MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

METODOLOGÍA PARA LA REALIZACIÓN DE AUDITORÍAS DE SEGURIDAD INFORMÁTICA DE INFRAESTRUCTURA DE REDES DE DATOS EN EMPRESAS DEL SECTOR INDUSTRIAL PESQUERO (UN ESTUDIO COMPARATIVO): DEL CANTÓN MANTA, PROVINCIA DE MANABÍ, ECUADOR.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante: JUAN CARLOS SENDÓN VARELA

Bajo la dirección de: ING. RUBEN ANTONIO PACHECO VILLAMAR

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Julio del 2019

Metodología para la realización de auditorías de seguridad informática de infraestructura de redes de datos en empresas del sector industrial pesquero (un estudio comparativo): del cantón Manta, Provincia de Manabí, Ecuador.

Methodology for conducting computer security audits of data network infrastructure in companies in the fishing industry (a comparative study): Manta canton, Manabí Province, Ecuador.

Resumen

La información es uno de los activos más significativos para una organización. Debido a las amenazas y los riesgos a los que se exponen los activos informáticos en las organizaciones, se vuelve muy importante contar con herramientas de control y supervisión que ayuden a la creación de una cultura de seguridad en estas, que revelen el estado de la Seguridad Informática. El presente trabajo de investigación tiene como objetivo determinar cuál es la metodología más adecuada para la realización de auditorías de seguridad informática a la infraestructura de redes de datos en las empresas del sector industrial pesquero del cantón Manta. A través de una revisión bibliográfica, modelos estadísticos y un análisis comparativo entre distintas metodologías, y con la ayuda de un cuestionario validado se evaluó la metodología más adecuada para la realización de este proceso de auditoría para garantizar la confiabilidad, disponibilidad, confidencialidad e integridad de la información; así como también, que minimice los riesgos en el uso de la tecnología. Como resultado se evidenció las deficiencias en la seguridad informática del objeto estudiado y se pudo corroborar que la alternativa más acorde a las características del sector es OSSTMM, debido a su complejidad media y de fácil implementación en aquellas organizaciones que inician procesos de reestructuración de los modelos de seguridad informática. Esta temática, como línea de investigación, ha recibido la atención de investigadores, observándose la necesidad de profundizar en su estudio, justificando su pertinencia y actualidad.

Palabras clave: Auditoria informática, metodologías, infraestructura física, disponibilidad.

Abstract

Information is one of the most significant assets of an organization. Due to the threats and risks to which IT assets are exposed in organizations, it becomes very important to have control and supervision tools that help to create a culture of security in these, that reveal the state of Security Computing. The objective of this research work is to determine the most suitable methodology for carrying out computer security audits to the data network infrastructure in the companies of the fishing industry of the Manta municipality. Through a literature review, statistical models and a comparative analysis between different methodologies, and with the help of a validated questionnaire, the most appropriate methodology was evaluated to carry out this audit process to guarantee the reliability, availability, confidentiality, and integrity of information; as well as minimizing the risks in the use of technology. As a result, the deficiencies in the computer security of the studied object were evidenced and it could be corroborated that the alternative more in line with the characteristics of the sector is OSSTMM, due to its medium complexity and easy implementation in those organizations that initiate restructuring processes of the models of computer security. This subject, as a line of research, has received the attention of researchers, observing the need to deepen its study, justifying its relevance and relevance.

Key words: Computer audit, methodologies, physical infrastructure, availability.

INTRODUCCIÓN

La información es uno de los elementos más valiosos para cualquier organización o persona en la actualidad, siendo un instrumento para crear ventaja competitiva frente a otros (Vásquez y Gabalán, 2015).

También, con la proliferación del internet como red global de comunicación, se ha visto un desarrollo muy significativo de las tecnologías y medios de comunicación, presentándose nuevas formas de acceder a la información (Chalén, Mideros y Ambuludi, 2010).

El crecimiento rápido de distintas tecnologías, como las redes inalámbricas, la computación en la nube, las aplicaciones de informática móvil, los teléfonos inteligentes y el Internet de las cosas (Internet-of-Things (IoT)), este último con una proyección de crecimiento, según Gartner, de 25 Billones para el 2020, han impactado a escala social mediante la transformación de muchas industrias, así como de nuestra vida cotidiana (Chalén et al., 2010; Yu, Sekar y Seshan, 2015; Zhang, Lee y Huang, 2003).

Sin embargo, debido a la falta de conocimiento de cómo proteger la información, o debido a la complejidad de aplicación de normas internacionales, muchas organizaciones no logran alcanzar sus objetivos (Vásquez y Gabalán, 2015).

Por el hecho de que es necesario asegurar la información, durante su procesamiento, almacenamiento y transmisión, en contra de amenazas y riesgos, surge la necesidad de articular mecanismos que ayuden en el control de los procesos sistemáticos para poder ejecutar evaluaciones objetivas del estado de las redes de datos en todo tipo de empresas, públicas o privadas, y para ello, se debería tener herramientas de control y supervisión que faciliten el descubrir vulnerabilidades en los sistemas de transmisión (INEN, 2016; ISO/IEC, 2014; Patcha, 2006; Zhang et al., 2003).

ISACA, como acrónimo del inglés Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), en su reporte anual realizado en octubre de 2017, confirma que la ciberseguridad sigue siendo muy dinámica y turbulenta a pesar del desarrollo continuo en este campo. En este informe también se revelan estudios de los primeros estados de la seguridad informática para el 2018, donde se destaca el desarrollo de la fuerza laboral de ciberseguridad y las tendencias actuales (ISACA, 2017).

En el reporte anterior, se evidencia un recelo por cambiar el presupuesto de seguridad en las empresas en 2018, un 53 % de los encuestados piensa aumentar un poco dicho presupuesto, frente a un 28 % que no realizarán ningún cambio al presupuesto de seguridad de la empresa. En estos valores se observa como aún hay organizaciones que no ven la seguridad de la información como algo importante o necesario para cumplir sus objetivos (ISACA, 2017).

En el mismo reporte, se puede observar como las empresas han experimentado un aumento en los ataques de seguridad en comparación con octubre de 2016. El 50 % mantiene que ha experimentado más ataques que años anteriores, y el 80 % ve muy probable, o probable, que sean atacados en el 2018 (ISACA, 2017).

Deloitte en 2017 realizó un estudio, donde participaron 50 empresas nacionales y multinacionales de diversas industrias en el Ecuador. Este análisis, tuvo como objetivo proveer una herramienta de comparación que permita a las organizaciones mejorar los aspectos estratégicos, tácticos y operativos en relación con la gestión de seguridad de la información (Deloitte, 2017, 2018).

Como resultado de este análisis, en el 50% de participantes se notó alguna brecha de seguridad en los últimos 12 meses, y de estos, en un 20% no se pudo determinar el impacto, debido a que no cuentan con un proceso de gestión de incidentes, evidenciando que el componente humano continúa siendo una pieza crítica en la gestión de seguridad de la información. Otro estudio realizado en octubre del 2018, evidencia una tendencia muy parecida (Deloitte, 2017, 2018).

La falta de suficiente presupuesto se encuentra entre las principales dificultades, lo cual es confirmado por más del 50% de los participantes en el estudio realizado por Deloitte, seguido muy de cerca por aspectos como la falta de visibilidad e influencia, y la falta de personal competente. Así mismo, casi el

75% de los participantes no mide el retorno de las inversiones en seguridad de información.

En este este mismo estudio, se pudo observar que el 36 % de las empresas no cuentan con un enfoque de monitoreo de seguridad de información, y que el 60 % no cuentan con un Centro de Operaciones de Seguridad (Deloitte, 2017, 2018).

En el resumen anual de seguridad 2017 del Centro de Investigación, Desarrollo y Soporte (TrendLabsS) de la compañía Trend Micro Inc. se expone a Equifax, una agencia de informes de crédito al consumidor, que fue noticia en septiembre de ese año al divulgar la información de identificación personal (PII) de alrededor de 145,5 millones de usuarios estadounidenses y 15,2 millones de usuarios del Reino Unido, viéndose involucrada en una violación que podría haber comenzado ya en mayo de 2017 (Micro Incorporated, 2017).

También, la compañía de viajes compartidos Uber se acercó al final de un año ya problemático, al revelar que 57 millones de registros de clientes y los conductores quedaron expuestos luego de una violación de datos en octubre de 2016 (Micro Incorporated, 2017).

Después de analizar los distintos casos y reportes anteriores, donde se puede evidenciar deficiencias en el campo de la seguridad informática en las organizaciones y lo expuestas que están a amenazas informáticas, se ve la necesidad de contar con herramientas de control que, a su vez, permitan evaluar los controles de seguridad informática.

Las auditorias de seguridad informática, serían una herramienta con la que pueden contar las organizaciones, siendo esta, muy eficaz y veraz para la realización de trabajos de control, teniendo en cuenta los avances tecnológicos y estándares internacionales ayudando a agilizar los procesos de Tecnologías de Información y Comunicación (TIC) en el análisis de los riesgos de seguridad informática a los auditores (Burgos y Campos, 2008; Arias, 2010).

La información recogida por estas auditorías les otorgará a los auditores un conocimiento real de los problemas en la red de datos de las organizaciones para prevenir eventos extraordinarios o para actuar de manera eficiente una vez ocurridos, además, de permitirles a las empresas prepararse para alcanzar estándares internacionales en el uso de los recursos tecnológicos (Arcentales y Caycedo, 2017).

Teniendo en cuenta que la Real Academia Española (RAE) define a la auditoría como la revisión contable de una empresa realizada por un auditor que es virtuoso de oír y revisar cuentas para la realización de evaluación de la manera económica, eficiente y eficaz en que se usa los recursos y el control de estos (Marrero, 2015; R.A.E., 2014).

Los antecedentes de la actividad de auditoría, como forma de supervisión, se remontan a tiempos de Egipto Antiguo, donde se utilizaba para evitar fraudes y desfalcos en las cuentas o en la construcción de obras públicas, estando presente ésta desde la antigüedad (Alvarez y Rivera, 2006).

También, Alvarez y Rivera (2006) en su artículo expone palabras de Montgomery en 1912, que dice que en los inicios de la auditoría, se enseñaba que los objetivos principales de esta actividad eran: la detección y prevención del fraude, la detección y prevención de errores.

La realización de planes de seguridad con el fin de proteger la información, como el activo más valioso de la organización, es una actividad que realizan las empresas u organizaciones. La auditoría informática, como herramienta de verificación y control, revela si el plan de seguridad informática se está cumpliendo y si se encuentra alineado a los objetivos de la organización. Para garantizar lo anterior, es necesario la realización de evaluaciones sistemáticas, es decir, periódicas y espontáneas para el análisis y evaluación del plan (Duque, 2017; Solarte, Rosero y Benavides, 2015; Tramullas, 2003).

Para la realización de las auditorías a las redes de datos o sistemas de comunicaciones de una organización, se llevarán a cabo determinadas acciones muy parecidas a otras auditorias, como son investigar, revisar, verificar, evaluar y recomendar. Algo muy importante es que estas deberán ser realizadas alineadas a los objetivos y características del negocio, para poder identificar y corregir las vulnerabilidades en los activos en riesgo, ya sean estos físicos o lógicos (Alfaro, Boulahia y Cuppens, 2008; Ruiz, López, y Soriano, 2011).

Un trabajo interesante, es el mecanismo ágil de auditoría a la seguridad informática de una red inalámbrica basada en la arquitectura AAA, cuyo objetivo es evaluar la efectividad de los controles implementados en la organización. Para la construcción del mecanismo, se analizó la norma ISO 27002 junto con la metodología OSSTMM y las mejores prácticas de seguridad en redes inalámbricas (Salinas, 2017).

González y Ponjuán (2014), hizo un recorrido por los referentes teóricos y metodológicos de la auditoría de información a partir de los cuales realiza un análisis de varios aspectos comunes que incluyen, tomados como muestra, 13 metodologías y modelos reportados en la literatura mundial.

Como se puedo observar, existen muchas propuestas de metodología para la realización de auditorías a la seguridad informática, la elección de una u otra dependerá de las necesidades reales de la organización o sector a la que va dirigida la metodología evaluada.

En adición a lo observado anteriormente, se puede decir que en la actualidad existe una rápida proliferación de las redes alámbricas e inalámbricas del tipo Wi-Fi y que las aplicaciones informáticas móviles han cambiado el panorama de la seguridad de las redes, creando nuevas vulnerabilidades que no existen en una red cableada fija, y sin embargo muchas de las medidas de seguridad probadas resultan ser ineficaces en estos casos (Gómez, Herrera, y Díaz, 2017).

Por lo tanto, se necesita desarrollar nueva arquitectura, nueva metodología y mecanismos para proteger y mantener las redes inalámbricas y las aplicaciones de computación móvil libre de incursiones no autorizadas en estas infraestructuras críticas (Zhang et al., 2003).

Cuando hablamos de una infraestructura crítica se refiere al conjunto de recursos, servicios, tecnologías de la información y redes, que en caso de sufrir un ataque causarían gran impacto en la seguridad de la organización, tanto física como económica, o en el normal funcionamiento de los procesos. De lo anterior se desprenden tres criterios: el número potencial de víctimas mortales o de lesiones graves que pueda producir, el impacto económico en función de las pérdidas y el deterioro de productos o servicios, incluido el posible impacto medioambiental y el impacto público producido por la alteración de la vida ciudadana (Ferrero, 2013).

Después de los análisis bibliográficos expuesto aquí, de la realización de una entrevista no estructurada al personal del departamento de TIC en las empresas del sector pesquero industrial del cantón Manta, además de la información brindada por estudiantes de prácticas preprofesionales en este sector, enviados por la universidad, se pudo observar la debilidad en las guías o metodologías para la realización de auditoría informática.

Considerando lo anteriormente explicado, se pudo constatar la necesidad de contar con una metodología para la realización de auditoria de la seguridad informática en la infraestructura de red de datos en las empresas del sector pesquero industrial. Esta metodología permitiría disminuir las vulnerabilidades que ponen en riesgo el buen funcionamiento de los procesos y los objetivos del negocio.

De lo anterior se desprende una serie de objetivos específicos que permiten comparar y evaluar la metodología más adecuada para el sector estudio, pudiéndose complementar con características que le aporten pertinencia, eficiencia, flexibilidad y proactividad.

El contextualizar el ambiente respecto a la seguridad informática en la industria pesquera del cantón Manta, como uno de los objetivos fundamentales en esta investigación, será desarrollado mediante una encuesta estructurada y validada, teniendo en cuenta factores y aspectos consultados en la bibliografía. Además, se determina cuáles son las metodologías con mayor potencial de ser utilizadas para la realización de auditorías de seguridad informática en las organizaciones y se comparan, por medios estadísticos, las distintas metodologías que permitan la realización de auditorías de seguridad informática enfocadas a infraestructuras de redes de datos empresariales.

Una evaluación, entre las distintas metodologías comparadas anteriormente, permitió determinar cuál es la que más se adapta a las empresas vinculadas a la industria pesquera del cantón Manta, Provincia de Manabí, Ecuador.

Además, el presente trabajo constituye una oportunidad de desarrollo en la revisión de los procesos de investigación en auditoria a la seguridad informática y en el estudio y desarrollo de la disciplina, basado en trabajos previos, que le sirven de fundamento, para permitir nuevas investigaciones dentro del plan de seguridad informática, e incluso proponiendo mejoras al mismo.

Desde el punto de vista económico, esta investigación permitiría disminuir gastos innecesarios en los procesos de TICs y evitaría generar en el mercado accionario o en los accionistas dudas, cuando se informa sobre intrusiones y pérdidas de información en el ente empresarial.

Además de las preocupaciones de los ejecutivos de las organizaciones, y en particular de los responsables del área de informática, que se generan en torno a la seguridad de la información, la presente investigación se justifica debido a que para este tipo de empresas no existen metodologías precisas que permitan auditar el control de cumplimiento y rol de la infraestructura informática, habiendo solamente auditorías sobre procesos de seguridad de la información.

Se ha podido evidenciar en la revisión bibliográfica, que no se ha trabajado mucho en lo que respecta a las metodologías para la realización de auditorías de seguridad informáticas en infraestructuras de redes de datos. La gran mayoría de los trabajos hacen referencia a los procesos de la auditoria de seguridad de información y no a una auditoría de control de cumplimiento de controles en las infraestructuras físicas de las redes internas en las organizaciones.

Finalmente, esta investigación se ha convertido en un reto profesional debido a que se realizarán contribuciones basadas en una realidad y de acuerdo con las mejores prácticas de seguridad.

MARCO TEÓRICO

En la presente sección se realiza una revisión literaria de trabajos relacionados y conceptos relevantes con el tema de estudio.

TRABAJOS RELACIONADOS

La información como activo de las organizaciones.

Concepto de información.

Según Capurro (2007), el conocimiento, en la actualidad, es parte de la acción en la que muestra el presupuesto y las consecuencias en los procesos cognitivos y prácticos que están relacionados con la búsqueda de la información almacenada en computadoras, así como con el diseño de dichos sistemas y su papel en la sociedad. El mismo autor cita una definición de la información como ciencia, planteada por Griffith, como objetivo de la producción, recolección, organización, interpretación, almacenamiento, recuperación, diseminación, transformación y uso de la información (Griffith, 1980).

Por otra parte, la RAE, plantea que la información es comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada y que, puede referirse a hechos o circunstancias que otros desconocen, pudiendo generar ventajas a quien dispone de ella.

La información en el contexto de las organizaciones.

En la actualidad, la valoración de la información como un recurso importante en las empresas resulta un hecho significativo, y que toda organización debe atender y administrar para poder enfrentar los retos del desarrollo actual. (Mavis, Rodríguez, Pardo, Licea y Fernández, 2017).

También, en un informe publicado por la empresa francesa vendedora de software Antidot, se expone que, en la actualidad, donde todo se mueve más rápido, la información plantea un desafío estratégico para las empresas, viéndose como un recurso y activo fundamental para cualquier organización, y la clave del negocio en la toma de decisión, la implementación de estrategias y la transferencia tecnológica, permitiendo ventajas competitivas y el valor de las partes interesadas a través de tecnologías de Información (Antidot, 2014; Fallis, 2013).

Aumento y diversificación de la información en las organizaciones.

La información que manejan en la actualidad las empresas es más compleja, estas registran un aumento significativo de sus datos (terabytes, petabytes y exabytes), creados por personas y máquinas y en algún caso puede llegar a cifra del orden de los zettabytes (ZB). (Camargo Vega et al., 2014).

Los datos que se generan pueden ser muy variados, desde páginas web, archivos de búsquedas, redes sociales, foros, correos electrónicos o producto de sensores del internet de las cosas (IoT) en diferentes actividades de las personas y estos se crean a una velocidad muy grande en comparación con lo que sucedía hace pocos años atrás (Yu et al., 2015).

Debido a este aumento y a que se rebasan los límites del modelo tradicional de negocio en lo referido a gestión de instalaciones físicas, las empresas han visto la necesidad de externalizar las tareas de procesamiento de datos a proveedores de servicios de computación en la nube, como Amazon Web Services (González-BBVA, 2015).

Las redes de datos, soporte de la información.

En el mundo actual, las Redes de datos y las Telecomunicaciones juegan un papel fundamental en la transmisión de información y el desarrollo de las funciones y transacciones en el mercado de las empresas (Rodríguez y González, 2015).

Las redes de datos han cambiado la manera en que a los usuarios llega la información, mejorando sus procesos y su capacidad de competir en el mundo de las telecomunicaciones, razón por la cual se debe adoptar soluciones para garantizar la disponibilidad de los servicios, disminuyendo la cogestión y los colapsos importantes. Estas redes y en especial las redes de área local (LAN), fueron diseñadas sin muchas exigencias en cuanto a los parámetros de calidad de servicio como retardo, tasa de pérdidas, entre otros aspectos, pero con el desarrollo de nuevas tecnologías de información y comunicación, se ha impulsado el desarrollo de las mismas, aspecto que ha impactado de manera positiva en la aparición de nuevos servicios y aplicaciones para los cuales las características o parámetros, anteriormente mencionadas, son esenciales (Ríos y Fermin, 2009).
Una LAN es una red de comunicación que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos. Su cobertura es pequeña, generalmente un edificio o un conjunto de edificios cercanos, es propiedad de la misma entidad propietaria de los dispositivos conectados a la red, puede llevar acarreada una inversión sustancial de capital, tanto en la adquisición como en el mantenimiento, de ahí que, la responsabilidad de la gestión de esta recae solamente en la organización que la utiliza (Stallings, 2008).

Estas redes LANs, pueden implementarse de forma cableada o inalámbrica. Por un lado, las redes cableadas no ofrecen flexibilidad en conexión, pero son más seguras para cualquier organización, por otro lado, las redes inalámbricas ofrecen parámetros de uso que proveen flexibilidad en la forma de conexión y de uso, movilidad e impacto frente a la estética de instalaciones y al ahorro de infraestructura, aspecto muy polémico en las redes cableadas de las organizaciones (Monsalve, Aponte y Chaparro, 2015).

Estándares de redes cableadas e inalámbricas.

El estándar más comúnmente utilizado en las redes de datos locales alámbricas es el Ethernet, especificada en las normas 802.3 del Instituto de ingenieros Eléctricos y Electrónicos, IEEE del inglés. En la actualidad, se pudo encontrar cuatro velocidades de datos diferentes en Ethernet utilizando el par trenzado sin blindaje (UTP) como medio para la transmisión: 10 Mb/s (10BASE-T), 100 Mb/s (100BASE-TX), 1 Gb/s (1000BASE-T) y 10 Gb/s (10GBASE-T) (Christensen et al., 2010).

Otro medio de transmisión alámbrica que se pudo encontrar en redes LAN del tipo Ethernet (802.3), a diferencia del par trenzado sin blindaje (UTP), es la fibra óptica. Este medio proporciona mayor ancho de banda que los medios de cobre, manejando servicios de voz, datos y video de mejor calidad (Kramer y Pesavento, 2002).

Por otra parte, tenemos las redes inalámbricas o también conocidas como Redes Inalámbricas de Área Local (WLAN), y en especial las del tipo

Wi-Fi, siendo la sigla para Wireless Fidelity, que literalmente significa Fidelidad inalámbrica. Esta tecnología permite la interconexión inalámbrica de dispositivos electrónicos y está recogida en las recomendaciones 802.11 de la IEEE (Rosero y Ponce, 2016).

Seguridad informática en las organizaciones. Concepto de la Seguridad informática.

Con el incremento acelerado del acceso a Internet y el volumen de intercambio de datos y servicios que brinda, la seguridad se ha convertido en una materia que gana cada vez más importancia para las ciencias de la computación. La seguridad informática no solamente busca proteger a los equipos y datos, sino también a las personas donde la educación y la concientización de los integrantes de una organización en temas de seguridad deben ser valoradas como herramientas útiles contra incidentes peligrosos (Manuel y Ibarra, 2018).

Las organizaciones en la actualidad contemplan la información como un recurso muy importante y como tal deberán incorporar prácticas estándar que permitan una mayor fluidez de las operaciones y negocios en un entorno altamente interconectado. Debido a este escenario, la información se convierte en un foco de acciones de posibles ataques y como tal se ha estado desarrollando prácticas de protección de la información relacionadas a antivirus, sistemas de detección de intrusos, cortafuegos, redes virtuales privadas, cifrado y otras que demandan un conocimiento especifico y personal especializado (Rosero y Ponce, 2016).

De ahí que se pudo definir a la seguridad informática como un conjunto de procedimientos, dispositivos y herramientas que reducen los posibles riesgos a los que se ven expuestos los bienes en una organización, donde se debe establecer normas que minimicen los riesgos en toda la infraestructura. Estos bienes pueden ser tangibles, como la infraestructura física, los servidores, lo seres humanos, las redes, entre otros, o intangibles, como la información, los servicios prestados, las aplicaciones instaladas, entre otros (Baquerizo y Guevara, 2016).

Las organizaciones y la seguridad informática.

Con el uso masivo de las redes informáticas y en especial de la red de redes, Internet, las organizaciones notaron enormes ventajas y posibilidades, convirtiendo a la información procesada, almacenada o transmitida en un activo de suma importancia para cualquier organización (Correa y Díaz, 2007).

Actualmente, en las organizaciones, los datos están más expuestos a ataques, que cuando se venía trabajando de forma aislada física y lógicamente en espacios y redes de comunicación de ámbito local, gestionados y controlados por personal de la propia organización y protegidos por cortafuegos, filtros de acceso y medidas de seguridad tradicionales (González y Julio, 2012).

Los ataques más importantes se deben principalmente a aspectos como las vulnerabilidades de software, malware, dispositivos móviles, personal interno y hackers, en la que cada año que pasa, además de aumentar el volumen absoluto de estas, el escenario de amenazas se va tornado más diversificado, con un trabajo más arduo de los grupos de ataque para descubrir nuevos caminos de ataques y cubrir sus rastros (Symantec, 2018).

En el mismo trabajo de Symantec (2018) se pudo observar que, a principios de enero de 2018, se descubrieron dos vulnerabilidades graves que afectaron a casi todos los chips de procesadores modernos. Conocido como Meltdown y Spectre, las vulnerabilidades podrían permitir a los atacantes obtener acceso no autorizado a la memoria de una computadora.

Estándares de seguridad informática de infraestructura física de redes de datos.

Para que una organización lleve a cabo una correcta gestión y administración de la Seguridad Informática (SI), deberá garantizar una serie de medidas preventivas y reactivas que permitan resguardar y proteger la información garantizando tres principios muy importantes, la confidencialidad, la disponibilidad e integridad de los datos (Baryolo et al., 2012; Burgos y Campos, 2008).

La confidencialidad garantiza que solo las personas autorizadas puedan hacer uso de la información. Por otro lado, la integridad de los datos garantiza una información integra, sin modificaciones por personas no autorizadas, y finalmente, la disponibilidad asegura que la información esté disponible cuando sea necesario y para el personal autorizado (Burgos y Campos, 2008; Galarza, 2018; Parada y Flórez, 2018).

Para garantizar en cumplimiento de los tres principios mencionados, existen organizaciones internacionales que se encargan de definir estándares y normas de gran aplicación a nivel mundial: ISO 17799, COBIT, ITIL, COSO, ISO Serie 27000 y Criterios de la Comisión de Control de Canadá (CoCo).

Si bien estos estándares no especifican o norman solamente aspectos relacionados con la infraestructura física de una red de datos, cada una de estas incluyen capítulos sobre la misma en sus estándares.

La ISO 17799 establece guías y principios generales que garantizan la gestión de la seguridad de la información en una organización (Burgos y Campos, 2008; ISO/IEC 17799, 2005).

Por otra parte, COBIT, acrónimo de “Control Objectives for Information and related Technology” (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar creado y desarrollado por Information Systems Audit and Control Foundation (ISACA). Este estándar se encarga de la gobernabilidad, el control, el aseguramiento y auditorias para TIC, basado en cinco principios básicos que son garantizados por la norma (ISACA, 2012).

Una norma que proporciona las mejores prácticas para la administración de los servicios de TI es ITIL, del acrónimo de “Information Technology Infrastructure Library”, inicialmente utilizada como una guía del gobierno y que en la actualidad es aplicable a cualquier organización (Melendez y Dávila, 2018; Sharifi, Ayat, Rahman y Sahibudin, 2008; Wegmann, Regev, Garret y Maréchal, 2008).

ISO 27000, es una serie de estándares que incluye, entre otras, definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034). En general, este conjunto brinda un marco para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoras de un Sistema de Gestión de la Seguridad de la Información (SGSI) (Estrada, 2011).

Factores que intervienen en la madurez de seguridad informática.

Un modelo de madurez es un conjunto de características, atributos, indicadores o patrones que representan la capacidad y la progresión en una disciplina particular, proporcionando un punto de referencia con el cual una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos y establecer metas y prioridades para la mejora (Curtis, Mehravari y Stevens, 2015).

El Modelo de Madurez de Capacidad de Ciberseguridad para Servicios de Tecnología de la Información (C2M2 para servicios de TI), es un ejemplo de modelo que proporciona ayuda a las organizaciones en la entrega de servicios de TI de todos los sectores, tipos y tamaños para evaluar la mejora de sus programas de seguridad cibernética (Curtis et al., 2015).

Para comenzar un análisis de madurez en una organización Maier, Moultrie y Clarkson (2012), plantean que va a depender de una serie de factores, como son:

a. Que la organización debe tener procesos estructurados y su cumplimiento en el área de dominio clave elegida, además de que estos estén habilitados de manera efectiva mediante la formalidad, la transparencia, las tecnologías y los informes.
b. La organización debe tener una estructura de organización apropiada con puestos de trabajo definidos, roles y políticas de capital humano para comenzar el análisis de la madurez.
c. La organización debe tener una actitud positiva, una mentalidad y una

conciencia hacia el ciclo de aprendizaje en el camino hacia la madurez en el área de dominio clave elegida.

d. La organización debe tener una actitud positiva, una mentalidad y una conciencia hacia el desarrollo de las habilidades de las personas en el camino hacia la madurez.

Para poder identificar y explorar el nivel de madurez en seguridad informática en una empresa, se debe tener en cuenta que las exigencias de seguridad deben estar asociadas a los objetivos comerciales de la organización, en la que se podrían identificar dominios que afectan la seguridad en la misma, como, la gobernanza de la organización, la cultura organizacional, la arquitectura de los sistemas y la administración del servicio (Saleh, 2011).

Edwards (2018), después de su revisión bibliográfica, coincide en gran medida con Saleh (2011) que, para alcanzar la madurez en la seguridad de la información, una organización debe tener una estrategia del programa de seguridad de la información que refleje las necesidades del negocio, que se actualiza constantemente para reflejar los cambios que ocurren en la estrategia y el entorno comercial.

Se expone un modelo de madurez de la seguridad de la información, donde integra tres aspectos o dimensiones fundamentales: la confiabilidad e integridad de la tecnología de seguridad (integridad de la información y aseguramiento de los sistemas de información), la integración de seguridad (negocios estratégicos, procesos y administración de programas) y la custodia de la seguridad (competencia de las personas, conciencia y liderazgo). Además, el autor, partiendo de lo anterior, ha identificado ocho áreas de dominio clave esenciales para lograr la madurez de la seguridad de la información: Integridad de la información, aseguramiento de los sistemas de información, habilitación empresarial estratégica, cultura de la seguridad / empleados conscientes, liderazgo de seguridad, competencia organizacional y madurez del trabajo en equipo, madurez de la gestión del programa / proyecto, madurez del proceso (Edwards, 2018).

Por otra parte, Villegas, Viloria y Blanco (2009) proponen un modelo para determinar la madurez, nombrado Modelo de Madurez de la Gestión de la Seguridad Informática (MMAGSI). Este modelo está bajo el contexto de una organización inteligente, donde es capaz de integrar eficazmente la percepción, la creación del conocimiento y la toma de decisiones.

Además, en el modelo anterior, se integran cinco niveles de madurez: inicio, crecimiento, desarrollo, madurez e inteligencia organizacional, donde cada uno posee sus características que fueron construidas con aspectos relacionados con la planificación estratégica, la cultura organizacional y los elementos de la organización, la gerencia, la estructura organizacional, así como los procesos y tareas.

El modelo COBIT, de ISACA, es un modelo que se utiliza para medir la madurez actual en el estado en que se encuentran los procesos relacionados con las TI de una empresa, para definir un estado de madurez requerido, y para determinar la brecha entre ellos y la forma de mejorar el proceso para alcanzar el nivel de madurez deseado. COBIT 5 inspirado en la ISO/IEC 15504 y los atributos de capacidad del proceso, presenta seis niveles de capacidad, el nivel 0, que representa organizaciones con procesos incompletos o no están implementado; nivel 1, es cuando una organización presenta procesos ejecutado alcanzando su propósito; un tercer nivel, el nivel 2, representa a una administración de TIC donde los procesos están gestionado, es decir, están planificado, supervisado y ajustado; un nivel 3, establecido, donde los procesos están implementado; el nivel 4, proceso predecible, donde estos ya están establecido y se ejecutan dentro de límites definidos para alcanzar sus resultados de proceso; y por último, el nivel 5, denominado proceso optimizado, es cuando existe un mejoramiento continuo de los procesos para cumplir con las metas empresariales (ISACA, 2012).

De la revisión bibliográfica, se ha podido identificar determinados factores que afectan y permiten medir el nivel de madurez tecnológica y de seguridad informática en una organización. Lo anterior permitió establecer once (11) variables: acerca de la empresa, acerca del jefe de TICs, políticas y normas utilizadas en la empresa, presupuesto, integración de tecnologías de seguridad informática, conocimiento de metodologías y normas, Incidencia, prevención y respuesta,

confiabilidad, comunicación de eventos, cultura organizacional y el personal técnico de la organización.

La auditoría de seguridad informática como herramienta para disminuir riesgos informáticos en las organizaciones.

Concepto de auditoria como herramienta de control.

La auditoría, según Muñoz (2002), es una revisión metódica, periódica e intelectual de los registros y resultados encontrados en una organización para poder medir y diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones.

Por otra parte, Álvarez (2004), plantea que la auditoría a la seguridad informática permite verificar el cumplimiento de los reglamentos, procedimientos e instrucciones vigente en materia de seguridad en las organizaciones y que esta debería realizarse al menos una vez al año. Esta se convierte en uno de los servicios de seguridad para mantenerse informado en todo momento de lo que está sucediendo o ha sucedido en el sistema y sin una política de auditoría, no hay manera de saber qué ha pasado ni por dónde han atacado ni qué han hecho los usuarios.

Además, con las auditorías se puede evaluar la madurez alcanzada en materia de seguridad informática; sin embargo, éstas también pueden ser utilizadas en los procesos de mejora continua, las cuales representan un valioso recurso para identificar retos y oportunidades, tomar decisiones oportunamente, concretar y hacerles seguimiento a las acciones necesarias a través de un ciclo PHVA (Planificar, hacer, verificar y actuar) (Yánez y Yánez, 2012a).

Yánez y Yánez (2012), resume los tipos de auditoría de acuerdo con los autores consultados, los mismo que se transcriben en la tabla 1.

Tabla 1.- *Tipos de Auditorias.*

Enfoque	Autor	Tipo de Auditoría
Según el objetivo de la auditoria	Peña Gutiérrez, Alberto (2010)	• Financiera. • Operativa. • Sociolaboral. • Medioambiental. • Ética. • Informática. • De Procesos de Calidad.
Según los elementos que intervienen	Gonzalbes, M.; Medina, J. (2003)	• De primera parte o Auditoría Interna (Auto-auditoria). • De segunda parte. • De tercera parte.
Según la actividad que se evalúa	Parsowith, S. (1999)	• De Sistemas. • De procesos. • De Productos. • De Cumplimiento. • Investigación. • Interna. • Externa de segunda parte. • Externa de tercera parte. • Operativa.

Fuente: Yánez y Yánez (2012)

En la tabla 1, Yánez y Yánez (2012) resume los tipos de auditorías conforme varios autores, destacándose el enfoque según el objetivo de la misma como es la auditoría informática Peña Gutiérrez (2010) donde se necesita que sea realizado por personal especializado garantizando la operatividad de los recursos tecnológicos de la empresa en un ambiente de seguridad y control eficiente, teniéndose la seguridad de que se cuenta con información verídica, integra, exacta y confiable, además de contener observaciones y recomendaciones que impliquen un ciclo de mejora continua de la tecnología de la información de la organización (Rodríguez y Verónica, 2011).

Por otra parte, Yánez y Yánez (2012b), mencionan trabajo de Gonzalbes y Medina (2003), donde destacan un enfoque de primera parte o auditoría interna como una orientación según los elementos que intervienen. Este enfoque se elabora en la propia empresa, a solicitud de la alta dirección, denominada también auto-auditoría.

Por último, se puede observar otra perspectiva según la actividad que se realiza teniéndose la auditoría de cumplimiento planteada por Parsowith. La auditoría de cumplimiento se dirige a comprobar si la organización auditada observa el cumplimiento de las metas y objetivos en la misma, obteniéndose datos que permiten evaluar y establecer los controles adecuados para la mejora continua (Cabezas, 2015; Yánez y Yánez, 2012).

A los fines planteados en esta investigación, y acogiendo la revisión realizada, se evaluó una metodología que permita la realización de auditoría interna a la seguridad informática basada en la comprobación del cumplimiento de los controles de seguridad en la infraestructura física de la red de datos en el sector estudiado.

Metodologías y estándares para la realización de auditorías a la seguridad informática.

Enfoques metodológicos para la auditoría de seguridad informática.

Consultado algunos conceptos y términos propios para la investigación, se puede destacar algunas metodologías para la realización de auditoría informática consultadas en la literatura, que, si bien no se enfocan un 100% a la auditoría de la seguridad informática en una infraestructura de red de datos, brindó una guía para poder elaborar la propuesta de esta investigación.

OSSTMM 3.0

Open Source Security Testing Methodology Manual (OSSTMM) en su versión 3, desarrollada por Pete Herzog de ISECOM (the Institute for Security and Open Methodologies), es un manual basado en una metodología que permite probar la seguridad operativa de las ubicaciones físicas, las interacciones humanas y todas las formas de comunicación, como inalámbrica, por cable, analógica y digital. Además, algo muy interesante de la misma es que se encuentra publicado bajo la licencia Creative Commons 3.0, permitiendo la libre utilización y distribución (Herzog, 2016a).

El documento que contiene la metodología expresa la libertad de lectura, distribución sin fines comerciales, aplicar en investigaciones académicas o comerciales, y es de uso gratuito. Este puede ser aplicado en los siguientes compromisos comerciales: pruebas, educación, consultoría e investigación.

Objetivos.

El objetivo principal de este manual es proporcionar una metodología científica para la caracterización precisa de la seguridad operacional, del inglés operational safety (OpSec), a través del examen y la correlación de los resultados de las pruebas de una manera consistente y confiable, además de poderse adaptar a casi cualquier tipo de auditoría, incluidas las pruebas de penetración, la piratería ética, las evaluaciones de seguridad, las evaluaciones de vulnerabilidad, la formación de Red Team y Blue Team1, entre otros. Está diseñado para la verificación de seguridad objetiva y la presentación de métricas a nivel profesional (Herzog, 2016a).

También se puede apreciar un segundo objetivo, proporcionar pautas que, cuando se siguen correctamente, permitirán al analista realizar una auditoría OSSTMM certificada. Estas pautas pueden asegurar que la prueba se realizó a fondo, incluyó todos los canales necesarios, la postura de la prueba cumplió con la ley y que los resultados se pueden medir de forma cuantificable y son consistentes, repetibles y que estos contienen solo hechos derivados de las pruebas mismas.

Alcance

En el documento de la metodología se aprecia el alcance de este, que es proporcionar descripciones específicas para las pruebas de seguridad operacional sobre todos los canales operativos, que incluyen redes humanas, físicas, inalámbricas, de telecomunicaciones y de datos, sobre cualquier vector, y la descripción de métricas derivadas y solo se enfoca en OpSec, y el uso de las palabras seguridad y protección se encuentran dentro de este contexto. Tabla 2

Tabla 2.- Clasificación de los canales.

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción es tanto física o psicológica.
	Físico	Comprende el elemento tangible de la seguridad donde la interacción

[1] Red Team proviene del ámbito militar y es utilizado en contraposición con el de Blue Team; atacante es Red y el defensor Blue. (Vigna, 2003)

		requiere esfuerzo físico o un transmisor de energía para manipular.
Seguridad Inalámbrica (SPECSEC)	Inalámbricos	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético EM.
Seguridad en las Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicación, digitales o analógicas, donde la interacción se lleva a cabo a través de un teléfono determinado o similar a las líneas de la red telefónica pública.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción se lleva a cabo a través de un cable establecido y líneas de la red cableadas.

Fuente: (Bracho, Cuzme y Pupiales, 2017; Valdez, 2013)

Implementación.

Para comenzar a hacer una prueba OSSTMM, se necesita hacer un seguimiento de lo que prueba (los objetivos), cómo los prueba (las partes de los objetivos probados y no las herramientas o técnicas utilizadas), los tipos de controles descubiertos y lo que no evaluó (objetivos y partes de los objetivos). Luego se realiza la prueba con el objetivo de poder responder las preguntas en el Informe de auditoría de prueba de seguridad, del inglés Security Test Audit Report (STAR), proporcionado por la metodología (Herzog, 2016a).

STAR proporciona la información de prueba específica sobre el estado del alcance de los beneficios de tener una aserción clara de las métricas de seguridad y los detalles para las comparaciones con las pruebas de seguridad anteriores o los promedios de prueba de la industria.

Bracho (2017) describe, haciendo uso de lo planteado por Herzog, las fases de la metodología OSSTMM, versión 3, donde hay cuatro fases en su ejecución: fase de Inducción, de Interacción, de Indagación y de Intervención.

En la primera fase de Inducción o planeación, como toda metodología para una auditoría en su fase inicial, es necesario conocer los requisitos, el alcance y las limitaciones de esta en dicho alcance.

Una segunda fase, la fase de interacción, se elabora un plan de auditoría con el objetivo de recopilar la información de la organización y sus sistemas informáticos, obteniéndose así información global de área que se va a auditar. Esta fase puede ser completada por medio de la observación, la entrevistas con los responsables e integrantes del grupo de TICs y de esta manera el auditor podrá definir concretamente el objetivo general, el alcance y las tareas de la auditoría (Bracho et al., 2017; Herzog, 2016b; Tejada, 2015).

En la fase de indagación o descubrimiento, es donde se llevan a cabo una serie de pruebas para determinar debilidades y fortalezas del sistema informático en la organización que es auditada cuyos resultados permitan detectar debilidades y fortalezas del sistema de información auditado y justifiquen la detección de las evidencias (Tejada, 2015).

Una última fase, la de intervención, es donde el auditor se centra en los recursos que los objetivos requieren en el alcance. Esos recursos pueden intercambiarse, cambiarse, sobrecargarse o dejar de existir por causa de penetración o interrupción al sistema. Esta fase, generalmente, constituye la etapa o fase final de

una auditoría o prueba de seguridad, garantizando que las interrupciones no afecten a las respuestas de las pruebas menos invasivas y porque la información, para hacer estas pruebas, no puede ser conocida hasta que otras fases se hayan completado (Herzog, 2016a).

El OSSTMM se ha convertido en un organismo complejo, pero con un nuevo enfoque en la legibilidad y la facilidad de uso, está lejos de ser complicado de usar.

OWASP

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones en las que se pueda confiar. Además, resuelve la seguridad en aplicaciones como un problema de personas, procesos y tecnología, dado que los enfoques más efectivos para la seguridad en aplicaciones requieren mejoras en todas estas áreas y se encuentra de forma abierta y gratuita (Owasp, 2017).

Por otra parte, Burato, Ferrara y Spoto (2017) describe a OWASP como un conjunto de pruebas de código abierto y gratuito diseñado para evaluar distintos parámetros como la velocidad, así como la cobertura y precisión de las herramientas y servicios para la detección de vulnerabilidades de software permitiendo entender sus fortalezas y debilidades.

OWASP incluyen una Guía de referencia y el documento de autoevaluación OWASP Top 10 donde se presentan los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP, la misma se publica y actualiza cada tres años por dicha organización, la última fue publicada en 2018 con los análisis recogidos en el 2017 (Owasp, 2017).

MAGERIT.

Las normas ISO/IEC-27000 se adaptan por cada país y las mismas han conducido a varias metodologías, como MAGERIT, elaborada y promovida por el Consejo Superior de Administración Electrónica de España, MEHARI, para la gestión y análisis de riesgos desarrollado por CLUSIF (Club de la Seguridad de la Información Francais, Francia), CRAMM (CCTA Risk Analysis and Management Method), fue desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA), aunque en la actualidad es propiedad de SIEMENS, y la misma es destinada a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y sus activos (Vicente, Mateos y Martín, 2014).

Objetivos.

Dentro de los principales objetivos de MAGERIT tenemos, por una parte, concientizar a los responsables de las TICs, en las organizaciones, de la existencia de riesgos y de la necesidad de gestionarlos, además de ofrecer un método sistemático para analizar los riesgos derivados del uso de las TICs y ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control en las organizaciones, además, de preparar a estas para los procesos de evaluación o auditoría, pudiendo logran la certificación o acreditación (Amutio, 2012).

Alcance.

La metodología MAGERIT abarca un gran espectro de intereses de sus usuarios, reflejando todo tipo de activos, todo tipo de aspectos de seguridad; en pocas palabras, todo tipo de situaciones, como cuando se requiere un estudio de las garantías de confidencialidad de la información, un estudio de los ficheros afectos a la legislación de datos de carácter personal, o cuando se requiere un estudio de la seguridad de las comunicaciones y de la seguridad perimetral, cuando sólo se requiere un estudio de la disponibilidad de los servicios o cuando se busca lanzar un proyecto de métricas de seguridad, debiendo identificar qué puntos interesa controlar y con qué grado de periodicidad y detalle (Amutio, 2012).

Según Martínez y Torres (2018), MAGERIT es una metodología para el manejo de la información, tanto digital como física dentro de una organización, contemplando al hardware, software, información electrónica, recurso humano, entre otros, como actores que consumen y producen información.

Implementación.

Existen dos grandes tareas que se llevan a cabo en MAGERIT y se combinan en el proceso gestión de riesgos una el análisis de riesgos, figura 1, una que permite determinar qué tiene la organización y estimar lo que podría pasar, la otra es el tratamiento de estos riesgos, permitiendo organizar la defensa concienzuda y prudente, vigilante de que no pase nada malo y también preparado para contener las emergencias que se puedan presentar, sobreviviendo a los incidentes y seguir operando en las mejores condiciones posibles, reduciendo el riesgo a un nivel residual que la dirección pueda asumir (Amutio, 2012).

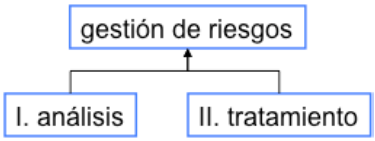

Figura 1. Gestión de riesgos, (Amutio Gómez, 2012)

En la etapa de análisis de riesgos, es donde consideran los activos, que son los elementos del sistema de información que soportan la misión de la organización, las amenazas, que son cosas que les pueden pasar a los activos anteriormente mencionados y que podrían causar un perjuicio y, por último, se considera la implementación de salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen daño. Con los elementos anteriormente mencionados se podría estimar el impacto, lo que podría pasar, y el riesgo, lo que probablemente pase, es decir, se podría realizar el tratamiento o gestión de los riesgos (Amutio, 2012).

COSO

COSO, Committee of Sponsoring Organizations of the Treadway Commission, surge en el año 1992, por la necesidad de integrar metodologías y conceptos en los niveles administrativo y operativos de una organización, permitiendo que sea más competitiva y que responda a las nuevas exigencias empresariales de la época, teniéndose una nueva perspectiva sobre el control interno recogida en el informe COSO I, que generalmente se conoce como Enterprise Risk Management (ERM) (Carpenter y Jones, 2015).

Este informe, se estableció como un marco por las empresas para mejorar sus actividades de control. Debido a la complejidad de las organizaciones al pasar el tiempo, se fue extendiendo el alcance de estudio del Informe COSO y se ha optado por hacer una actualización, así ha emitido el COSO III o COSO 2013 en el que se desarrollan los 5 componentes ya conocidos en anteriores informes, a través de 17 principios y puntos de enfoque (Otiniano y Miranda, 2015).

Objetivos.

COSO, se enfoca en varios objetivos principales, los recursos, estratégicos y operacionales, Informes e Indicadores de cumplimiento, analizándose los riesgos ambientales y de procesos (COSO, 2013; Jaime, Henao y Loyo, 2012).

Alcance.

Este marco está enfocado a toda la empresa u organización, principalmente a la dirección, permitiendo operaciones efectivas y eficientes, además del logro de Informes financieros confiables y el cumplimiento de las leyes y regulaciones. En las organizaciones modernas se puede evidenciar una gran cercanía entre las distintas áreas de esta y los sistemas de información computacionales, de ahí que este marco ha sido replanteado su alcance al área informática para ser coherente con los momentos actuales (Burgos y Campos, 2008).
Implementación.

COSO III o también conocido como COSO 2013, se desarrollan los 5 componentes ya conocidos en la versión anterior a través de 17 principios y puntos de enfoque. Tabla 3

Tabla 3.- Principios de control interno COSO.

Ambiente de control
1. Compromiso con la integridad y los valores éticos.
2. Supervisión independiente de la junta de directores.
3. Estructuras, líneas de reporte, autoridades y responsabilidades
4. Atraer, desarrollar y retener personas competentes.
5. El personal es responsable del control interno.
Evaluación de riesgos

6. Objetivos claros especiales.
7. Riesgos identificados para el logro de los objetivos.
8. Potencial de fraude considerado.
9. Importantes cambios identificados y evaluados.
Actividades de control
10. El control activo, seleccionado y desarrollado.
11. Controles generales de TI seleccionados y desarrollados.
12. Controles desarrollados a través de políticas y procedimientos.
Información y comunicación
13. Información de calidad obtenida, generada y utilizada.
14. Información de control interno comunicada internamente.
15. Información interna comunicada externamente.
Actividades de monitoreo
16. Evaluaciones continuas y / o separadas realizadas
17. Deficiencias de control interno evaluadas y comunicadas.

Fuente: Graham (2015); Moeller (2014)

NIST 800-115

NIST 800-115, es una guía técnica o pautas para evaluar y probar la seguridad de la información y la misma fue publicada en 2008 por el Laboratorio de Tecnología de la Información (ITL) adscrito al Instituto Nacional de Estándares y Tecnología (NIST) del gobierno de los Estados Unidos de Norteamérica. NIST, promueve la economía de los Estados Unidos y el bienestar público al proporcionar un liderazgo técnico para la medición de infraestructuras y aplicación de normas en el país (Scarfone, Souppaya, Cody y Orebaugh, 2008).

Objetivos.

El propósito de este documento es proporcionar pautas para que las organizaciones planifiquen y realicen pruebas y evaluaciones de seguridad de la información técnica, analicen los hallazgos y desarrollen estrategias de mitigación. Esta Evaluación de Seguridad de la Información (ESI), es organizada como un proceso para determinar cuan eficazmente es una organización en la evaluación frente a objetivos específicos de seguridad, definiendo como activos y objetos de evaluación los servidores, redes de datos, procedimientos y personas.

Alcance.

Estas pautas presentan técnicas y métodos de prueba y examen que una organización podría usar como parte de una evaluación, ofreciendo información a los evaluadores sobre su ejecución y el posible impacto de amenazas que pueden tener en los sistemas y redes. Para que esta evaluación sea exitosa y tenga un impacto positivo en la seguridad de un sistema de información los elementos más allá de la ejecución de las pruebas y el examen deben respaldar el proceso técnico (Hahn y Govindarasu, 2011; Scarfone et al., 2008).

Esta guía realiza una descripción general de los elementos claves de las pruebas y evaluaciones de seguridad técnica, especificando determinadas técnicas, teniendo en cuenta sus beneficios, limitaciones y recomendaciones para su uso. De ahí que la guía no propone un programa completo para la evaluación de la seguridad de la información (Hahn y Govindarasu, 2011).

Implementación.

La NIST SP 800-115 propone un proceso de ESI compuesto por tres fases. La planificación, esta fase es muy importante, donde se recolecta información sobre los activos que serán evaluados, las amenazas que se presentan para estos activos y cuáles serían los posibles controles para mitigar esas amenazas si son materializadas. Por otra parte, la fase de ejecución identifica las vulnerabilidades, a fin de comprobarlas según la planificación establecida, aplicándose técnicas y métodos de evaluación propios del objetivo de la ESI que será evaluado.

Y, por último, la fase de post-ejecución, donde se lleva a cabo el análisis de las vulnerabilidades que se han encontrado en la fase anterior para determinar la raíz causa de su presencia, estableciendo recomendaciones para su mitigación y desarrollar el informe final (Hahn y Govindarasu, 2011).

ITIL

Con el pasar del tiempo, se ha visto como las organizaciones van dependiendo de las herramientas informáticas para llevar a cabo sus procesos y poder lograr sus objetivos empresariales, de ahí que la complejidad de los procesos ha hecho crecer la demanda y necesidad de las entidades, ya sea públicas o privadas, de disponer de guías técnicas que les permitan gestionar su infraestructura TI más fácilmente, dando así soporte a los objetivos del negocio (Iqbal y Nieves, 2011).

Debido a las necesidades anteriormente planteadas, el gobierno británico, en la década de los 80 del siglo pasado ideó y desarrollo una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costos derivados de los recursos de TI, naciendo la idea a través de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico para la creación de ITIL (del inglés Information Technology Infrastructure Library) (Ríos, 2014).

Después de actualizaciones, desde su lanzamiento en la década de los 80, en el año 2011 se establece ITIL Ver 3 por AXELOS, una empresa conjunta, creada en 2013 por la oficina del gabinete en nombre del gobierno de Su Majestad (HMG) en el Reino Unido, donde las mejores prácticas son detalladas en cinco publicaciones principales, Estrategia de Servicio de ITIL Ver 3, Diseño de servicio de ITIL Ver 3, Transición del servicio de ITIL Ver 3, Operación de servicio de ITIL Ver 3 y Mejora continua del servicio de ITIL Ver 3 (AXELOS, 2007; Iqbal y Nieves, 2011; Ríos, 2014).

Objetivos.

ITIL describe procesos, procedimientos y tareas para permitir que cualquier organización pueda integrarse a la estrategia del negocio, entregar valor y un mínimo valor de competencia para que la misma esté a la vanguardia y pueda competir en el mercado. Este también, establece una línea base para planear, implementar y medir los servicios definidos por el negocio, demostrando su cumplimiento, midiendo y definiendo mejoras (Ríos, 2014).

Alcance.

El conjunto de buenas prácticas de ITIL, se aplica a la gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones. Estas buenas prácticas se recopilaron gracias al aporte de diversos expertos. ITIL se considera en la actualidad como el marco de trabajo y la filosofía compartida por quienes utilizan las mejores prácticas ITIL en sus organizaciones (Ríos, 2014).

Implementación.

Como ya hemos visto, ITIL Ver 3 está conformado por 5 documentos figura 2, cada uno proporciona la guía necesaria para un enfoque integrado según lo requerido por la especificación estándar ISO / IEC 20000 y se representa en forma de flujo de funcionamiento o ciclo de vida que representa a estas publicaciones.

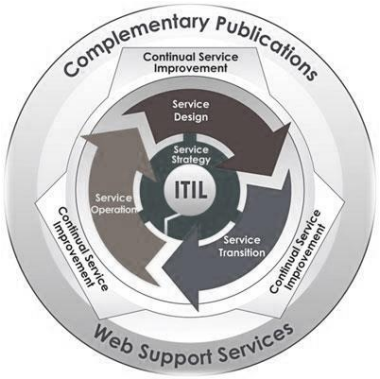

Figura 2. Flujo de funcionamiento de ITIL / Relación con las publicaciones. (S. Ríos, 2014)

El ciclo de Deming, como estrategia para la mejora continua de la calidad.

La mayoría de los procesos de gestión de tecnología en las organizaciones tienen objetivos que se desean cumplir presentando su estructura y tareas a desarrollar. Estos objetivos se intentan conseguir desarrollando unos contenidos a través de la realización de actividades, en las que finalmente se realiza el proceso de evaluación para comprobar si los mismos han sido cumplidos, de no ser así se tomarían acciones pertinentes para la redefinición de los objetivos en caso de que fuera necesario (Pérez, 2011b).

Para el proceso de redefinición y mejoras que se plantean en los procesos de gestión de las tecnologías de la información pueden tomarse los trabajos realizados por William Edwards Deming, (Deming, 1989), que, en un intento de fomentar y simplificar la utilización del modelo de dirección estratégica de la tecnología y basándose en un concepto ideado por Walter A. Shewhart desarrollado en 1939, adaptó el mismo al ciclo de Shewhart a la denominada rueda de Deming o ciclo Deming (PDCA, del inglés plan-do-check-act, esto es, planificar-hacer-verificar-actuar), (véase figura 3). El autor lo difundió usándolo como ciclo de mejora para la gestión (Benavides y Quintana, 2007; Deming, 1989; Mondelo, 2015).

Mavis (2017), en su trabajo propone el ciclo de mejoras para diagnosticar la gestión de la información en una empresa de servicios informáticos del sector turístico con un enfoque de arquitectura de información empresarial, debido al carácter sistémico y de mejora continua, teniendo en cuenta que la mejora continua es una actividad recurrente para aumentar la capacidad para cumplir los requisitos (Manuel García, Quispe y Ráez, 2003), de este procedimiento. Una vez que se complete el ciclo del procedimiento, se vuelve a retomar la primera fase para evaluar el impacto de las mejoras propuestas en la gestión de la información. En este caso se puede apreciar la utilización del ciclo Deming.

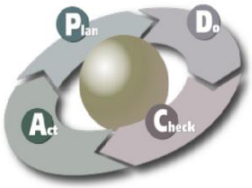

Figura 3. Ciclo de mejoras continua, PDCA. (Pérez, 2011a)

En el ciclo de mejoras de Deming, los datos, que se obtienen de la observación, anteceden a la fase de Planificación o Plan, donde su importancia está en los objetivos y procesos necesarios para alcanzar los resultados requeridos por la organización, y ésta antecede a la fase Acción o Do que es el experimento para la implementación de nuevos procesos y se recomienda realizarlos a través de pruebas piloto para ir verificando su correcto funcionamiento antes de su aplicación final, en la etapa Check, el estudio, en otras palabras, es el experimento que, tras ser verificada en la etapa Check, se traduce en la Actuación o Act, donde se lleva a cabo la intervención (Delgado, Chamba y Santana, 2018; Mondelo, 2015).

En el año 2018, se desarrolló una nueva versión de ITIL, la versión 4 siendo publicado su primer módulo a principio del año 2019. Esta versión, que seguirá publicando módulos durante el año 2019, proporciona una imagen holística de la prestación de servicios de TI, permitiendo transitar con éxito en el mundo digital moderno e integra conceptos de modelos como Lean IT, Agile y DevOps. AXELOS, plantea que, debido a la velocidad de cambio en las organizaciones, se debe continuar con las habilidades de los módulos intermedios de ITIL v3 para que se pueda enfrentar los desafíos inmediatos de TI (AXELOS, 2019).

ESTANDARES TIA/EIA.

Las Normas y Publicaciones de Ingeniería de Telecommunications Industry Association (TIA) están diseñadas para servir al interés público eliminando malentendidos entre fabricantes y compradores, facilitando la intercambiabilidad y mejora de productos, y ayudando al comprador a seleccionar y obtener con la menor demora el producto adecuado para su necesidad particular. La misma no aborda todos los problemas de seguridad asociados con su uso o con todos los requisitos reglamentarios aplicables (Telecommunications Industry Association, 2001).

Dentro de estos estándares se presentan algunos que están más enfocados a la infraestructura de telecomunicaciones, como son, ANSI/TIA/EIA-568-B.1, B.2 Y B.3, estas recomendaciones fueron emitidas en el año 2001 para remplazar a las ANSI/TIA/EIA-568-A.

La ANSI/TIA/EIA 568-B.1, son normas de cableado y relacionadas, las ANSI/TIA/EIA 568-B.2, se refieren a los componentes para el cableado de Par Trenzado No blindado (en inglés: Unshielded Twisted Pair o UTP) y ANSI/TIA/EIA 568-B.3, referido a los componentes de cableado con fibra óptica (Betancourt, Cevallos y Aguilar, 2013).

Como ANSI/TIA revisa los estándares cada 5 años, donde los estándares se reafirman, anulan o revisan de acuerdo con las actualizaciones enviadas, las nuevas versiones

de ANSI/TIA/EIA 568 vieron la luz en February 2009. ANSI/TIA-568-C.0, es el primer documento emitido en ese entonces donde se especifican los requisitos para el cableado de telecomunicaciones genéricas, además de los requisitos para la estructura del sistema de cableado, las topologías y las distancias, la instalación, el rendimiento y las pruebas (Ansi/Tia-568-C.0, 2009).
Un segundo documento, el TIA-568-C.1, abarca los requerimientos para la implementación del cableado estructurado en edificios comerciales en un entorno de campus. Define los términos, especifica la topología del cableado, enumera los requisitos de cableado, establece distancias de cableado, establece las telecomunicaciones configuraciones de salida / conector y proporciona información adicional útil (Ansi/Tia-568-C.1, 2009).

El tercer documento, el ANSI/TIA-568-C.2, especifica los requisitos mínimos para el cableado de telecomunicaciones de par trenzado balanceado (por ejemplo, canales y enlaces permanentes) y componentes (por ejemplo, cable, conectores, hardware de conexión, cables de conexión, cables de equipos, cables de área de trabajo y puentes) que se utilizan en las tomas y conectores de telecomunicaciones y entre edificios en un entorno de campus. Esta Norma también especifica los procedimientos de prueba de campo y los procedimientos de medición de referencia de laboratorio aplicables para todos los parámetros de transmisión (TIA-568-C.2, 2009).

Otras normas y publicaciones de Ingeniería de Telecommunications Industry Association (TIA) son las recogidas en los documentos ANSI/TIA-569. En estos se pudo ver diferentes escritos como son, ANSI/TIA/EIA-569-A, El objetivo principal de esta norma es proporcionar especificaciones de diseño y orientación para todas las instalaciones de edificios relacionadas con los componentes y sistemas de cableado de telecomunicaciones. Este estándar identifica y aborda seis componentes destacados de la infraestructura del edificio: instalación de entrada al edificio, sala (s) de equipos, Backbone Pathways, Salas de telecomunicaciones, vías horizontales y áreas de trabajo (Ansi/tia/eia-569-A, 2012).

También tenemos la norma ANSI/TIA/EIA-569-B (2012), donde se especifica los requisitos para vías y espacios de telecomunicaciones. Como las telecomunicaciones hoy en día han evolucionado mucho, en comparación a años anteriores, donde incluye voz, datos y video, se han establecido estándares para garantizar la operatividad, flexibilidad, capacidad de administración y longevidad de estos sistemas críticos de soporte comercial. Esta norma describe de manera concisa los elementos de diseño arquitectónico de las vías de cableado y salas dedicadas para equipos de telecomunicaciones.

TIA/EIA 606 A, como otro estándar de esta familia de estándares, abarca lo relacionado a la administración para la infraestructura de telecomunicaciones en edificios comerciales, cableado y rutas horizontales, cableado y rutas verticales, puestas a tierra, espacios y retenedores de fuego y tiene como objetivo aumentar el valor de la inversión del propietario del sistema en la infraestructura mediante la reducción de la mano de obra, gasto de mantener al sistema, extendiendo la vida útil del sistema y proporcionando un servicio efectivo a los usuarios (ANSI/TIA/EIA/606A, 2006).

El alcance de esta norma es asignar identificadores a los componentes de la infraestructura, además de especificar reportes presentando la información en grupos de registros y los requerimientos gráficos y símbolos. Esta determina 4 clases de administración dependiendo de la complejidad de la infraestructura a administrar, por una parte, la Clase 1, es cuando existe un solo cuarto de equipo que hace la función de cuarto de Telecomunicaciones y además no existen cuartos adicionales de Telecomunicaciones, ni cableado vertical.

En una infraestructura de Clases 2, existe uno o múltiples espacios de Telecom (un cuarto de equipo con uno o varios cuartos de Telecom) e incluye los elementos de la Clase 1 más cableado vertical, conexiones a tierra, retenedores de fuego; por otra parte, la Clases 3, es cuando existen áreas del tipo campus (incluyendo edificios y cableado externo), también incluye los elementos de la Clase 2 más, identificadores por edificio e identificadores para el cableado externo y por último la Clase 4, que presentan múltiples SITES (cuartos de equipo), incluye los elementos de la Clase 3 más identificación para cada SITE, identificadores para elementos entre campus.

ANSI/TIA/EIA-607, es la primera edición del estándar norteamericano para unión y conexión a tierra (puesta a tierra) de telecomunicaciones, esta fue publicado por TIA en 1994, luego parte de la Electronic Industries Alliance (EIA), como ANSI/TIA/EIA-607, estableciendo los requisitos de conexión a tierra y unión de telecomunicaciones para edificios comerciales (Linares et al., 2014).

ESTÁNDARES ISO.

Actualmente, el activo más importante en las organizaciones, la información, se ve amenazado de manera diversas, aumentando los niveles de riesgos sobre este, por lo que se ve la necesidad de contar con la habilidad de identificar y eliminar vulnerabilidades sobre los activos. De ahí la importancia de que estas cuenten con un Sistema de Gestión de Seguridad de la Información (SGSI), que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros y establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros (ISOtools, 2013).

También, en la guía ISOtools (2013), se plantea que, para poder cumplir con los objetivos de evaluar, establecer controles y plantearse estrategias, se pudo utilizar la norma ISO 27001:2013 para una solución de mejora continua en base a la cual puede desarrollarse un SGSI. La ISO 27001 es un sistema enfocado en el ciclo de mejora continua o rueda de Deming, que consiste, como ya sabemos, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act).

Los requisitos definidos en la norma 27001: 2013, son genéricos y tienen por objetivo ser aplicables a todas las organizaciones sin importar el tipo, tamaño o naturaleza (Instituto Nacional de Normalización de Chile, 2013).

Dentro de la serie ISO/IEC 27000, encontramos la ISO/IEC 27002: 2013, la misma que se encarga de la selección, implementación y gestión de controles teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización (Coster, Andy;Magee, 2017).

Este Estándar Internacional ISO/IEC (2013), está diseñado para ser utilizado por organizaciones que tienen la intención de:

a) seleccionar controles dentro del proceso de implementación de un SGSI basado en el estándar ISO/IEC 27001;
b) implementar los controles adecuados para un SGSI;
c) desarrollar pautas específicas para la gestión de su SGSI.

METODOLOGÍA.

Estudio

En primer lugar, en esta investigación de tipo descriptivo, se realiza un estudio de caracterización del sector industrial pesquero del cantón Manta, Provincia de Manabí, Ecuador apreciándose un enfoque cuantitativo, donde se obtiene información de la madurez de la seguridad informática de este sector de estudio mediante datos recolectados por un cuestionario estructurado y validado.

Luego, se realizó un análisis descriptivo de las metodologías, para identificar su potencial aplicación en la realización de auditorías de seguridad informática en el sector estudiado.

Una evaluación entre las distintas metodologías comparadas anteriormente es realizada para determinar cuál es la que más se adapta a las empresas vinculadas a este estudio.

Técnica utilizada

Implementación de cuestionario vía on–line de manera anónima.

Ámbito

Se encuestó a los jefes de sistemas de 12 empresas del sector pesquero industrial del cantón Manta, Ecuador.

Tipo de muestreo

El estudio de una muestra permite, de manera más rápida y económica, conocer y extrapolar los resultados de esta en una población de estudio (Casal y Mateu, 2003; Otzen y Manterola, 2017).

Las muestras pueden ser obtenidas de dos maneras, por medio estocástico (aleatorio) y no probabilísticos, en la que el muestreo estocástico o probabilístico, permite a cada elemento de estudio tener la misma probabilidad de ser incluido en la muestra. Por otra parte, el muestreo no probabilístico va a depender de ciertas características, criterios, etc., que el investigador considere, quedando estas muestras en ocasiones con más sesgo (Otzen y Manterola, 2017; Supo, 2014a).

Debido a los objetivos planteados, el acceso a la información y lo planteado anteriormente por los autores, en esta investigación se ha seleccionado un muestreo no probabilístico por conveniencia estratificado, donde no se garantiza que todos los elementos que integran a la población tengan la misma oportunidad de ser incluidos en la muestra y no depende de la probabilidad sino de causas relacionadas con la investigación y el acceso a las fuentes de información (Sampieri, Fernández y Baptista, 2014; Supo, 2014a).

Este muestreo no probabilístico por conveniencia, o Intencional, permite considerar aquellas empresas del sector pesquero industrial de Manta supuestamente típicas de la población que se desea conocer decidiendo cuales integrarán la muestra de acuerdo a la percepción y a los que se tiene fácil acceso y se determinó que los jefes de sistemas o TIC de las organizaciones sean las fuentes de información por el nivel de experiencia en los temas que involucra la investigación (López, 1997; Ruiz et al., 2011).

Población y muestra

En esta investigación la cantidad de empresas encuestadas fueron 12, de un total de 15 que están registradas en la nómina de industrias activas afiliadas a la cámara de industrias de Manta, perteneciente al sector pesquero industrial del cantón Manta.

El interés fundamental es estudiar a la población y no a la muestra (Supo, 2014). En este caso el planteamiento es factible por la cantidad de empresas a encuestar, donde la población es muy parecida a la muestra, teniéndose casi el 100 % de la población.

Trabajo de campo

El periodo de realización de la encuesta fue el comprendido entre el 3 y el 7 de agosto de 2018, de lunes a domingo de manera on-line.

La duración media de la encuesta fue de 15-30 minutos, cumpliendo todo el cuestionario.

Proceso de validación del instrumento.
Para García, Rodríguez y Carmona (2009): “El desarrollo de concesionario o instrumento de medición es un proceso laborioso y complejo y requiere la comprobación de su utilidad antes de su aplicación”.

Esta investigación, se consideró lo planteado por los autores y se realiza un proceso de validación, primero del contenido, luego de la confiabilidad interna del instrumento y finalmente la validación del constructo, del cuestionario de recolección de datos para comprobar si el mismo mide aquello para lo que fue diseñado.

Utilizando como antecedente parte del estudio de Maroco y Garcia (2006) y de Ledesma (2004) los cuales tuvieron como objetivo: presentar y discutir el método de Cronbach (Cronbach, 1951), con énfasis en la inferencia sobre este índice y en las propuestas alternativas a este método de estudio de la consistencia interna. En estos estudios se evidenció que ninguna prueba es definitiva e incluyen limitaciones, además, expone dos aplicaciones que ayudan a la comprobación de la validez, que son SPSS y el STATISTICA.

En esta investigación, se utiliza SPSS, para la validación del instrumento de recolección.

A continuación, se presenta la metodología que se utilizó para la validación del instrumento en esta investigación:

Paso 1: Realización de consultas o entrevistas no estructuradas a especialistas involucrados en contexto de la investigación.

Paso 2: Determinación de los componentes del Instrumento con las variables de la investigación, basados en la bibliografía consultada.

Paso 3: Se diseñó el instrumento de tipo escala con base en la metodología establecida: (apoyo

del juicio de expertos para la validación del contenido).

En este paso se midió el grado en que el instrumento refleja el dominio específico de las dimensiones, subdimensiones y los ítems que fueron aplicados (Cruz y Muñoz, 2015).

Se utilizaron cuatro categorías de evaluación de expertos, suficiencia, claridad, coherencia y relevancia, que dependió de los indicadores establecidos para emitir una calificación por cada experto para luego realizar un análisis de validez y consistencia del instrumento con la determinación del coeficiente de concordancia W de Kendall, obteniéndose a partir del análisis de los índices o medias de cada categoría (Dorantes, Hernández y Tobón, 2016).

Paso 4: Se validó el instrumento por medio de técnicas estadísticas, especialmente Alfa de Cronbach, que es un coeficiente que sirve para medir la fiabilidad de una escala de medida. De esta manera se realizó un análisis de consistencia interna para evaluar la homogeneidad intrínseca del instrumento siendo este una medida del error instrumental (Bhatnagar, Kim y Many, 2014; Salas y Monte, 2012).

En este paso se determinó si existe correlación entre los ítems y el total, utilizando SPSS como herramienta estadística.

Paso 5: Por último, se procedió a la validación de constructo, utilizando el coeficiente de alfa de Cronbach para determinar la correlación que existe entre los dominios y el índice total.

En este último paso se ejecutó un análisis factorial para ver si es necesario reducir las dimensiones o dominios (Fernández, 2015; Nuviala, Grao, Teva, Pérez y Blanco, 2013).

Características de la encuesta

La encuesta se encuentra configurada por un total de 69 preguntas, incluidas las relativas a los datos identificativos de la empresa a efectos estadísticos y de contacto.

Los dominios en que se encuentra dividida son:

1. Información general organizacional.
2. Gestión de procesos basados en competencia en la organización.
3. Marco normativo.
4. Gestión estratégica administrativa-financiera-operacional en seguridad informática.
5. Gestión de riesgos en seguridad informática.
6. Gestión de auditoria en seguridad informática.
7. Infraestructura de red de datos: continuidad operativa y servicio empresarial.
8. Excelencia en seguridad informática.
9. Clima organizacional en seguridad informática.

Con la encuesta anterior, se pudo conocer la madurez en seguridad informática de la infraestructura de redes de datos en el sector industrial pesquero del cantón Manta, Provincia de Manabí, Ecuador.

Comparativa.

El análisis comparativo constituye una de las herramientas metodológicas más interesantes y útiles para el estudio de muchos fenómenos. En este trabajo investigativo, para la comparación de las metodologías y normas consultadas en la bibliografía, se utilizaron dos métodos, con el fin de detectar las semejanzas o diferencias que se establecen entre las mismas variables.

Uno de los métodos para la realización de comparativas entre opciones o variables relacionadas de las opciones, es el llamado no paramétrico, que no requiere de hipótesis sobre la distribución de los datos, estableciendo ciertas propiedades que debe satisfacer el conjunto de posibilidades, resultando más fáciles de implementar a diferencia del paramétrico, que, son un tipo de pruebas de significación estadística que cuantifican la asociación o independencia entre una variable cuantitativa y una categórica (E. González, Álvarez y Arias, 1996; Lajo, Bartolomé, Andrés,

Miguel y Cabrera, 2002; Pértega y Fernández, 2006; Rubio y Berlanga, 2012).

En el presente trabajo se utilizará el método no paramétrico para la comparación directa de opciones.

Además, se ha pretendido realizar un análisis comparativo por medio de la técnica de comparación pareada, el llamado Proceso Analítico Jerárquico o más conocido del inglés AHP (Analytic Hierarchy Process).

La comparación pareada permite comprobar la convergencia de una lista de alternativas (Marin, Aragonés y García, 2014), usando entre 7 y 9 niveles en la comparación para proporcionar suficiente rango de incertidumbre, sin complicar en exceso el proceso de comparación, cumpliendo con los planteamientos de criterios coincidente con los planteados por Saaty en su escala binaria que se muestra en la Tabla 4 (Saaty, 1987; Saaty, 2008).

Tabla 4.- Escala de comparación binaria de Saaty.

Escala numérica	Definición	Explicación
1	Igual importancia	Los dos elementos contribuyen igualmente a la propiedad o criterio.
3	Moderadamente más importante un elemento que el otro	El juicio y la experiencia previa favorecen a un elemento frente a otro.
5	Fuertemente más importante un elemento que en otro	El juicio y la experiencia previa favorece fuertemente a un elemento frente a otro.
7	Mucho más fuerte la importancia de un elemento que la del otro	Un elemento domina fuertemente. Su dominación está probada en la práctica.
9	Importancia extrema de un elemento frente al otro	Un elemento domina al otro con el mayor orden de magnitud posible.
2,4,6,8	Valores intermedios entre dos juicios adyacentes	Se usan como valor intermedio entre las anclas de juicios explícitas de los niveles 1, 3, 5, 7 y 9

Fuente: R. W. Saaty (1987)

Por último, se podría emitir juicio de valor, resultado de la evaluación comparativa, coherente a las características de empresas del sector objeto de estudio, cumpliendo con el alcance de esta investigación.

ANÁLISIS DE RESULTADOS.

Teniendo en cuenta la metodología propuesta para esta investigación, se realizaron determinados procedimientos que evidenciaron resultados concluyentes en este estudio.

En nuestra metodología de recolección de datos, se ha seleccionado un muestreo no probabilístico por conveniencia estratificado, no depende de la probabilidad sino de causas relacionadas con la investigación y el acceso a las fuentes de información (Sampieri et al., 2014; Supo, 2014a).

El tipo de muestreo, que se plantea en el párrafo anterior, fue el concluyente debido a que el instrumento no fue completado por toda la población, evidenciándose una limitación en este estudio.

El problema fundamental en la recolección de datos fue debido a que se realizó de manera autónoma y vía on-line, para garantizar la confidencialidad del origen de la información. Lo anterior originó, que tres (3) empresas no contestaran al instrumento y por razón de tiempo, no se pudo esperar a que lo completaran.

Debido a lo anterior, se vio la necesidad de validar nuestro estudio por medios estadísticos con la utilización de herramientas como el SPSS.

Validación del estudio.

Para esta validación, se planteó una pregunta de investigación: ¿El número de respuestas al cuestionario tiene que ver con cómo es

evaluada la seguridad informática en las empresas?

Teniendo en cuenta el enunciado de esta pregunta se pudo plantear la presencia o ausencia de hipótesis y como este enunciado es una proposición, la validación llevará una hipótesis (Supo, 2014b).

Supo (2014b), propone un procedimiento para llevar a cabo la prueba de hipótesis, que fueron planteados por Fisher hace 50 años y este los actualizó. Los pasos del procedimiento son:

- Primero: plantear el sistema de hipótesis.
- Segundo: establecer el nivel de significancia.
- Tercero: elegir del estadístico de prueba.
- Cuarto: dar lectura al p-valor calculado.
- Quinto: tomar una decisión estadística.

De la pregunta anteriormente planteada se desprenden dos hipótesis:

La primera, la hipótesis nula, que se denota con la letra H mayúscula y el número cero, H0:

H0: El número de respuestas al cuestionario No tiene que ver con cómo es evaluada la seguridad informática en las empresas.

Por otra parte, la segunda, la hipótesis alterna, que se denota por la letra H mayúscula y el número uno:

H1: El número de respuestas al cuestionario tiene que ver con cómo es evaluada la seguridad informática en las empresas.

Luego del planteamiento de las hipótesis, se establece un nivel de significancia (alfa) de un 5%, según la bibliografía. Este nivel de significancia permite saber cuánto de probabilidad de error tipo I se está dispuesto a aceptar. En esta investigación se está dispuestos a aceptar un 5% o menor de error aceptando la hipótesis H1 (Supo, 2014b).

Seleccionar el estadístico de prueba es fundamental para este procedimiento estadístico. El Tau b de Kendall, es el seleccionado que se utiliza mayormente en variables ordinales como nuestro caso (Bello, Bello, García y Casas, 2016).

Dando lectura al p-valor calculado por el software estadístico, en la Tabla 5, se puede observar que el Valor de P es igual a 0,587 = 58,7 %.

Tabla 5.-*Correlaciones con Proporción de respuestas con Media total (índice Total).*

			Índice Total	Proporcion de Respuestas
Tau_b de Kendall	índice Total	Coeficiente de correlación	1,000	,121
		Sig. (bilateral)		,583
		N	12	12
	Proporción de Respuestas	Coeficiente de correlación	0,121	1,00
		Sig. (bilateral)	0,583	
		N	12	12

Fuente: Autor.

Dado que el P valor es mucho mayor que 0,05, valor de nivel de significancia que permite determinar cuánto se está dispuesto a aceptar si se opta por la H1, entonces, se rechaza la hipótesis H1 del investigador.

Además, en la figura 4 se puede apreciar la distribución entre la proporción de respuestas, teniendo en cuenta que la población es 15 empresas del sector pesquero industrial de Manta y los que respondieron al instrumento fueron 12, y el índice total de como respondieron. Se puede ver que no hay una distribución lineal definida y que las variables no se correlacionan en gran medida (Morales, 2012).

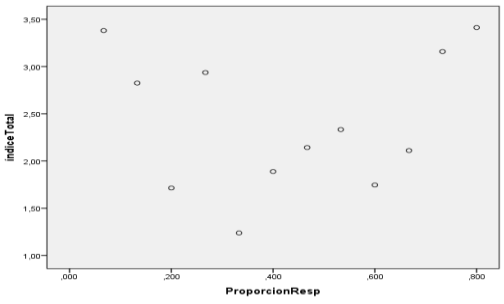

Figura 4. Distribución de Correlación entre la Proporción de respuestas y la Media Total.

Con una probabilidad de error de 0,587 = 58,7 %, se pudo concluir que el número de respuestas al cuestionario No tiene que ver con cómo es evaluada la seguridad informática en las empresas.

En este caso se acepta la hipótesis nula y se rechaza la hipótesis del investigador.

Validación de contenido.

En la metodología planteada, en el paso 3 del proceso de validación del instrumento, se realiza la validación del contenido de este. En este paso se midió el grado en que el instrumento refleja el dominio específico de las dimensiones, subdimensiones y los ítems que fueron aplicados.

En una primera parte, se aplicó el formato de evaluación de pares experto, en la que se utilizó cuatro categorías de evaluación de expertos, suficiencia, claridad, coherencia y relevancia, que dependiendo de los indicadores establecidos se emitió una calificación por cada experto para su validación, figura 6.

Tabla 6.-Resultados de la evolución de expertos.

Nro. Juez	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	MEDIA TOTAL
Juez_1	4,000	3,986	4,000	3,500	3,872
Juez_2	3,889	3,478	3,420	3,377	3,541
Juez_3	4,000	3,870	3,870	3,783	3,881
					3,764

Fuente: Autor.

Se planteó una escala de valoración, apoyado en la bibliografía consultada, para emitir un juicio de valor: (Dorantes et al., 2016).

0<=Media total< 2 NO FAVORABLE.
2<=Media total < 3 DEBE MEJORAR.
3>=Media total <=4 FAVORABLE.

Teniendo en cuenta la escala anterior y observando que la media total es de 3,764, valor comprendido entre 3 y 4, se concluyó que la evaluación por parte de los expertos fue favorable.

No siendo esto suficiente, se realizó un análisis de validez y consistencia del instrumento con las distintas evaluaciones emitidas por los expertos. Para esto, se determinó el coeficiente de concordancia W de Kendall, obteniéndose a partir del análisis de los índices o medias de cada categoría.

Para esta validación, se plantea una pregunta de investigación: ¿Existe concordancia entre la calificación dada por los expertos?
Siguiendo el procedimiento para llevar a cabo la prueba de hipótesis, desarrollado en la validación del estudio, se plantearon dos hipótesis:

H0: NO Existe concordancia entre la calificación dada por los expertos.

Por otra parte, la segunda, la hipótesis alterna, que se denota por la letra H mayúscula y el número uno:

H1: Existe concordancia entre la calificación dada por los expertos.

Estableciendo un nivel de significancia (alfa) de un 5%, según la bibliografía, estaríamos dispuesto a aceptar un 5% o menos de error aceptando la hipótesis H1.

La prueba W de Kendall, es el estadístico seleccionado para medir el grado de correlación y consistencia interna de las variables entre los expertos (Dorantes et al., 2016).

Tabla 7.-Resultados de estadísticos de prueba.

N	3
W de Kendall	0,869
Chi-cuadrado	7,821
gl	3
Sig. asintótica	0,04980

Fuente: Autor.

Dando lectura al p-valor calculado por el software estadístico, en la Tabla 7, se puede observar que el valor de P (Sig. Asintótica) es igual a 0,04980 = 4,980 %. Como se puede observar, el P valor es de 0,0498<0,05.

Con una probabilidad de error de 0,04980 = 4,980 %, se pudo concluir que existe concordancia entre la calificación dada por los expertos, validándose el contenido del instrumento.

En este caso se acepta la hipótesis alterna (investigador) H1 y se rechaza la hipótesis nula H0.

Validación de la confiabilidad.

En este paso se evaluó la validez del instrumento por medio de técnicas estadísticas, especialmente con el estadístico Alfa de Cronbach, que es un coeficiente que sirve para medir la fiabilidad de una escala de medida, realizando un análisis de consistencia Interna para evaluar la homogeneidad intrínseca del instrumento, con la determinación si existe correlación entre los ítems y la media total, utilizando SPSS como herramienta estadística (Bhatnagar et al., 2014; Cronbach, 1951; Melián, 2007; Milton, 2010; Salas y Monte, 2012).

Tabla 8.- Resumen de procesamiento de casos.

		N	%
Casos	Válido	12	100,0
	Excluido	0	0,0
	Total	12	100,0

Fuente: Autor.

Tabla 9.- Estadísticas de fiabilidad.

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0,983	0,982	66

Fuente: Autor.

La tabla 9, muestra el coeficiente alfa de Cronbach total del instrumento que fue 0.983 superior al mínimo aceptable de 0.7 considerado en la bibliografía. El número de elementos corresponde al número de preguntas consideradas en el instrumento.

Tabla 10.- Estadísticas de los primeros 5 ítems o elementos del total de elemento.

ítems		Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
	índice Total	157,0	2195,2	0,99	0,982
1	Ítem 1	157,0	2232,9	0,314	0,983
2	Ítem 2	156,9	2205,6	0,604	0,983
3	Ítem 3	156,9	2191,4	0,693	0,983
4	Ítem 4	157,4	2214,9	0,638	0,983
5	Ítem 5	156,8	2206,0	0,666	0,983

Fuente: Autor.

La Media de la escala si se elimina el elemento, indica el valor que tendría la media en el caso de eliminar cada uno de los elementos. La Correlación elemento-total corregida, es el coeficiente de homogeneidad corregido. Si es cero o negativo se elimina o se replantea la pregunta. En Alfa de Cronbach si se elimina el elemento, equivale al valor de Alfa si eliminamos cada uno de los ítems. Así por ejemplo se pudo ver que, si eliminamos el elemento 1 de la tabla 10, Alfa mejoraría de 0,314 a 0,983. Como se puede ver, el nuevo valor que tendríamos si eliminaríamos el elemento 1 no es tan significativo, teniendo en cuenta que el coeficiente de alfa ya es 0,983. (ver tabla anterior)

Debido a lo anterior, se decide mantener los ítems que presentan una correlación no tan significativa con el índice Total.
Se concluye que el instrumento presenta una alta confiabilidad, quedando validado el mismo.

Validación de constructo.

Para esta prueba, se establecieron los grupos del instrumento y se calificó a cada uno de los ítems de manera grupada a manera de índice. Se presentaron los índices de cada dimensión, así como del total.

La validación de constructo hace referencia a la correlación dominio- total, es decir, cada uno de los dominios con el total, a diferencia de la confiabilidad que es la correlación ítem-total.

Para la validación del constructo se planteó una prueba de Hipótesis, partiendo de una pregunta de investigación: ¿Existe correlación entre los dominios y el índice total del instrumento?

H0: NO Existe correlación entre los dominios y el índice total del instrumento.

H1: Existe correlación entre los dominios y el índice total del instrumento.

Se establece un nivel de significancia (alfa) α = 5% = 0,05.

Tabla 11.- Correlaciones índice total con cada uno de los dominios.

		índice Total	Índice B	Índice C	Índice D	Índice E
índice	Correlación de Pearson	1	,553	,754	,932	,918
	Sig. (bilateral)		,062	,005	,000	,000
	N	12	12	12	12	12
		Índice F	Índice G	Índice H	Índice I	Índice J
índice	Correlación de Pearson	,945	,942	,684	,924	,932
	Sig. (bilateral)	,000	,000	,014	,000	,000
	N	12	12	12	12	12

Fuente: Autor.

En la tabla de correlaciones se puede apreciar la alta correlación que existe entre los dominios y el índice total del instrumento dado que se obtienen en la gran mayoría de los casos un valor superior al 0,500 y un error muy por debajo de nivel de significancia establecido a 0,05 o 5 %.

Con una probabilidad de error menor al 0,05 = 5 % como promedio, se pudo concluir que Existe correlación entre los dominios y el índice total del instrumento, validándose la hipótesis H1. Cada uno de los dominios tiene una buena correlación, una correlación altamente significativa con el resultado global del instrumento. Esto es una prueba de la validez de constructo.

En la tabla siguiente, se puede observar otra manera de validación de constructo de un instrumento a través de Alfa de Cronbach, pero en este caso no para evaluar los ítems, sino para evaluar los dominios.

Tabla 12.- Resumen de procesamiento de casos.

		N	%
Casos	Válido	12	100,0
	Excluido	0	0,0
	Total	12	100,0

Fuente: Autor.

Tabla 13.- Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
0,950	9

Fuente: Autor.

El Alfa de Cronbach para las correlaciones dominio-total, es de 0,950. El resultado anterior muestra la alta correlación que existe, teniendo en cuenta que este coeficiente oscila entre 0 y 1, siendo 0,950 bastante significativo.

Se concluye que la validez de constructo del instrumento ha sido validada con éxito de dos maneras, uno por medio del coeficiente de Cronbach, para evaluar los dominios y la otra se planteó una prueba de hipótesis para demostrar que Existe correlación entre cada uno de los dominios y el índice total del instrumento. De esta manera queda validado el constructo.

Análisis de resultados del cuestionario.

Una vez aplicado el cuestionario, tabulados y validados los datos, se procedió a identificar aquellos aspectos que impactan de manera directa en la auditoria de seguridad informática en la infraestructura física de la red de datos en las empresas del sector pesquero industrial del cantón Manta.

Estos aspectos o indicadores permiten realizar la comparación entre varias opciones de metodología para la realización de auditoría a la seguridad informática a la infraestructura física de la red consultadas en la bibliografía.

Una evaluación, entre las distintas metodologías comparadas anteriormente, permitió determinar cuál es la que más se adapta a las empresas vinculadas a la industria pesquera del cantón Manta, Provincia de Manabí, Ecuador, además de, incorporar características que enriquezcan la metodología escogida.

Si bien no se analizarán todos los ítems del cuestionario en este artículo, se tendrán en cuenta aquellos que aporten aspectos significativos para esta evaluación.

Un primer factor que fue analizado es el que permitió conocer información general organizacional.

En la figura 5, se puede evidenciar que más del 50% de los encuestados respondieron que empleados en la organización presentan algún estudio universitario o equivalente.

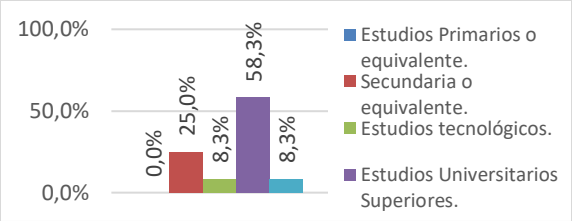

Figura 5. Nivel de escolaridad alcanzado por los integrantes de la organización.

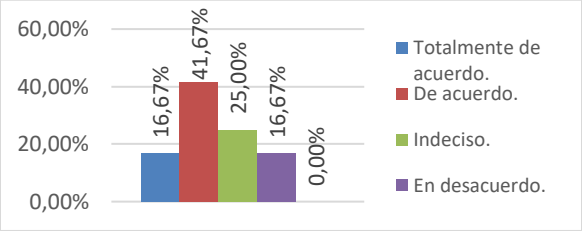

Figura 6. Existencia de planes de auditoría de seguridad informática.

Por otra parte, en la figura 6, se muestra la gráfica de los resultados obtenidos en otro ítem del factor o dimensión que permitió conocer la información general organizacional. En figura, observamos que el 58,34% informan que existe algún plan de auditoría de la seguridad informática en la organización, pero no se pudo dejar a un lado, que el 41,67% de los interrogados han planteado un desconocimiento o desacuerdo con la existencia de planes de auditoría, evidenciándose una falencia en este aspecto en algunas empresas del sector.

Una segunda dimensión o factor fue analizado en este estudio y es la que se encarga de la gestión de procesos basados en competencia en la organización.

En esta dimensión, se trajo a este articulo el resultado de algunos factores que muestran la experticia que tiene el personal de la empresa en cuanto a la gestión de seguridad informática y/o en las operaciones de seguridad informática. Además, permitiendo conocer el nivel de experticia de los integrantes de la organización en cuanto a la madurez en seguridad informática.

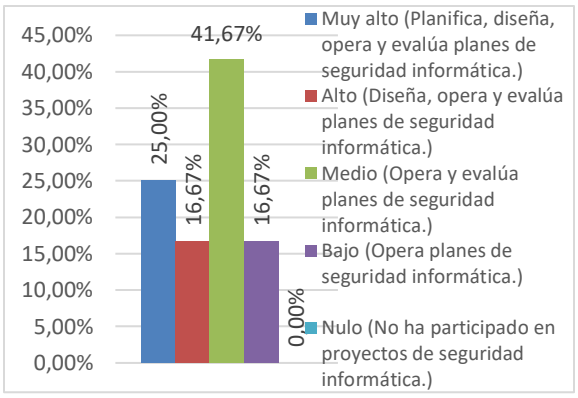

Figura 7. Nivel de experticia que tiene el personal de la empresa en cuanto a la gestión y operaciones de seguridad informática.

En la figura 7, se muestra que el nivel de experticia que tiene el personal de la empresa en cuanto a la gestión y/o en las operaciones de seguridad informática es de un nivel medio a bajo, siendo este un factor que afecta de alguna manera a la seguridad informática de la organización.

Otro ítem de esta dimensión es coherente con los resultados anteriores, figura 8. Este, que trata sobre el nivel de conocimiento sobre las normas, metodologías y herramientas para la realización de auditorías a la seguridad informática en la infraestructura de red de datos en la organización, se observa que el 50% de los jefes de TIC que completaron el cuestionario creen que el nivel va de competente a principiante.

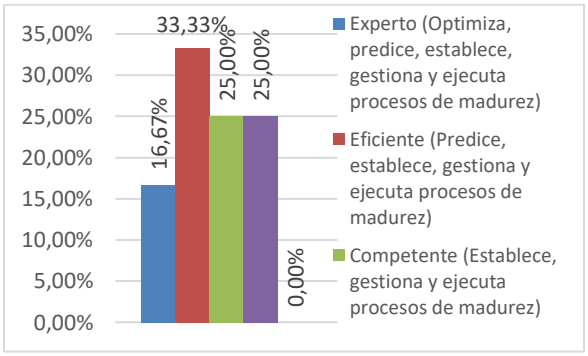

Figura 8. Nivel de conocimiento sobre las normas, metodologías y herramientas para la realización de auditorías a la seguridad informática en la infraestructura de red de datos en la organización.

La revelación anterior, figura 8, es muy importante dado que se observó que una metodología o norma muy compleja en su implementación no sería muy factible, debido al nivel de preparación de los que van a estar en ese proceso.

La figura 9, muestra que la norma con la que más se familiarizan es la ISO 27001, aunque conocen otras en una menor medida.

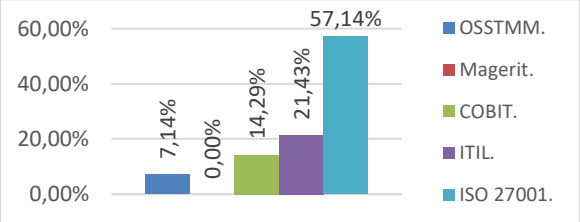

Figura 9. Metodologías que más conoce el jefe de TIC para realizar auditoría a la seguridad informática.

Un tercer dominio o dimensión, está relacionado con el marco normativo. En este, se recoge la existencia, actualización y mejoras continuas de normativas en la infraestructura física de red.

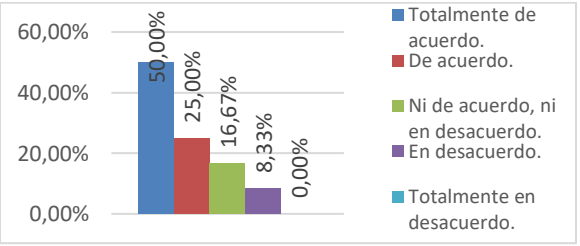

Figura10. Aplicación de normas y/o estándares reconocidos para mejoras de la seguridad informática en la infraestructura física de red.

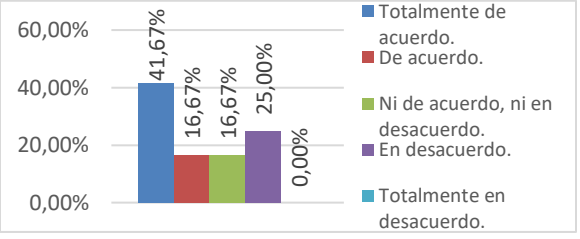

Figura11. Actualización periódica de algún tipo de normas o estándares para mejoras continuas de la seguridad informática en la infraestructura física de red.

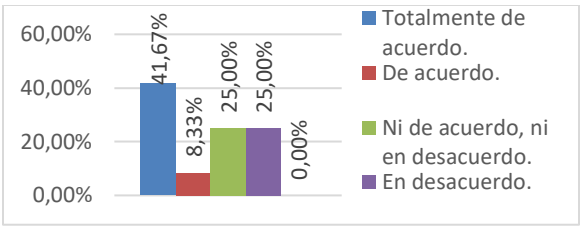

Figura12. La organización tiene un sistema para mejoras continua en los controles y procesos de auditoría informática.

En las figuras anteriores, se pudo observar que, si bien aplican algunas normas o estándares para la mejora de la seguridad informáticas, existen problemas en sus actualizaciones y en la existencia de sistemas de mejoras continua en los controles y procesos de auditoria informática.

Dentro de la dimensión vinculada a la gestión estratégica administrativa-financiera-operacional en seguridad informática, se extraen algunos ítems representativos y que podrían aportar al análisis comparativo de este trabajo.

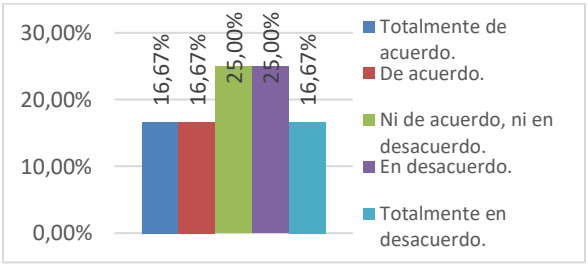

Figura13.Asignación de presupuesto para la seguridad informática.

En cuanto a la disponibilidad de un presupuesto para la seguridad informática, se puede apreciar que 4 jefes de TIC de las organizaciones, que representan el 33,34% de los encuestados, manifestaron que de una manera u otra se destinan recursos económicos dentro del presupuesto para la seguridad informática. Por otra parte, el 66,66% informan que no existe una asignación dentro del presupuesto para esta actividad.

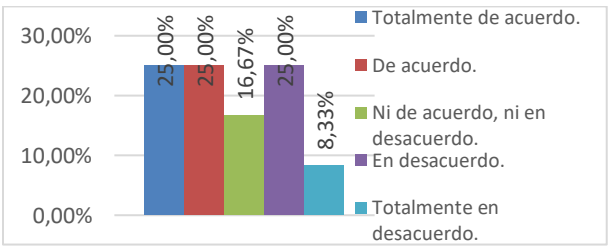

Figura14. El presupuesto de la organización cubre las necesidades para la seguridad informática.

La figura 14, en complemento a la figura 13, muestra que de la baja asignación que se tiene en el presupuesto de estas empresas para la seguridad informática, solo el 50% de los jefes de TIC creen que el mismo cubre las necesidades para estas funciones.

A pesar de lo anteriormente expuesto, la organización ha logrado la habilitación de TI con el programa de seguridad en el área de seguridad informática. En la figura 15, se muestra que el 50% de las respuestas al cuestionario evidencian este logro.

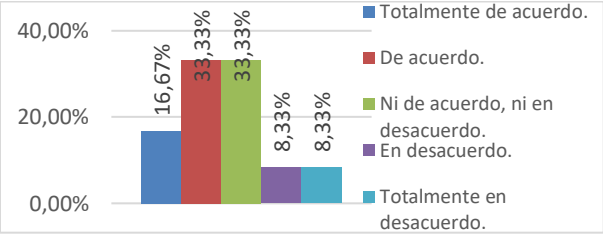

Figura15. Logro en la habilitación de TI con el programa de seguridad en el área de seguridad informática.

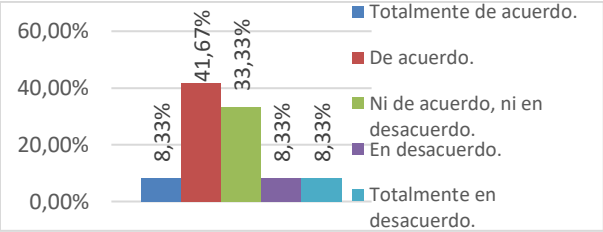

Figura16. Formulación de métricas de riesgo en la infraestructura física de la red de la empresa.

La figura 16 y 17, en la dimensión gestión de riesgos en seguridad informática, muestra que en las organizaciones se han materializado determinados riesgos de la seguridad informática y que de una manera u otra se han formulado métricas para medir estos niveles de impacto, evidenciándose, aunque bajo, un determinado nivel de manejo de métricas.

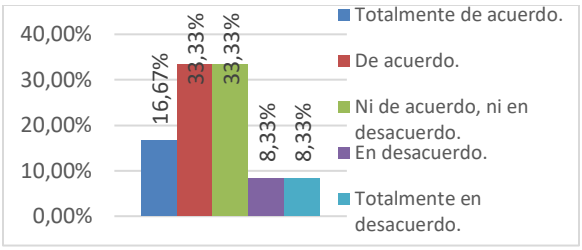

Figura17. Materialización de riesgos de la seguridad de información en las redes de datos en los últimos dos años.

Un problema que se puede observar en las respuestas a este cuestionario por parte de los responsables del departamento de TIC es la poca comunicación de los riesgos.

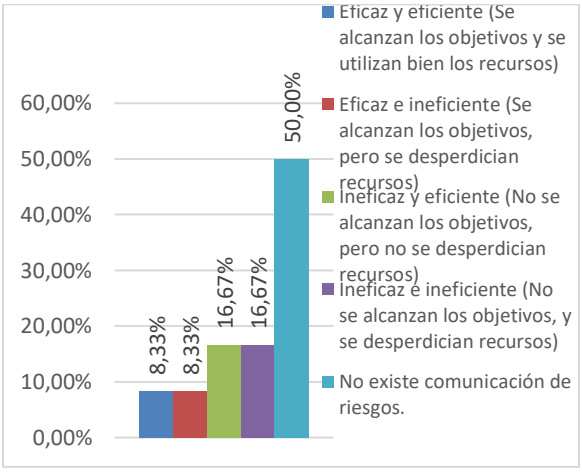

Figura18. Nivel de comunicación tiene su organización sobre los riesgos relacionados con la seguridad informática.

Una sexta dimensión en el cuestionario analizó la gestión de auditoría en seguridad informática en las empresas del sector pesquero industrial en el municipio Manta.

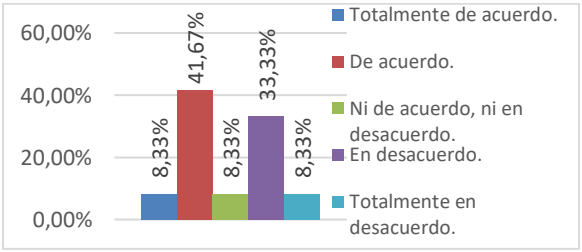

Figura 19. Aplicación de alguna metodología para la realización de auditoría a la seguridad informática de la infraestructura de red de datos de la empresa.

En la figura anterior, figura 19, se puede apreciar que el 50% de los jefes de los

departamentos de TIC en las empresas, plantean que aplican de alguna metodología para la realización de auditoría a la seguridad informática de la infraestructura de red de datos de estas.

Por otra parte, se puede observar en la figura 20, que solo el 25% de los encuestados creen que existe algún factor externo o interno que no permiten implementar una metodología para la realización de auditoría a la seguridad informática en la infraestructura de red de datos de la empresa.

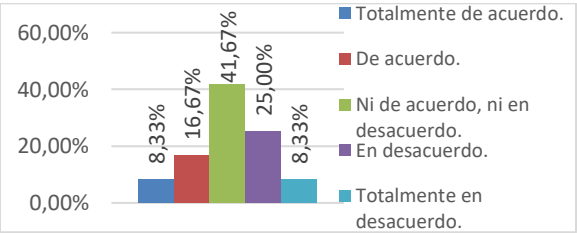

Figura 20. Factores externos e internos que no permiten implementar una metodología para la realización de auditoría a la seguridad informática en la infraestructura de red de datos de la empresa.

Una séptima dimensión incluida en el cuestionario, que cubre aspectos relacionados con la infraestructura de red de datos: continuidad operativa y servicio empresarial, es analizado a continuación.

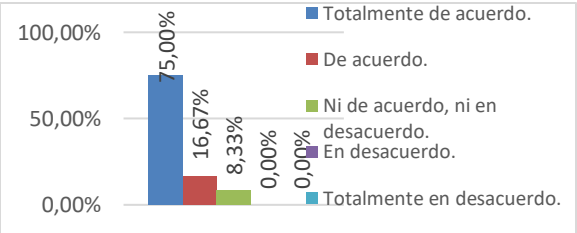

Figura 21. El nivel de impacto sobre el negocio es alto al interrumpir la red de datos en la empresa.

La figura 21 muestra el nivel de impacto que tendría sobre el negocio si se interrumpe la red de datos en la empresa. En lo anterior se evidencia que este impacto sería significativo, el 91,67% de los jefes de TIC manifiestan que el negocio se vería muy afectado por estas incidencias.

Dos dimensiones se tuvieron en cuenta para el final del instrumento de recolección de datos, excelencia en seguridad informática y clima organizacional en seguridad informática. De la primera, se pudo extraer la existencia de comunicación entre departamentos y directivo en cuanto a la seguridad informática.

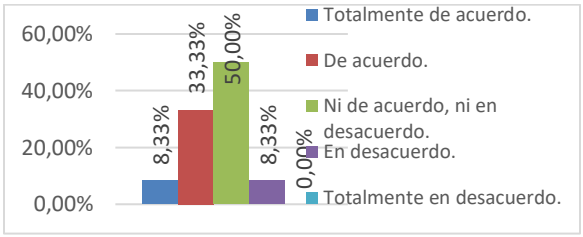

Figura 22. Implementación de forma efectiva sistemas de flujo de información horizontal y vertical interdepartamental para la seguridad informática.

En la figura 22 se pudo observar que en las empresas existe un problema en la comunicación entre los departamentos y los mandos superiores, algo parecido a las observado en la figura 18.

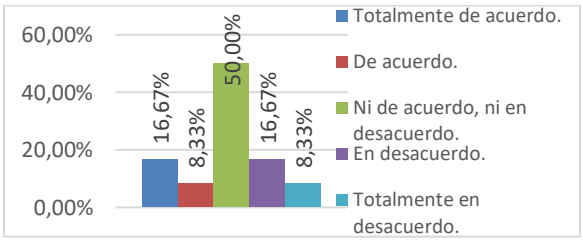

Figura 23. Su organización realiza de manera efectiva encuestas de satisfacción a los usuarios sobre la seguridad informática.

Solo el 25% de los encuestados manifiestan que en su organización realizan de manera efectiva encuestas de satisfacción a los usuarios sobre la seguridad informática contra el 75% que plantean que no se realiza.

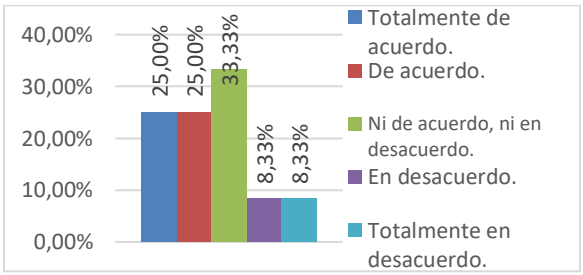

Figura 21. Existencia de un equipo apropiado para la seguridad informática de las TI.

En las respuestas a la última dimensión, el clima organizacional en seguridad informática, se aprecia niveles significativos, donde el 50% de

los jefes de TIC plantean que su equipo es el adecuado para gestión y operaciones de la seguridad informática en la empresa.

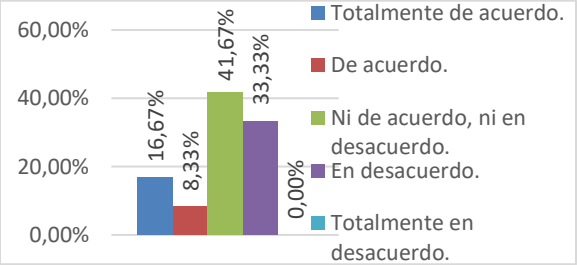

Figura 22. Su organización cuenta con certificaciones de seguridad informática.

En esta última figura, se puede apreciar que la mayoría de las empresas no cuentan con certificaciones en el área de seguridad informática, solo el 25% manifiesta que sí poseen.

Luego de analizado algunos resultados de la aplicación del instrumento validado y mostrados de forma narrativa, emitimos algunas conclusiones importantes que permitió llevar a cabo el análisis comparativo entre distintas metodologías, para así poder seleccionar la metodología más adecuada para las empresas del sector pesquero industrial del cantón Manta, Ecuador.

De manera general se puede apreciar que el personal presenta un buen grado académico, permitiendo tener un nivel de conocimiento medio en cuanto a normas y metodologías de auditoría a la seguridad informática de la infraestructura de red de datos de estas. La experticia del personal, en gestión y operaciones de la seguridad informática, es de un nivel medio a bajo. Esto es muy importante tenerlo en cuenta dado que una metodología muy compleja sería contraproducente.

La norma con la que más se familiarizan es la ISO 27001, aunque conocen otras en una menor medida como la COBIT e ITIL.

Algunas empresas utilizan algún plan de seguridad informática, mientras el 41,67% de los encuestados plantean que no utilizan ninguno. Existen problemas en las actualizaciones y en la existencia de sistemas de mejoras continua en los controles y procesos de auditoria informática.

Existe poca asignación en el presupuesto para la seguridad informática, solo el 50% de los jefes de TIC creen que el mismo cubre las necesidades para estas funciones, a pesar de lo anteriormente expuesto, la organización ha logrado la habilitación de TI con el programa de seguridad en el área de seguridad informática.

En las organizaciones se han materializado determinados riesgos de la seguridad informática y que de una manera u otra se han formulado métricas para medir los niveles de impacto, evidenciándose, aunque sea bajo, un determinado nivel de manejo de métricas, pero existe poca comunicación de los riesgos, presentándose un problema en la comunicación entre los departamentos y los mandos superiores. El nivel de impacto que tendría sobre el negocio si se interrumpe la red de datos en la empresa es muy alto.

El 50% de los jefes de los departamentos de TIC en las empresas, plantean que aplican alguna metodología para la realización de auditoría a la seguridad informática de la infraestructura de red de datos de estas y que no existe ningún factor externo o interno que permita la no implementación de una metodología para la realización de auditoría a la seguridad informática en la infraestructura de red de datos de la empresa.

No se realizan de manera efectiva encuestas de satisfacción a los usuarios sobre la seguridad informática de ahí que no se conoce la opinión de los integrantes de la organización sobre el manejo de la seguridad informática.

Se pudo apreciar la necesidad de certificaciones en el área de seguridad informática, solo el 25% manifiesta que sí poseen.

Análisis comparativo de distintas metodologías consultadas en la bibliografía.

Luego de todo un análisis estadístico, producto de un instrumento validado estadísticamente, se ha podido obtener el estado de la seguridad informática en el sector objeto de estudio.

De este análisis, se pudo extraer una serie de criterios que permitió comparar entre distintas metodologías para la realización de auditorías de seguridad informática de infraestructura de redes de datos en empresas del sector industrial

pesquero del cantón Manta, provincia de Manabí, Ecuador.

En primer lugar, se extrajeron los criterios que al parecer impactan más en el sector objeto. Con estos criterios se realizó un análisis comparativo entre las distintas metodologías que se determinaron más acorde para la realización de este tipo de auditoria.

Para disminuir los niveles de sesgo en el análisis comparativo, se procedió a realizar dicha comparativa por medio de dos métodos registrados en la bibliografía consultada, uno un método abreviado de comparación pareada y la otra comparación por medio del método multicriterio AHP (Analytic Hierarchy Process), planteado por Saaty. (Marin et al., 2014; R. Saaty, 1987)

Análisis comparativo simplificado.

Para este análisis, se procede a realizar la tabla o matriz de criterios, figura 23, se basó en los resultados del cuestionario aplicado, en la que se determinaron los siguientes criterios: facilidad de implementación, costo de implementación, utilización de métricas cuantitativas, utilización de formatos OpSec, enfoque a infraestructura física de la red y se ponderó según el nivel de importancia para el estudio y basado en una escala.

Criterio a criterio	Facilidad de implementación	Costo de implementación	Utilización de métricas cuantitativas	Utilización de formatos OpSec	Enfoque a infraestructura física de la red	Total de fila	Peso criterio Total suma %
Facilidad de implementación		3	2	2	2	9	15,00
Costo de implementación	3		4	4	3	14	23,33
Utilización de métricas cuantitativas	4	2		3	2	11	18,33
Utilización de formatos OpSec	4	2	3		1	10	16,67
Enfoque a infraestructura física de la red	4	3	4	5		16	26,67
					Suma total de filas:	60	100,00

Figura 23. Matriz de criterios.

Escala para el llenado de las celdas no sombreadas:

1: El criterio X (fila) es un criterio mucho menos importante que el criterio Y (columna)
2: El criterio X (fila) es un criterio menos importante que el criterio Y (columna)
3: El criterio X (fila) es un criterio igual de importante que el criterio Y (columna)
4: El criterio X (fila) es un criterio más importante que el criterio Y (columna)

5: El criterio X (fila) es un criterio mucho más importante que el criterio Y (columna)

En la figura 23, los subcriterios de la izquierda se comparan con los subcriterios de arriba en cuanto a su importancia.

	Facilidad de implementación						
Alternativa a alternativa	OSSTMM	OWASP	MAGERIT	COSO	COBIT	Total de fila	Peso criterio Total suma %
OSSTMM		3	4	5	5	17	28,33
OWASP	3		4	5	5	17	28,33
MAGERIT	2	2		5	4	13	21,67
COSO	1	1	1		2	5	8,33
COBIT	1	1	2	4		8	13,33
					Suma total de filas:	60	100,00

Figura 24. Matriz de comparación por pares de las principales alternativas con respecto a la facilidad de implementación.

En la figura 24, las alternativas de la izquierda se comparan con las de arriba con respecto a la facilidad de implementación, obteniéndose el peso del criterio o vector.

	Costo de implementación						
Alternativa a alternativa	OSSTMM	OWASP	MAGERIT	COSO	COBIT	Total de fila	Peso criterio Total suma %
OSSTMM		3	4	5	4	16	26,67
OWASP	3		4	5	4	16	26,67
MAGERIT	2	2		4	4	12	20,00
COSO	1	1	2		2	6	10,00
COBIT	2	2	2	4		10	16,67
					Suma total de filas:	60	100,00

Figura 25. Matriz de comparación por pares de las principales alternativas con respecto al costo de implementación.

Muy parecido a la matriz de facilidad de implementación, en la figura 25, las alternativas de la izquierda se comparan con las de arriba con respecto al costo de implementación.

En la figura que se presenta a continuación, las alternativas de la izquierda se comparan con las de arriba con respecto a la utilización de métricas cuantitativas.

		Utilización de métricas cuantitativas					
Alternativa a alternativa	OSSTMM	OWASP	MAGERIT	COSO	COBIT	Total de fila	Peso criterio Total suma %
OSSTMM		4	4	4	4	16	26,67
OWASP	2		2	4	4	12	20,00
MAGERIT	2	4		4	4	14	23,33
COSO	2	2	2		4	10	16,67
COBIT	2	2	2	2		8	13,33
					Suma total de filas:	60	100,00

Figura 26. Matriz de comparación por pares de las principales alternativas con respecto a la utilización de métricas cuantitativas.

		Utilización de formatos OpSec					
Alternativa a alternativa	OSSTMM	OWASP	MAGERIT	COSO	COBIT	Total de fila	Peso criterio Total suma %
OSSTMM		4	4	4	4	16	26,67
OWASP	2		4	4	4	14	23,33
MAGERIT	2	2		4	4	12	20,00
COSO	2	2	2		3	9	15,00
COBIT	2	2	2	3		9	15,00
					Suma total de filas:	60	100,00

Figura 27. Matriz de comparación por pares de las principales alternativas con respecto a la utilización de formatos OpSec.

La figura 27, mostró la matriz para el criterio correspondiente, en esta las alternativas de la izquierda se comparan con las de arriba con respecto a la utilización de formatos del tipo OpSec, del inglés operational safety.

Finalmente, en la figura 28, se muestran las alternativas de la izquierda comparadas con las de arriba con respecto al enfoque a infraestructura física de la red.

		Enfoque a infraestrusctura física de la red					
Alternativa a alternativa	OSSTMM	OWASP	MAGERIT	COSO	COBIT	Total de fila	Peso criterio Total suma %
OSSTMM		5	4	5	4	18	30,00
OWASP	1		2	3	3	9	15,00
MAGERIT	2	4		4	3	13	21,67
COSO	1	3	2		2	8	13,33
COBIT	2	3	3	4		12	20,00
					Suma total de filas:	60	100,00

Figura 28. Matriz de comparación por pares de las principales alternativas con respecto al enfoque a infraestructura física de la red.

		Resultados			
Criterios/Alternativas	OSSTMM	OWASP	MAGERIT	COSO	COBIT
Facilidad de implementación	4,25%	4,25%	3,25%	1,25%	2,00%
Costo de implementación	6,22%	6,22%	4,67%	2,33%	3,89%
Utilización de métricas cuantitativas	4,89%	3,67%	4,28%	3,06%	2,44%
Utilización de formatos OpSec	4,44%	3,89%	3,33%	2,50%	2,50%
Enfoque a infraestrusctura física de la red	8,00%	4,00%	5,78%	3,56%	5,33%
Valor total de cada alternativas:	27,81%	22,03%	21,31%	12,69%	16,17%
				Total:	100,00%

Figura 29. Matriz de los resultados por cada alternativa comparada.

Para calcular los valores de la figura anterior, se tomaron los valores porcentuales de cada criterio en la matriz de criterio y se multiplicó por el valor porcentual de cada alternativa de la tabla del mismo criterio.

En la figura 29, se pudo apreciar el resultado del análisis comparativo, donde la opción OSSTMM, tiene el mayor valor porcentual, que permitió tener a esta alternativa como la más y mejor evaluada comparadas con las otras alternativas.

Análisis comparativo por medio del método multicriterio AHP, planteado por Saaty.

Como en el método anterior, en este análisis comparativo se construye primeramente la matriz de criterios basado en el cuestionario y la bibliografía consultada.

La figura que a continuación se presenta, se obtiene siguiendo la escala de Saaty, que va desde 1, que representa Igual importancia entre los criterios que se comparan, y 9 que representa la importancia extrema de un elemento frente al otro, ver tabla 14.

Criterio a criterio	Facilidad de implementación	Costo de implementación	Utilización de métricas cuantitativas	Utilización de formatos OpSec	Enfoque a infraestrusctura física de la red
Facilidad de implementación	1	1/3	1	1/3	1/3
Costo de implementación	3	1	3	3	1/3
Utilización de métricas cuantitativas	1	1/3	1	1	1/3
Utilización de formatos OpSec	3	1/3	1	1	1/5
Enfoque a infraestrusctura física de la red	3	3	3	5	1
TOTAL	11	5,00	9,00	10,33	2,20

Figura 30. Matriz de criterios.

Tabla 14.- Matriz normalizada.

Matriz normalizada					Medias
0,09	0,07	0,11	0,03	0,15	0,09
0,27	0,20	0,33	0,29	0,15	0,25
0,09	0,07	0,11	0,10	0,15	0,10
0,27	0,07	0,11	0,10	0,09	0,13
0,27	0,60	0,33	0,48	0,45	0,43

Fuente: Autor

La matriz normalizada, se obtiene de dividir el valor comparativo entre criterios por el total correspondiente, por otra parte, la media es el promedio de cada fila de la matriz normalizada. Estos valores ayudaron a determinar la mejor alternativa en la matriz de resultados.

En este método, primeramente, se comprobó si la matriz de criterio está construida correctamente, donde el sesgo sea aceptable y por ende la matriz consistente.

Para lo anterior, se planteó la metodología para la prueba de hipótesis:

1.- Plantear prueba de hipótesis: ¿La matriz de criterios es consistente según su normalización?

H0: La matriz de criterios NO ES consistente según su normalización.

H1: La matriz de criterios ES consistente según su normalización.

2.- Se establece un nivel de significancia de 0,1, según literatura.

3.- La prueba estadística: Comparación por medio del método multicriterio AHP. Escala de Saaty.

4.- Calculo de la razón de consistencia (CR)

$$RI = \frac{1{,}98 * (n-2)}{n}$$

$$CI = \frac{(nmax - n)}{(n-1)}$$

$$CR = \frac{CI}{RI}$$

Donde, RI: Consistencia aleatoria.
CI: Índice de consistencia.
CR: Relación de consistencia.
n: número de criterios = 5

*nmax: El resultado de la sumatoria de cada valor de M*C*Media.

Mc * Media
0,463
1,357
0,548
0,671
2,397
nmax: 5,436

Mc*Media, es el resultado de la multiplicación de la matriz de criterio por la media o vector (multiplicación de una matriz por un vector). (Marín et al., 2014; Sánchez et al., 2015)

Entonces:

$$RI = \frac{1{,}98 * (5-2)}{5} = 1{,}188$$

$$CI = \frac{(5{,}436 - 5)}{(5-1)} = 0{,}109$$

$$CR = \frac{0{,}109}{1{,}188} = 0{,}092$$

5.- Lectura del valor:

$$Como\ CR\ es\ < que\ 0{,}1$$

Se pudo concluir que la matriz de criterios ES consistente según su normalización, considerándose un nivel aceptable de consistencia y quedando así validada la matriz de criterio (R. Saaty, 1987).

Luego de validar la consistencia de la matriz de criterio, se procedió a la construcción de las matrices de las alternativas por cada criterio.

	Facilidad de implementación				
Criterio a criterio	OSSTMM	OWASP	MAGERIT	COSO	COBIT
OSSTMM	1	1	3	5	5
OWASP	1	1	3	5	5
MAGERIT	1/3	1/3	1	5	3
COSO	1/5	1/5	1/5	1	1/3
COBIT	1/5	1/5	1/3	3	1
TOTAL	2,73	2,73	7,53	19,00	14,33

Figura 31. Matriz de comparación por pares de las principales alternativas con respecto a la facilidad de implementación.

En la figura 31, se realiza un procedimiento muy similar al realizado en el método anterior, la diferencia es que se colocan los valores siguiendo la escala de Saaty, por ejemplo, el valor 5 en la intercepción de la fila OSSTMM y la columna COSO, se observó que el primero es fuertemente más importante que el otro en cuanto a este criterio. De ahí que lo contrario, fila COSO con columna OSSTMM es 1/5.

Tabla 15.- Matriz normalizada

Matriz normalizada					Medias
0,37	0,37	0,40	0,26	0,35	0,35
0,37	0,37	0,40	0,26	0,35	0,35
0,12	0,12	0,13	0,26	0,21	0,17
0,07	0,07	0,03	0,05	0,02	0,05
0,07	0,07	0,04	0,16	0,07	0,08

Fuente: Autor

De la tabla anterior, se pudo extraer las medias o vector, el cual se utilizó para realizar la matriz final de comparación.

Medias o vector: (0,35; 0,35; 0,17; 0,05; 0,08)
De igual manera se obtienen los vectores de cada alternativa para cada criterio.

Vector de comparación por pares de las principales alternativas con respecto al costo de implementación.

Medias o vector: (0,33; 0,33; 0,17; 0,05; 0,11)

Vector de comparación por pares de las principales alternativas con respecto a la utilización de métricas cuantitativas.

Medias o vector: (0,39; 0,17; 0,25; 0,12; 0,07)

Vector de comparación por pares de las principales alternativas con respecto a la utilización de formatos OpSec.

Medias o vector: (0,43; 0,24; 0,16; 0,05; 0,11)

Vector de comparación por pares de las principales alternativas con respecto al enfoque a infraestructura física de la red.

Medias o vector: (0,47; 0,10; 0,20; 0,08; 0,16)

	Resultados					
Criterio/Alternativa	Facilidad de implementación	Costo de implementación	Utilización de métricas cuantitativas	Utilización de formatos OpSec	Enfoque a infraestrusctura física de la red	Priorización
OSSTMM	0,35	0,33	0,39	0,43	0,47	0,41
OWASP	0,35	0,33	0,17	0,24	0,10	0,21
MAGERIT	0,17	0,17	0,25	0,16	0,20	0,19
COSO	0,05	0,05	0,12	0,05	0,08	0,07
COBIT	0,08	0,11	0,07	0,11	0,16	0,13
Ponderación o medias de Matriz de criterios	0,09	0,25	0,10	0,13	0,43	1

Figura 32. Matriz de los resultados por cada alternativa comparada.

En la figura 32, los valores se obtienen de la multiplicación de la matriz de las medias de comparación por pares de las principales alternativas con respecto a cada uno de los criterios por las medias de la matriz de criterios. (multiplicación de una matriz por un vector) (Marin et al., 2014; Millo-sánchez et al., 2015).

De la figura anterior, se deduce que la metodología OSSTMM es la mejor opción en el análisis comparativo por medio del método multicriterio AHP, muy trabajado por Saaty.

Al culminar el análisis comparativo del tipo cuantitativo, en la que se utilizó un método estadístico para inferir cual es la metodología o alternativa más adecuada para el sector objeto de estudio, se procedió a realizar un análisis cualitativo de las principales características de las mismas metodologías con apoyo de la literatura consultada.

OSSTMM, es una metodología que está en constante revisión y actualización. Aunque se necesita entrenamiento y práctica su facilidad de uso es media (Veintimilla, 2016).

El ámbito de aplicación de esta metodología es para todo tipo de organizaciones, pymes y hasta instituciones educativas. El entorno de aplicabilidad es muy amplio, pasando por la seguridad física, que comprende el elemento humano de la comunicación donde la interacción es tanto física o psicológica, además los elementos tangibles de la seguridad. Otro ámbito que comprende esta metodología es la seguridad Inalámbrica, donde se tiene en cuenta todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético. La seguridad en las comunicaciones es otro del ámbito de aplicación de esta, que se encarga de todas las comunicaciones telefónicas ya sea digital como analógica y los sistemas electrónicos y de redes de datos donde la interacción se lleva a cabo a través de un cable establecido y líneas de la red cableadas (Herzog, 2016b).

De ahí que puede ser aplicada a servidores, siendo muy dinámico y potente en el diseño (Fernández, 2012).

Esta metodología está ampliamente documentada, utiliza plantillas para prevenir riesgos innecesarios dado que se integra y cumple todos los estándares que emite la seguridad de la información y establece valores o niveles de evaluación de vulnerabilidades, pudiéndose estimar impacto. Cuenta con

manuales fáciles de entender y aplicar (Barzola y Cedeño, 2017; Orlando y Inti, 2016; Vega, 2016).

Por otra parte, la metodología OWASP, se centra solo en la parte web, es muy didáctica e instructiva. Su ámbito de aplicación es todo tipo de organizaciones orientadas a la web, enfocado solo a los entornos web y aplicaciones enfocadas a la web y no es tan agresiva como lo puede ser OSSTMM (Fernández, 2012; Veintimilla, 2016).

Esta metodología es de fácil uso, donde se usan controles muy conocidos en el Top Ten. Además, esta debe combinarse con otras herramientas y metodologías para que la auditoría sea más completa y requiere entrenamiento, practica y certificaciones (Barzola y Cedeño, 2017).

OWASP no establece valores o niveles de evaluación de vulnerabilidades y no es capaz de estimar impacto, además de no poder adaptarse a las normas 27000 (Bonilla y Vinicio, 2017; Orlando y Inti, 2016).

Una tercera alternativa de comparación en este estudio es la metodología MAGERIT, creada por el Consejo Superior de Administración Electrónica de España, para la gestión y análisis de riesgos, ofreciendo un método sistemático para el análisis de los riesgos derivados del uso de las (TICs), y al mismo tiempo prepara a la organización para procesos de evaluación, auditoría, certificación o acreditación (Amutio, 2012).

Esta metodología permite el tratamiento de la información, ya sea digital o física dentro de una organización, en la que se garantiza la disponibilidad de los servicios o cuando se busca proyectar métricas de seguridad, identificando qué hay que controlar y con qué frecuencia y detalle.(Amutio, 2012; Martínez y Torres, 2018).

MAGERIT utiliza dos grandes tareas y se combinan en el proceso gestión de riesgos una el análisis de riesgos y la otra es el tratamiento de estos riesgos (Amutio, 2012).

Esta metodología se basa en la probabilidad de que una amenaza se materialice sobre cualquier activo de una organización provocando consecuencias negativas.

Una cuarta alternativa es COBIT, que más que una metodología es un modelo, dedicado a proveer lineamientos avanzados en áreas de alto interés, como la arquitectura empresarial, gestión de activos y servicios y el gerenciamiento de la innovación en Tecnología Información (TI).

Este modelo cubre la empresa de extremo a extremo, ayudando a cambiar la visión de los directivos de la organización para tomar la responsabilidad de gobernar y gestionar los activos relacionados con TI dentro de sus propias funciones, ayudando en la satisfacción de los usuarios con los servicios de TI (Vega, 2016).

COSO, como última alternativa en este estudio, se enfoca en varios objetivos principales, los recursos, los estratégicos, de operacionales, Informes e Indicadores de cumplimiento, analizándose los riesgos ambientales y de procesos, viéndose este como un marco de uso por parte de toda la organización (COSO, 2013; Jaime et al., 2012).

Este marco tiene su alcance a toda la empresa u organización, principalmente a la dirección, permitiendo operaciones efectivas y eficientes, además del logro de Informes financieros confiables y el cumplimiento de las leyes y regulaciones, conteniendo directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno y debido a la gran cercanía que hoy existe entre las áreas de una empresa y los sistemas de información computarizados, ha sido replanteado su alcance al área informática (Burgos y Campos, 2008).

Una vez concluido con el análisis cualitativo, donde se ha podido observar las bondades y deficiencias de las alternativas estudiadas, se pudo emitir el siguiente juicio de valor.

La alternativa que describe OSSTMM se elige de entre las demás porque cubre, entre otros, el ámbito de la seguridad física comprendiendo al elemento humano de la comunicación donde la interacción es tanto física como psicológica, además los elementos tangibles de la seguridad como lo es la infraestructura física de la red de datos son tenidos en cuenta, mientras que la metodología OWASP cubre únicamente las aplicaciones web, no adaptándose a las normas 27000.

OSSTMM, es una metodología que está siendo actualizada por los aportes de buenas prácticas de la comunidad siendo esta no muy compleja y de fácil implementación en aquellas organizaciones que inician procesos de reestructuración de los modelos de seguridad informática, presentando formatos y métricas, no probabilísticas como en MAGERIT, sino operativas y reales.

CONCLUSIONES

Luego del proceso de revisión bibliográfica, la consulta de opiniones de expertos en la línea de investigación desarrollada, la ejecución de los pasos definidos en la metodología propuesta para este trabajo de investigación, así como la ejecución de los procedimientos correspondientes, se obtuvo resultados que permiten arribar a una serie de conclusiones, a saber:

- La realización de un cuestionario validado y contrastado permitió obtener datos que permiten tener información de cómo es manejada la seguridad en el sector industrial pesquero del cantón Manta, Provincia de Manabí, Ecuador; además, permitió conocer el tipo de herramientas que utilizan para la realización de auditoria a la seguridad informática en la infraestructura física de la red de datos. Como resultado del análisis de la información recopilada a través de este cuestionario, se pudo observar que las empresas, aunque cuentas con un personal calificado en el área de las de TICs, no manejan de manera eficiente los aspectos relacionados a la seguridad informática en general.

- Se encontró, que la experticia del personal, en gestión y operaciones de la seguridad informática, es de un nivel medio a bajo, aspecto importante para el análisis comparativo de las metodologías, dado que una metodología muy compleja sería contraproducente.

- Otro aspecto muy importante que permitió el cuestionario aplicado fue que las organizaciones, a pesar de la baja asignación que se tiene en el presupuesto de estas empresas para la seguridad informática, han logrado la habilitación de la infraestructura de TI con programas de seguridad en el área de seguridad informática, aunque no manejan modelos o metodologías para la realización de auditorías a la seguridad informática en la infraestructura física de la red de datos.

Además, se encontró que la norma con la que más se familiarizan es la ISO 27001, aunque conocen otras en una menor medida como la COBIT e ITIL.

Se ha podido observar que en las empresas existe un problema en la comunicación entre los departamentos y los mandos superiores, algo parecido a lo observado en el nivel de comunicación de los riesgos en la organización. Estas no realizan de manera efectiva encuestas de satisfacción a los usuarios sobre la seguridad informática.

De lo recogido en el cuestionario aplicado y resumido anteriormente, se pudo observar también que, si bien aplican algunas normas o estándares para la mejora de la seguridad informática, existen algunas empresas que no actualizan sistemas de mejora continua para los controles y procesos de auditoria informática.

A modo de recomendación para las empresas, se aconseja no solo utilizar algún estándar, como el ISO 27001 que es muy bueno y que organiza todo el aspecto documental de un Sistema de Gestión de la Seguridad Informática (SGSI), sino que también tengan procesos de verificación de ese sistema para ver si se está cumpliendo realmente. Además, de que la alta dirección entienda que los procesos de TI son tan importantes como otros en la organización y los tengan en cuenta en el presupuesto.

Concluido el análisis estadístico, producto de la aplicabilidad del instrumento, se pudo obtener el estado de la seguridad informática en el sector objeto de estudio. Además, se extrajeron una serie de criterios que permitió comparar entre distintas metodologías para la realización de auditorías de seguridad informática en la infraestructura de redes de datos en empresas del sector industrial pesquero del cantón Manta, provincia de Manabí, Ecuador.

Con estos criterios se realizó un análisis comparativo entre las distintas metodologías

que se encontraron más acorde para la realización de este tipo de auditoria. Para este análisis, se utilizaron dos métodos registrados en la bibliografía consultada: primero un método abreviado de comparación por pares, y el otro basado en la comparación por medio del método multicriterio AHP (Analytic Hierarchy Process), planteado por Saaty.

Culminado el análisis comparativo del tipo cuantitativo, en el que se utilizaron dos métodos estadísticos para inferir cual es la metodología o alternativa más adecuada para el sector objeto de estudio, se procedió a realizar un análisis cualitativo de las principales características de las mismas metodologías con apoyo de la literatura consultada.

Ambos análisis corroboraron que la alternativa más acorde a las características del sector objeto de estudio es OSSTMM, siendo esta una metodología que está en constante revisión y actualización. Aunque se necesita entrenamiento y práctica, su facilidad de uso es media.

OSSTMM, es una metodología actualizada constantemente por la comunidad. Esta es de complejidad media y de fácil implementación en aquellas organizaciones que inician procesos de reestructuración de los modelos de seguridad informática, como las del sector pesquero industrial del cantón Manta, presentando formatos y métricas, no probabilísticas como en MAGERIT, sino más bien, operativas y reales.

Durante el presente trabajo de investigación, se presentó una limitación que se constituyó en un factor de riesgo para el éxito de esta: la recolección de los datos de los jefes de las TICs de las empresas del sector.

Lo anterior se debió en parte a que se realizó de manera autónoma y vía on-line, para garantizar la confidencialidad del origen de la información resultando que tres (3) empresas, de las 15 que representan la población, no contestaran al instrumento y por razón de tiempo, no se pudo esperar a que lo completaran.

Para evaluar la afectación del riesgo indicado, se vio la necesidad de validar nuestro estudio por medios estadísticos con la utilización de herramientas como el SPSS y modelos estadísticos. Para esta validación, se planteó una pregunta de investigación: ¿El número de respuestas al cuestionario tiene que ver con cómo es evaluada la seguridad informática en las empresas? Y dos hipótesis como inferencia de estimación, H0 y H1. Siendo la hipótesis H0 la aceptada o confirmada de la siguiente manera: con una probabilidad de error de 0,587 = 58,7 %, se pudo concluir que el número de respuestas al cuestionario No tiene que ver con cómo es evaluada la seguridad informática en las empresas. En este caso se acepta la hipótesis nula y se rechaza la hipótesis del investigador, quedando de esta manera validado el estudio con las muestras tomadas.

Lo anterior demostró que no siempre un estudio con pocas muestras es improcedente, siempre y cuando se demuestre su validez desde el punto de vista estadístico.

El presente trabajo ha constituido un tema de actualidad en el área académica y de investigación. El desarrollo de este como línea de investigación en seguridad informática, partiendo de bibliografía contrastada y verificada, permite mejoras sobre esta investigación.

Teniendo en cuenta lo anterior, se deja abierta la línea de investigación para avanzar a otros niveles dentro de la misma, el nivel aplicativo, que permitió comprobar la aplicabilidad, repetibilidad y reproducibilidad de la metodología en otros sectores de la producción y los servicios, ya sean públicos o privados, permitiendo adaptar esta metodología a estos sectores.

Otro trabajo futuro que se desprende del presente estudio podría ser un análisis desde el punto de vista económico, donde la metodología evaluada en el sector industrial pesquero del cantón Manta, se pueda aplicar para responder a una pregunta de investigación: ¿La metodología OSSTMM disminuye gastos innecesarios en los procesos de TICs en el sector objeto? De la pregunta anterior se podrían plantear las hipótesis H0 y H1. La hipótesis H1 sería: La metodología OSSTMM disminuye gastos innecesarios en los procesos de TICs en las empresas y la H0: La metodología OSSTMM NO disminuye gastos innecesarios en los procesos de TICs en las empresas objeto. Una disminución de gastos innecesarios en los procesos de TICs permitiría una estabilidad y confianza en los accionistas, clientes y proveedores.

Un estudio del tipo comparativo también podría realizarse en el futuro, en la que se aplique las otras metodologías aquí evaluadas a la empresa del sector donde se implemente la metodología OSSTMM y por medio de los datos obtenidos de determinadas variables de estudio, comprobar la correlaciones entre estas y la concordancia de los resultados obtenidos de la aplicabilidad del instrumento.

Además, el instrumento de recolección de datos, fruto de la investigación, podría ser aplicado a otros sectores sociales como universidades y escuelas para determinar la madurez de los procesos de seguridad informática. Para lo anterior, se podría realizar un análisis de componentes principales (PCA) o un análisis factorial para simplificar o factorizar la estructura del instrumento y adaptarla al sector objeto de estudio.

Por otro lado, se ha podido evidenciar en la revisión bibliográfica, que no se ha trabajado mucho en lo que respecta a las metodologías para la realización de auditorías de seguridad informática en infraestructuras física de redes de datos, y que la gran mayoría de los trabajos hacen referencia a los procesos de la auditoria de seguridad de información y no a una auditoría de control de cumplimiento de controles en las infraestructuras físicas de las redes internas en las organizaciones.

Por último, esta investigación se convirtió en un reto profesional debido a que se realizaron contribuciones basadas en una realidad estadística y de acuerdo con las características del sector objeto.

Referencias Bibliográficas

Alfaro, J., Boulahia, N., y Cuppens, F. (2008). Complete analysis of configuration rules to guarantee reliable network security policies. *International Journal of Information Security*, *7*(2), 103-122. https://doi.org/10.1007/s10207-007-0045-7

Alvarez, C. V., y Rivera, Z. (2006). La auditoria como proceso de control: concepto y tipología, *37*(2), 53-60.

Álvarez, M. (2004). *Seguridad informatica para empresas y particulares*. MC GRAW HILL. https://doi.org/978-84-481-4008-3

Amutio, M. (2012). MAGERIT V3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 127. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Ansi/Tia-568-C.0. (2009). *Ansi/Tia-568-C.0-2009*.

Ansi/Tia-568-C.1. (2009). *Ansi/Tia-568-C.1-2009*.

Ansi/tia/eia-569-A. (2012). Ansi/tia/eia-569-a (csa t530), *2*.

ANSI/TIA/EIA-569-B. (2012). Standard ANSI / TIA / EIA-569-B Pathways and Spaces. Design Considerations.

ANSI/TIA/EIA/606A. (2006). ANSI/TIA/EIA/606A Quick Reference Guide.

Antidot. (2014). Linked Enterprise Data. *Linked Enterprise Data*, 85-101. https://doi.org/10.1007/978-3-642-30274-9

Arcentales, D., y Caycedo, X. (2017). Auditoría informática: un enfoque efectivo Computer audit: an effective approach Auditoria informática: uma abordagem efetiva, *3*, 157-173.

AXELOS. (2007). OGC - ITIL v3 - Service Lifecycle - Introduction ITIL.pdf.

Baquerizo, M., y Guevara, C. (2016). Análisis de la seguridad en los sistemas de e-Gobierno mediante el problema SAT. *Inge Cuc*, *12*(1), 73-79. https://doi.org/10.17981/ingecuc.12.1.2016.07

Baryolo, O. G., Vivian, D. C., Sentí, E., Rodrigo, I. R., Camejo, B., Isabel, D. C., y Rodríguez, G. (2012). Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones. *Acimed*, *23*(2), 187-200. Recuperado de http://scielo.sld.cu/pdf/aci/v23n2/aci08212.pdf

Barzola, L. M. P., y Cedeño, E. S. Y. (2017). *Análisis de vulnerabilidades en la infraestructura tecnológica de una*

empresa, utilizando herramientas de test de intrusión.

Bello, M., Bello, R., García, M. M., y Casas, G. (2016). Estudio estadístico del efecto de la similaridad entre rankings en la selección de personal en un contexto competitivo A statistical study about the effect of the ranking similarity in the personnel selection in a non-cooperative context, *XXXVIII*(3), 257-264. Recuperado de http://www.rii.cujae.edu.cu

Benavides, C., y Quintana, C. (2007). Un modelo para la gestión estratégica de los recursos tecnológicos: el ciclo de mejora y despliegue de matrices QFD. *Economía industrial*, (365), 195-206. Recuperado de http://dialnet.unirioja.es/servlet/articulo?codigo=2473061

Betancourt, P., Cevallos, A., y Aguilar, D. (2013). Evaluación técnica de la red de fibra óptica de CELEC EP - TRANSELECTRIC a través de la cual la empresa TRANSNEXA S.A. E.M.A., 1-9.

Bhatnagar, R., Kim, J., y Many, J. (2014). Candidate Surveys on Program Evaluation: Examining Instrument Reliability, Validity and Program Effectiveness. *American Journal of Educational Research*, *2*(8), 683-690. https://doi.org/10.12691/education-2-8-18

Bonilla, C., y Vinicio, M. (2017). *Elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos y su incidencia en la seguridad de la información de la Empresa Automekano Cía. Ltda., de la Ciudad de Ambato.* Recuperado de http://repositorio.uta.edu.ec/handle/123456789/24534

Bracho, C., Cuzme, F., y Pupiales, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3 : caso de estudio. *Maskana*, (December), 307-319.

Burato, E., Ferrara, P., y Spoto, F. (2017). Security analysis of the OWASP benchmark with Julia. *CEUR Workshop Proceedings*, *1816*, 242-247.

Burgos, J., y Campos, P. (2008). Modelo Para Seguridad de la Información en TIC. *Ceur-Ws.Org*, 20.

Cabezas, J. (2015). La Auditoría De Cumplimiento Y Su Incidencia En La Gestion. Recuperado de http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/1893/1/cabezas_bj.pdf

Capurro, R. (2007). Epistemología y ciencia de la información. *Revista Venezolana de Información, Tecnología y Conocimiento*, *21*(1), 11-29.

Carpenter, T., y Jones, K. (2015). Online Early — Preprint of Accepted Manuscript preprint accepted manuscript. *Journal of International Accounting Research*, *90*(4), 1395-1435. https://doi.org/10.2308/accr-50982

Casal, J., y Mateu, E. (2003). Tipos de muestreo. *Revista Epidemiología y Medicina Preventiva*, *1*(1), 3–7. https://doi.org/10.1111/j.1541-0064.2008.00202.x

Chalén, M., Mideros, L., y Ambuludi, W. (2010). “ Auditoria De La Seguridad De Una Red De Datos ”, (4).

Christensen, K., Reviriego, P., Nordman, B., Bennett, M., Mostowfi, M., y Maestro, J. (2010). IEEE 802.3az: The road to energy efficient Ethernet. *IEEE Communications Magazine*, *48*(11), 50-56. https://doi.org/10.1109/MCOM.2010.5621967

Correa, C. A. P., y Díaz, H. P. (2007). Las Amenazas Informáticas: Peligro Latente Para Las Organizaciones Actuales. *Revista Gti*, *6*(16). Recuperado de http://revistas.uis.edu.co/index.php/revistagti/article/view/1259

COSO. (2013). Internal Control — Integrated Framework. *Committee of Sponsoring Organizations of the Treadway Commission*, (May), 10. https://doi.org/978-1-93735-239-4

Coster, Andy;Magee, S. (2017). Checklist for Standard ISO / IEC 27002 : 2013 Information Security Code of Practice Checklist for Standard ISO / IEC 27002 : 2013 - Information Security Code of

Practice, 1-11.

Cronbach, L. . (1951). Coefficient alpha and the internal s t r u c t u r e of tests* lf~ j. cronbach. *Pyshometrika*, *16*(3).

Cruz, Ó., y Muñoz, A. (2015). Validación de Instrumento para Identificar el Nivel de Vulnerabilidad de los Trabajadores de la Salud a la Tuberculosis en Instituciones de Salud. *Med Segur Trab*, *61*(241), 448-467. https://doi.org/10.1017/CBO9781107415324.004

Curtis, P., Mehravari, N., y Stevens, J. (2015). Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0, (April). Recuperado de http://www.sei.cmu.edu

Delgado, L., Chamba, J., y Santana, J. (2018). Plan de Recuperación ante Desastres para la reactivación económica del sector Productivo. *SINAPSIS*, *1*(Nº 12). https://doi.org/ISSN 1390 – 9770

Deloitte. (2017). Seguridad de la Información en Ecuador 2017. Recuperado de https://cybersecurity.isaca.org/state-of-cybersecurity#3-part-1-february

Deloitte. (2018). *Ciberseguridad.Encuesta 2018 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Ecuador*.

Deming, E. (1989). Reacción en Cadena: Calidad, Productividad, Reducción de Costes, Conquista del Mercado. *Calidad, productividad y competitividad: la salida de la crisis*, *53*, 160. https://doi.org/10.1017/CBO9781107415324.004

Dorantes, J., Hernández, J. S., y Tobón, S. (2016). Juicio de expertos para la validación de un instrumento de medición del síndrome de Burnout en la docencia. *Ra Ximhai*, *12*(6), 327-346.

Duque, Y. G. (2017). PLAN DE SEGURIDAD INFORMÁTICA.

Edwards, M. M. (2018). Identifying Factors Contributing Towards Information Security Maturity in an Organization. *College of Engineering and Computing Nova Southeastern University*, (1027), 246. https://doi.org/ProQuest-10746212

Estrada, A. C. (2011). Seguridad Por Niveles, 709. Recuperado de http://www.etnassoft.com/biblioteca/seguridad-por-niveles/

Fallis, A. . (2013). "Impacto De Las Nuevas Tecnologías De La Información Y La Comunicación En La Educación". *"Impacto De Las Nuevas Tecnologías De La Información Y La Comunicación En La Educación"*, *53*(9), 1689-1699. https://doi.org/10.1017/CBO9781107415324.004

Fernández, A. (2015). Aplicación del análisis factorial confirmatorio a un modelo de medición del rendimiento académico en lectura. *Revista de Ciencias Económicas*, *33*(2), 39. https://doi.org/10.15517/rce.v33i2.22216

Fernández, M. (2012). Auditorías y seguridad.Comparativa metodologías.

Ferrero, J. A. (2013). La ciberguerra. génesis y evolución. *Commons, Globals*, 81-98.

Galarza, C. (2018). Design and implementation of a secure data network for the Pontificia Universidad, *4*, 123-137.

García, Manuel, Quispe, C., y Ráez, L. (2003). Mejora continua de la calidad en los procesos. *Industrial Data*, *6*, 89-94. https://doi.org/10.15381/idata.v6i1.5992

García, María, Rodríguez, F., y Carmona, L. (2009). Validación de cuestionarios. *Reumatologia Clinica*, *5*(4), 171-177. https://doi.org/10.1016/j.reuma.2008.09.007

Gómez, E., Herrera, N., y Díaz, M. (2017). Un enfoque para la optimización de pagos móviles para el sistema de transporte utilizando (NFC) a través de Cloud Computing. *Enfoque UTE*, *8*(1), 31. https://doi.org/10.29019/enfoqueute.v8n1.130

González-BBVA, F. (2015). *Reinventar la empresa en la era digital*.

González, D., y Julio, R. (2012). Cloud Computing y Seguridad.

Recsi2012.Mondragon.Edu. Recuperado de http://recsi2012.mondragon.edu/es/programa/recsi2012_submission_35.pdf

González, E., Álvarez, A., y Arias, C. (1996). Análisis no paramétrico de eficiencia en explotaciones lecheras. *Investigación agraria*, *2*(1), 173-190. Recuperado de http://www.unioviedo.es/fidalgo/papers/invagrec.pdf

González, M., y Ponjuán, G. (2014). Metodologías y modelos para auditar la información: Análisis reflexivo. *Revista General de Informacion y Documentacion*, *24*(2), 233-253. https://doi.org/10.5209/rev_RGID.2014.v24.n2.47402

Graham, L. (2015). *Internal Control Audit and Compliance.Documentation and Testing Under the New COSO Framework*. (I. A. rights reserved. ohnWiley y Sons, Ed.). JohnWiley y Sons, Inc., Hoboken, New Jersey.

Griffith, B. (1980). Key papers in information science. *Kantor.Comminfo.Rutgers.Edu*. Recuperado de http://kantor.comminfo.rutgers.edu/619phd/readings/InformationScience.pdf

Hahn, A., y Govindarasu, M. (2011). An evaluation of cybersecurity assessment tools on a SCADA environment. *IEEE Power and Energy Society General Meeting*, 1-6. https://doi.org/10.1109/PES.2011.6039845

Herzog, P. (2016a). OSSTMM: The Open Source Security Testing Methodology Manual: v3. *Isecom*, 213. Recuperado de http://www.isecom.org/mirror/OSSTMM.3.pdf

Herzog, P. (2016b). OSSTMM: The Open Source Security Testing Methodology Manual: v3. *Isecom*, 213.

INEN. (2016). ECUATORIANA NTE INEN-ISO / IEC 27000, *Cuarta edi*.

Instituto Nacional de Normalización de Chile. (2013). Norma Iso 27001:2013.

Iqbal, M., y Nieves, M. (2011). ITIL Version 3-Libro 1-Service Strategy ITIL. *Service Management*, *34*(19), 1-396. https://doi.org/10.1016/j.im.2003.02.002

ISACA. (2012). *COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa*.

ISACA. (2017). State of Cybersecurity 2017, 22. Recuperado de https://cybersecurity.isaca.org/state-of-cybersecurity#3-part-1-february

ISO/IEC. (2014). ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. *October*, *3*, 38. Recuperado de http://www.iso.org/iso/catalogue_detail?csnumber=42103

ISO/IEC 17799. (2005). ISO/IEC 17799. *Control*, 1-170.

ISOtools. (2013). La norma ISO 27001, Aspectos clave de su diseño e implementación., 1-6.

Jaime, G., Henao, C., y Loyo, Y. (2012). Tesis doctoral: Identificación y evaluación de amenazas a la seguridad de infraestructuras de tr ansporte y distribución de electricidad.

Kramer, G., y Pesavento, G. (2002). Ethernet Passive Optical Network (EPON): building a next generation optical access network. *IEEE Communications Magazine*, 66-73.

Lajo, M. R., Bartolomé, M., Andrés, J. M., Miguel, M. De, y Cabrera, F. (2002). Análisis dimensional de las opiniones de los alumnos universitarios sobre sus profesores: comparación entre técnicas paramétricas y no-paramétricas. *Revista de investigación Educativa.*, *20*(2). https://doi.org/ISSN:0212-4068

Ledesma, R. (2004). AlphaCI: un programa de cálculo de intervalos de confianza para el coeficiente alfa de Cronbach. *Psico-USF (Impresso)*, *9*(1), 31-37. https://doi.org/10.1590/S1413-82712004000100005

Linares, J. L., Redorta, J., Nardone, G., Papagno, C., Romo, M., y Nardone, G.

(2014). TIC HOY, La revista comercial oficial de BICSI.

López, P. (1997). Población, muestra y muestreo., 69-74.

Maier, A. M., Moultrie, J., y Clarkson, P. J. (2012). Assessing organizational capabilities. *Reviewing and Guiding the Development of Maturity Grids*, *59*(1), 138-159. Recuperado de https://www.wiso-net.de/document/ECON__687937566

Manuel, C., y Ibarra, J. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios Ramón Ventura Roque Hernández *. *Paakat: Revista de Tecnología y Sociedad*, *número 14,*. https://doi.org/DOI: http://dx.doi.org/10.18381/Pk.a8n14.318

Marin, J., Aragonés, P., y García, M. (2014). Intra-rater and inter-rater consistency of pair wise comparison in evaluating the innovation competency for university students. *Working Papers on Operations Management*, *5*(2), 24-46. https://doi.org/http://dx.doi.org/10.4995/wpom.v5i2.3220

Maroco, J., y Garcia, T. (2006). Qual a fiabilidade do alfa de Cronbach? *Laboratório de psicologia*, *4*(1), 65-90. https://doi.org/10.14417/lp.763

Marrero, M. M. (2015). La Auditoría de Gestión , una alternativa para los auditores internos en las empresas cubanas The Administration Audit , an alternative for the internal auditors in cuban companies, (2), 1-9.

Martínez, E., y Torres, G. (2018). Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes. *UDA AKADEM*, *1*(1), 38-47. Recuperado de http://revistas.uazuay.edu.ec/index.php/uaakadem/article/view/129

Mavis, L. S., Rodríguez, D. D. M., Pardo, Y. M., Licea, A. C., y Fernández, T. D. (2017). Experiencia en el diagnóstico de la Gestión de Información con Enfoque de Arquitectura de Información Empresarial (Experience in the Diagnostic of Information Management with a Business Information Architecture Approach). *GECONTEC: Revista Internacional de Gestión del Conocimiento y la Tecnología*, *5*(1), 1-16. Recuperado de https://www.upo.es/revistas/index.php/gecontec/article/view/1897

Melendez, K., y Dávila, A. (2018). Adoption ' s problems of information technology service management models . A systematic literature review • Problemas en la adopción de modelos de gestión de servicios de tecnologías de información . Una revisión sistemática de la literatura, *85*(204), 215-222.

Melián, L. (2007). E-books: el rol de las expectativas en las escalas de calidad. *El comportamiento de la empresa ante entornos dinámicos: XIX Congreso anual y XV Congreso Hispano Francés de AEDEM*, 6.

Micro Incorporated, T. (2017). 2017 Annual Security Roundup: The Paradox of Cyberthreats. Recuperado de https://documents.trendmicro.com/assets/rpt/rpt-2017-Annual-Security-Roundup-The-Paradox-of-Cyberthreats.pdf

Millo-sánchez, R., Cristina, I., Verona, P., Vargas, J. A., Hernández, T. R., Central, U., … Clara, S. (2015). Matrices dispersas en Java para el procesamiento de grandes volúmenes de datos. *Rev. Cuba. Ciencias Informáticas*, (November), 1-8.

Milton, V. (2010). Confiabilidad y coeficiente Alpha de Cronbach Licenciado Educación Mención Matemática y Física . Profesor de Educación Integral, *12*(2), 248-252. https://doi.org/10.1007/s00259-006-0152-0

Moeller, R. R. (2014). *Executive's Guide to COSO Internal Controls.Understanding and Implementing the New Framework*. (R. R. M. A. rights Reserved, Ed.). John Wiley y Sons, Inc., Hoboken, New Jersey.

Mondelo, P. (2015). Deming malentendido : Cómo dar de comer alpiste a los leones Deming misinterpreted : How to feed lions with birdsheed. *ORP journal*, *4*, 3-10.

Monsalve, J., Aponte, F., y Chaparro, F. (2015). Security analysis of a WLAN network

sample in Tunja, Boyacá, Colombia. *Dyna*, *82*(189), 226-232. https://doi.org/http://dx.doi.org/10.15446/dyna.v82n189.43259

Morales, P. V. (2012). Muestras probabilísticas o aleatorias. *Estadística aplicada a las Ciencias sociales*, 2-3. Recuperado de http://web.upcomillas.es/personal/peter/investigacion/Tama%F1oMuestra.pdf

Muñoz, C. (2002). *Auditoría en sistemas computadonales* (PRIMERA ED). Mexico: Prentice Hall.

Nuviala, A., Grao, A., Teva, M., Pérez, R., y Blanco, D. (2013). Validez de constructo de la escala motivos de abandono de centros deportivos. *Revista Internacional de Medicina y Ciencias de la Actividad Fisica y del Deporte*, *16*(61), 1-15. https://doi.org/10.15366/rimcafd2016.61.001

Orlando, O. C. F., y Inti, P. C. (2016). *Análisis y evaluación de riesgos y vulnerabilidades del nuevo portal web de la Escuela Politécnica Nacional, utilizando metodologías de hackeo ético.* https://doi.org/10.1103/PhysRevX.7.041008

Otiniano, B., y Miranda, J. (2015). Universidad Nacional de Trujillo. *Lexus*, *4*(None), 37.

Otzen, T., y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio Sampling Techniques on a Population Study. *Int. J. Morphol*, *35*(1), 227-232. https://doi.org/10.4067/S0717-95022017000100037

Owasp. (2017). OWASP Top 10 - 2017. *OWASP Top 10*, 22. https://doi.org/1

Parada, D. J., y Flórez, A. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas, *29*(1), 27-38. Recuperado de http://dx.doi.org/10.4067/S0718-07642018000100005

Patcha, A. (2006). Network Anomaly Detection with Incomplete Audit Data. Recuperado de http://scholar.lib.vt.edu/theses/available/etd-07192006-152001/

Pérez, A. V. (2011a). Plan---do---check---act en una experiencia tic en el aula: desde la idea a la evaluación. *Edutec-e*, (36), 1-12.

Pérez, A. V. (2011b). Plan-do-check-act en una experiencia tic en el aula: desde la idea a la evaluación. *Edutec. Revista Electrónica de Tecnología Educativa*, (36), 1-12. Recuperado de http://www.edutec.es/revista/index.php/edutec-e/article/view/398

Pértega, D., y Fernández, P. (2006). Investigación Métodos no paramétricos para la comparación de dos muestras Métodos no paramétricos para la comparación de dos muestras, 109-113. Recuperado de http://www.agamfec.com/antiga2013/pdf/CADERNOS/VOL13/VOL13_2/07_Investigacion.pdf

R.A.E. (2014). Diccionario de la lengua española. *Eucarionte*. Recuperado de http://lema.rae.es/drae/?val=eucarionte

Ríos, R., y Fermin, J. (2009). Análisis de tráfico de una red local universitaria. *Revista Electrónica de Estudios Telemáticos*, *8*(2), 93-114. https://doi.org/ISBN:1856-4194

Ríos, S. (2014). ITIL v3 Manual íntegro. *B-able*, 101.

Rodríguez, D., y González, E. (2015). Vulnerabilidad en redes de datos. propuesta para analizar e identificar riesgos. *ENTELEQUIA*, *18*(primavera 2015), 113-122.

Rodríguez, Q., y Verónica, K. (2011). Auditoria Informatica a la supertendencia de Telecomunicaciones, 149.

Rosero, C., y Ponce, M. (2016). Factores de Satisfaccion en los Usuarios de Seguros de Vehículos. *Revista RES NON VERBA*, *6*(1), 85-96.

Rubio, M., y Berlanga, V. (2012). Cómo aplicar las pruebas paramétricas bivariadas t de Student y ANOVA en SPSS . Caso práctico . *Revista d'Innovació i Recerca en Educació*, *5*, 83-100. https://doi.org/10.1344/reire2012.5.2527

Ruiz, A., Gómez, J., y Padilla, N. (2011).

myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux. *Adminso.Es*. Recuperado de http://www.adminso.es/images/9/9c/Alberto_PFC.pdf

Saaty, R. (1987). The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, *9*(3-5), 161-176. https://doi.org/10.1016/0270-0255(87)90473-8

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83. https://doi.org/10.1504/IJSSCI.2008.017590

Salas, A. M., y Monte, P. R. G. (2012). Características psicométricas del «cuestionario para la evaluación del síndrome de quemarse por el trabajo» en maestros mexicanos. *Revista de Educacion*, *2*(359), 260-273. https://doi.org/10.4438/1988-592X-RE-2011-359-094

Saleh, D. M. F. (2011). International Journal of Computer Science and Security (Ijcss). *International Journal of Computer Science and Security*, *5*(3), 316-337. https://doi.org/ISSN (Online): 1985-1553

Salinas, Y. C. A. (2017). Magíster en Auditoría de Tecnologías de la Información.

Sampieri, R., Fernández, C., y Baptista, P. (2014). *Metodología de la investigación*. (S. A. D. C. . McGRAW-HILL / INTERAMERICANA EDITORES, Ed.), *Journal of Chemical Information and Modeling* (6ta ed., Vol. 53). Mexico: Marcela I. Rocha Martínez. https://doi.org/10.1017/CBO9781107415324.004

Scarfone, K., Souppaya, M., Cody, a., y Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. *NIST Special Publication*, *800*, 115. https://doi.org/10.6028/NIST.SP.800-115

Sharifi, M., Ayat, M., Rahman, A. A., y Sahibudin, S. (2008). Lessons learned in ITIL implementation failure. *Proceedings - International Symposium on Information Technology 2008, ITSim*, *1*, 8-11. https://doi.org/10.1109/ITSIM.2008.4631627

Solarte, F. N. S., Rosero, E. R. E., y Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 492-507. Recuperado de http://learningobjects2006.espol.edu.ec/index.php/tecnologica/article/view/456

Stallings, W. (2008). *Comunicaciones y redes de computadores*. (David Fayerman Aragón, Ed.) (Séptima ed). Mexico: PEARSON EDUCACIÓN, S. A.

Supo, J. (2014a). *Cómo elegir una muestra*. Recuperado de http://bioestadistico.com/virtual/049-temei/Lanzamiento/Jos Supo - Cmo elegir una muestra.pdf

Supo, J. (2014b). *Cómo probar una hipótesis: El ritual de la significancia estadística*.

Symantec. (2018). ISTR Internet Security Threat Report, *23*. Recuperado de http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

Tejada, E. C. (2015). *Auditor de seguridad informática. IFCT0109*. (IC Editorial, Ed.). IC Editorial. Recuperado de https://books.google.com.ec/books?id=8a3KCQAAQBAJ

Telecommunications Industry Association. (2001). Ansi/Tia/Eia-568-B.2-2001, *2*(May), 1-139.

TIA-568-C.2. (2009). *TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling and Components Standards*.

Tramullas, J. (2003). El inventario de recursos de información como herramienta de la auditoría de información. *El Profesional de la Informacion*, *12*(4), 256-260. https://doi.org/10.1076/epri.12.4.256.16899

Valdez, A. (2013). OSSTMM 3. *Revista de Información, Tecnología y Sociedad*, 29.

Vásquez, F., y Gabalán, J. (2015). Información y ventaja competitiva. Coexistencia exitosa en las organizaciones de vanguardia. *El Profesional de la Información*, *24*(2), 149. https://doi.org/10.3145/epi.2015.mar.08

Vega, M. (2016). Analisis comparativo entre sistemas OSSTMM y COBIT 5.0 para la mitigacion de riesgos.

Veintimilla, T. (2016). Desarrollo de una guía técnica estándar para aplicar herramientas de ethical hacking en redes de datos, dirigido a PYMES.

Vicente, E., Mateos, A., y Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems*, *66*, 1-12. https://doi.org/10.1016/j.knosys.2014.02.018

Vigna, G. (2003). Teaching network security through live exercises: Red team / blue team, capture the flag, and treasure hunt. En *IFIP Advances in Information and Communication Technology* (Vol. 125, pp. 3-18). https://doi.org/10.1007/978-0-387-35694-5

Villegas, M., Viloria, O., y Blanco, W. (2009). Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizaciones Inteligentes. *7th Latin American and Caribbean Conference for Engineering and Technology*, *1*(1), 1-10. Recuperado de http://www.laccei.org/LACCEI2009-Venezuela/p188.pdf

Wegmann, A., Regev, G., Garret, G. A., y Maréchal, F. (2008). Specifying services for ITIL service management. *2008 International Workshop on Service-Oriented Computing: Consequences for Engineering Requirements, SOCCER'08*. https://doi.org/10.1109/SOCCER.2008.7

Yánez, J., y Yánez, R. (2012a). Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones. *Ingeniería Industrial. Actualidad y Nuevas Tendencias*, *3*(9), 83-92. Recuperado de http://www.redalyc.org/html/2150/215026158006/

Yánez, J., y Yánez, R. (2012b). Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones. *Ingeniería Industrial. Actualidad y Nuevas Tendencias*, *3*(9), 83-92.

Yu, T., Sekar, V., y Seshan, S. (2015). Handling a trillion (unfixable) flaws on a billion devices. *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV*, 1-7. https://doi.org/10.1145/2834050.2834095

Zhang, Y., Lee, W., y Huang, Y. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 1-16. https://doi.org/10.1023/A.1024600519144

ANEXOS