**Analítica diagnóstica: herramienta de análisis de la información para el cumplimiento de los controles ISO 27001.**

Sandra Yorlen Herreño Ballen 1

Carlos Eduardo Cortes Silva 2

**Resumen**

En este artículo se muestran las consideraciones encontradas tras una revisión bibliográfica rigurosa y metodológica, para poder definir a la analítica diagnóstica como una herramienta poderosa y necesaria dentro del proceso de análisis de información, que se adelanta en la planeación de una auditoría que tiene el alcance de la norma ISO 27001:2013 y orientada a la verificación del cumplimiento y diagnóstico de los controles expuestos en el anexo A de la misma norma, en concordancia con lo implementado en el Sistema de gestión de Seguridad de la Información (SGSI), buscando definir las bondades y ventajas que se tiene con su utilización y justificando su apropiación dentro de este tipo de procesos, a partir del cumplimiento de las 3 V del Big Data.

Se definen los controles que pueden ser implementados por medio de software y a partir de esto se plantea la posibilidad de trabajar con grandes cantidades de información (logs de los sistemas) que necesitan de herramientas tecnológicas que permitan su manipulación y manejo para poder encontrar comportamientos y de esta manera diagnosticar la implementación de los controles y sus posibles falencias, buscando ahondar [[1]](#footnote-1)en la contextualización de la empresa a auditar y como soporte en los hallazgos de auditoría.

Se soporta teóricamente que la analítica diagnóstica sirve como herramienta para el auditor en el momento de adelantar el proceso de planeación de la auditoría, bajo la premisa que le ayuda a procesar los logs de los sistemas de información y le entregará un reporte gerencial sobre el cumplimiento o no de los controles soportados sobre software, dándole así una contextualización más precisa y herramientas contundentes para la visita técnica.

**Palabras Claves: Analítica diagnóstica, Controles ISO 27001, análisis de información para auditoría.**

**Abstract**

This article shows the considerations found after a rigorous and methodological bibliographic review, to be able to define diagnostic analytics as a powerful and necessary tool within the process of information analysis, which is in advance of the planning of an audit having the scope of ISO 27001:2013 and aimed at the verification of compliance and diagnosis of the controls set out in Annex A of the same standard, in accordance with the implementation in the SGSI (Information Security Management System), seeking to define the benefits and advantages that one has with its use and justifying its appropriation within this type of processes, from the fulfillment of the 3 V of Big Data.

The controls that can be implemented by means of software are defined and from this the possibility of working with large amounts of information (systems logs) is raised they need technological tools that allow their manipulation and management to be able to find behaviors and thus diagnose the implementation of controls and their possible shortcomings, seeking to delve into the contextualization of the company to be audited and as support in the audit findings.

It is theoretically supported that diagnostic analysis serves as a tool for the auditor at the time of advancing the planning processes of the audit, under the premise that helps you process the logs of the information systems and will provide you with a management report on the compliance or not with the supported controls on software, thus giving you a more precise contextualization and forceful tools for the technical visit.

**Key words: Diagnostic analytical, Controls ISO 27001, analysis of information for audit.**

**Introducción**

El éxito de una auditoria parte de una buena planeación y del ejercicio mismo de auditoría que hace el auditor al momento de hacer las revisiones de información (Casierra Velasco & Gil Espinosa, 2019). En este sentido, si se logra darle herramientas al auditor para que fortalezca la etapa de planeación, se estaría ganando en eficiencia, facilitando al auditor datos con los cuales soportar posibles riesgos y hallazgos, que pueden ser profundizados en la etapa de ejecución de la auditoría.

Bajo esta perspectiva, la utilización de herramientas para la recopilación y posterior análisis de información, con el fin de adelantar la preparación de la visita de auditoria es fundamental, puesto que al tener clara la contextualización del Sistema de Gestión de Seguridad de la Información (SGSI) dentro de la entidad[[2]](#footnote-2), permite tener una perspectiva más clara del Sistema y de las posibles brechas de seguridad y eventuales hallazgos, que le pueden dar al auditor un marco de referencia con el cual abordar la visita a la empresa.

Bajo esta perspectiva, la pregunta evidente estaría orientada a identificar como la analítica diagnóstica ayuda al análisis de información preliminar de una auditoría sobre el cumplimiento de los controles definidos en la norma Técnica Colombiana ISO 27001 anexo A. En el anexo A de la norme técnica, se puede observar que la cantidad de sistemas de información o software pueden ser diversos, numerosos y por ende los archivos log que pueden generarse de dichas herramientas, tienen cantidades de información exponenciales (López D. , 2012), por lo cual es muy dispendioso que una persona pueda adelantar su revisión. Es así que se plantea la siguiente pregunta ¿cómo la analítica diagnóstica contribuye al trabajo del auditor, al trabajarse como una herramienta para el análisis de información preliminar, buscando que de evidencias del cumplimiento de los controles plasmados en la norma ISO 27001 anexo A.

Es así que, la analítica de datos inmersa dentro de Big data, presenta diferentes escenarios los cuales van desde el diagnóstico de situaciones hasta la predicción de comportamientos. Dada la naturaleza de la auditoría, la cual pretende encontrar comportamientos que no son acordes a un parámetro a partir de cruces de información que almacenados en un data warehouse, sirven como insumo al auditor en el momento de realizar una auditoría.

**Metodología**

El presente documento se construye a partir de una investigación adelantada por medio de un diseño cualitativo e interpretativo de tipo documental (Hernández, 2014), el cual permite definir y analizar procedimiento de selección, acceso y registro de la muestra documental base para todo el análisis, condensadas en una matriz bibliográfica que permite definir las unidades de estudio y un análisis profundo de los hallazgos adelantados en los antecedentes.

Por otro lado, se construyó un mapa mental en el cual se trata de visualizar lo encontrado, las necesidades frente a la investigación y sobre todo definir el objetivo sobre el que se trabajó. En este instrumento se logró relacionar la información dada por los textos de la muestra, consiguiendo identificar y definir las categorías de análisis.

**Procedimiento**

Se adelantó el proceso de búsqueda y acceso a los documentos para su lectura y revisión (Fernández, Baptista, & Hernández, 2014), según las categorías analíticas que se iban definiendo durante el proceso, teniendo en cuenta el bosquejo de la investigación se fundamentó en lo esencial y en la investigación de las categorías de análisis definidas para la unidad de estudio. En este sentido, se puede observar que el análisis es permanente en el transcurso del proceso investigativo y es el fundamento de todo el desarrollo, logrando consolidar las categorías analíticas iniciales (definidas a priori), completar con nuevas categorías que especifican el trabajo, justificar ciertos criterios empíricos como resultado de la comparación entre dichas categorías y del hallazgo de otras. Al final, por lo cual, con el análisis se contempla un papel muy importante en el desarrollo de la investigación, pues guían todo el proceso, ayudando al cumplimiento de los objetivos, y aportando claridad, minuciosidad y rigor al análisis realizado sobre el objeto de investigación. Las categorías elegidas para la investigación fueron: Auditoria, planeación para la visita de auditoría, controles de la norma ISO 27001 anexo A y Analítica diagnóstica.

**Resultados y discusiones.**

En la actualidad, una gran cantidad de empresas adelantan la adopción de Sistemas de gestión de calidad orientados a diferentes procesos, donde definen que uno de los más trabajados es el de Seguridad de Información bajo el estándar ISO 27000, toda vez que, dadas las dinámicas de hoy día, la información se presenta como un activo fundamental para el crecimiento y búsqueda de valor de las empresas.

En este sentido, los estándares ISO presentan a la auditoria como una necesidad dentro de la implementación de un sistema de gestión orientado al mejoramiento continuo y para el Sistema de Gestión de Seguridad de la Información (SGSI) desarrollado sobre la norma ISO/IEC-27001:2013 (Icontec, 2013), dichas empresas optan por el montaje de los documentos que solicita la norma y el desarrollo de los controles expuestos en el anexo A de la misma, por medio de la implementación de varios software de carácter específico. En este orden de ideas, algunos de los controles definidos pueden conllevar al cumplimiento por medio de la implementación de software que genera actividades sobre uno o varios numerales de norma como lo expone (Dávalos, 2018). En este sentido, al hacer una revisión no exhaustiva de los sistemas de seguridad de información actuales, frente a los controles de la norma, en la siguiente tabla se listan los controles aplicables:

**Tabla No. 1: Controles aplicables**

|  |  |
| --- | --- |
| SOFTWARE | CONTROLES APLICABLES  ISO IEC 27001:2013 Anexo A |
| Directorio Activo | A6.1.1, A6.1.2, A7.3.1, A9.2.1, A9.2.3, A9.2.4, A9.2.6, A9.3.1, A9.4.1, A9.4.2, A9.4.3, A9.4.4, A9.4.5, A11.2.8, A12.4.2, A12.6.2, A13.1.1, A13.1.2 |
| Sistemas de gestión de usuarios por aplicativo. | A6.1.2 |
| Sistema Gestor de Proyectos. | A6.1.5, A14.1.1 |
| Herramienta de inventario de infraestructura | A6.2.1 |
| Herramienta de gestión de identidades. | A6.2.2, A9.1.2 |
| Herramientas de teletrabajo. | A6.2.3, A9.1.2, A13.1.1 |
| VPN | A6.2.4, A9.1.2, A13.1.1 |
| Sistemas de seguridad perimetral. | A6.2.5, A9.1.2 |
| DLP | A6.2.6, A9.1.2, A11.1.3, A12.2.1, A12.4.2, A18.1.3 |
| LMS para capacitación | A7.2.1, A7.2.2 |
| Herramientas para concientización | A7.2.1 |
| Herramientas de BPM | A7.3.1, A9.2.2 |
| Herramientas de inventario de infraestructura | A8.1.1, A8.1.2, A8.1.4, A14.2.6 |
| Sistemas de gestión documental. | A8.1.1, A8.1.2, A8.2.1, A8.2.2, A8.2.3, A8.3.1 |
| Sistemas de gestión de información. | A8.2.1, |
| Herramientas de borrado seguro. | A8.3.2 |
| Software para cifrado | A8.3.3, A13.1.2, A13.2.1, A18.1.5 |
| Sistemas SSO. | A9.2.1, A9.2.3, A9.2.6, A9.4.1, A9.4.2 |
| Herramientas de Gestión de usuarios | A9.2.2, A9.2.3 |
| gestión de usuarios por Sistema de información. | A9.2.3, A9.2.6, A9.4.1, A9.4.2 |
| Gestores de contraseñas. | A9.2.4, A9.3.1, A9.4.3, A9.4.4, A9.4.5, A10.1.2 |
| Software para cifrado. | A10.1.1 |
| Servicios de certificado interno. | A10.1.1 |
| Sistemas cerrados de tv. | A11.1.1, A11.1.3 |
| Sistemas de detección de intrusos (Físico). | A11.1.1, A11.1.3, A11.1.4 |
| Sistemas de acceso físico (Talanqueras, puertas electrónicas, etc.). | A11.1.2 |
| Sistemas de biometría. | A11.1.2 |
| Sistema de registro de acceso. | A11.1.2 |
| Sistemas contra incendios | A11.1.4 |
| software de UPS | A11.2.2 |
| Software para control de generadores de energía | A11.2.2 |
| Sistemas de cableado inteligente | A11.2.3 |
| Sistema de hojas de vida de equipos | A11.2.4 |
| Sistemas de inventario. | A11.2.5, A11.2.6 |
| Sistema de gestión del SGSI | A12.1.1 |
| Sistemas de control de versiones. | A12.1.2, A18.1.5, A14.2.2, A14.2.3, A14.2.4, A14.2.6 |
| Sistema de inventario de infraestructura y software | A12.1.4, A18.1.5, A18.1.2 |
| Sistemas antimalware | A12.2.1 |
| Sistemas de pruebas de penetración. | A12.2.1, A16.1.3 |
| Sistemas de backup. | A12.3.1 |
| Sistemas de almacenamiento en nube. | A12.3.1 |
| Sistemas de bases de datos. | A12.4.1, A14.2.6, A14.3.1 |
| Logs de cada sistema de información empresarial. | A12.4.1 |
| Sistemas de gestión de logs - SIEM. | A12.4.1, A12.4.3 |
| Directivas de Sistema Operativo | A12.4.4 |
| Sistema de gestión y administración de firewall | A12.5.1, A13.1.1, A13.1.2, A14.1.2 |
| Sistema de gestión de vulnerabilidades | A12.6.1 |
| Logs de Sistema Operativo y gestión de parches. | A12.6.1 |
| Sandbox. | A12.6.1 |
| Sistemas de gestión de redes y analizadores de tráfico. | A12.6.1, A13.1.1, A13.1.3, A14.1.2 |
| Sistemas para gestión de riesgos. | A12.6.1, A16.1.4 |
| Sistemas de Detención de Intrusos (IDS) | A13.1.2, A18.1.3 |
| Sistemas de Prevención de Intrusos (IPS) | A13.1.2, A18.1.3 |
| WAF | A13.1.2 |
| DAM | A13.1.2 |
| Certificados digitales. | A10.1.1, A13.2.1, A14.1.3 |
| Correo electrónico | A13.2.3, A16.1.2 |
| Sistemas para pruebas automáticas. | A14.2.3, A14.2.8, A14.2.9, |
| Sistemas para gestión de incidentes. | A16.1.5 |
| Sistemas de ingeniería forense. | A16.1.5, A16.1.7 |
| Sistemas para gestión de conocimiento. | A16.1.6 |
| Sistemas para implementar el DRP. | A17.1.2 |
| Sistemas de balanceo de carga. | A17.2.1 |

**Tabla 1: Controles que se pueden implementar con software de seguridad de información (ISO 27001, 2013).[[3]](#footnote-3)**

Al revisar la tabla anterior, se puede observar que el 68.4% de los controles definidos por la norma, pueden ser implementados por medio de software, por lo cual es bastante complejo el tener una contextualización completa del SGSI y más aún, lograr definir un diagnóstico de la implementación del sistema dentro de una empresa, por ende, la labor del auditor se complejiza por la cantidad de conocimientos técnicos que se deben manejar y la cantidad de información que se debe revisar (Drljača & Latinović, 2016) en sus diferentes investigaciones.

Sin embargo, todos los softwares implementados generan una gran cantidad de información estándar en forma de logs, la cual concretiza el actuar de dicha herramienta en la operación diaria de la empresa o entidad, haciendo que sea una fuente invaluable de información, siempre y cuando sea entendible, validada y verificada (Kuna , Pautsch , Rey, Cuba, & Villatoro, 2011).

La auditoría es un proceso de evaluación que ayuda a la empresa a darle continuidad a su crecimiento y mejoramiento continuo, presentándola como una herramienta que le permite a la alta dirección, afianzar lo que se ha desarrollado dentro del SGSI y la forma de verificar, desde un punto de vista autónomo, el cumplimiento o no de las consideraciones mínimas definidas a la luz de un estándar o de un criterio de auditoría.

La auditoría al ser un proceso sistemático, independiente y documentado (Icontec, 2018), conlleva a que esté organizado de tal manera que permita cumplir con su objetivo. Es ahí donde la planeación, ejecución y finalización de la auditoria, entran a formar parte de dicho proceso y cada uno de ellos es un engranaje valioso para el cumplimiento de las metas de la auditoría.

La planeación es la etapa más importante, toda vez que es en ella se definen los objetivos de la auditoría, la forma como se van a alcanzar, es así que se empieza a entender como la empresa adoptó el estándar y las posibles falencias dentro de dicha adopción. Este trabajo netamente analítico es fundamental para hacerse una idea de todo el sistema y conlleva más del 60% del tiempo total dedicado a la auditoría(Dávalos, 2018).

Es aquí entonces, donde la información suministrada por la empresa permite vislumbrar todo el SGSI y se empiezan a tener ciertas limitantes técnicas, en virtud de las herramientas que dispone la empresa, como solución para el control de posibles riesgos y el cumplimiento de los controles de la norma (Zárate, 2018).

Para realizar una adecuada planeación se sugiere responder las siguientes preguntas

(López D. , 2017).

¿Es necesario analizar las herramientas utilizadas en la empresa?

¿El auditor está en la capacidad técnica de realizar dichos análisis?

¿Cuál es el nivel de profundidad que se puede alcanzar en una auditoria?

¿El analizar un software y cómo está implementado sirve de algo dentro del proceso de auditoria?

Teniendo como marco todas estas preguntas, se puede observar que poco a poco hay necesidades por conocer más a fondo a la empresa, el SGSI, las herramientas, las implementaciones y en general, la estructura planteada para solventar los problemas a nivel de seguridad de la información, pero también hay limitantes frente a todo esto, tales como , el poco tiempo para adelantar una auditoria, la gran cantidad de documentación que puede aportar el auditado como soporte a la auditoria, los conocimientos técnicos para lograr una profundidad frente a las herramientas técnicas (las cuales las puede solventar un auditor técnico o experto técnico), la innumerable cantidad de herramientas existentes en el mercado y en fin, que hacen de la auditoria un proceso complejo (Macias, 2016), entre otros, sin contar con que el auditado busca esconder las falencias para que no se generen hallazgos según (Alcívar & Espinoza, 2018).

Es aquí donde la misma tecnología puede ser el salvavidas de este proceso, en la medida que puede generar herramientas que ayuden al auditor para hacer más efectivo el análisis de la información en esa etapa de planeación (Tinoco, Aguirre, & Merchán, 2019), buscando darle mayor profundidad al análisis, pero sin requerir de conocimientos técnicos avanzados ni de tiempo adicional y sobre todo, soportado en evidencias como lo busca el proceso de auditoría.

Bajo esta perspectiva, desde hace varias décadas se empieza a acuñar los conceptos de Big data y analítica de datos, soportada en consideraciones específicas que se deben cumplir para poder adelantar este tipo de desarrollos(Fernandes, 2019) . Es así como los conceptos de velocidad, variedad y volumen de información (conocidas como las 3 V) aparecen como los ejes fundamentales para poder implementar procesos de analítica buscando que ese océano de datos e información provea de consideraciones específicas para tomar decisiones.

En este punto, al revisar lo que se tiene hasta ahora sobre la investigación adelantada, se puede observar que las 3 V se cumplen a cabalidad, dado que se tienen grandes volúmenes de información (logs de cada sistema por cada acción ejecutada dentro de un lapso de tiempo), variedad (múltiples tipos de logs dependiendo de los softwares con información variada según el objetivo del mismo) y velocidad (todos los días y a cada momento los sistemas siguen activos y siguen generando datos en sus logs).

Ya teniendo este avance, es hora de empezar a ahondar en el desarrollo y verificar las herramientas que la analítica de datos propone para poder implementar este proceso y es ahí donde investigadores como (Alcívar & Espinoza, 2018), (Kuna, y otros, 2010), (Williams, 2020) y (Hernández & Dueñas, 2009) definen 4 posibilidades de trabajo, a saber:

1. **Analítica Descriptiva**: Es la más básica y permite definir lo que sucedió en el pasado, descrito a partir de los datos.
2. **Analítica Diagnóstica:** Permite definir el por qué sucedió un hecho por medio de correlaciones de datos históricos, pudiendo profundizar en el problema e identificar tendencias y patrones.
3. **Analítica Predictiva:** Este análisis permite predecir lo que puede ocurrir a partir de la definición de tendencias, agrupaciones y excepciones y justificado en los análisis descriptivos y diagnósticos bajo perspectivas estadísticas y comportamentales.
4. **Analítica Prescriptiva:** Este es el análisis más complejo y permite definir acciones para orientarse a un objetivo o en su defecto prevenir los riesgos asociados a algunas acciones.

La figura No 1 muestra el nivel de complejidad que conlleva cada análisis y se puede observar la contribución que adelanta cada uno de ellos a la entidad o empresa que la desarrolla, teniendo claridad que cada análisis requiere de los anteriores para poder lograr los objetivos de cada analítica.



**Figura 1**: Tipos de Analítica. Tomado de https://tienda.digital/4-tipos-de-analisis-de-datos-para-mejorar-la-toma-de-decisiones/

Observando estas herramientas y haciendo los cruces con el objetivo de la auditoria se puede identificar que tanto la analítica descriptiva como la diagnóstica pueden ser elegidas para el proceso a adelantar, toda vez que las otras dos analíticas están orientadas a la predicción del futuro, cosa que la auditoría no hace (Williams, 2020), entre otros.

Pero ¿Cuál tipo de analítica se debe elegir para solucionar este problema?, la analítica diagnóstica permitiría el modelo de procesos de trabajo y del cumplimento de los mismos a partir de la especificación de patrones que se adapten al modelo propuesto y es ahí donde la analítica descriptiva no permite generar patrones y, por ende, a pesar de tener que adelantarla, no es el fin último del análisis (Alcívar & Espinoza, 2018).

Bajo esta perspectiva (Sendón, Herrera, & Fernández, 2020) dan luces frente a la necesidad de adelantar auditorías de sistemas con la ayuda de analítica de datos y proponen esta posibilidad como una necesidad frente al auge de los sistemas de información y a la necesidad de profundizar en las consideraciones técnicas frente a los cumplimientos de norma.

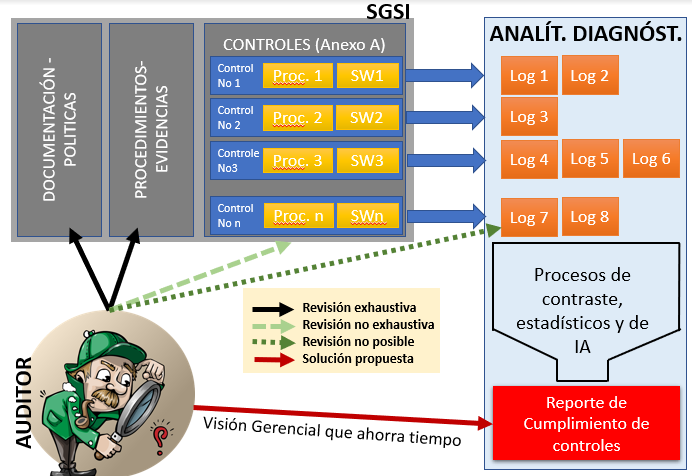
Teniendo en cuenta la disertación adelantada y en concordancia (Adamyk, Adamyk, & Khorunzhak, 2014), entre otros, se puede definir que la analítica diagnóstica se presenta como una herramienta ideal para el proceso de análisis de información en la etapa de planeación de una auditoria, la cual, siguiendo un proceso como el definido por la metodología CRISP-DM, expuesta por (Clark, 2018), puede generar modelos de trabajo lo suficientemente fuertes, como para poder describir la implementación de los controles de la norma ISO 27001 en su anexo A dentro de una empresa (Manaseer & Alawneh, 2019)

Las bondades de utilizar este tipo de herramientas están direccionadas frente al análisis de grandes volúmenes de información, a partir del estudio de los archivos de log de las diferentes herramientas en correlación con los controles implementados y los numerales de norma sobre los cuales se implementan dichas herramientas, tal como lo define, (Drljača & Latinović, 2016).

Al revisar esta perspectiva se puede observar que, al no tener una herramienta como esta, dicha labor sería muy difícil, toda vez que descifrar los logs no es una tarea sencilla y adicionalmente el correlacionarlos, investigar la información de cada uno de ellos y apropiar toda la data es prácticamente imposible para un auditor, tal como lo concluye (López D. , 2012), entre otros.

Por último Yánez & Yánez (2012) plantean que un sistema de analítica diagnóstica optimiza el tiempo a partir de una buena extracción de los datos, su respectiva trasformación y la generación de indicadores que den evidencia de lo encontrado en la información suministrada y que sirvan de referencia para poder ahondar en la implementación del SGSI, buscando que la mejora continua se dé a partir de evidencias precisas y con soportes facticos que permitan dar una visión gerencial y de crecimiento, buscando el fortalecimiento de la seguridad de la información y la resiliencia empresarial.

Bajo esta perspectiva, la siguiente figura representa la solución al problema planteado:



**Figura 2**: Modelo de analítica diagnóstica como solución del problema. Fuente: Creación propia.

Se puede observar que se plantea una solución de analítica diagnóstica, a partir de los logs generados por los sistemas de información utilizados como herramientas para adelantar los controles definidos en el Anexo A de la norma ISO 27001, toda vez que es muy difícil que un auditor llegue a ese nivel de profundidad dados los conocimientos técnicos requeridos para cada una de las herramientas (las cuales son muchas y muy diversas) y en el entendido que las empresas requieren, cada vez más, la colaboración de personas externas que observen el sistema de manera concienzuda, lo evalúen con la mayor profundidad posible y generen hallazgos que permitan la mejora continua de la empresa.

Cabe resaltar que los procesos de contraste, estadísticos y de inteligencia artificial sobre los cuales se estructura el análisis diagnóstico, se sale del alcance de esta investigación, pero se deja como recomendación para la continuidad de la misma, en el entendido que, se acepta la hipótesis de que la analítica diagnóstica sirve como herramienta para el auditor en el momento de adelantar el procesos de planeación de la auditoría, bajo la premisa que le ayuda a procesar los logs de los sistemas de información y le entregará un reporte gerencial sobre el cumplimiento o no de los software implementados para el cumplimiento de controles, dándole así una contextualización más precisa y herramientas contundentes para la visita técnica.

# Conclusiones

Se acepta con base en las evidencias teóricas de varios autores, la posibilidad de trabajar con analítica diagnóstica como herramienta para el auditor, frente a la necesidad de ahondar en la contextualización de la implementación del SGSI dentro de una empresa, de la mano de herramientas de software que ayudan a cumplir los controles definidos por la norma ISO 27001 en el anexo A, toda vez que: Se pueden sistematizar, son cantidades muy grandes de información que requieren de herramientas tecnológicas específicas para el caso y el auditor no puede llegar a ese nivel de profundidad por sí solo.

La analítica diagnóstica se presenta como una herramienta direccionada al análisis de grandes volúmenes de información para describir fenómenos y es la apropiada para analizar los archivos de log de las diferentes herramientas implementadas dentro del desarrollo de los controles de la norma ISO 27001:2013 en su anexo A.

Al realizar el análisis antes expuesto, se le da al auditor una herramienta concreta y basada en evidencias en la cual puede encontrar información valiosa sobre la implementación de dichos sistemas y su cumplimiento frente al numeral de norma, haciendo que el nivel de contextualización y entendimiento del SGSI sea mucho mayor y de esta manera pueda ayudar a la identificación de brechas y en consecuencia a un mejoramiento continuo.

La cantidad de software que puede ser implementado dentro de un proyecto de seguridad de información es bastante alto, alcanzando un aproximado del 68% de los controles definidos por la norma, y optimizando el tiempo en el análisis de la información.

# Referencias

Adamyk, O., Adamyk, B., & Khorunzhak, N. (2014). Auditing of the software of computer accounting system. *CEURS WS - Ternopil National Economic University*, 1-8.

Alcívar, M., & Espinoza, M. (2018). Técnicas de inteligencia de negocio para generación de indicadores de auditoría interna para el software ERP SAP R/3. *IV Congreso Científico Internacional Sociedad del Conocimiento: Retos y Perspectivas*, 1-20.

Clark, A. (2018). The machine learning audit-CRISP-DM Framework. *ISACA JOURNAL*, 1-6.

Crosa, J. (2008). *Análisis de eventos de seguridad en servidores, usando técnicas de minería de datos.* Madrid: Universidad Politecnica de Madrid.

Dávalos, Á. (2018). Auditoria de seguridad de información. *Fides Et Ratio*, 19-30.

Drljača, D., & Latinović, B. (2016). Frameworks for audit of an information system in practice. *Journal of Information Technology and Applications*, 78-85.

Fernandes, G. (2019). Desenvolvimento du projetos du data science. *iNuTech*, 1-17.

Fernández, C., Baptista, P., & Hernández, R. (2014). *Metodología de la Investigación.* México: Mc Graw Hill.

Gallardo, J. (2009). *Metodología para el desarrollo de proyectos en minería de datos CRISP-DM.* Madrid: Universidad Politecnica de Madrid.

Hernández, C., & Dueñas, M. (2009). Hacia una metodología de gestión del conocimiento basada en minería de datos. *UIG -COMTEL 2009*, 79-95.

Icontec. (2013). *NTC-ISO.IEC 27001.* Bogotá: Icontec.

Icontec. (2018). *GTC-ISO 19011 Directrices para la auditoría de los sistemas de gestión.* Bogotá: Icontec.

ISO 27001. (2013). ISO 27001,Anexo A.

Kuna , H., Pautsch , G., Rey, M., Cuba, C., & Villatoro, F. (2011). Avances en procedimientos de la explotación de información con algoritmos basados en la densidad para la identificación de outliers en bases de datos. *XIII Workshop de Investigadores en Ciencias de la Computación*, 248-252.

Kuna, H., Caballero, S., Rambo, A., Meinl, E., Steinhilber, A., & Pautch, G. (2010). Avances en procedimientos de la explotación de información para la identificación de datos faltantes, con ruido e inconsistentes. *WICC 2010 - XII Workshop de Investigadores en Ciencias de la Computación*, 137-141.

López, D. (2012). *Analysis of the possibilities of use of Big Data in organizations.* Cantabria: Universidad de Cantabria.

López, D. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica ESPOL – RTE*, 51-69.

Macias, M. (2016). *Diseño del plan de gestión para seguridad de la información basado en las normas ISO 27000.* Guayaquil: Universidad de Guayaquil.

Manaseer , S., & Alawneh, A. (2019). On cyber security auditing awareness: case of information and communication technology sector. *International Journal of Computer Science and Information Security (IJCSIS)*, 144-150.

Marca, V. (2015). *Método de auditoría para la seguridad de sistemas de información bajo el modelo ISO 27000.* La Paz: Universidad Mayor de San Andres.

Moreno, J. (Madrid). *Herramientas para la evaluación de la seguridad de bases de datos utilizando tecnicas de big data.* 2015: Universidad de Ccastilla-La Mancha.

Sendón, J., Herrera, J., & Fernández, L. (2020). Análisis comparativo entre distintas metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP). *Revista Ibérica de Sistemas e Tecnologias de Informação*, 352-367.

Susanto, H., Nabil, M., & Chee, Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences IJECS-IJENS*, 23-29.

Tinoco, D., Aguirre, F., & Merchán, V. (2019). *Guía de auditoría para la evaluación del control interno de ti en las entidades públicas.* Quito: Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE.

Villarreal, V. (2018). *Comparación de metodologías para auditoría informática: caso de estudio detección de valores anómalos para la prevención de fraudes.* Quito: Universidad Central del Ecuador.

Williams, M. (2020). Applying data security in a cloud service consumer business an exploratory qualitative inquiry. *Proquest No. 28262820*, 24.

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

Zárate, Y. (2018). *Auditoría en servicios teleinformáticos.* Lima: Universidad Nacional de Educación.

1. Log: Archivo de texto que permite verificar cronológicamente los acontecimientos en un sistema. [↑](#footnote-ref-1)
2. SGSI. Sistema de Gestión de Seguridad y Privacidad. ISO 27001.

   ISO 27001. Norma Técnica Colombiana. [↑](#footnote-ref-2)
3. ISO 27001, Anexo A. La tabla de los controles es tomada de la Norma Técnica específicamente en el Anexo A. [↑](#footnote-ref-3)