DOI: https://doi.org/10.23857/dc.v9i3.3463

Ciencias Técnicas y Aplicadas
Artículo de Investigación

Análisis de mecanismos de Autenticación, Autorización y Contabilización para mejorar la seguridad en entornos empresariales

Analysis of Authentication, Authorization and Accounting mechanisms to improve security in business environments

Análise de mecanismos de Autenticação, Autorização e Contabilidade para melhorar a segurança em ambientes de negócios

María Rosa Pazmiño Muñoz [I]
maria.pazmino@espam.edu.ec
https://orcid.org/0009-0009-1846-4122

Jessica Johanna Morales Carrillo [II]
jmorales@espam.edu.ec
https://orcid.org/0000-0002-8986-744

Correspondencia: maria.pazmino@espam.edu.ec

*__Recibido:__ 29 de mayo de 2023 *__Aceptado:__ 12 de junio de 2023 * __Publicado:__ 24 de julio de 2023

I. Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta, Ecuador.
II. Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta, Ecuador.

Resumen

En esta investigación realizada se busca analizar los mecanismos de los protocolos AAA, que corresponden al acróstico en el idioma inglés Authentication (autenticación), Authorization (autorización) y Accounting (contabilización), estos procesos en los ámbitos empresariales despliegan sistemas de seguridad distribuidos que dan mayor seguridad en áreas de redes y de servicios de red frente a los accesos no autorizados. Esto ayuda a dar mayor garantía en el control de los usuarios que se conectan a dicha red y así con el tiempo tener una mejor auditoria de las actividades realizadas por los usuarios que han ingresado a la red. Los mecanismos AAA fueron diseñados para resolver estos tipos de problemas, ya que en muchas empresas no contaban con un control en los accesos de los usuarios con respectos a los activos conectados a la red y los usuarios no autorizados tenían un fácil acceso. De acuerdo a la revisión sistemática que se realizó se permitió conocer los canales que se requiere mayor, permitiendo dar soluciones a las vulnerabilidades que pueden darse dentro de los entornos empresariales.

Palabras Claves: Seguridad Informática; Mecanismos AAA.

Abstract

This research carried out seeks to analyze the mechanisms of the AAA protocols, which correspond to the acrostic in the English language Authentication (authentication), Authorization (authorization) and Accounting (accounting), these processes in business fields deploy distributed security systems that provide greater security in areas of networks and network services against unauthorized access. This helps to give greater guarantee in the control of the users who connect to said network and thus, over time, have a better audit of the activities carried out by the users who have entered the network. The AAA mechanisms were designed to solve these types of problems, since in many companies they did not have control over user access to assets connected to the network and unauthorized users had easy access. According to the systematic review that was carried out, it was possible to know the channels that are most required, allowing solutions to the vulnerabilities that can occur within business environments.

Keywords: Informatic security; AAA mechanisms.

Resumo

Esta pesquisa realizada busca analisar os mecanismos dos protocolos AAA, que correspondem ao acróstico na língua inglesa Authentication (autenticação), Authorization (autorização) e Accounting (contabilidade), esses processos nas áreas empresariais implantam sistemas de segurança distribuídos que proporcionam maior segurança em áreas de redes e serviços de rede contra acessos não autorizados. Isso ajuda a dar maior garantia no controle dos usuários que se conectam à referida rede e assim, ao longo do tempo, ter uma melhor auditoria das atividades realizadas pelos usuários que entraram na rede. Os mecanismos AAA foram pensados para solucionar esses tipos de problemas, pois em muitas empresas não havia controle sobre o acesso dos usuários aos ativos conectados à rede e usuários não autorizados tinham facilidade de acesso. De acordo com a revisão sistemática realizada, foi possível conhecer os canais mais requisitados, permitindo soluções para as vulnerabilidades que podem ocorrer dentro dos ambientes empresariais.

Palavras-chave: Segurança informática; Mecanismos AAA.

Introducción

Cuando decimos mecanismos de seguridad tratamos de los métodos que se usan para la transmisión y a la vez la transportación de la información que esta sea segura, una de las mejores maneras de realizar estos procesos es usando los protocolos AAA, primero se consigue la autenticación mediante una propuesta de identidad (nombre de usuario) y a su vez con la demostración de sus credenciales (contraseñas), segundo se autoriza una vez concedido los privilegios a usuarios o entidades todo esto se basa mediante su identidad ya autenticada, y como ultimo tenemos la contabilización que lleva un control del consumo de los recursos, por lo cual se da a conocer el uso de estos mecanismos AAA con la finalidad de tener una mejor seguridad en entornos empresariales. (Shashi Bhushan, Manoj Kumar, Pramod Kumar, 2022).

La tecnología ha avanzado tan rápido en los últimos 20 años que los temas de seguridad informática parecen haber pasado desapercibidos. Cualquier debilidad en una aplicación, sensor o infraestructura tecnológica deriva en un riesgo de ciberataque (Briceño, 2020), la autenticación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario ya que la autenticación no siempre está relacionada con estos (Romero, Figueroa, Vera, Alava, Parrales, Alava, Murillo, Castillo, 2018). En la mayoría de los escenarios, el objetivo del ataque no está al alcance o visible; es decir, hay barreras o etapas que hay que superar para alcanzar el objetivo

principal. Para ello, hay que determinar medidas de acceso y superar estos obstáculos (Fabia Cuzme-Rodriguez, Marcelo Leon-Gudiño, Luis Suarez-Zambrano, Mauricio Dominguez-Limaico, 2019).

Cuando se habla de seguridad de sistemas informáticos, las amenazas pueden materializarse por elementos externos como ataques o catástrofes físicas, como vandalismo, robos, incendios, pueden ser cuestiones derivadas del mal uso por parte de los usuarios de los recursos que la organización pone a su disposición (Abad, Cañarte, Villamarin, Mezones, Delgado, Toala, Figueroa, Romero Castro, 2019).No solo se debe prestar atención a los ataques intencionales, sino también a posibles fallas de software o hardware que atenten contra la seguridad, tratando de minimizar los riesgos asociados al acceso y utilización de un determinado sistema de forma no autorizada o malintencionada, para revelar, utilizar, modificar o destruir accidental o intencionalmente la información que en este se encuentre (Bracho, Cuzme, Pupiales, Suarez, Peluffo, Moreira, 2017).

Un mecanismo de identificación se expresa como yo soy el nombre de usuario XXX, tecleando una contraseña. Por otra parte, un mecanismo de contabilidad registra las acciones del usuario autorizado (Bertolin, 2019). Un concepto importante cuando discutimos los controles administrativos es la capacidad de exigir su cumplimiento. Si no tenemos la autoridad o la capacidad para garantizar que se cumplan nuestros controles, son peores que inútiles, porque crean una falsa sensación de seguridad (Briceño, 2021).

Es un requisito que se admitan métodos de autenticación alternativos con diferentes tipos de credenciales, con el objetivo de dispositivos IoT en escenarios de implementación aislados (Chandramouli, Liebhart, Pirskanen, 2019).

Los mecanismos AAA actuales asumen un único punto de consolidación para la identidad, la decisión de política y la aplicación, junto con un único mecanismo de contabilidad. A pesar de usar técnicas de separación estrictas, es posible que no sea posible una operación exitosa sin interrumpir algunas de las mejoras prometidas de NFV con respecto a la agilidad, la escalabilidad y la resiliencia. (Sabella, Irons-Mclean, Yannuzzi, 2022). Conjuntamente con la seguridad, contabilidad/registro significa el registro de las cantidades de eventos y operaciones, y el almacenamiento de información sobre ellos. En términos de seguridad, la importancia de los datos contables radica en su disponibilidad sustentando la confianza y el cumplimiento. Los registros son fuentes de información centrales para el sistema común y el análisis de fallas (Wang, Ranjan, Chen, 2017).

Es común hablar de seguridad informática y de seguridad de la información, como si fueran el mismo termino, y a primera vista, parecería ser. Sobre todo, si se tiene en cuenta que, en la actualidad, gracias

al constante desarrollo tecnológico, se tiende a digitalizar todo tipo de información y a manejarla a través de un sistema informático. (Bracho-Ortega, Cuzme-Rodríguez, Pupiales-Yépez, Suárez-Zambrano, Peluffo-Ordóñez, Moreira-Zambrano, 2017). El código de autenticación de mensajes hash utiliza el mecanismo de hashing, pero lo eleva un poco. En lugar de usar un hash que cualquiera puede calcular, incluye en su cálculo una clave secreta de algún tipo. (Santos, 2020). Aunque normalmente se hace referencia a AAA en relación con los sistemas de autenticación, en realidad es un concepto fundamental para la seguridad. La falta de cualquiera de estos cinco elementos puede resultar en un mecanismo de seguridad incompleto. Las siguientes secciones analizan la identificación, la autenticación, la autorización, la auditoría y la rendición de cuentas. (Chapple, Stewart, Gibson, 2018).

Los mecanismos de autenticación, autorización y contabilidad ya existentes se pueden utilizar para la autenticar la identidad de las aplicaciones SDN y las diversas entidades de red, los permisos y el comportamiento de las aplicaciones y las entidades de la red se puede recopilar desde el servidor AAA, IDS, Firewalls, etc. Y procesados para obtener la puntuación de confianza en tiempo real. Cualquier incidente de seguridad o una brecha también puede afectar el puntaje de confianza. (Bhushan, Kumar, Kumar,2022).

El control de acceso a la red y sus recursos consta de tres mejores elementos: autenticación, autorización y contabilidad. Juntos, este marco se abrevia como AAA (autenticación, autorización y contabilidad) y se pronuncia triple A. Ocasionalmente, verá el acrónimo AAAA (autenticación, autorización, contabilidad y auditoría) para enfatizar aún más los estándares de monitoreo y seguridad involucrados en estos procesos; sin embargo, la mayoría de los profesionales de seguridad de TI envuelven la auditoría en la contabilidad y, por lo tanto, usan el acrónimo AAA (West, 2021). Aunque son diseños de ruta corta, el retraso de transmisión durante la autenticación sigue siendo grande y puede reducirse porque hay más de un salto involucrado en el procedimiento. (Dartmann, Song, Schmeink, 2019).

Materiales y Métodos

En el desarrollo de la investigación se empleó la Revisión Sistemática de Literatura permitiendo la búsqueda, clasificación y análisis de la información recopilada.

Definición para la búsqueda

El proceso se inició con definir los diferentes criterios de búsqueda considerando la relación que exista entre los artículos analizados con el estudio de la seguridad informática y los mecanismos AAA para la seguridad de entornos empresariales, efectuado la búsqueda en plataformas como Google Académico, Springer y Scielo; se consideró para la selección los artículos de los últimos 5 años con respecto al tema a investigar. Para obtener mayores criterios del contenido de búsqueda se optó también por investigar las siglas en el idioma inglés ya que traduciéndolas no se muestra mayor información.

Ejecución de la búsqueda

Con la información seleccionada, se procedió a organizarla en una matriz para llevar un mejor orden en ir describiendo cada dato adquirido de los 16 artículos seleccionados; en la tabla 1 se demuestra cada uno de los campos con los que se trabajó para una mejor organización de los datos. Cabe recalcar, que todos artículos se les consideró su fecha de publicación que estos sean publicados a partir del año 2019.

Tabla 1

Campos que se consideran en la recopilación de información.

Campos	Descripción
Titulo	Tema del Articulo
Autor, Año de publicación	Los datos del autor y el año en el que fue publicado
Metodología	Qué tipo de metodología fue empleado para realizar el análisis del mismo
Aporte	En que ha aportado esta información.

Análisis de los resultados

Se visualizaron los datos obtenidos de los 16 artículos analizados, en los que se tuvo como resultados los mecanismos AAA para la mejora de entornos empresariales y permitió identificar la información más relevante sobre los estos mecanismos.

Resultados y Discusión

Luego de haber llevado a cabo el análisis sistemático, criterios de búsqueda y ejecución, se logró obtener un sinnúmero de artículo e investigación aplicadas, sin embargo, y de acuerdo con la pertinencia y relevancia a la información se seleccionó 16 artículos considerando los criterios descritos, todo ellos enmarcado a los mecanismos de seguridad y/o mecanismos AAA para mejorar la seguridad en entornos empresariales. En la tabla 2 podemos visualizar de manera organizada y descriptiva, el aporte de cada artículo.

Tabla 2

Análisis sistemático de los mecanismos AAA para mejorar la seguridad

#	Titulo	Autores	Metodología / Normas Iso	En que se basa el documento	Aporte
1	Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking	Edgar Vega Briceño (2020)	Método Evaluativo	Seguridad informática	Brindar una guía para desarrollar aspectos de planificación y ejecución necesarios para las evaluaciones de seguridad informática.
2	Introducción a la seguridad informática y el análisis de vulnerabilidades	Martha Irene Romero Castro, Grace Liliana Figueroa Moran, Denisse Soraya vera Navarrete (2018)	Metodología Analítica	Mecanismo de autenticación	Dar a conocer los conceptos relacionados sobre la seguridad informática, las bases principales, sus componentes, definiciones sobre virus entre otros, también temas que abordan sobre los diferentes mecanismos de autenticación.
3	La ciberseguridad practica aplicada a las redes, servidores y navegadores web	Wagner Abad, Tania Cañarte, Elena Villamarin, Henry Mezones, Ángel Delgado, Frankling Toala, Alberto Figueroa, Vicente Romero (2019)	Metodología Analítica	Seguridad informática	Es que ayuda a garantizar los parámetros de confidencialidad, integridad y disponibilidad mediante la herramienta pentesting.
4	Auditoría de seguridad informática siguiendo la metodología osstmmv3	Cristian Bracho-Ortega, Fabián Cuzme-Rodríguez, Carlos Pupiales-Yépez, Luis Suárez-Zambrano, Diego Peluffo-	Método Analítico	Seguridad informática	Un análisis que permite determinar los valores numéricos de cada uno de los ítems, para así

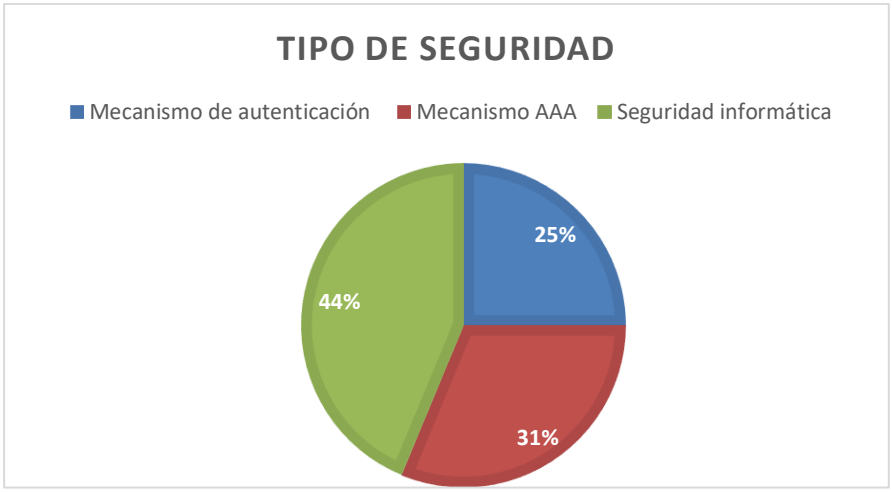
		Ordóñez, César Moreira-Zambrano (2017)			comprender la aplicación y deficiencia o excesos de los controles operacionales de dichas organizaciones
5	Seguridad ofensiva: metodología de hacking ético en la web	Fabián Cuzme-Rodríguez, Marcelo León-Gudiño, Luis Suárez-Zambrano and Mauricio Domínguez-Limaico1(2019)	Método Investigativo	Seguridad informática	Genera políticas, protocolos y un plan de aseguramiento de la información basado a las metodologías controladas en términos de seguridad
6	Redes informáticas	Miguel Lederkremer (2019)	Método Investigativo	Mecanismos AAA	Permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado, considerando los riesgos.
7	Seguridad de la información	Edgar Vega Briceño (2021)	Método Investigativo	Seguridad informática	Ayuda a permitir a acceder a una gran cantidad de información que conlleva a una gran cantidad de problemas de seguridad
8	Enfoque holístico de la criptografía cuántica en ciberseguridad	Shashi Bhushan, Manoj Kumar, Pramod Kumar (2022)	Método Investigativo	Mecanismos AAA	Debate los conceptos que se presentan en los desafíos en las areas de la criptografía tanto cuántica como cibernéticas, dentro del comercio electrónico cuántico, colación cuántica, ciberseguridad.
9	5g para el mundo conectado	Devaki Chandramouli, Rrainer Liebhart, Juho Pirskanen (2019)	Método Investigativo	Mecanismo de autenticación	Una guía útil para los profesionales de las telecomunicaciones, expertos en operadores de redes, desarrolladores de aplicaciones y analistas de negocios.
10	Orquestar y automatizar la seguridad para el internet de las cosas	Anthony Sabella, Rik Irons-Mclean, Marcelo Yannuzzi (2018)	Método Investigativo	Mecanismos AAA	Los nuevos surgimientos de estándares y arquitecturas para ayudar a los profesionales - técnicos a fortalecer sistemáticamente sus entornos.
11	Computación en la nube	Lizhe Wang, Rajiv Ranjan, Jinjun Chen (2017)	Método Investigativo	Seguridad informática	Sobre los cambios del uso de hardware físico y plataformas habilitadas para software administradas localmente al de servicios virtualizados.
12	Guía oficial de certificados ccnp y ccie security core scor 350-701	Omar Santos (2020)	Método Investigativo	Mecanismo de autenticación	Gestiona las identidades visibles y segmentaciones de redes de seguridad de la infraestructura firewalls y sistemas de prevención de intrusiones de cisco redes privadas virtuales.

13	Internet de las cosas, seguridad y privacidad en el ciberespacio.	Sandeep Saxena, Ashok Kumar Pradhan (2022)	Método Investigativo	Seguridad informática	Proporciona una visión general de los protocolos ligeros y los mecanismos criptográficos para lograr la seguridad y privacidad en las aplicaciones.
14	Guía de redes de compTIA network	Jill West (2021)	Método Investigativo	Mecanismos AAA	Corresponde al contenido de los objetivos del examen, incluidos protocolos, topologías, hardware, diseño de red, seguridad y soluciones de problemas.
15	(Isc)2 guía de estudio oficial para profesionales de seguridad de sistemas de información certificados por cissp	Mike Chapple, James Michael Stewart, Darril Gibson (2018)	Método Investigativo	Mecanismos AAA	Seguridad y gestión de riesgos seguridad de activos ingeniería de seguridad de comunicaciones y redes, gestión de identidades y accesos de evaluación y pruebas de seguridad operaciones de seguridad, desarrollo de software seguridad.
16	Análisis de big data para sistemas ciberfísicos	Guido Dartmann, Houbing Song, Anke Schmeink (2019)	Método Investigativo	Mecanismo de autenticación	Examina el procesamiento de señales de sensores, pasarelas, optimización y la toma de decisiones, la movilidad inteligente y la implementación de algoritmos de aprendizaje automático de sistemas integrados.

De acuerdo con los aportes de la información que se ha recopilado, se muestra un análisis detallado donde se permite determinar que es necesario acogerse a las recomendaciones que brinden una guía para un desarrollo de aspectos de planificación y ejecución en las evaluaciones de seguridad para así se garantice todos los parámetros de confiabilidad, integridad y disponibilidad mediante los mecanismos AAA esto ayuda a comprender, así con los nuevos surgimientos de estándares y arquitecturas ayudan a los profesionales – técnicos a fortalecer sistemáticamente, cada aspecto de la aplicación, las deficiencias o excesos de controles operacionales de seguridad que se estarían manejando en los entornos empresariales.

Es importante destacar que los mecanismos AAA(autenticación, autorización y contabilidad), no ha sido potencializado, debido a ello se puede apreciar en la información sistematizada, que uno de los mecanismos que prevalece en cuestiones de seguridad de sistemas, es le mecanismo de autenticación, que de acuerdo con los datos, muestra que el 44% de las investigación lo aplican; cabe destacar que la autenticación es uno de los primero criterios considerados en AAA, sin embardo se lo emplea de manera independiente tal como se muestra del en Gráfico 1.

Gráfico 1. Identificación de los tipos de seguridad aplicada en sistemas



Por otra parte se describe en la clasificación de tipos de seguridad a "Seguridad informática" donde se recopila información general como: el uso de herramientas de pentesting, controles operacionales, políticas, mecanismos criptográficos. Lo que se evidencia de manera general con el 25% de su aplicación. A pesar de ser un campo nuevo a explorar, los mecanismos de AAA (autenticación, autorización y contabilidad) en sistemas empresariales, se emplean en un 31% de acuerdo con la información recopilada.

Como es de conocimiento general y según el analisis que se ha recopilado de la informacion en todo entorno empresarial es necesario tener un sistema informatico cuya finalidad de este, a parte de brindar informacion a los usuarios, es tener una mayor seguridad de la misma y que cada uno de los usuarios para poder acceder a ella tiene que pasar por un proceso de autenticacion de sus datos que va de la mano con la autorizacion, que es lo mas relevante de este analisis, adicional ya el sistema en si debe contar con la contabilizacion de accesos de dichos ususarios.

Según Bhushan, Kumar, Kumar (2022) los mecanismos de autenticación, autorización y contabilidad ya existentes se pueden utilizar para autenticar la identidad de las aplicaciones SDN y las diversas entidades de red. Los permisos y el comportamiento de las aplicaciones y las entidades de la red pueden monitorearse en busca de anomalías y proporcionarse a los sistemas propuestos, que de acuerdo con lo analizado en esta investigación, las autoras estan totalmente de acuerdo con lo mencionado, considerandolo como una alternativa sensilla que no solo puede ser implementada en entornos empresariales; ciberseguridad, redes y sistemas informáticos en genral puede implementar

AAA, donde lo primordial es identificar a que recursos puede acceder el usuario y qué operaciones puede realizar.

Conclusiones

La revisión sistemática de la información ha permitido evidenciar, que a pesar del pasar del tiempo y contando con el acceso a información y datos tecnológicos siendo un universo muy grande y en muchos casos muy complejo de manejar, y más al tratarse de la seguridad e integridad de la información, ya que existen muchos procesos que no se pueden visualizar para los usuarios involucrados en entornos empresariales.

La mayoría de los entornos empresariales requieren sistemas informáticos para los cuales es de suma importancia la Seguridad Informática, para ello se requiere emplear los mecanismos AAA, que proporcionan un mejor control al iniciar cualquier proceso interno. Dentro de estos mecanismos se evidencia que el más utilizado es la autenticación de los usuarios que ha sido considerado en la práctica, como una manera de asegurar los accesos de manera fiable a los sistemas.

Los mecanismos AAA busca minimizar los riesgos provenientes de muchas partes, pueden ser estos por medio de la entrada de datos, ya sean estos por el medio en que se transporta, el hardware que se usa para transportar la información, los mismos dispositivos usados para recibirlos.

Estos procesos que tienen que ver con la parte de la seguridad informática genera una creciente que abarca numerosos elementos de diferentes aspectos: recursos humanos, tecnológicos, económicos, etc. En lo que se muestra que no solo es para los aspectos informáticos y de telecomunicaciones, sino que también hace muchas referencias a los entornos empresariales.

Contribución de los autores

Pazmiño Muñoz María Rosa: Conceptualización, Metodología, Investigación, Análisis formal de los datos, Redacción – borrador original del artículo. **Morales Carrillo Jessica Johanna:** Validación, Revisión y Edición del artículo.

Referencias

Anthony Sabella, Rik Irons-Mclean, Marcelo Yannuzzi. (2022). Orquestar y automatizar la seguridad para el Internet de las cosas. Obtenido de https://www.google.com.ec/books/edition/Orchestrating_and_Automating_Security_fo/SjFbDwAAQBAJ?hl=es-419&gbpv=1

Bertolin, J. A. (2019). Seguridad de la información. Redes, informática y sistemas de información. 281.

Briceño, E. V. (2020). PLANIFICACION Y EJECUCION DE EVALUACIONES DE SEGURIDAD INFORMATICA DESDE UN ENFOQUE DE ETHICAL HACKING. AREA DE INNOVACION Y DESARROLLO, S.L. doi:https://doi.org/10.17993/tics.2020.3

Briceño, E. V. (2021). seguridad de la informacion. 20. doi:https://doi.org/10.17993/tics.2021.4

Cristian Bracho Ortega, Fabian Cuzme Rodriguez, Carlos Pupiales Yepez, Luis Suarez Zambrano, Diego Peluffo Ordoñez, Cesar Moreira Zambrano. (2017). Auditoria de seguridad informatica siguiendo la metodologia OSSTMMv3: caso de estudio. Obtenido de file:///C:/Users/Eduardo%20Chavarr%C3%ADa/Downloads/edison-timbe-1471-4400-1-ce%20(4).pdf

Devaki Chandramouli, Rainer Liebhart, Juho Pirskanen. (2019). 5G para el mundo conectado (Primera ed.). Library of Congress Catalogin-in-Publication Data. Obtenido de https://www.google.com.ec/books/edition/5G_for_the_Connected_World/6-qGDwAAQBAJ?hl=es-419&gbpv=1&dq=authentication,+authorization+and+accounting+mechanisms&pg=PA314&printsec=frontcover

Edgar Vega Briceño. (2020). Planificacion y ejecucion de evaluaciones de seguridad informatica desde un enfoque de ethical hacking.

Fabia Cuzme-Rodriguez, Marcelo Leon-Gudiño, Luis Suarez-Zambrano, Mauricio Dominguez-Limaico. (2019). Offensive Security: Ethical Hacking Methodology on the Web . 3. Obtenido de https://www.researchgate.net/profile/Fabian-Cuzme-Rodriguez/publication/328367829_Offensive_Security_Ethical_Hacking_Methodology_on_the_Web/links/5e6001b1299bf1bdb854162b/Offensive-Security-Ethical-Hacking-Methodology-on-the-Web.pdf

Guido Dartmann, Houbing Song, Anke Schmeink. (2019). Project Manager. Obtenido de https://www.google.com.ec/books/edition/Big_Data_Analytics_for_Cyber_Physical_Sy/pL2iDwAAQBAJ?hl=es-419&gbpv=1&dq=authentication,+authorization+and+accounting+mechanisms&pg=PA68&printsec=frontcover

Lizhe Wang, Rajiv Ranjan, Jinjun Chen. (2017). Computación en la nube. Taylor & Francis Group. Obtenido de https://www.google.com.ec/books/edition/Cloud_Computing/KglEDwAAQBAJ?hl=es-419&gbpv=1&dq=authentication,+authorization+and+accounting+mechanisms&pg=PA62&printsec=frontcover

Martha Irene Romero Castro, Grace Liliana Figueroa Moran, Denisse Soraya Vera Navarrete, Jose Efrain Alava Cruzatty, Galo Roberto Parrales Anzules, Christhian Jose Alava Mero, Angel Leonardo Murillo Quimiz, Miriam Adriana Castillo Merino. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. AREA DE INNOVACION Y DESARROLLO, S.L. doi:http://dx.doi.org/1017993/IngyTec.2018.46

Mike Chapple, James Michael Stewart, Darril Gibson. (2018). (ISC)2 Guía de estudio oficial para profesionales de seguridad de sistemas de información certificados por CISSP. Pete Gaughan. Obtenido de https://www.google.com.ec/books/edition/ISC_2_CISSP_Certified_Information_System/Mr5TDwAAQBAJ?hl=es-419&gbpv=1&dq=authentication,+authorization+and+accounting+mechanisms&pg=PA8&printsec=frontcover

Santos, O. (2020). Guia oficial de certificados CCNP y CCIE Security Core SCOR 350-701. Cisco Press. Obtenido de https://www.google.com.ec/books/edition/CCNP_and_CCIE_Security_Core_SCOR_350_701/w1_dDwAAQBAJ?hl=es-419&gbpv=1

Shashi Bhushan, Manoj Kumar, Pramod Kumar. (2022). Enfoque holístico de la criptografía cuántica en ciberseguridad. Library of Congress Cataloging-Publication Data. doi:10.1201/9781003296034

Vega Briceño, E. (2020). PLANIFICACION Y EJECUCION DE EVALUACIONES DE SEGURIDAD INFORMATICA DESDE UN ENFOQUE DE ETHICAL HACKING. ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

Wagner Manuel Abad Parrales, Tania Cecibel Cañarte Rodríguez, María Elena Villamarin Cevallos , Henry Luis Mezones Santana, Ángel Rolando Delgado Pilozo, Franklin Jhimmy Toala Arias, Juan Alberto Figueroa Suárez , Vicente Fray Romero Castro. (2019). La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. AREA DE INNOVACION Y DESARROLLO, S.L. doi:http://doi.org/10.17993/IngyTec.2019.59

West, J. (2021). Guía de Redes de CompTIA Network. CompTIA Network. Obtenido de https://www.google.com.ec/books/edition/CompTIA_Network+_Guide_to_Networks/bFUzEAAAQBAJ?hl=es-419&gbpv=1&dq=authentication,+authorization+and+accounting+mechanisms&pg=PA648&printsec=frontcover