ISSN impreso 1996-6660 / ISSN online 2519-5719
DOI: https://doi.org/10.31381/perfiles_ingenieria.v18i18.5403

Las TICs como parte del proceso de auditoría

ICTs as part of the Audit Process

Augusto P. Cortez Vásquez[1], Ronald U. García Conde[2], Manuel B. Cortez Vásquez[3]

RECIBIDO: 22 de Julio del 2022
ACEPTADO: 04 de noviembre del 2022

Resumen

El cambio constante ocurre tanto en nuestra mente como en nuestro medio, y nos hace cada vez más sensibles frente a ello. Estos cambios pueden dar lugar a acciones erradas que deben ser corregidas mediante acciones de auditoría. Basta con observar alrededor nuestro para confirmar que los avances tecnológicos han revolucionado todos los sectores y han generado que los procesos de auditoria estén en permanente evolución. Las tecnologías de información, así, constituyen la piedra angular para lograr el éxito de las empresas. La auditoría cobra mayor relevancia si consideramos que, al mismo tiempo que aparecen nuevas tecnologías en el mercado, se incrementan las decisiones no acertadas que ponen en riesgo la información que constituye uno de los activos más importantes de toda organización. Preocupa, entonces, a las empresas, cada vez más, el incremento de la
vulnerabilidad de sus sistemas y los riesgos a los que se someten. El presente trabajo busca contextualizar el proceso de **auditoría** informática que identifique las debilidades de la seguridad de los sistemas informáticos de la empresa, y se proponen acciones con el propósito de reducir las implicancias.

Palabras claves: auditoria, estándares, evidencia, riesgos, Tecnología de Información y Comunicación, auditoria informática

Abstract

The acceleration of change takes place both in our minds and in our environment, making us increasingly sensitive to it. These changes may lead to erroneous actions that must be corrected through audit actions. It is enough to look around us and confirm that it is a reality, technological advances have revolutionized all sectors, thus generating audit processes that are in permanent evolution; Today, information technologies are the cornerstone for the success of companies. The audit becomes more relevant, if we consider that, at the same time that new technologies appear on the market, incorrect decisions are increasing that put "information" at risk, which constitutes one of the most important assets of any organization. Therefore, companies are increasingly concerned about the increase in the vulnerabilities of their systems and the risks to which they are subjected. The present work seeks to contextualize the IT audit process by identifying the weaknesses in aspects of the security of the company's IT systems,

undertaking actions with the purpose of reducing the implications.

Keywords: Audit, standards, evidence, risks, Information Technology and communications, computer audit.

[1] Forma parte del **grupo de investigación Biomedical de la Universidad Nacional Mayor de San Marcos** (UNMSM),y del Departamento de Ciencias de la Computación. <acortezv@unmsm.edu.pe>, <cortez_augusto@yahoo.fr>
[2] Universidad Tecnológica del Perú. Lima, Perú.
[3] Universidad Inca Garcilaso de la Vega. Lima, Perú.

I. INTRODUCCIÓN

El cambio siempre ha sido acelerado, eso no es ninguna novedad, y no podemos reclamar singularidad al respecto. El mundo empresarial no es la excepción y en este cambio la tecnología de las comunicaciones ha logrado ocupar un lugar preponderante en toda organización. Esto nos lleva a dilucidar la necesidad de tener la información organizada y sistematizada de acuerdo con los avances tecnológicos y convertirla en una herramienta indispensable dentro del mundo actual. Sin embargo, los avances tecnológicos constituyen un medio al mismo tiempo que una herramienta que modifica, no solo la gestión de los negocios, sino incluso la gestión en que la auditoria aborda los riesgos y controles. Existen diferentes situaciones o escenarios que conducen a trabajar de formas diferentes, por lo que el nivel de riesgo en cada situación particular puede variar. La función auditora puede enfocarse en la realización de los procesos convencionales de aseguramiento y convertirse en un vínculo entre la estrategia de la organización y los equipos que han de lograrla, con el propósito de ampliar las capacidades, mejorar la eficiencia, gestionar riesgos principales y dedicarse a actividades que agreguen valor.

El uso de tecnología para el manejo de información causa un impacto en todas las profesiones. Este impacto puede variar dependiendo de la percepción y el criterio de las personas. Por eso, es necesario que el auditor complemente su labor con dichas herramientas innovadoras de tecnología. El ritmo actual del cambio es tan rápido que las malas decisiones ejecutadas, como los retrasos para responder, pueden provocar altos costos. El impacto del uso de las TICs para la optimización de sus procesos ha propiciado establecer técnicas dentro de una revisión de auditoría, de tal forma que se fomente la confianza en el correcto uso de la tecnología, lo que repercute favorablemente en el ambiente de control y en los registros contables financieros (Morales, 2019).

El presente artículo pretende articular conceptos necesarios para cumplir los objetivos de la auditoría informática, lo cual incluye la utilización eficiente y analítica de la eficiencia de los diversos sistemas informáticos, verificar el cumplimiento de la Normativa vigente y pertinente. El propósito es contribuir a la calidad del proceso de auditoría.
Conscientes de que la información digital constituye un ingrediente fundamental dentro de las organizaciones, resulta imperativo programar auditorías a los sistemas de información y comunicación con mayor frecuencia para llevar un control y así obtener la confiabilidad en los sistemas y contar con niveles de seguridad aceptables. Para realizar correctamente el proceso de auditoría a las TIC, es necesario comprender bien los conceptos de sistemas, información y tecnologías de las comunicaciones, e involucrarse en el entorno informático para garantizar que el auditor juzgue la naturaleza de la problemática e identifique los riesgos que enfrentará al planificar y realizar la auditoría (Yañez, 2015).
El Foro Económico Mundial se pronunció mediante un informe del año 2019 sobre los riesgos globales y los clasificó en económico, ambiental, geopolítico, social, y tecnológico. Existen riesgos tecnológicos dentro de los top 10 en cuanto a su probabilidad e impacto. La cuarta posición es ocupada por el riesgo de fraude o robo de datos, y en la quinta posición el riesgo de ciberataques.

Considerando el impacto, aparecen el riesgo de ciberataques, y el riesgo de caída de infraestructura de información crítica en las posiciones séptima y octava, respectivamente.
A partir de este ranking, se infiere que los riesgos tecnológicos mencionados son críticos para las empresas y deben ser considerados para gestionarlos adecuadamente.

Se han realizado algunas estadísticas entre las que destaca el Informe de Ciberseguridad (2019) elaborado por ISACA, resultado de una encuesta aplicada a altos directivos de instituciones de la ciberseguridad a nivel

mundial. En este documento, encabeza la lista el **phishing** (44%), el **malware** (31%) y la
ingeniería social (27%). Estos indicadores han causado gran preocupación en las empresas en el área de **ciberseguridad** (Audiconsulti, 2019).
De lo anteriormente expuesto, se infiere la necesidad de realizar periódicas auditorías informáticas, los cuales minimizan los riesgos tecnológicos y evitan poner en peligro la información de la organización.
No hay duda de que, al momento de elegir el auditor, debe asegurarse de que tenga la capacidad de implementar procedimientos, verificar rigurosamente los recursos tecnológicos de comunicación, garantizar la confidencialidad, integridad, disponibilidad, y confiabilidad de la información. Estos rasgos son generados en los diferentes procesos mediante los programas automáticamente. No es de extrañar, por lo tanto, que se busque garantizar que los resultados entregados en el informe de auditoría permitan que la alta dirección disponga de una medición más precisa de la eficiencia y eficacia de los recursos tecnológicos que se disponga (Cuellar Triana & Pinilla Castañeda, 2015).

INFORMACIÓN

Generalmente, utilizamos la palabra información para referirnos a un saber cómo contenido, plasmado en un medio físico, como un libro, manual o dispositivo de almacenamiento electromagnético. Estos indican hacia dónde se dirige el saber registrado como constancia o evidencia. La información se define como una secuencia de datos que articulados configuran un mensaje. En un sentido más general, la información reviste importancia y utilidad debido a que ayuda a la toma de decisiones en forma relevante, oportuna y útil, de allí que debe cumplir una serie de requisitos, entre los cuales cabe destacar (Yañez, 2015):

- **Exactitud:** la información debe ser precisa y libre de errores.
- **Completitud:** La información debe ser completa; es decir, no debe faltar ni incluir información no relevante.
- **Economicidad:** El costo de obtener la información debería ser menor que el beneficio proporcionado.
- **Confianza:** la información que se obtiene debe garantizar calidad, tanto de los datos utilizados como de las fuentes de información.
- **Relevancia:** La información obtenida debe ser relevante y oportuna para la toma de decisiones, y no considerar aquella que no aporte valor alguno.
- **Nivel de detalle:** La información debe presentarse en forma clara y precisa, sin ambigüedades de cuerdo al área a la destina.
- **Verificabilidad:** La información debe poder ser contrastada y comprobada en cualquier momento.

LOS SISTEMAS DE INFORMACIÓN

Existe una diversidad de definiciones de sistemas de información. Algunos autores, en un sentido muy general, la definen como un conjunto de datos que están relacionados con el propósito de administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante que sirve en cada uno de los procesos de la organización. Su objetivo principal es gestionar los datos de tal forma que se puedan recuperar fácilmente con total seguridad. Los sistemas de información permiten distribuir selectivamente la información necesaria para los procesos de toma de decisiones que ayuden a un buen desempeño de las funciones de negocio de la empresa de acuerdo su plan estratégico (Valencia Duque, Tamayo Arias, & Osorio López, 2015)

LA EVIDENCIA DIGITAL

Algunos autores se refieren a la información como la principal mercancía que se intercambia cotidianamente alrededor del mundo, de lo cual se deriva la circulación masiva de información en los intercambios intra e interinstitucionales. El término **evidencia digital** ha adquirido real importancia como insumo fundamental de la auditoría moderna, siendo considerada como todo registro informático que se almacena en un soporte informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación. Los especialistas en auditoria coinciden en señalar que uno de los pilares en cualquier proceso auditor es la forma como se obtiene la evidencia. No obstante, en los últimos años, este insumo se ha transformado, pasando de un soporte de naturaleza análoga a digital, con las implicancias derivadas que conllevan (Valencia Duque, Tamayo Arias, & Osorio López, 2015).
Actualmente, dado el crecimiento exponencial de información gracias a la virtualidad, cobran mayor relevancia las evidencias digitales, debido a que los ciberdelincuentes intentan cambiar o eliminar por completo este tipo de pruebas. Pero esto no es suficiente para sacarlos de problemas (Sanchis, 2018).

La importancia de las evidencias digitales viene por los siguientes aspectos:

- Permite obtener una copia veraz e irrefutable de los hechos.
- Permite comparar el original con las evidencias digitales, dando la posibilidad de determinar si el original ha sido modificado
- Permite restaurar información eliminada, incluso si se elimina el disco duro.
-

AUDITORÍA INFORMÁTICA

La auditoría de sistemas o auditoría informática se dedica precisamente al proceso de revisión de los sistemas de información (SI) y

tecnologías de la información (TI) cuya finalidad es identificar hallazgos, reducir los riesgos e implementar controles adecuados con el propósito de proteger su información crítica y valiosa. Como lo señala Cuellar, se sustenta en una revisión transparente, objetiva, selectiva y sistemática de las políticas, procesos, normas, funciones y actividades de la empresa con el propósito de producir un informe acerca del uso eficiente de los recursos informáticos, de la comunicación, la entrega oportuna y relevante de la información, pero también de las deficiencias encontradas. De este modo, se formulan sugerencias y recomendaciones para subsanarlas (Cuellar Triana & Pinilla Castañeda, 2015).

HALLAZGOS

Todos los procesos de auditoría tienen como común denominador el hallazgo. Un hallazgo de auditoría consta de algún registro, documento o declaración, que aparece durante el proceso auditor, que pueda ser utilizado para evaluar si se cumple o no lo que se está auditando. La norma ISO 9000:2015, respecto a los sistemas de gestión de la calidad, presenta el concepto de "hallazgos de auditoria" como *«Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoria»* (9000:2015, s.f.).

RIESGOS

La noción de riesgo en informática se concibe como cualquier tipo de vulnerabilidad que pueda producir pérdidas de datos, accesos no autorizados, ruptura de la integridad y caídas del sistema. Debe tenerse en cuenta la importancia de las condiciones y circunstancias al momento de ocurridos los hechos de tal forma que se garantice que se actúe con justicia, objetividad y realismo. Todo lo que el riesgo comporta y hace incalculable se deja a responsabilidad definitiva de la decisión de las personas.

Las causas más comunes de estos riesgos son los siguientes:

- Errores humanos ocasionados por una administración incorrecta de los recursos.
- Accidentes, desastres y robos a nivel de hardware. Se incluyen también hurtos y desastres naturales.
- Intrusiones o amenazas a nivel de software que pueden derivar en daños irreparables.

Según Areitio, en el nivel más simple, el proceso de gestión de riesgos identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización (Areitio, 2008). En concordancia con lo establecido por la NIC 200, respecto del riesgo de auditoría, , al momento de emitir opinión sobre los estados financieros de una entidad, es posible que emita opiniones inapropiadas por lo que deberá apelar a la objetividad y transparencia (Mesén, 2009).

Mesen clasifica los riesgos de la siguiente forma:

1. **Riesgo inherente**: son los riesgos que son inherentes a la naturaleza de la entidad, por tanto, independientes de todo sistema de control interno establecidos por las autoridades (Mesén, 2009).
2. **Riesgo de control**: se refiere al riesgo de que una representación errónea que pudiera ocurrir en una aseveración se acumule con representaciones erróneas en otros saldos (Mesén, 2009).
3. **Riesgo de detección**: ocurre cuando el auditor no detecta una representación errónea en una afirmación, lo cual impide que el auditor pueda diseñar los procedimientos de auditoría acertados, para detectar y tomar acciones precisas sobre las incorrecciones materiales que se presentasen.
   Nótese que, el riesgo de detección es responsabilidad del auditor y consiste, fundamentalmente, en la posibilidad de que este cometa errores durante el proceso de auditoría que lo puedan conducir a emitir una opinión errónea.

.

AUDITORÍA INTERNA

Las organizaciones y los equipos de auditores están integrados por varias personas que presentan diversas percepciones y en ocasiones tienen diferentes intereses y expectativas, las que pueden ser causa de riesgos. Las empresas, por tanto, deben preocuparse no solo en mitigar estos riesgos, sino que deberán asumirlos. Desde este punto de vista, la auditoria puede desempeñar un papel fundamental. Por ejemplo, puede prestar atención inmediata a las vulnerabilidades que no están asociadas a ninguna amenaza con el objetivo de aprovecharlas, compartir prácticas empresariales que se identifiquen durante la organización, e incluso brindar apoyo en proyectos especiales. Se incluye también crear herramientas digitales para respaldar otras funciones empresariales.

Desafíos de personal

La auditoría asume su función como un gran desafío, que se traduce en encontrar una combinación adecuada de profesionales de diversas disciplinas, altamente capacitados, con conocimientos tanto del negocio como de tecnologías de la información y una experiencia técnica reconocida, los mismos que deben ser prestados de otras dependencias o emplear recursos externos a la organización.

Supervisión del Comité de Auditoría

El éxito del proceso de auditoría requiere la participación del Comité de Auditoría en su conjunto. Para el logro de estos objetivos, se deben incluir:

- Evaluaciones con retroalimentaciones permanentes y continuas.
- Propiciar la confianza y compromiso con las demás gerencias mediante reuniones del Directorio conjuntas.
- Uso de métricas que permita formular, coleccionar, analizar, interpretar y evaluar resultados (Salazar, 2022).

ESTÁNDARES INTERNACIONALES QUE EL AUDITOR DEBE CONTEMPLAR EN UNA AUDITORÍA DE TIC

Teniendo en cuenta que el producto obtenido debe expresarse formalmente y estar librado de subjetividades, el auditor de las TIC debe tener conocimiento pleno de los estándares internacionales de auditoría, lo que le permitirá identificar vulnerabilidades que pudieran estar asociadas a los activos de la empresa, lo que incluye las debilidades en el nivel físico de la organización.

Puesto que la información es un activo dentro de la empresa, debe resguardarse su uso y protección y garantizar que esta se encuentre disponible solamente para los empleados autorizados. Existen normas establecidas enfocadas en la Auditoría de Sistemas de información y comunicaciones, para lo que es imperativa la verificación de su cumplimiento, ya que garantiza el control de los procesos y la seguridad del manejo de las técnicas implementadas (Tejada, 2020). Es menester dejar deja evidencia del registro de todos los movimientos realizados, de tal forma que en cualquier momento los usuarios puedan verificar los cambios que se realicen (Cuellar Triana & Pinilla Castañeda, 2015).

Las **Normas Internacionales de Auditoría** (NIA) (en inglés, International Standards on Auditing) consisten en una serie de normas establecidas por la Federación **Internacional** de Contadores (IFAC, por sus siglas en inglés), que tienen como finalidad uniformizar las prácticas realizadas por los auditores. Entre ellas tenemos el ISA 250 e ISA 540. También destacan las normas ISO 27001, que ponen de relieve la necesidad de preservar la confidencialidad, integridad y disponibilidad de datos y de los sistemas implicados en su tratamiento (Albarracin, 2021). La norma ISO 27005 agrupa una serie de recomendaciones con indicadores de riesgo que muestran si la empresa tiene alta probabilidad de ser sometida a un riesgo que sobrepasa lo permitido (ISO 27005, 2017). El cumplimiento de la certificación ISO 27001, por su parte, demuestra que se ha obtenido conformidad en la implementación del sistema de gestión de seguridad de la información atendiendo a la norma internacional de buenas prácticas (IsoTools, s.f.).

HABILIDADES DEL AUDITOR DE TIC

En lo que toca a las características fundamentales que debe cumplir un auditor, o equipo auditor, todos están de acuerdo en que deben ser calificados, competentes e independientes. Lo primero se refiere a cumplir un andamiaje de conocimientos tanto en aspectos legales como en aspectos tecnológicos que le permitan realizar su trabajo, preferiblemente avalados por alguna certificación en la que se avale la formación en auditoría con el conocimiento acerca de sistemas de información. La aceleración del cambio tiene lugar en nuestra mente, así como en nuestro medio, convirtiéndonos cada vez más sensible frente a ellos, por lo que requerimos cada vez más personas competentes. Una persona competente no solo es calificada, sino que tiene la cualidad de asumir responsabilidades y cumplir obligaciones a cambio de sus servicios, responsabilidades y obligaciones, de tal forma que pueda desenvolverse con naturalidad dentro de su trabajo, enfrentando obstáculos y sorteando adversidades. De todo lo anterior, resulta claro que el auditor debe ser una persona independiente; es decir, una persona que no tenga ningún vínculo con el objeto de que se está auditando, debe poseer habilidades y destrezas que le permita conseguir evidencias. Entre esas habilidades podemos mencionar:

- Tener actitud positiva
- Poseer mente analítica
- Propensión para escuchar
- Capacidad de negociación
- Proactividad
- Trabajo en equipo

De lo dicho anteriormente, se infiere que la capacitación y la experiencia obtenida por el auditor es una condición imperativa para obtener mejores resultados, pues proporciona a la empresa fluidez y agilidad, que le permiten detectar fácilmente los puntos críticos que se presenten durante los procedimientos definidos por el área de TIC. Lo que al auditor le interesa es poner de relieve el orden y la claridad en sus observaciones, relatando lo sucedido y lo que podría suceder si no se levantan las mismas. Resulta, por lo tanto, imperativo aprender a determinar cuáles son los puntos de vista que deberán tenerse en cuenta al momento de redactar el informe. Se debe resaltar la calidad para que la alta dirección pueda tomar conocimiento de las fortalezas y debilidades detectadas durante la auditoria. El auditor tendrá la responsabilidad de redactar un buen informe, que le permitirá implementar cambios favorables, alcanzar las metas propuestas y proveer las herramientas necesarias para que su empresa funcione de la mejor forma, y satisfaga los requerimientos de todos sus clientes. Asimismo, la administración se fortalecerá con la opinión emitida por el auditor, pues esta mejora los procesos e implementa controles con el firme propósito de alcanzar mejores resultados, lo que redundará en alcanzar la tranquilidad de la administración (Cuellar Triana & Pinilla Castañeda, 2015).

El insumo principal para lograr un buen proceso de auditoria es la evidencia, a partir de la cual se extraerán conclusiones que sirvan de sustento y fortalezca su opinión. De lo anteriormente expuesto se infiere que la evidencia obtenida debe ser suficiente y competente. Lo primero hace alusión a la cantidad, mientras que lo segundo a la calidad de la evidencia.

VENTAJAS DE REALIZAR UNA AUDITORÍA INFORMÁTICA

Realizar una **auditoría** informática reporta los siguientes beneficios:

- Optimizar los sistemas informáticos existentes
- Eliminar vulnerabilidades, y reducir sustancialmente los riesgos a los que se exponen los sistemas informáticos
- Prevenir incidentes que vulneren la seguridad
- Marcar un horizonte de actuación, para reducir el impacto de los incidentes de seguridad ocasionados
- Mantener actualizados las políticas y procedimientos que garanticen la seguridad informática
- Promover una cultura de respeto a las leyes y normativas para evitar multas o sanciones
- Mejorar el flujo de trabajo y permitir el teletrabajo seguro
- Adoptar medidas para mejorar la imagen empresarial, lo que propiciará una comunicación constructiva y un adecuado bienestar laboral.

Fases de una auditoría

El proceso de auditoria se realiza en varias fases, como se muestra en la siguiente figura.

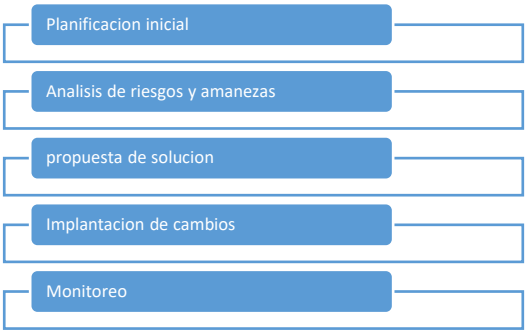

Figura 1. *Fases de una auditoría. Elaboración propia*

1 **Planificación inicial:** Estudio de la forma en la que funciona el negocio, y énfasis en la interacción con sus sistemas informáticos y la seguridad**.**
2 **Análisis de riesgos y amenazas:** Análisis exhaustivo de los riesgos que pueden vulnerar los procesos de la empresa, identificar las amenazas, debiendo elaborar un plan sobre cómo evaluar las consecuencias ocasionadas.
3 Plantear **soluciones** para eliminar o mitigar las consecuencias derivadas de los riesgos y establecer un plan de prioridad de implementación de los cambios.
4 Tener un calendario bien definido en el que se señalen expresamente los cambios necesarios, los que deberán contemplar modificaciones en las políticas de seguridad
5 Monitorear permanentemente los resultados y verificar si se están alcanzando los objetivos; de no ser, realizar las modificaciones y ajustes necesarios.

TÉCNICAS DE UNA AUDITORÍA INFORMÁTICA

Existen varias técnicas de auditoría informática que coinciden en definir los procedimientos que se usan en su desarrollo. Las más comunes son:

- Estudio general
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaración
- Certificación
- Observación
- Cálculo

HERRAMIENTAS

Las herramientas utilizadas son fundamentales para el logro de los objetivos de un proceso de auditoría. Su uso adecuado permitirá ejecutar acciones definidas en las técnicas. Entre las principales tenemos: cuestionarios, entrevistas, listas de verificación, trazas y software de interrogación.

1 Los **cuestionarios** permiten obtener información y documentación de todo el proceso de la organización, que requiere ser auditado.
2 La entrevista sirve para obtener información más específica mediante cuestionarios o el **interrogatorio**.
3 Las listas de chequeo (**checklist)**, constan de un conjunto de preguntas realizadas en determinado orden, redactadas en lenguaje formal y sistematizado, expresadas de forma coherente y sin ambigüedades, de tal forma que facilite al auditado su comprensión y responda claramente.

CONCLUSIONES

La principal contribución del presente trabajo no es proveer una técnica o herramienta relevante, sino en la sistematización y organización del proceso de planeación de una auditoría.

La conclusión más razonable respecto a una auditoría informática es la elección del auditor y la forma misma de la elección, lo que permitirá implementar procedimientos para la verificar si los recursos tecnológicos y de comunicación son los adecuados y sin poner en riesgo la confiabilidad, integridad, disponibilidad y confidencialidad de la información generada mediante los programas ejecutados. Los resultados incluidos en el informe de auditoría permitirán a los directivos de la empresa disponer con una medición más precisa de la eficiencia y eficacia de los recursos tecnológicos que usa la empresa.

Para realizar cambios en el interior de la empresa auditada, es menester que el auditor presente los resultados de sus hallazgos en un informe objetivo en donde se resalta la posibilidad de emprender acciones que brinden oportunidad de mejora. Por supuesto, todo ello debe estar amparado en su experiencia y conocimiento en dichos procesos.

Finalmente, los reportes de no conformidad podrían ser de mucha utilidad, porque podrían conducir a oportunidades de mejora y permitir a la administración tomar decisiones oportunas enmarcadas en un plan de mejora continua y permanente

CONFLICTOS DE INTERÉS

No existen conflictos de interés sobre el trabajo de investigación.

REFERENCIAS

9000:2015, i. (s.f.). *plataforma de navegación en línea (obp)*. recuperado el 02 de 04 de 2022, de https://www.iso.org/obp/ui/es/#iso:std:iso:9000:ed-4:v1:es

Albarracin, l. (2021). auditoría informática dentro de la empresa "promaelec" de la ciudad de quevedo, en tiempo de covid-19. *universidad y sociedad, 13*(5). recuperado el 15 de 03 de 2022, de http://scielo.sld.cu/scielo.php?script-=sci_arttext&pid=s2218-36202021000500345

Areitio, j. (2008). *seguridad de la información.* madri, españa: paraninfo.

Audiconsulti. (2019). *la importancia de la auditoría de sistemas*. recuperado el 03 de 04 de 2022, de https://www.audiconsulti.com/importancia-de-la-auditoria-de-sistemas/

Cuellar triana, n., & pinilla castañeda, o. m. (2015). el papel del auditor frente a una auditoria sobre tic. obtenido de https://ciencia.lasalle.edu.co/contaduria_publica/266

Iaasb. (2018). *2018 handbook of international quality control, auditing, review, other assurance, and related services pronouncements.* recuperado el 06 de 04 de 2022, de https://www.iaasb.org/publications/2018-handbook-international-quality-control-auditing-review-other-assurance-and-relted-services-26

Iso 27005. (2017). *¿cómo identificar los riesgos?* recuperado el 05 de 04 de 2022, de https://www.pmgssi.com/20-17/01/iso-27005-como-identificar-los-riesgos/

Isotools. (s.f.). *sistemas de gestión la seguridad de la información*. recuperado el 12 de 02 de 2022, de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Mesén, v. (2009). el riesgo de auditoría y sus efectos sobre el trabajo del auditor independiente. *tec empresarial*, 9-12. obtenido de https://dialnet.unirioja.-es/servlet/articulo?codigo=3201923

Morales, f. (2019). *tecnologia de la informacion como herramientas de ajuditoria.* mexico. obtenido de https://contaduriapublica.org.mx/2019/10/01/tecnologia-de-la-informacion-como-herramienta-de-la-auditoria/

Quintana, a. (2016). *tecnicas para auditoria de sistemas informaticos*. http://www.dspace.-uce.edu.ec/handle/25000/14183?mode=full

Salazar, j. (2022). *métricas para un programa de auditoria de cumplimiento efectivo.* obtenido de https://www.delitosfinancie-ros.org/wpcontent/uploads/2016/04/s7_auditoria_jose_mauricio_salazar.pdf

Sanchis, e. (01 de 10 de 2018). *peritos informáticos*. obtenido de https://peritosinformaticos.com/que-son-las-evidencias-digitales

Tejada, m. (2020). auditoría a los sistemas como herramienta para examinar los procesos en las empresas. *faeco SAPIENS, 3*(1), 64-74. Recuperado el 02 de 04 de 2022, de https://revistas.up.ac.pa/index.php/-faeco_sapiens/article/view/1072/892

Valencia Duque, F. J., Tamayo Arias, J. A., & Osorio López, K. (2015). Tecnologías de información y comunicaciones en el control fiscal colombiano. *Administración y Desarrollo*, 208-233. Obtenido de http://esapvirtual.esap.edu.-co/ojs/index.php/admindesarro/article/view/13

Yañez, C. (2015). Enfoque metodológico de auditoría a las tecnologías de información y comunicaciones. Obtenido de https://www.google.com/-search?client=firefoxbd&q=enfoque+metodol%c3%93gico+de+auditor%c3%8da+a+las+tecnolog%c3%8das+de+informaci%c3%93n+y+comunicaciones