NORMAS Y ESTÁNDARES EN AUDITORÍA: UNA REVISIÓN DE SU UTILIDAD EN LA SEGURIDAD INFORMÁTICA

STANDARDS AND FRAMEWORKS IN AUDITING: A REVIEW OF THEIR UTILITY IN INFORMATION SECURITY

Martha Margarita Minaya Macias[1*]

[1] Universidad Laica Eloy Alfaro de Manabí, Extensión en El Carmen. ORCID: https://orcid.org/0000-0003-2406-8192. Correo: mminaya_m4@hotmail.com

Renelmo Wladimir Minaya Macias[2]

[2] Universidad Laica Eloy Alfaro de Manabí, Extensión en El Carmen. ORCID: https://orcid.org/0000-0002-0418-6864. Correo: renelmo.minaya@uleam.edu.ec

Mayra Lorena Intriago Navarrete[3]

[3] Unidad Educativa Fiscal ¨Dr. Wilfrido Loor Moreira¨. ORCID: https://orcid.org/0009-0003-1096-4196. Correo: mlorena2205@hotmail.com

Javier Agustín Intriago Navarrete[4]

[4] Escuela Superior Politécnica Agropecuaria de Manabí ¨Manuel Félix López¨. ORCID: https://orcid.org/0009-0002-9883-841X. Correo: j_avitino@hotmail.com

*** Autor para correspondencia:** mminaya_m4@hotmail.com

Resumen

El presente trabajo realizó una revisión teórica sobre las normas y estándares internacionales que se emplean en auditorías informáticas, destacando su utilidad en la seguridad informática. La investigación fue de tipo explotratoria; los antecedentes tomados fueron mayormente de alcances descriptivos, explicativos y escasos casos aplicativos. Se empleó un enfoque cualitativo para interpretar y presentar las distintas teorías que en la investigación bibliográfica se analizaron sobre las normas y estándares en auditorías y su utilidad en la seguridad informática. La bibliografía consultada se trató de artículos de alto impacto, encontrados con búsquedas realizadas en repositorios y bases de datos reconocidas; además, se consideraron trabajos de investigación de culminaciones de estudios asegurando siempre que la información recopilada fuera actualizada y tuviera una alta calidad académica y científica. Como resultado se reconoce a la auditoría

informática como una herramienta fundamental para promover la transparencia y la confianza en el entorno digital. Sobre la utilidad de las Normas y estándares en la seguridad informática se constató que su implementación es esencial para proteger los activos de información, proporcionar un marco sólido para abordar los desafíos de seguridad y para mejorar la gestión de riesgos.

Palabras clave: auditoría, informática, seguridad, estándares

Abstract

The present work conducted a theoretical review on international standards and frameworks used in IT audits, highlighting their importance in cybersecurity. The research followed an exploratory approach, relying mainly on descriptive and explanatory literature with limited practical case studies. A qualitative approach was employed to interpret and present various theories gathered from the literature review regarding standards and frameworks in IT audits and their significance in cybersecurity. The consulted bibliography consisted of high-impact articles sourced from reputable repositories and databases. Additionally, research studies were included to ensure up-to-date and academically sound information. As a result, IT auditing was recognized as a fundamental tool for promoting transparency and trust in the digital environment. Regarding the utility of standards and frameworks in cybersecurity, their implementation was found to be essential in safeguarding information assets, providing a robust framework for addressing security challenges, and enhancing risk management.

Keywords: *udit, IT (Information Technology), security, standards*

Fecha de recibido: 26/04/2023
Fecha de aceptado: 19/06/2023
Fecha de publicado: 21/06/2023

Introducción

En la actualidad el uso de las tecnologías es una necesidad ante un mundo cada vez más interconectado; los softwares y las redes informáticas se han convertido en una herramienta vital para acceder al creciente número de productos y servicios que hoy se ofrecen por esta vía. Se destaca el empleo de la tecnología en instituciones educativas públicas y privadas en los diferentes niveles de enseñanza, pues la conectividad y el acceso a la información son fundamentales para el desarrollo de las actividades académicas.

> Sobre el uso de la tecnología en el Ecuador el Instituto de estadísticas y censos (INEC, 2021) plantea: En el Ecuador el 70.7% de la población nacional usa internet, el 77.1% de la población urbana se conecta a internet y el 56.0% de la rural. Además el uso de equipamiento tecnológico aumenta cada año, en el 2020 el 62.9% de la población ecuatoriana contaba con un celular activado, 67.7% en el área urbana y 52.4% % en el área rural y el 51.5% de los ecuatorianos usaban celular inteligente¨(pp.13-18).

Es entonces imperioso que se vele por la calidad de los productos de software que se ofrecen, la seguridad de los equipos tecnológicos y de la información, así como la de los procesos digitales que cada vez son más empleados en la dinámica social y podrían ser obstaculizados ante la falla de un dispositivo, una red deficiente o una aplicación móvil, web o incluso de escritorio, que no garantice a los usuarios la debida usabilidad.

En este contexto, adquiere relevancia el desarrollo de auditorías informáticas (AI), también conocidas como "Auditorías de TI" (ATI). Estas auditorías experimentaron su auge en los años 60, cuando se comenzaron a vincular aspectos de organización, estrategia de TI y negocios en el ámbito empresarial, con el propósito de alcanzar los objetivos establecidos por las organizaciones. Con el transcurso del tiempo, la ATI se ha vuelto más compleja debido al creciente uso de las tecnologías y al aumento de la automatización de procesos en las organizaciones (Imbaquingo, y otros, 2020).

En este orden de ideas la AI es reconocida como una herramienta para que las organizaciones identifiquen posibles fallas desde el análisis de riesgos y así poder minimizar o neutralizar su impacto. Su ejecución permite evaluar y garantizar la efectividad, eficiencia y seguridad de los sistemas y procesos tecnológicos; aspiración que se logra con éxito siempre que el auditor sea un profesionales capacitados y actualizados en ATI para hacer frente a los nuevos retos y asegurar la protección de los activos digitales de las empresas.

Los resultados de evaluación de una auditoría informática se obtienen al constatar en qué medida las organizaciones cumplen con las normas, estándares y procedimientos vigentes. Al concluir una auditoría se ofrece el informe de resultados con los principales hallazgos y las recomendaciones que permiten mejorar la seguridad de los sistemas informáticos de la organización y garantizar el cumplimiento de las leyes y regulaciones relacionadas con la seguridad de la información (Lourido, 2019).

Es preciso destacar que las normas y los estándares de calidad son conceptos diferentes que se utilizan en las auditorías informáticas. Las normas de calidad son directrices que se establecen para garantizar que se cumplan los requisitos de calidad en los productos o servicios. En el contexto de las auditorías informáticas, las normas de calidad pueden incluir estándares de seguridad, prácticas recomendadas para la gestión de riesgos, procesos de gestión de la calidad y otros requisitos que se deben cumplir para garantizar que se cumplan los objetivos de la auditoría.

Por otro lado, los estándares de calidad son especificaciones técnicas que se utilizan para medir la calidad de los productos o servicios. En el contexto de las auditorías informáticas, los estándares de calidad pueden incluir medidas de seguridad, medidas de rendimiento y medidas de confiabilidad que se utilizan para evaluar el estado de los sistemas y procesos auditados.

Puede decirse que las normas de calidad son requisitos que se deben cumplir para garantizar que se cumplan los objetivos de la auditoría, mientras que los estándares de calidad son medidas específicas que se utilizan para evaluar la calidad de los sistemas y procesos auditados. Ambos son importantes en las auditorías informáticas, ya que ayudan a garantizar que se cumplan los requisitos de calidad y se mejore continuamente el desempeño de los sistemas y procesos auditados.

Especificamente la metodología MARGERIT, tan conocida en auditorías informáticas, no es una norma o estándar oficialmente reconocido o establecido por algún organismo regulador o de estandarización. En cambio, es una metodología desarrollada por el profesor universitario español Luis Joyanes Aguilar y su equipo de trabajo, que se enfoca en la gestión y desarrollo de proyectos informáticos

MARGERIT es un acrónimo que significa "Metodología de Aplicación y Gestión de la Evaluación de Riesgos de los Sistemas de Información y Telecomunicaciones". Esta metodología proporciona un marco de trabajo

para la identificación, análisis y evaluación de riesgos en proyectos de tecnología de la información y telecomunicaciones (Zapata, 2021).

Como se ha planteado MARGERIT no es un estándar oficial, pero si una metodología reconocida y utilizada en la industria de tecnología de la información y telecomunicaciones, especialmente en España y América Latina. Es importante tener en cuenta que el uso de MARGERIT no garantiza por sí solo la seguridad de los sistemas de información y telecomunicaciones, sino que es una herramienta que puede ayudar en la gestión de riesgos y en la toma de decisiones informadas en proyectos de tecnología.

La presente investigación se proyecta como objetivo generar: Realizar una revisión teórica sobre las normas y estándares de calidad que se emplean en auditorías informáticas, llegando a especificar en su utilidad en la seguridad informática.

Las preguntas de investigación que se plantearon en este estudio permitieron encausar su desarrollo:

¿Qué fundamentos teóricos permiten conceptualizar el término auditoría informática y las normas y estandares que para su desarrollo se emplean?

¿Cuáles normas y estándares se destacan en auditorías informática?

¿Cuál es la utilidad de la aplicación de las normas y estandares en la seguridad informática?

Como resultados se presenta la conceptualización de auditoría informática, así como los fundamentos teóricos de los aspectos asociados a su desarrollo. Luego, se ofrecen una explicación sobre las normas y estándares recomendadas según la finalidad de la auditoría, llegando a fundamentar su función : ISO 27001 para la gestión de la seguridad de la información, COBIT para la gestión de TI, ITIL para la gestión de servicios de TI y PCI DSS para la seguridad de datos de usuarios.

Finalmente, se destaca la utilidad que en la seguridad informática han tenido las normas y estándares aplicados en auditorías. Se destaca que para realizar una auditoría informática de manera efectiva, es necesario contar con un marco de referencia que establezca los principios, objetivos y procesos que se deben seguirse en esta evaluación. Este marco de referencia está compuesto por normas y estándares que proporcionan directrices y mejores prácticas para el desarrollo de la auditoría informática.

La revisión teórica realizada en esta investigación se concretó al consultar fuentes con alto nivel de actualización y con un aporte significativo sobre el tema abordado. La información obtenida se clasificó según su aporte y se procesó por pregunta de investigación para dar respuesta a cada una de ellas y así ofrecer una mejor comprensión de la auditoría informática y promover la adecuada aplicación de normas y estándares en este campo.

Materiales y métodos

La investigación se basó en el análisis teórico empleando métodos científicos que orientaron el razonamiento de lo general a lo específico, considerando perspectivas de otros investigadores y llegando a plantear conclusiones propias de esta investigación. Se pudo profundizar en las Normas y estándares que se emplean para desarrollar auditorías informáticas, empleando el método analítico sintético que permitió hacer argumentaciones. Fue posible desmembrar los aspectos asociados a la temática de estudio y realizar un análisis que se complementó con los aportes de investigaciones actualizadas relacionadas con el tema.

El enfoque cualitativo expuesto por (Hernández-Sampieri & Mendoza, 2018) se empleó para interpretar y presentar las distintas teorías que en la investigación bibliográfica se analizaron sobre las Normas y estándares

aplicados en auditorías informáticas y las relacionadas con la seguridad informática. Al tratarse de un artículo de revisión se realizó un estudio exploratorio que permitió sentar las bases del trabajo de investigación; los antecedentes tomados fueron mayormente de alcances descriptivos, explicativos y en el menor de los casos aplicativo (Jimenez, 2018).

La bibliografía consultada se trató de artículos publicados en revistas de alto impacto, encontrados con búsquedas realizadas en repositorios y bases de datos reconocidas (Science Research, Scopus, Science Direct, SciELO, Redalyc, Latindex y el Google académico). Además, se consideraron algunos libros y trabajos de investigación de culminaciones de estudios que presentan resultados de auditorías informáticas donde se aplicaron Normas y estándares para lograr la seguridad informática en diferentes contextos. Se aseguró que la información recopilada tuviera una alta calidad académica y científica. Al gestionar la información teórica para respaldar esta investigación, se consideró cuidadosamente su nivel de actualización.

Puede decirse que en el estudio concretamente se llevó a cabo un análisis y una síntesis de la teoría, se describió y explicó el fenómeno investigado, que es el impacto de las Normas y estándares en auditorías informáticas sobre la seguridad informática. Además, se examinó cómo estas normas y estándares han influido en la protección de la información y la prevención de vulnerabilidades en los sistemas tecnológicos.

Resultados y discusión

Seguridad informática

La seguridad informática es la disciplina que se ocupa de salvaguardar la confidencialidad y la integridad de la información almacenada en sistemas informáticos. Sin embargo, no existe una técnica infalible que garantice la total invulnerabilidad de un sistema. Se pueden implementar medidas de protección a nivel lógico, como el desarrollo de software seguro, así como a nivel físico, que abarca aspectos como el suministro eléctrico. Además, las amenazas pueden surgir tanto de programas maliciosos instalados en el equipo del usuario, como virus, como de ataques remotos realizados por delincuentes que se conectan a Internet y acceden a sistemas ajenos (Silva, 2019).

Es posible argumentar que en la seguridad informática la toma de conciencia es fundamental y estar constantemente actualizado sobre las mejores prácticas y tecnologías disponibles para proteger la información. Si bien no existe una solución perfecta, un enfoque integral y proactivo en la implementación de medidas de seguridad, se pueden mitigar en gran medida los riesgos y contribuir a un entorno más seguro para la información en los sistemas informáticos.

Auditoría informática

La auditoría informática implica la revisión exhaustiva de la información con el objetivo de asegurar su precisión. Su propósito principal es mejorar la utilidad de la información para los usuarios, al tiempo que verifica la autenticidad, integridad y calidad de la información generada por el sistema (Deream Arom Jimenez Ortiz & Ayala, 2019). Puede decirse que la auditoría informática se convierte en una herramienta fundamental para promover la transparencia y la confianza en el entorno digital.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones

La auditoría informática de desarrollo de proyectos o aplicaciones tiene como objetivo principal verificar la seguridad de los programas, asegurando que las ejecuciones realizadas por la máquina sean precisamente las planificadas y no otras. Una auditoría de aplicaciones implica la observación y el análisis de cuatro aspectos fundamentales: análisis de seguridad de hardware, software y red, cumplimiento de las políticas y procedimientos de seguridad informática, cumplimiento de las normativas en ciberseguridad y protección de datos y análisis de la formación del personal en seguridad informática. (Arcentales-Fernández & Caycedo-Casas, 2017). Este tipo de auditoría informática se convierte en una herramienta esencial para garantizar la calidad y la seguridad en el ámbito de la informática.

Auditoría Informática de Comunicaciones y Redes

En el contexto de las comunicaciones y redes la auditoría informática examina los dispositivos utilizados en las redes de una organización con el fin de identificar posibles vulnerabilidades y ofrecer soluciones para mejorar tanto la infraestructura como el rendimiento de la red. Los auditores encargados de llevar a cabo este tipo de auditoría deben poseer conocimientos especializados en diversos tipos de redes de comunicación (Lagua, 2022). Resulta evidente que esta auditoría busca evaluar y mejorar la seguridad y eficiencia de las redes organizacionales, proponiendo correcciones y soluciones adecuadas para garantizar un funcionamiento óptimo.

Auditoría en seguridad informática

La auditoría de seguridad informática puede abarcar tanto una evaluación general de la seguridad de un sistema informático, como auditorías más específicas que se centran en áreas informáticas particulares. En ambos casos, se considera tanto la seguridad física como la seguridad lógica. La seguridad física se enfoca en proteger el hardware, los medios de almacenamiento de datos, así como los edificios e instalaciones que los albergan, teniendo en cuenta riesgos como incendios, sabotajes, robos o desastres naturales. Por otro lado, la seguridad lógica se centra en el uso seguro del software, la protección de datos, procesos y programas, así como el acceso ordenado y autorizado de los usuarios a la información (Santana, 2018).

Etapas de una auditoría informática

Para iniciar una auditoría previamente se deben conocer las necesidades específicas de la organización donde se realizará. Según (Zambrano, 2020) existen tres etapas generales en la metodología de una auditoría informática: planeación, ejecución y dictamen como se muestra en la siguiente tabla:

Tabla1. Etapas de una auditoría informática

Etapas	Pasos a realizar
Planeación de la Auditoria de Sistemas	1. Identificar el origen de la auditoría. 2. Realizar una visita preliminar al área que será evaluada. 3. Establecer los objetivos de la auditoría. 4. Determinar los puntos que serán evaluados en la auditoría. 5. Elaborar planes, programas y presupuestos para realizar la auditoría.

	6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría. 7. Asignar los recursos y sistemas computacionales para la auditoría.
Ejecución de la Auditoria de Sistemas	1. Realizar las acciones programadas para la auditoría. 2. Aplicar los instrumentos y herramientas para la auditoría. 3. Identificar y elaborar los documentos de oportunidades de mejoramiento encontradas. 4. Elaborar el dictamen preliminar y presentarlo a discusión. 5. Integrar el legajo de papeles de trabajo de la auditoría
Dictamen de la Auditoria de Sistemas	1. Analizar la información y elaborar un informe de situaciones detectadas. 2. Elaborar el Dictamen final. 3. Presentar el informe de auditoría.

Fuente: (Zambrano, 2020)

En cambio (Trujillo, Merlos, Gallegos, & Conzuelo, 2020) plantea que no existe una metodología estandarizada para auditorías informáticas, pero si numerosos estudios que hacen sus propuestas o las implementan. Es posible argumentar que las metodologías utilizadas en áreas como la evaluación de riesgos, pruebas de seguridad y análisis forense están diseñadas con el propósito de cumplir con las normas y estándares establecidos en cada campo. Estas metodologías representan enfoques sistemáticos y estructurados para abordar diferentes aspectos de seguridad y protección de datos.

En primer lugar, la evaluación de riesgos es fundamental para identificar y comprender los posibles peligros y amenazas que podrían afectar la integridad de un sistema, una infraestructura o incluso la seguridad de las personas. Las metodologías de evaluación de riesgos se basan en estándares y mejores prácticas reconocidos, como ISO 31000, que proporcionan directrices para identificar, analizar y evaluar los riesgos de manera efectiva. Estas metodologías se centran en la identificación de vulnerabilidades, la estimación de las consecuencias potenciales y la determinación de las medidas de mitigación adecuadas (Escuela Europea de Excelencia , 2018)

En segundo lugar, las pruebas de seguridad desempeñan un papel crucial en la validación y verificación de la efectividad de los controles de seguridad implementados. Estas pruebas se basan en metodologías bien establecidas, como las pruebas de penetración, que buscan identificar y aprovechar las vulnerabilidades de un sistema para evaluar su resistencia a los ataques. Las pruebas de seguridad se rigen por estándares y marcos de referencia reconocidos, como el OWASP Testing Guide, que brindan una guía exhaustiva para llevar a cabo pruebas de seguridad de manera rigurosa y coherente (Revo, Made, & Agus, 2020).

En tercer lugar, el análisis forense se utiliza para investigar y recopilar evidencia digital en casos de incidentes de seguridad o delitos informáticos. Las metodologías de análisis forense digital se basan en estándares y pautas reconocidos, como los establecidos por el NIST (National Institute of Standards and Technology) en su serie de publicaciones SP 800-86, que proporcionan directrices detalladas sobre la recopilación, preservación, examen y presentación de evidencia digital de manera forensemente sólida (Gonzalez & Carranza, 2022).

Se puede postular que las metodologías utilizadas en la evaluación de riesgos, pruebas de seguridad, análisis forense y otras áreas relacionadas están diseñadas para seguir normas y estándares reconocidos. Estas normas y estándares proporcionan una base sólida y confiable para abordar los desafíos en cada campo y garantizar la efectividad de las medidas de seguridad implementadas. Al adoptar y aplicar estas metodologías de manera consistente, las organizaciones pueden fortalecer su postura de seguridad y protección de datos, mitigar riesgos y responder eficazmente a incidentes o violaciones de seguridad.

Norma o estándar recomendada para las auditorías informáticas según su finalidad

ISO/IEC 27000

La norma ISO/IEC 27000 es un vocabulario estándar utilizado en el Sistema de Gestión de Seguridad de la Información (SGSI). Por otro lado, la norma ISO/IEC 27001 es una certificación para organizaciones y establece los requisitos detallados para implementar el SGSI, que se representa en la Figura 1. Esta norma es la más importante dentro de la familia y adopta un enfoque de gestión de riesgos, promoviendo la mejora continua de los procesos. La norma ISO/IEC 27002 proporciona un conjunto de buenas prácticas para la gestión de la seguridad de la información. Por su parte, la norma ISO/IEC 27003 ofrece directrices para la implementación del SGSI. La norma ISO/IEC 27004 se enfoca en las métricas utilizadas para la gestión de la seguridad de la información. Finalmente, la norma ISO/IEC 27005 aborda la gestión de riesgos en seguridad de la información. En resumen, estas normas y otras de la familia ISO 27000, forman parte de un conjunto integral de estándares que cubren diversos aspectos de la seguridad de la información y el SGSI (Coloma-Baños, Cañizares-Galarza, Romero-Fernández, & Quintana-Cifuentes, 2022).

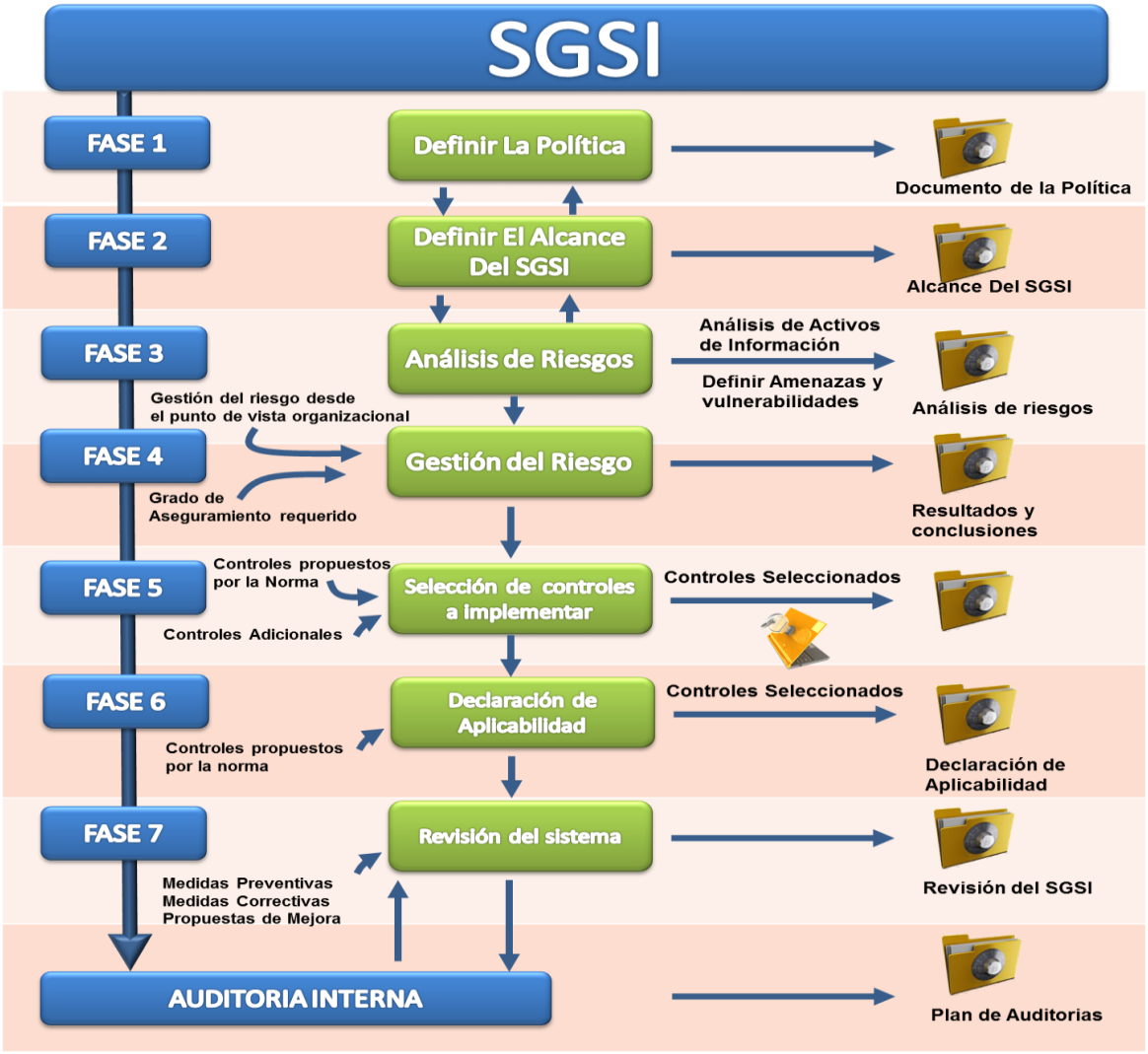

Figura 1. Sistema de Gestión de la Seguridad Informática
Fuente: https://www.normas-iso.com/iso-27001/

Es oportuno adentrarse en la norma ISO/IEC 27001:2013, pues esta define las normas para la gestión de la seguridad de la información y establece los requisitos para un sistema de gestión de seguridad de la información (SGSI); incluye además la identificación de riesgos, la implementación de medidas de seguridad y la gestión continua de la seguridad de la información. El certificado ISO 27001 le interesa a cualquier tipo de empresa sin importar su tamaño y actividad. El factor clave para decidir sobre la implantación de un sistema de gestión de la seguridad de la información radica en la importancia que los activos de información tienen dentro de una organización como elementos imprescindibles para la obtención de sus objetivos. Actualmente, a nivel mundial ISO 27001 es la norma de referencia para certificar la seguridad de la información en las

organizaciones; en el año 2017 se realizó una revisión de esta Norma, donde se han introducido algunas aportaciones o más bien correcciones a la norma ISO 27001:2013; es válido especificarlas tal como se refieren en (ISO 27000, 2022):

-Activos de información: Se sustituye el término "activos asociados a la información" por "la información y otros activos asociados a la información"

-Con esto se quiere precisar que el objeto de un inventario de activos es la información y sus activos asociados, en lugar de establecer solamente como requisito el tener un inventario de activos asociados a la información.

-Se elimina la Cláusula 6.1.3 y el Anexo A, control 8.1 sobre la responsabilidad en el uso de los activos de información en toda la cadena de uso.

El estándar ISO/IEC 27002:2013 proporciona un conjunto de controles de seguridad de la información que se pueden implementar en un SGSI. En la actualidad dispone de: 35 propósitos de control, 14 dominios y 114 inspecciones; abarcan desde la gestión de activos hasta la seguridad física y ambiental. ISO 27002 es un resumen de buenos hábitos para la Protección de datos que describen verificaciones y objetivos de fiscalización. En cambio, ISO 27003 sirve como soporte para el estándar 27001 e indica los lineamientos generales requeridos para la correcta introducción del SGSI. Incluye orientación sobre cómo implementar con éxito un SGSI (Carrillo & Asto, 2021).

En cambio, ISO/IEC 12207:2017 define un marco para el ciclo de vida del software y establece los procesos y actividades que se deben realizar en cada fase del ciclo de vida del software, desde la planificación hasta la evaluación (Alarcón & Risco, 2020).

ISO/IEC 20000-1:2018 establece los requisitos para la gestión de servicios de TI y proporciona un marco para la gestión de servicios de TI que se pueden implementar en una organización. Este estándar incluye la planificación del servicio, la gestión de la entrega del servicio y la mejora continua del servicio. Comúnmente las organizaciones implementan primero ITIL y después certifican en ISO / IEC 20000. Comienzan con ITIL porque este estándar ayuda a comprender los procesos, a identificar las áreas que necesitan mejorar y a estar familiarizadas con la metodología de trabajo. Luego, cuando ya conocen sus procesos, pueden intentar obtener la certificación ISO / IEC 20000-1 que les permitirá destacar entre los competidores (Veritier, 2020).

ISO 31000 se trata de un estándar internacional que establece las directrices para que cualquier tipo de organización, sea cual sea su sector y tamaño, pueda considerar el riesgo como elemento generador de valor. Se basa en 11 principios que encajan con toda la estructura y objetivos de la organización y que están relacionadas con las normativas de la implementación de riesgos (EALDEN, 2022).

Las normas mencionadas son ampliamente reconocidas y certificadas a nivel mundial, brindan confianza y transparencia en la protección de la información. En conjunto, estos estándares ofrecen un enfoque integral para abordar los desafíos de seguridad informática y gestionar eficientemente los riesgos asociados. Al implementar estas normas, las organizaciones pueden fortalecer su postura de seguridad y demostrar su compromiso con la protección de la información sensible. En definitiva, la adhesión a estos estándares internacionales es un paso fundamental hacia una mayor seguridad informática y una mejor gestión de riesgos en un entorno cada vez más digitalizado y vulnerable.

ITIL (Information Technology Infrastructure Library) es un estándar global ampliamente utilizado en la gestión de servicios de tecnología de la información (TI); proporciona un conjunto de prácticas y procesos

recomendados para el diseño, entrega, operación y mejora continua de los servicios de TI en una organización. El objetivo principal de ITIL es alinear los servicios de TI con las necesidades del negocio, mejorando la eficiencia y efectividad de la gestión de los servicios de TI. Proporciona un marco de trabajo flexible y escalable que se adapta a diferentes tipos y tamaños de organizaciones. Es una librería de buenas prácticas, pues se compone de una serie de libros y publicaciones que describen las mejores prácticas en diferentes áreas de la gestión de servicios de TI. Estas áreas incluyen la estrategia de servicios, el diseño de servicios, la transición de servicios, la operación de servicios y la mejora continua de servicios. Cada una de estas áreas abarca diferentes procesos y funciones que ayudan a gestionar de manera efectiva los servicios de TI (Peña-Casanova & Anias-Calderón, 2020).

COBIT (Control Objetives for Information Systems and Related Technology) es un modelo de evaluación y monitoreo que introduce una nueva forma de trabajar para los profesionales del campo de los sistemas. Este modelo incorpora buenas prácticas de control en las tecnologías de la información (TI). Su objetivo principal es garantizar la seguridad de las TI, considerándolas como un recurso fundamental para alcanzar los objetivos empresariales en un mercado cada vez más digitalizado y diverso. Por esta razón, el COBIT resulta muy útil para auditores y expertos que se dedican al control de los procesos informáticos. Aunque no es el modelo más técnico, se caracteriza por exigir un nivel más elevado de procesos, pues cuenta con 4 procesos y 24 dominios; es considerado una herramienta de gobierno de TI (Zambrano, 2020).

PCI DSS, en su versión 3.2: Payment Card Industry Data Security Standart, se toma en cuenta como la normativa principal para el desarrollo de controles sobre la matriz de riesgos informáticos. El desarrollo y mantenimiento de red segura, protección de datos de los usuarios, son sus dominios y objetivos de control, así como el programa de gestión de vulnerabilidades, métodos de control de acceso, testing regular de las redes y el mantenimiento de un sistema de gestión de seguridad informática. Está conformado por 12 requisitos básicos que, agrupados en 6 secciones conocidas como objetivos de control (Guerra, 2019)

Al considerar estas importantes normas y estándares en el ámbito de la seguridad informática, se destaca la importancia de adoptar un enfoque integral y estructurado para garantizar la protección de la información y los activos en el entorno digital. ITIL proporciona un marco sólido para la gestión de servicios de TI, asegurando la alineación con las necesidades del negocio. COBIT, por su parte, introduce buenas prácticas de control y seguridad en las tecnologías de información, ofreciendo un enfoque de gobierno de TI. Por último, PCI DSS establece requisitos de seguridad específicos para la protección de datos de tarjetas de crédito en el sector de pagos con tarjeta.

Al adoptar estas normas, las organizaciones pueden fortalecer su postura de seguridad y mitigar los riesgos asociados a la gestión de la información. Es esencial comprender que estas normas no son soluciones independientes, sino que se complementan entre sí, brindando un enfoque holístico y eficiente para garantizar la seguridad informática. Con la implementación de estos estándares las organizaciones pueden demostrar su compromiso con la protección de la información, fortalecer la confianza de los clientes y asegurar el cumplimiento de las regulaciones pertinentes. En definitiva, estas normas desempeñan un papel fundamental en la construcción de un entorno digital seguro y confiable en el que las organizaciones puedan prosperar y cumplir con los desafíos de seguridad actuales y futuros.

A continuación, presento una tabla que resume la utilidad de importantes normas y estándares en el campo de la seguridad informática. Estas normas y estándares, como ISO/IEC 27000, ITIL, COBIT y PCI DSS, desempeñan un papel crucial en el fortalecimiento de la seguridad de la información en las organizaciones.

Cada uno de ellos ofrece directrices y mejores prácticas en áreas específicas, abordando aspectos clave de la gestión de riesgos, la protección de datos, la entrega de servicios de TI y el cumplimiento de estándares de seguridad. Esta tabla proporciona una visión general de la utilidad que cada uno de estos estándares puede aportar en la implementación de estrategias efectivas de seguridad informática.

Tabla 2 Funciones, área e implementación de los estándar COBIT, ITIL, ISO 27000 y PCI DSS

Área	COBIT	ITIL	ISO 27000	PCI DSS
Funciones	Mapeo de procesos IT	Mapeo de la gestión de niveles de servicio en IT	Marco de referencia de seguridad de la información	Desarrollo de controles sobre la matriz de riesgos informáticos.
Áreas	4 procesos y 24 dominios	9 procesos	10 Dominios	12 Requisitos básicos que se agrupan en 6 sesiones.
¿Para qué se implementa?	Auditoría de Sistema de información	Gestión de niveles de servicio	Cumplimiento del estándar de seguridad	Protección de datos de los usuarios. Mantenimiento de red segura. Gestión de vulnerabilidades. Mantenimiento de un sistema de gestión de seguridad informática

Fuente: Elaboración propia

Resulta evidente que la norma ISO/IEC 27000 brinda un marco común de terminología y conceptos en el ámbito de la seguridad de la información, facilita la comunicación y el entendimiento entre profesionales del sector. ITIL, por su parte, se enfoca en la gestión de servicios de TI y proporciona pautas para mejorar la entrega y operación de servicios seguros.

En este orden de ideas COBIT, con su enfoque en el control y la seguridad de las tecnologías de la información, permite a las organizaciones establecer prácticas sólidas de control interno y garantizar la alineación de los objetivos de seguridad con los objetivos del negocio. En cuanto a PCI DSS, se concentra en la protección de los datos de tarjetas de crédito y establece requisitos estrictos para prevenir el fraude y proteger la información sensible de los clientes.

Por la relevancia que tiene para el trabajo la utilidad de las normas y estándares en la seguridad informática, se presenta la siguiente tabla resumen. En esta se destaca la utilidad de los estándares internacionales en la seguridad informática, incluyendo ISO/IEC 27000, ITIL, COBIT y PCI DSS. Estos estándares proporcionan un marco sólido y mejores prácticas para la gestión de la seguridad de la información, la gestión de servicios de TI y el cumplimiento de requisitos de seguridad en el sector de pagos con tarjeta.

Tabla 3. Utilidad de estándares internacionales en la seguridad informática

Estándar	Utilidad en la seguridad informática
ISO/IEC 27000	Proporciona un vocabulario estándar para el Sistema de Gestión de Seguridad de la Información (SGSI)
ITIL	Ofrece mejores prácticas en la gestión de servicios de tecnología de la información (TI)
COBIT	Introduce buenas prácticas de control y seguridad en las tecnologías de información (TI)
PCI DSS	Establece requisitos de seguridad para la protección de datos de tarjetas de crédito en el sector de pagos con tarjeta (Payment Card Industry)

Fuente: Elaboración propia

Esta tabla resume la utilidad principal de cada estándar en la seguridad informática. Cabe mencionar que cada estándar tiene un alcance y enfoque específico en términos de seguridad, por lo que pueden abordar diferentes aspectos de la seguridad de la información en distintos contextos. Puede decirse que los estándares y normas en seguridad informática, como ISO/IEC 27000, ITIL, COBIT y PCI DSS, desempeñan un papel fundamental en el fortalecimiento de la seguridad de la información en las organizaciones; proporcionan directrices claras y prácticas recomendadas que permiten a las empresas establecer y mantener un entorno seguro para sus sistemas y datos.

La adopción de estas normas ayuda a garantizar la confidencialidad, integridad y disponibilidad de la información, así como a mitigar los riesgos asociados a posibles amenazas y vulnerabilidades. Al seguir las mejores prácticas definidas en estos estándares, las organizaciones pueden establecer procesos sólidos de gestión de riesgos, implementar controles adecuados y realizar auditorías efectivas para evaluar y mejorar continuamente su postura de seguridad.

Conclusiones

En la revisión de los fundamentos teóricos que definen el término auditoría informática esta se reconoce concretamente como una herramienta fundamental para promover la transparencia y la confianza en el entorno digital y entre los tipos de auditoría se destaca la de seguridad informática que puede abarcar tanto una evaluación general de la seguridad de un sistema informático, como auditorías más específicas que se centran en áreas informáticas particulares.

El estudio teórico realizado facilitó la comprensión de diferentes normas y estándares que se aplican en auditorías informáticas, con áreas diversas y funciones muy específicas, donde se destacaron: ISO 27001 para la gestión de la seguridad de la información, COBIT para la gestión de TI, ITIL para la gestión de servicios de TI y PCI DSS para la seguridad de datos de usuarios.

Al indagar sobre la utilidad de las Normas y estándares en la seguridad informática se aprecia que su implementación es esencial para proteger los activos de información y mantener la confianza de los clientes; pues proporcionan un marco sólido para abordar los desafíos de seguridad, ayudando a las organizaciones a establecer controles efectivos, mejorar la gestión de riesgos y fortalecer la resiliencia frente a las amenazas en constante evolución en el panorama de la seguridad cibernética.

Referencias

Alarcón, C. C., & Risco, D. C. (2020). *"Método para la Gestión del Desarrollo del Software, basada en la NTP ISO/IEC 12207:2006 en la Municipalidad Provincial de Chiclayo".* Universidad Nacional Pedro Ruiz Gallo, FACULTAD PROFESIONAL DE INGENIERÍA DE SISTEMAS , Lambayeque, Perú. Obtenido de https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/9369/Lozano_Alarc%c3%b3n_Claudia_Celeste_y_Montenegro_Risco_Diana_Carolina.pdf?sequence=1&isAllowed=y

Arcentales-Fernández, D. A., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Revista: Dominio de la Ciencia, 3* (mon), 157-173. doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.

(2019). *AUDITORíA DE REDES, APLICANDO LA METODOLOGíA OSSTMM V3,PARA EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL.* UNIVERSIDAD TECNICA DE AMBATO, FACULTAD DE TECNOLOGíAS DE LA INFORMACION TELECOMUNICACIONES E INDUSTRIAL, Ambato. Ecuador. Obtenido de http://repositorio.uta.edu.ec/handle/123456789/30101

Bailon, W. A. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. *CIENCIAMATRIA Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, 15.

Carrillo, L. M., & Asto, M. S. (2021). *PROPUESTA DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002:2013 PARA PROPICIAR LA SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE INFORMÁTICA DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN – HUÁNUCO -2019.* Universidad Nacional ¨Hermilio Valdizan¨ , ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS, HUÁNUCO – PERÚ. Obtenido de https://repositorio.unheval.edu.pe/handle/20.500.13080/7093

Coloma-Baños, N. C., Cañizares-Galarza, F. P., Romero-Fernández, A. J., & Quintana-Cifuentes, M. V. (2022). La seguridad informática para la toma de decisiones en el distrito de educación 12d03.Mocache-Ecuador. *Revista CIENCIAMATRIA, VIII*(4). Obtenido de https://cienciamatriarevista.org.ve/index.php/cm/article/view/898/1495

Deream Arom Jimenez Ortiz, & Ayala, J. C. (2019). *Estado del Arte de la Auditoría informática y su importancia para las empresas.* Universidad Nacional de Piura , Escuela profesional de contabilidad , Piura. Perú. Obtenido de https://repositorio.unp.edu.pe/bitstream/handle/UNP/1971/FCC-JIM-ORT-2019.pdf?sequence=1&isAllowed=y

EALDEN. (2022). *EALDEN* . Recuperado el 5 de JUNIO de 2023

Escuela Europea de Excelencia . (2018). *Escuela Europea de Excelencia. Campus virtual* . Recuperado el 6 de Junio de 2023, de https://www.escuelaeuropeaexcelencia.com/2018/05/como-realizar-la-evaluacion-de-riesgos-segun-iso-310002018/

Gonzalez, B. A., & Carranza, A. V. (2022). *Propuestav de un estandar nacional que facilite determinar la admisibilidad de la evidencias digital en delitos informáticos en Costa Rica* . Tesis de Maestría , Universidad CENFOTEC , Maestría en Ciberseguridad . Obtenido de https://repositorio.ucenfotec.ac.cr/bitstream/handle/123456789/305/%c3%81lvarez%20Gonz%c3%a1lez%20Brandon%20y%20Villegas%20Carranza%20Alex%20Daniel-MSEG_abril2022.pdf?sequence=1&isAllowed=y

Guerra, J. P. (2019). *Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones financieras de la economía popular y solidaria basada*

en las buenas prácticas de la PCI DSS, caso de estudio Cooperativa. Universidad Internacional SEK, Facultad Arquitectura e Ingeniería.

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* Ciudad de México: Mc Graw Hill Education. Obtenido de https://virtual.cuautitlan.unam.mx/rudics/?p=2612

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., Torre, J. D., & Jácome, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *RISTI: Revista Ibérica de Sistemas y Tecnologias de Informaçión*(E32). Obtenido de https://media.proquest.com/media/hms/PFT/1/YWfNH?_s=NOsfrJmgv8WbV%2FTdqPf5wzusmtU%3D

INEC. (2019). *Tecnología de la Información y Comunicación.* Obtenido de www.ecuadorencifras.gob.ec

INEC. (2021). *Indicadores de tecnología de a información y la comunicación.* Encuesta multipropósito, Quito. Obtenido de https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Boletin_Multiproposito_Tics.pdf

ISO 27000. (2022). *ISO 27001*. (USA, Productor) Obtenido de https://normaiso27001.es/

ISO 27000. (s.f.). *El certificado ISO 27001 le interesa a cualquier tipo de empresa sin importar su tamaño y actividad. El factor clave para decidir sobre la implantación de un ISO 27001*. (USA, Productor, & La entidad) Recuperado el 6 de Junio de 2023, de https://normaiso27001.es/

Jimenez, W. E. (2018). *Publicar investigación científica.* . Manta: Ediciones Uleam.

Lagua, S. B. (2022). *Auditoría informática en la empresa Corporación Impactex Cía. Ltda. de la ciudad de Ambato.* Universidad Técnica de Ambato, Facultad de Contabilidad y Auditoría. , Ambato. Obtenido de http://repositorio.uta.edu.ec/bitstream/123456789/36112/1/T5536i.pdf

Lourido, W. A. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. *CIENCIAMATRIA: Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, V*(1). doi:https://doi.org/10.35381/cm.v5i1.248

Peña-Casanova, M., & Anias-Calderón, C. (2020). Integración de marcos de referencia para gestión de Tecnologías de la Información. *Revista Ingeniería Industrial* , *XLI*(1). Obtenido de https://www.redalyc.org/journal/3604/360464918003/html/

(2021). *PROPUESTA DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002:2013 PARA PROPICIAR LA SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE INFORMÁTICA DE LA UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN – HUÁNUCO -2019.* UNIVERSIDAD NACIONAL "HERMILIO VALDIZAN", ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS. Obtenido de https://repositorio.unheval.edu.pe/handle/20.500.13080/7093

Revo, D. R., Made, A. S., & Agus, E. P. (2020). Testing for Information Gathering Using OWASP Testing Guide v4 (Case Study : Udayana University SIMAK-NG Application). *JITTER- Jurnal Ilmiah Teknologi dan Komputer , 1*(1).

SantanaI, J. K. (2018). La importancia de los desarrollos informáticos en los procesos administrativos. *Revista Polo del Conocimiento, 3*(1). Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/viewFile/378/450

Silva, C. P. (2019). *Auditoría de redes, aplicando la metodología OSSTMM V3, para el Ministerio de Inclusión Económica y Social.* Universidad Técnica de Ambato, Facultad de Tecnología de la Información , Ambato. Ecuador. Obtenido de http://repositorio.uta.edu.ec/handle/123456789/30101

Tobar, R. A., & Ordoñez, A. F. (2015). *ESTUDIO PARA LA IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA SECRETARIA DE EDUCACION DEPARTAMENTAL DE NARIÑO BASADO EN LA NORMA ISO/IEC 27001.* Trabajo de Grado presentado como requisito para optar el título de Especialista en Seguridad Informática, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD, ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA.

Trujillo, S. E., Merlos, J. C., Gallegos, M. S., & Conzuelo, L. L. (2020). Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y . *Revista: Ideas en Ciencias de la Ingeniería, 1*(1). Obtenido de https://revistacoatepec.uaemex.mx/index.php/ideasingenieria/article/view/14591

Vega, E. E., & Cisternas, R. C. (2016). *Análisis corporativo entre sistemas OSSTMM y COBIT 5.0 para la mitigación de riesgos.* Santiago de Chile.

Veritier, C. (2020). *ITIL e ISO / IEC 20000 análisis, comparación y su relación con Agile.* Universidad de Cantabria, MÁSTER OFICIAL EN EMPRESA Y TECNOLOGÍASD DE ÑA INFORMACIÓN . Obtenido de https://repositorio.unican.es/xmlui/bitstream/handle/10902/20750/VERITIER%2cCARLOS.pdf?sequence=1&isAllowed=y

Zambrano, R. C. (2020). *PLAN DE IMPLANTACIÓN DE LA NORMATIVA PCI-DSS EN LA COOPERATIVA DE AHORRO Y CRÉDITO LA BENÉFICA.* Trabajo Fin de Master, Universidad Internacional de La Rioja (UNIR), Maestría: Máster universitario en Seguridad Informática, El Carmen. Ecuador.

Zapata, J. (2021). *Aplicación de metodología Margerit en la Gestión de Riesgos de Tecnologías de la Información en la agencia Metro Santana Elena.* Universidad Nacional Pedro Ruiz Gallo. , Lambayeque. Perú.