%20-%20ST004141.PDF

VELAZCO Rubén, Conviértete en un hacker ético con Kali Linux, Articulo [Online], publicado [3 marzo 2020], p. 1. Disponible en internet: https://www.softzone.es/programas/linux/kali-linux/

VILA Juan, La metodología XP: la metodología de desarrollo de software más exitosa, Articulo [Online], Publicado [8 julio 2016], p. 1. Disponible en internet: https://proagilist.es/blog/agilidad-y-gestion-agil/agile-scrum/la-metodologia-xp/

ANEXOS

Anexo 1. Carta al asesor

San Juan de Pasto, 20 de Enero de 2021

SEÑORES:
COMITÉ CURRICULAR
PROGRAMA DE INGENIERIA DE SISTEMAS

Asunto: Visto bueno de la propuesta de investigación

Saludo de Paz y Bien.

Yo, Arturo Eraso Torres identificado con cédula de ciudadanía Nro. 98381704, expreso que revise el documento denominado "SISTEMA DE DETECCIÓN DE INTRUSOS APLICADO A REDES DE PYMES" presentado por los estudiantes, YEHISON HAMMER ESPAÑA MONTAÑO y ANDERSON DAVID SOLARTE CAICEDO, de octavo semestre y doy el visto bueno,

Agradeciendo su atención.

Atentamente,

ARTURO ERASO TORRES

Mg. Software Libre

Anexo 2. Encuesta

UNIVERSIDAD CESMAG
FACULTAD INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO

ENCUESTA DIRIGIDA A LAS PYMES CON EL FIN DE MEDIR EL NIVEL DE SEGURIDAD CON QUE CUENTAN.

Objetivo: Conocer las vulnerabilidades y poder contribuir a su mejora.
Instrucciones.

Por favor, le solicitamos marcar una sola respuesta cuando sea necesario y llenar los espacios en blanco cuando así se requiera.

Esta encuesta dura aproximadamente 5 minutos:

Basándose en su propia experiencia:

1. ¿Qué función desempeña en la empresa?
   _____
2. ¿Cuánto tiempo lleva trabajando en la empresa?
   a. Menos de un año
   b. De 1 año a 2
   c. De 2 a 4 años
   d. De 4 a 6 años
   e. 6 años o mas
3. ¿Cuántos computadores cuenta en la red de la empresa?
   a. De 1 a 3
   b. De 3 a 5
   c. De 5 a 8
   d. De 8 a 12
   e. Más de 12

4. ¿Cuenta con un departamento o encargado de seguridad informática?
    a. Si
    b. No
5. Con cuales de los siguientes dispositivos cuenta en la empresa:
    a. Routers
    b. Switchs
    c. Repetidores
    d. Puentes
    e. Otros

    ¿Cuál? _____
6. ¿Qué servicios de red se maneja en la organización?
    a. Protocolo de trasferencia de hipertexto(HTTP)
    b. Protocolo seguro de transferencia de hipertextos(HTTPS)
    c. Protocolo de correo (SMTP)
    d. Protocolo de configuración dinámica de host (DHCP)
    e. Protocolo de trasferencia de archivos (FTP)
    f. Protocolo simple de administración de red (SNMP)
    g. Secure Shell (SSH)
    h. Telnet
    i. Otros

    ¿Cuál? _____
7. ¿Quién es responsable de instalar y mantener el software de seguridad en los equipos de la Pyme?
    a. Empleados
    b. Administrador
    c. Personal de TI
    d. No hay Responsable
8. ¿Tiene software antivirus instalado en tu computadora?
    a. Sí
    b. No
    c. No sé
9. Considera que han tenido problemas de seguridad donde se vea comprometida la información de la empresa o usuarios en los últimos años.
    a. Si
    b. No
10. Se realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
    a. Si
    b. No
    c. No lo se

11. Tiene proyectado invertir en seguridad informática en los siguientes
    a. 3 meses
    b. 6 meses
    c. 1 año
    d. 2 años
    e. Más de 2 años
12. ¿Cuenta con firewall en su red?
    a. Si
    b. No
13. ¿Tiene implementado algún tipo de solución o mecanismos de seguridad?
    a. Si
    b. No
    ¿Cual? _____
14. Su empresa ha sido víctima o a sufrido algún tipo de ataque informático
    a. Si
    b. No
    ¿Cuál? _____
15. Tiene algún conocimiento de los IDS o IPS
    a. Si
    b. No
    ¿Cuál? _____

Gracias por su colaboración