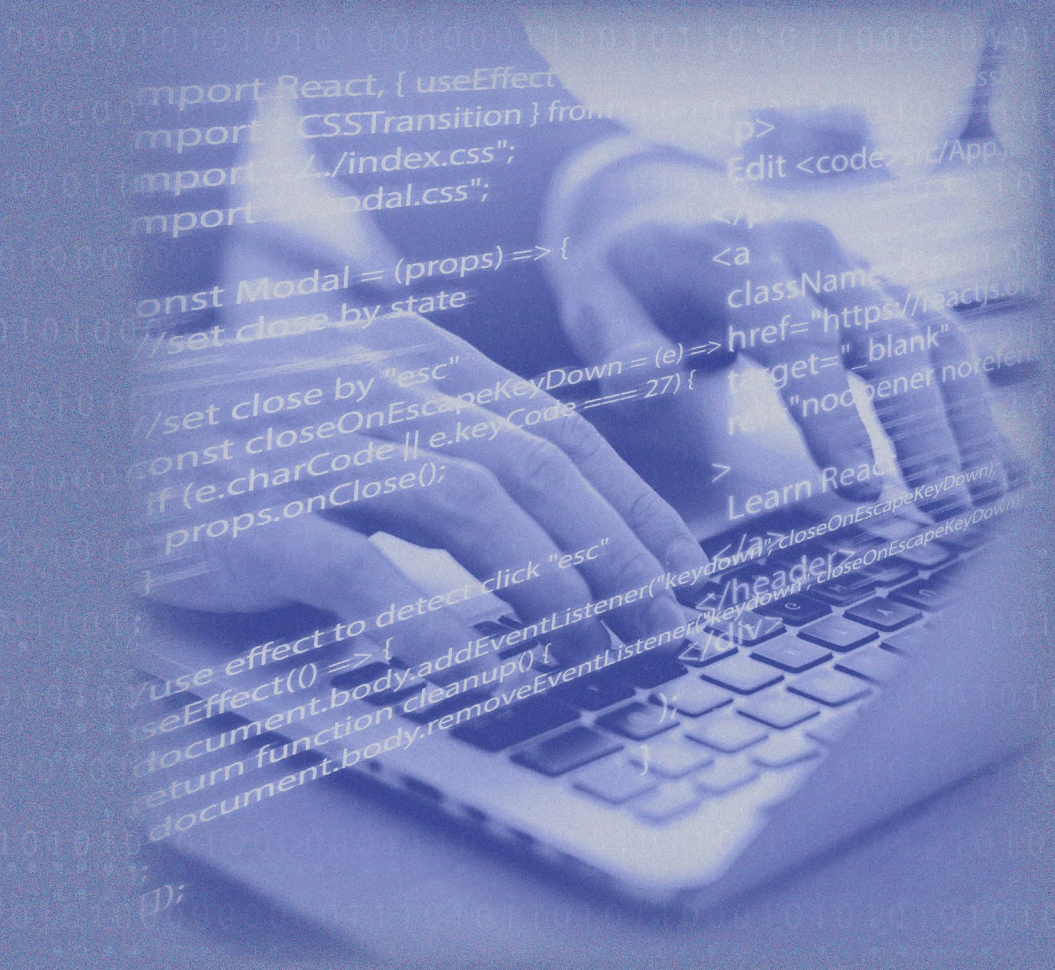
Un estudio contemporáneo de la auditoría en informática



Jeny Haideé Espinosa Barajas
José Rafel Baca Pumarejo
Héctor Gabino Aguirre Ramírez

astra editorial

Un estudio contemporáneo de la Auditoría en Informática

astra
editorial

Un estudio contemporáneo de la Auditoría en Informática

Jeny Haideé Espinosa Barajas
José Rafel Baca Pumarejo
Héctor Gabino Aguirre Ramírez

astra
editorial

Un estudio contemporáneo de la Auditoría en Informática / **Autores**: Jeny Haideé Espinosa Barajas, José Rafael Baca Pumarejo y Héctor Gabino Aguirre Ramírez. Tamaulipas, México, 2024.

Publicación electrónica digital: descarga y *online*; detalle de formato: EPUB.

Primera edición

ISBN: **979-13-87631-35-2**

DOI: **https://doi.org/10.61728/AE24002547**

Edición y corrección: **Astra Ediciones**

Esta investigación fue dictaminada por pares académicos.

HECHO EN MÉXICO | MADE IN MEXICO

Contenido

Capítulo 1

Introducción

1.1 Evolución del concepto de Auditoría de la informática

Para hablar de auditoría en informática se debe de reflexionar acerca de su evolución en base al acelerado cambio tecnológico, el concepto de auditoría en informática ha evolucionado al mismo ritmo, reflexionar sobre los cambios tecnológicos de la computación es recordar los escenarios de la misma en cuanto a las características físicas y operativas de las versiones anteriores de las máquinas computacionales tradicionales, representadas por las de tipo mainframe. Era la época en que realmente se dudaba de que las máquinas portátiles fueran dispositivos serios de sistemas de información empresarial, y que el internet se consideraba solo una herramienta de comunicación por correo electrónico e intercambio de documentos de texto.

Hoy en día las tecnologías de la información y las comunicaciones (TIC) han evolucionado y son una pieza fundamental de nuestras actividades diarias. Desde las operaciones comerciales y los servicios gubernamentales hasta la comunicación personal y el entretenimiento, los sistemas de TIC desempeñan un papel fundamental para permitir la eficiencia, la innovación y la conectividad. Sin embargo, con la adopción generalizada de las TIC, surge la necesidad crítica de garantizar su uso responsable y seguro.

Estudiar esta disciplina del conocimiento de la auditoría del uso de las TIC, es asimilar e indagar el conocimiento y operación de una práctica esencial que se orienta a la evaluación de la eficacia, la administración y el desempeño de riesgos en los sistemas de la información implementados mediante las TIC. Implica afrontar el reto que representa describir las complejidades de la auditoría en el contexto de las TIC y brindar información valiosa para profesionales, auditores y tomadores de decisiones que buscan navegar con confianza en los cambiantes paisajes digitales.

1.2 La seguridad en la informática

En este escenario la seguridad informática se basaba entonces en gran medida en mainframes con instalaciones cerradas y protegidas, así mismo presenciamos la irrupción de los primeros virus informáticos. En esta

circunstancia los auditores internos y externos, solían tener reducidas habilidades en los controles de los sistemas informáticos, y existían grandes huecos de conocimiento al respecto por parte de los auditores, los especialistas en seguridad de sistemas y sus promotores. Es difícil establecer el conjunto de eventos que contribuyeron a cambiar nuestra visión del mundo acerca de la auditoría informática y que la hayan convertido en una específica área del conocimiento. Tuvo de cierta manera que ver el impacto mundial de la Red Mundial de Información, la Web, que se ha convertido en el factor causal de los problemas de auditoría, seguridad y control interno, ligados a los controles informáticos que han venido a ser más complejos hoy en día.

1.3 Panorama de la auditoría en informática

La presente obra se enfoca en exponer el panorama relacionado a los factores técnicos como profesionales que rodean a la auditoría actual, a los especialistas en el control interno y seguridad en un entorno de los sistemas de información, con el propósito comprender y asimilar por parte de los interesados las cuestiones clave de las auditorías informáticas.

Si bien esta propuesta contempla la seguridad informática y la interna en el contexto del personal de la auditoría, se incluye como parte de la evolución descrita a los especialistas en control. Es conveniente mencionar que hoy en día algunos profesionistas no tienen títulos que se orienten a estas disciplinas de auditoría, seguridad y controles internos, muchos profesionales en diversas disciplinas tienen la responsabilidad de instalar buenos controles informáticos y mantenerlos para que estos sean operativos. Los auditores informáticos son los principales responsables de evaluar estos controles.

1.4 Estructuración de los temas abordados

Los capítulos de este libro, que se describen a continuación, cubren este propósito mediante el desarrollo de los principales conceptos asociados a la auditoría en informática de una manera accesible y condensada para que los alumnos asimilen los principales conceptos acerca de esta

disciplina y se desempeñen en las organizaciones con habilidades y adecuado conocimiento:

Capítulo 1. Introducción: El capítulo se desenvuelve en el panorama de la auditoría en informática pasando por un recorrido por el tiempo más reciente refiriendo a las características de la 4ª y 5ª generación de computadoras a partir de la máquina más representativa como la denominadas mainframes, así mismo se aborda la transición evolutiva a la computación personal de manera que las primeras computadoras portátiles irrumpían sin perfilar las futuras necesidades de la seguridad para su operación y funcionamiento. Luego se describe el concepto de la seguridad a partir de las primeras manifestaciones de contaminación vía rutinas externas que se adherían a los núcleos de los sistemas operativos, sucesos que antecedieron por primera vez la aparición de los nombrados virus informáticos. Así mismo se introduce y desarrolla de forma concreta el concepto de auditoría de informática y expone el panorama relacionado a los factores técnicos y profesionales que conforman la auditoría en informática actual. Y posterior a la representación de la visión actual de la auditoría informática se desarrolla una explicación de los temas que se desarrollan en cada capítulo de la obra.

Capítulo 2. Auditoría en Informática. En este apartado se desarrolla el concepto de auditoría en informática, su evolución, el significado que ha tenido en paralelo a la evolución tecnológica computacional. Para ello se desarrolla su historia para dar una visión concreta de esta disciplina cada vez más crucial para el uso y la utilización de las TIC en todas las instituciones u organizaciones. En esta intención se definen los propósitos de la auditoría en informática, así como la exposición de las ventajas y limitaciones que la auditoría tiene en los contextos en donde se ha de llevar a cabo. Se describen de manera concreta los tipos de auditoría que existen pasando por la Administrativa, la Financiera, y de manera especial la auditoría informática. También se explican y se describen las áreas de aplicación y se abordan los profesionales que han protagonizado el desempeño de llevar a cabo estos procesos, para ello se ilustran los tipos de auditores, como son los auditores internos, los auditores externos y los equipos combinados. Para lo anterior se desarrollan a detalle las características de los auditores, el perfil del auditor, y la formación académica

que estos profesionistas tienen, su posible formación complementaria, así como su formación empírica que constituyen el perfil de habilidades y destrezas necesarias para abordar este reto. En esta sección también se exponen los principios del auditor, así como los principios que deben regir a un auditor.

Capítulo 3. Control Interno y Seguridad. Esta sección aborda la relación del Control Interno y la Seguridad y describe que ambos elementos constituyen un binomio crítico para que las organizaciones ejecuten sus procesos con el mayor éxito posible, para ello los sistemas de control ameritan de las TIC para llevarse a cabo y esta actividad forma parte fundamental del proceso de auditoría de informática, en este sentido el capítulo analiza el concepto de lo que representa el control interno, la importancia que tiene, establece los tipos de control interno que hay, define los componentes del control interno, asimismo define cada una de las acciones de control. Describe el concepto de riesgo en función de un significado del control interno; detalla los tipos de riesgos que hay, ilustra los mecanismos de medición, así como la forma de manejar los riesgos y desemboca en la definición de los riesgos en el área de TIC, de tal forma que esta sección describe una panorámica de estos elementos cruciales en la auditoría en informática.

Capítulo 4. Metodologías para realizar una auditoría. Este capítulo se dedica al análisis de la metodología que se sigue para realizar una auditoría en informática, establece el concepto del proceso metodológico para llevarse a cabo. Así mismo ilustra las etapas que implica llevar a cabo una auditoría. En este propósito describe un ejemplo completo de una auditoría en informática, con el propósito práctico de replicar el proceso para los interesados.

Capítulo 5. Metodologías y buenas prácticas para realizar una auditoría. Este capítulo desarrolla la parte teórica practica de adecuar la ejecución de una auditoría en el ámbito de la informática para medir la efectividad con que este importante proceso se lleva a cabo. En este sentido se describen y establecen los marcos y estándares para que la auditoría de informática garantice la coherencia y la calidad en las prácticas de auditoría, para este objetivo se analiza cómo se han definido varios marcos y estándares. En primera instancia se aborda el proceso

de la Metodología y se ilustra su concepto, establece las etapas de una auditoría, se ilustra un ejemplo de una auditoría en informática y en este proceso se abordan formatos de ejemplo para realizar los procesos de la auditoría en informática, ejemplificando un formato para registrar los avances en el cumplimiento de la auditoría en informática. Además, se aborda el tema de las buenas tareas en la auditoría de la informática, describiendo el modelo COBIT, el COSO y el ITIL y en base a esta estructura de análisis se le brinda al lector la práctica de revisión al resolver reactivos relacionados a este tema crucial.

Capítulo 6. Norma ISO. Esta sección se dedica al análisis de la Norma ISO cuyas letras constituyen el acrónimo de las palabras inglesas *International Organization for Standardization* que desde 1946, cuando organismos internacionales tenían por objetivo regular y establecer estándares para la fabricación *International Federation of National Standarzing* (ISA) y el organismo *United Nations Standards Coordinating Committee* (UNSCC)) y que aglutinaron a 25 países que ratificaron estas normas en Londres. En este objetivo el capítulo explora marcos y estándares ampliamente reconocidos, como el ISO, su historia, su consolidación a constituir una certificación, se analiza a detalle en que consiste la norma ISO, se establecen cuáles son los requisitos para lograrla. Una vez lograda la certificación ISO se analizan cuáles son las ventajas para lograrla, de igual manera y de manera especial se analiza la relación ISO y las TIC, se aborda también la implementación de la norma ISO en las TIC, así mismo se analiza la norma ISO/IEC 25000 y la norma ISO/IEC 27000. Respecto al proceso que representa una auditoría en informática se ilustran algunas situaciones en informática, las responsabilidades asignadas en dicho proceso, el ciclo Planear-Hacer-Revisar-Proceder a la gestión de un proceso, tareas que se ejecutan en una auditoría en informática, y el punto de finalización de un proceso de auditoría y con ello el establecimiento de un seguimiento cercano y riguroso para que el auditoría asegure que se llevan a la práctica las mejoras en los estándares de operación de los procesos implicados.

Capítulo 7. La Auditoría en Informática en la Nube

El capítulo se centra en la importancia de la auditoría en los entornos de computación en la nube, un proceso esencial para asegurar la segu-

ridad, el cumplimiento normativo y la gestión eficiente de los recursos en la nube. Con el creciente uso de la nube, la auditoría se vuelve crítica para gestionar riesgos como la seguridad de los datos y la privacidad. En este sentido se aborda la Auditoría de Sistemas en la Nube con IA donde se subraya que el procesamiento de datos en la nube ha transformado la gestión de datos, y a la vez ha generado riesgos que requieren una auditoría constante, y ante este reto la (IA) es clave para la detección de anomalías y gestión de riesgos en tiempo real. En este sentido la IA permite auditorías continuas y más profundas, identificando patrones inusuales y comportamientos sospechosos sin intervención constante. Así mismo la IA puede anticipar vulnerabilidades mediante modelos predictivos y mejorar la eficiencia al analizar grandes volúmenes de datos rápidamente. En este proceso la auditoría en la nube aborda varios factores críticos: Seguridad de datos para proteger los datos sensibles, el Cumplimiento de normativas como GDPR, HIPAA, PCI DSS, Gestión de identidades y accesos: para asegurar el acceso autorizado, asi como elementos de operación tales como Evaluación de infraestructura y configuración de seguridad: Comprobación de la correcta configuración de redes y firewalls que asegurarían la Optimización de costos, Monitoreo y detección de incidentes, los Planes de recuperación ante desastres. Se mencionan los serios desafíos en la Implementación de IA y aborda las aplicaciones Comunes de IA en Auditoría de la Nube y las Herramientas para la Auditoría en la Nube tales como AWS CloudTrail y AWS Config , Google Cloud Audit Logs, Microsoft Azure Security Center y Cloud Security Posture Management (CSPM).

Capítulo 8. Consideraciones éticas y legales en el proceso de la auditoría en informática. Este apartado de la obra aborda las consideraciones éticas y legales en el proceso de la auditoría en informática. Las Consideraciones éticas representan las reglas y normas que constituyen el espíritu de servicio que los profesionales que se desempeñan en auditoría en informática, deben de tener y llevar a la práctica para asegurar el funcionamiento adecuado del procesamiento de datos al servicio de las organizaciones, de tal forma que la seguridad y la confianza en las herramientas informáticas y los recursos humanos que las manejan, así como los que supervisan esta esencial relación formen un binomio que

permita y mantenga el círculo virtuoso de operatividad predecible y confiable del procesamiento, almacenamiento y aplicación de la información. La parte de consideraciones legales está representada por las normas jurídicas que han sido formuladas para regir los procesos donde la informática está siendo usada como herramienta de trabajo en las empresas. Los códigos legales, así como la estructura de leyes y cláusulas que se han establecido al respecto contribuyen a que el estudiante reciba una preparación que le hagan consciente de la parte legal que rodea a los procesos que salvaguardan la información de las entidades productivas en su dinamismo dentro del sistema económico nacional e internacional. Para lo anterior esta sección también ilustra sobre los conceptos de código de ética profesional y conducta que han sido sistematizados de acuerdo con los requerimientos de orden, corrección y seguridad que debe de haber al interior de las organizaciones en especial aquellos que deben de seguir los profesionales de la informática que se desempeñan en esta delicada área de la auditoría de informática.

Ejercicio: Diagnóstico, respuestas breves

Instrucciones: Responde las siguientes preguntas de forma clara y breve.

1.- ¿Conoces el trabajo que se realiza en una auditoría en informática?
2.- ¿Has participado en el equipo de trabajo de alguna auditoría en informática?
3.- ¿Conoces las características que debe de tener un auditor/a?
4.- ¿Has escuchado sobre las normas internacionales correspondientes a diversas áreas comerciales y de procesos?
5.- ¿Conoces los componentes del control interno informático?

Capítulo 2

Las Tecnologías de Información y Comunicación

2.1 Evolución Histórica de las Tecnologías de la Información y Comunicación

Realmente es un viaje fascinante la evolución de las Tecnologías de la Información y la Comunicación (TIC) que han transformado nuestra vida diaria, la forma de trabajar y comunicarnos. En seguida, se narran las etapas significativas en la evolución de las TIC:

•Antes del siglo XX.

Las primeras formas de TIC se remontan a civilizaciones antiguas, donde se utilizaban sistemas como señales de humo, la corneta, la piedra, mensajeros, papel papiro, palomas, las cartas y la botella para las comunicaciones a larga distancia. Sin embargo, estos tenían un alcance muy limitado. Estos medios de comunicación antiguos se describen en seguida (Comunicare, 2019):

- **Señales de humo:** Las señales de humo fueron un medio utilizado para contactar a personas que estaban en otros lugares o para avisar la ubicación de alguna persona o grupo de personas.
- **Corneta:** Este instrumento sonoro también permitió disminuir las distancias, a través del sonido se alertaba o se avisaba a las personas sobre algún suceso.
- **Piedra**: La piedra fue utilizada antes de la invención del papel para plasmar signos y símbolos. La desventaja es que, por este medio, el contenido solo podía ser interpretado por las personas que conocían los signos utilizados.
- **Mensajero**: En este tipo de comunicación los mensajes eran enviados de forma oral a través de una persona. Dicha persona recorría toda una trayectoria para entregar el mensaje.
- **Papel Papiro**: El papel papiro era producto de una planta acuática y este medio era muy usado para escribir mensajes.
- **Palomas**: En la antigüedad también se utilizaron las palomas para enviar mensajes a personas de otros sitios lejanos.
- **Carta:** Las cartas en papel son otro medio de comunicación, en ellas se escribía un mensaje, se lo colocaba en un sobre y el correo se encargaba de organizar el envío.

- **Botella**: La botella era un medio de comunicación muy usado por los marinos. El procedimiento consistía en arrojar una botella con el mensaje en el interior para que viajara por el mar hasta que alguien tuviera la suerte de encontrarlo.

•Siglo XX – El Telégrafo y el Teléfono.

A fines del siglo XIX e inicios del siglo XX se desarrollaron los sistemas del telégrafo y el teléfono, que revolucionaron las comunicaciones a larga distancia, mientras que el teléfono permitió la comunicación por voz.

- Telégrafo. Es "un sistema de comunicación que permitió transmitir con rapidez y a distancia mensajes codificados" (Real Academia Española, s.f., definición 1) (figura 1).

Figura 1. Telégrafo

Nota: Adaptado de *Telegraph* [Fotografía], por Kaspersky Daily, 2015. https://latam.kaspersky.com/blog/telegraph-grandpa-of-internet/5641/

- Teléfono. Es el "conjunto de aparatos e hilos con los cuales se transmite a distancia la palabra y toda clase de sonidos por la acción de la electricidad" (Real Academia Española, s.f., definición 1).

Mediados del siglo XX - La computadora.

El invento de la computadora en la mitad del siglo XX marcó un momento crucial en la evolución de las TIC. Las primeras computadoras eran enormes y se usaban principalmente con fines científicos y militares.

La primera generación de computadoras sucedió entre los años de 1940 y 1950. Siendo la primera computadora comercial electrónica diseñada en el año de 1946 por J. Presper Eckert y John Mauchly, la cual llevo el nombre de ENIAC (*por sus siglas en inglés, Electronic Numerical Integrator and Computer*), y fue utilizada para ejecutar cálculos balísticos y cálculos matemáticos complejos. Las primeras computadoras utilizaban tubos al vacío (Espitia, 2023).

Posterior a ello, John Bardeen, Walter Brattain y William Shockley en 1947 inventaron el transistor. Este componente admitió crear computadoras de menor tamaño y por consiguiente más económicas; ya que el transistor por el hecho de ser más reducido consumía menos energía en comparación con los tubos al vacío. Después de ello se desarrollaron los circuitos integrados (Espitia, 2023).

Décadas de 1960 y 1970.

Los precursores de Internet: durante este período, la unidad de Defensa de Estados Unidos inició la creación de ARPANET, precursor de la Internet moderna. ARPANET utilizó conmutación de paquetes para transmitir datos entre computadoras, sentando las bases para la creación de redes globales.

- La Internet se define como la "red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación" (Real Academia Española, s.f., definición 1).
- ARPANET integró una red sin nodos centrales en el año de 1969 (la primera en su tiempo), y estaba constituida por medio de cuatro universidades en Estados Unidos: Universidad de California Los Ángeles (UCLA), Universidad de California Santa Barbara (UCSB), Universidad de Utah y *Stanford Research Institute* (SRI) (Trigo, s.f.).

Década de 1980 - Computadoras personales.

La década de 1980 vio el surgimiento de las computadoras personales (PC), como la IBM PC (figura 2) y Apple Macintosh (figura 3). Esto hizo que la informática fuera accesible para individuos y empresas, lo que llevó a una revolución informática.

Figura 2. IBM PC modelo 5150

Nota: Adaptado de IBM PC *Modelo 5150* [Fotografía], por Linked in, 2019. https://es.linkedin.com/pulse/nacimiento-de-la-ibm-pc-modelo-5150-a-david-garza-mar%C3%ADn

Figura 3. Primera Apple Macintosh

Nota: Adaptado de *Apple Macintosh* [Fotografía], por Home Computer Museum, s.f. https://www.homecomputermuseum.nl/collectie/apple/apple-macintosh/

Década de 1990: la World Wide Web (WWW).

La invención en 1989 de la *World Wide Web* por parte de Tim Berners-Lee, junto con la creación de navegadores web como Mosaic y Netscape, hicieron que Internet fuera fácil de usar. Esto marcó el comienzo de la rápida expansión de Internet. Mosaic fue el primer navegador para la red de Internet que mostraba una interfaz gráfica, Netscape se desarrolló a partir de Mosaic. Después surgieron otros navegadores como Internet Explorer de la empresa Microsoft (Ranchal, 2018).

Década de 2000: Revolución móvil e inalámbrica.

La proliferación de teléfonos móviles y redes inalámbricas permitió a las personas acceder a Internet desde prácticamente cualquier lugar. Esta era también vio la aparición de los teléfonos inteligentes, que combinan informática, comunicación y entretenimiento en un solo dispositivo.

La primera generación de la red móvil celular utilizaba una tecnología analógica. Posteriormente, surge la segunda generación (2G) gracias a los progresos de la tecnología digital. La 2G prestaba servicios de mejor calidad, mayor capacidad y más funciones que los sistemas analógicos, específicamente integraba las tecnologías de: sistema mundial para comunicaciones móviles, con entrada múltiple por división de tiempo, código y sistema celular digital personal (ITU, 2010).

Después, por la necesidad de mayor velocidad, compatibilidad mundial y servicios multimedios llevó a la creación de sistemas de tercera generación (3G). Aquí existe una revolución móvil de la telefonía. La telefonía móvil y dispositivos inalámbricos con tecnología 3G, envían y reciben datos con rapidez y permiten llamadas de voz, servicios de multimedia modernos como las videollamadas y la banda ancha móvil (ibid.).

Década de 2010 - Computación en la nube y Big Data.

Los servicios tecnológicos de la nube como Google Cloud y Amazon Web Services (AWS) se hicieron prominentes, permitiendo a empresas e individuos almacenar y acceder a datos y aplicaciones de forma remota. El

proceso de estos servicios computacionales se realiza por medio de la red de Internet. Estos, son propiedad de los proveedores de servicios y están hospedados en los mismos. De esta manera, las empresas que utilizan dichos servicios se comprometen a realizar un pago a los proveedores del servicio. Por ejemplo, las instituciones educativas usan servicios apoyados en la nube para brindar la entrega de software a pedido: Microsoft Office 365 ofrece sus versiones en línea de Excel, Word y Power Point (Cisco Networking Academy, 2023b).

Las tecnologías Big Data surgieron para manejar grandes cantidades de datos generados en línea. A palabras de la Oficina de Información Científica y Tecnológica para el Congreso de la Unión (INCYTU, 2018), el Big Data, también llamado macrodatos o datos masivos, son cantidades enormes de información ya que su variedad, velocidad y volumen de producción demandan métodos y tecnologías expertos para su manejo. Y al igual que Oracle (2023), refieren que los datos tienen tres propiedades principales denominadas las 3 v's:

- Volumen. - se relaciona con el procesamiento de datos no estructurados a gran escala.
- Velocidad. - se refiere al tiempo para transmitir datos.
- Variedad. - se refiere a la diversidad de datos disponibles en el mundo digital.

Por añadidura, se pueden incluir otras propiedades a los datos como la variabilidad por los cambios en el tiempo, la veracidad por la confiabilidad de las fuentes y el valor, es decir qué tan útiles son. Estas propiedades pueden ser combinadas dentro del mismo conjunto, pero antes de analizar los datos existe la necesidad de depurarlos, estandarizarlos y catalogarlos de forma adecuada. A este proceso se le denomina gestión de datos. Y para extraer sus cualidades se utiliza el Big Data Analytics, un método avanzado de procesamiento que manejan el vasto volumen y su complejidad (INCYTU, 2018).

Década de 2020: Internet de las cosas (IoT) y 5G.

La Internet de las Cosas (IoT, por sus siglas en inglés Internet of Things) se ha vuelto cada vez más frecuente conectando objetos cotidianos a la red. Los hogares inteligentes pueden contar con sensores de movimiento, agua, luz, de timbre y de temperatura. También puede haber sensores en semáforos, camiones de transporte, estacionamientos, cámaras de seguridad, trenes y aviones. IoT está integrado por una gran cantidad de sensores y dispositivos inteligentes que se encuentran enlazados a la red de Internet. Tanto los sensores como los dispositivos se encargan de reunir y compartir datos para que las entidades como empresas, ciudades, gobiernos, escuelas, hospitales, y las personas las usen y evalúen. Los dispositivos digitales funcionan según los programas informáticos y los datos suministrados (Cisco Networking Academy, 2023a).

Por otra parte, el despliegue de redes 5G promete conexiones a Internet aún más rápidas y confiables, mejorando aún más las capacidades y el rendimiento de IoT. La red 5G constituye en la tecnología móvil su quinta generación. Así también, permite una reducción en la latencia, una mejora en la flexibilidad de los servicios inalámbricos, y una velocidad mayor. Además, brinda 20 Gbps como velocidad máxima teórica, y al ofrecer menor latencia perfecciona el rendimiento de las aplicaciones comerciales (Cisco Systems, Inc., 2023).

Futuro: Inteligencia artificial (IA) y Computación Cuántica.

Es probable que el futuro de las TIC esté fuertemente influenciado por la IA. Los avances en IA impulsados por hardware más potente y conjuntos de datos masivos están revolucionando industrias como la atención médica, las finanzas y el transporte.

Según la UNESCO (2023), la inteligencia artificial “es el diseño de máquinas o sistemas que imitan funciones cognitivas propias de las personas, tales como percibir, procesar, analizar, organizar, anticipar, interactuar, resolver problemas y, más recientemente, crear” (p.15).

La IA, está sostenida de información, que almacena, analiza, clasifica y ordena; en otras palabras, está basada en datos. El sistema reconoce patrones y probabilidades en esos datos, los codifica, procesa y organiza.

Y genera un modelo. El modelo está diseñado para tomar decisiones y ofrecer respuestas a consignas determinadas. La IA funciona a través de algoritmos (conjunto metódico de pasos, una serie de instrucciones lógicas que se emplean para realizar cálculos, resolver problemas y tomar decisiones) (UNESCO, 2023).

Por otro lado, la computación cuántica tiene el potencial de resolver problemas complejos a velocidades increíbles en comparación con las computadoras clásicas. Empresas como IBM, Google y nuevas empresas trabajan en esta frontera.

Microsoft (2023), menciona que el término "cuántica" en "computación cuántica" alude a la mecánica cuántica que el sistema utiliza para calcular los resultados. En física, un cuanto es la unidad discreta más pequeña posible de cualquier propiedad física. De forma habitual, se refiere a las propiedades de las partículas atómicas o subatómicas, como los electrones, los neutrinos y los fotones. Entonces, en la computación cuántica los equipos cuánticos aprovechan el comportamiento único de la física cuántica, como la superposición, el entrelazamiento y la interferencia cuántica, y lo aplican al cálculo. Esto incluye nuevos conceptos en los métodos de programación típicos.

La evolución de las TIC sigue avanzando por lo tanto es pertinente hacer una aclaración acerca de este recorrido histórico condensado porque lo anterior es una descripción general simplificada y que cada una de estas etapas abarca numerosos avances e innovaciones.

Evolución de las generaciones de la máquina computacional desde su nacimiento como tal:

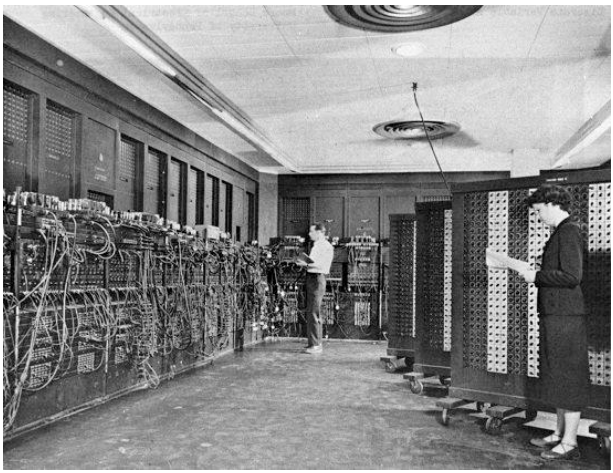
¡En efecto! Aquí se hace un repaso histórico de las cinco generaciones de computadoras las cuales se han titulado así porque el cambio tecnológico ha sido agrupado por las características técnicas en el progreso de la potencia de cálculo y la velocidad de la máquina computacional:

1. Primera generación (se desarrolló en las décadas de 1940 a 1950): tubos de vacío

- La primera generación de computadoras dependía de tubos de vacío para su procesamiento.

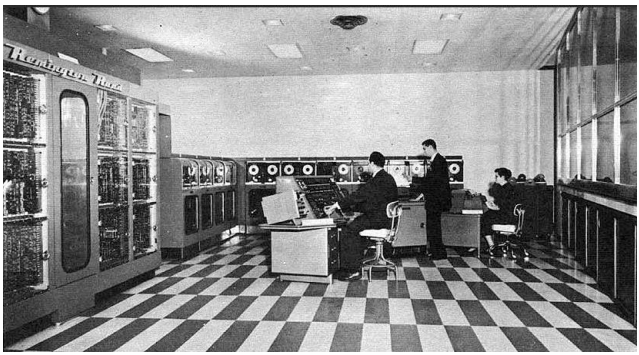
- Estas máquinas eran enormes, caras y consumían mucha energía.
- ENIAC (Computadora e Integrador Numérico Electrónico) (figura 4), UNIVAC (Computadora Automática Universal) (figura 5) y Mark 1 (figura 6), son ejemplos notables de esta época.
- La programación se realizó utilizando lenguaje de máquina, lo que requería mucha mano de obra.

Figura 4. ENIAC



Nota: Adaptado de *Historia de la Computadora*: ENIAC [Fotografía], por Tecnología + informática, s.f. https://www.tecnologia-informatica.com/historia-de-la-computadora-eniac/

Figura 5. UNIVAC



Nota: Adaptado de El UNIVAC, *el primer computador comercial de Estados Unidos* [Fotografía], por ETSINF-UPV, 2021. https://museo.inf.upv.es/univac2/

Figura 6. Mark I

Nota: Adaptado de IBM's ASCC *introduction* [Fotografía], por IBM, s.f. https://www.ibm.com/ibm/history/exhibits/markI/markI_intro.html

2. Segunda generación (fue durante las décadas de 1950 y 1960): transistores

- La segunda generación introdujo transistores, que eran más pequeños, más confiables y energéticamente más eficientes en comparación con los tubos de vacío.
- Se utilizó programación en lenguaje ensamblador, lo que facilitó un poco la programación.
- IBM 1401 e IBM 7094 (figura 7) son ejemplos de esta generación.
- Para el almacenamiento se utilizó memoria de núcleo magnético.

Figura 7. IBM 7094

Nota: Adaptado de *Data Processing System* [Fotografía], por IBM, s.f. https://www.ibm.com/ibm/history/exhibits/mainframe/mainframe_PP7094.html

3. Tercera generación (se registró en las décadas de 1960 y 1970): circuitos integrados (CI)

- Los circuitos integrados (CI) o microchips fueron desarrollados en la tercera generación, que redujeron de forma notable el costo y el tamaño de las computadoras.
- Nacieron lenguajes de programación como COBOL y Fortran, lo que hizo que la programación fuera más accesible.
- IBM System/360 (figura 8) y DEC PDP-8 son computadoras notables de esta época.
- Los sistemas operativos se volvieron más sofisticados.

Figura 8. IBM System/360

Nota: Adaptado de IMB *System 360/65* [Fotografía], por Museo de Informática García Santesmase, 2021. https://www.fdi.ucm.es/migs/catalogo/ibm_system_360_65/

4. Cuarta generación (ocurrió durante las décadas de 1970 y 1980): microprocesadores

- La cuarta generación introdujo los microprocesadores, que integraban todos los componentes de la CPU en un solo chip.
- Esto llevó al surgimiento de las computadoras personales (PC) como Apple II (figura 9) e IBM PC.
- Se desarrollaron interfaces gráficas de usuario (GUI) y el mouse, lo que hizo que las computadoras fueran más fáciles de usar.
- Los medios de almacenamiento evolucionaron hasta convertirse en disquetes y discos duros.

Figura 9. Apple II

Nota: Adaptado de *Apple II plus* [Fotografía], por Museo de Informática García Santesmase, 2021. https://www.fdi.ucm.es/migs/catalogo/apple_ii_plus/

5. Quinta Generación (se inició en la década de 1980- al presente): VLSI e IA

- La quinta generación trajo la integración a muy gran escala (VLSI), que permitió la creación de computadoras potentes y compactas.
- La atención se centró en la Inteligencia Artificial (IA), con el desarrollo de sistemas expertos y redes neuronales.
- Las computadoras personales continuaron evolucionando y las computadoras portátiles se hicieron populares (figura 10).
- La World Wide Web y la Internet revolucionaron el uso de los equipos de cómputo, conectando a las personas a nivel mundial.
- La informática móvil, los teléfonos inteligentes y las tabletas surgieron como tecnologías destacadas.

Figura 10. Computadora portátil

Nota: Adaptado de *Computadora Personal* (PC) [Fotografía], por EcuRed, s.f. https://www.ecured.cu/Computadora_personal

Es importante señalar que la industria informática continúa evolucionando rápidamente, con avances como la computación cuántica, la biocomputación y más en el horizonte, ampliando los límites de lo que las computadoras pueden hacer.

2.2 Elementos que integran las TIC

Las TIC, desde su surgimiento han facilitado el manejo de la información, permitiendo a las personas construir nuevas experiencias y prácticas de una forma inmediata y sin importar el espacio físico (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, [UNESCO], 2021a).

¿Pero, qué elementos integran las TIC?

Los elementos que integran las TIC son los recursos de software, hardware y las redes de comunicación de información. Cada uno de estos elementos realiza una función específica para que las personas puedan realizar tareas a través de las TIC.

2.2.1 Hardware

La Real Academia de la Lengua Española precisa la palabra hardware como el "conjunto de aparatos de una computadora" (Real Academia Española, s.f., definición 1). El autor Tanenbaum (2000) puntualiza el

hardware como el grupo de circuitos electrónicos integrados, dispositivos periféricos y memoria.

Si se habla de computadoras personales o portátiles, el hardware se compone de todo lo tangible, como, por ejemplo:

•Gabinetes y fuentes de alimentación.
•Tarjeta madre.
•Unidad de Procesamiento Central.
•Sistemas de refrigeración.
•Memoria.
•Tarjetas adaptadoras.
•Unidades de disco duro.
•Dispositivos de almacenamiento óptico.
•Puertos, cables, adaptadores.
•Dispositivos de entrada, como el teclado, mouse, escáner, pantalla táctil, lápiz digital, cámaras, micrófonos, entre otros.
•Dispositivos de salida, como monitores, proyectores, impresoras, bocinas, cascos de realidad virtual, entre otros.

En el caso de los dispositivos de hardware en una red, se pueden mencionar:
a) Dispositivos finales:
•Computadoras personales.
•Computadoras portátiles.
•Servidores.
•Tablet.
•Smartphone.
•Impresoras.
•Escáner.
•Cámaras.
•Teléfonos IP.

b) Dispositivos intermediarios:
•Switches
•Routers

•Puntos de acceso
•Módems

c) Medios:
•Medios para red del área local (LAN).
•Medios para red del área extensa (WAN).
•Medios inalámbricos.
•Medio de nube.

2.2.2 Software

La Real Academia de la Lengua Española especifica que la palabra software es un "conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora" (Real Academia Española, s.f., definición 1).

Así mismo, se conoce como software a las aplicaciones, paquetes, herramientas y programas informáticos. De forma general, cualquier tipo de software es utilizado para una tarea específica como diseñar o gestionar aplicaciones, crear nuevos elementos informáticos, innovar procesos o administrar información. Existe una gran variedad de ejemplos, desde trabajar con simples procesadores de texto, sistemas de contabilidad, páginas web, o soportes enormes de telecomunicaciones en las organizaciones (Arimetrics, 2022).

De acuerdo con TecnoMagazine (2023), el software puede ser clasificado por la función que realiza:

Software de Aplicación

El software de aplicación se refiere a la diversidad de programas que se usan en las organizaciones todos los días, como por ejemplo: la suite de Microsoft Office (Word, Excel y PowerPoint), los gestores de correo electrónico, los gestores de la mensajería instantánea o de videoconferencia, los navegadores para acceder a Internet, los juegos en la red, antivirus, anti-espías, aplicaciones contables y médicas, software de inventarios, software de administración, entre otras.

Para los dispositivos móviles el software aplicativo puede ser Facebook, WhatsApp, Twitter, Netflix, apps de pronóstico de tiempo, juegos, entre otras.

El Software de Sistema

El software de sistema administra los recursos de una computadora para que estos funcionen de manera adecuada. Mac OS, Microsoft Windows, Android, Gnu/Linux y iOS, son ejemplos de sistemas operativos. Asimismo, se integran en este tipo de software los controladores, los cuales permiten la conexión entre un recurso y las y los usuarios, permitiendo la correcta ejecución de los mismos (dispositivos de entrada/salida como las conexiones universales, mouse, teclados, los discos duros externos, escáner e impresoras).

Este tipo de software puede ser categorizado de la siguiente manera:

- Las utilidades del sistema operativo como desfragmentar y optimizar las unidades.
- Los diferentes tipos de sistemas operativos: de escritorio y móviles.
- La diversidad de herramientas que se usan para corregir algún error.
- Cualquier tipo de servidor de datos.
- La diversidad de controladores.

Software de Programación

Este tipo de software es un lenguaje que permite crear instrucciones bajo sintaxis para satisfacer las necesidades de las y los usuarios (C#, PHP, ASP, Ruby, entre otros).

La categorización del software de programación es:

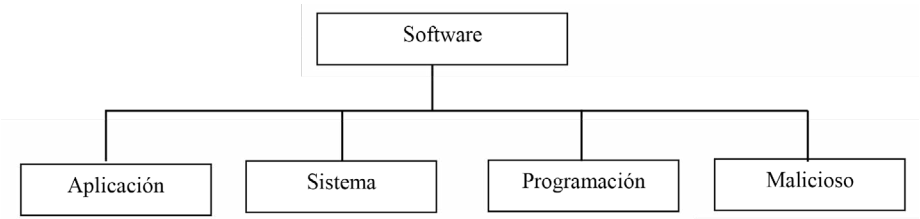
- Los compiladores.- son los encargados de ejecutar aplicaciones en el sistema operativo y de aprobar la compatibilidad.
- Los entornos de desarrollo integrado.- se relacionan con los recursos destinados a perfeccionar la productividad en el desarrollo.
- Programas informáticos para texto.- este tipo de programas se usan para facilitar la lectura y escritura de un código.
- Los depuradores de código.- se encargan de eliminar los códigos basura.

Software Malicioso

El software malicioso se relaciona con los cibercrímenes y ciberdelitos. Son aplicaciones maliciosas que dañan los equipos tecnológicos o que roban información personal o institucional. Algunos ejemplos son los virus, rootkits, backdoors, troyanos, dialers, gusanos, spyware y keyloggers.

La figura 11, resume los tipos de software clasificados por su función.

Figura 11. Tipos de software clasificados por su función

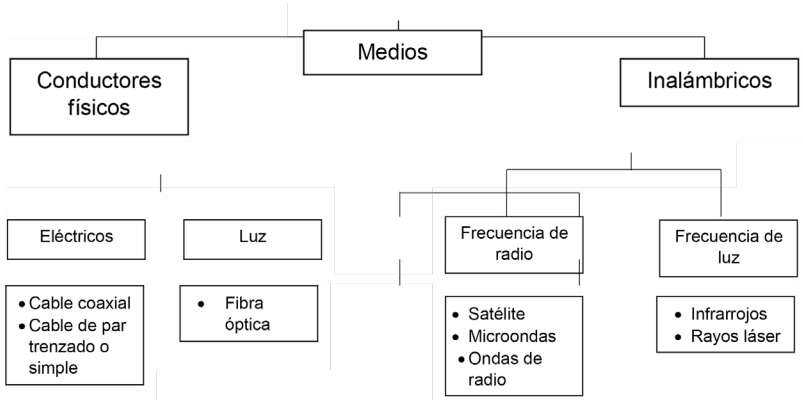


Nota: Datos tomados de TecnoMagazine (2023)

2.3 Redes de comunicación de datos

Una red de datos transmite y recibe información a través de recursos electrónicos. Toda la representación de los datos se hace con dígitos binarios. Un canal de transmisión es el medio por el cual transitan los datos entre dos puntos; la capacidad y velocidad varía según los medios (Cohen y Asín, 2014). La figura 12 muestra los medios más utilizados.

Figura 12. Medios de transmisión



Nota: Datos obtenidos de Cohen y Asín (2014).

A través de la conectividad se puede conectar hardware para establecer comunicación horizontal (entre sitios eficaces de la institución), vertical (alta dirección y mandos intermedios y operativos) y hacia el exterior (proveedores y clientes) (Cohen y Asín, 2014).

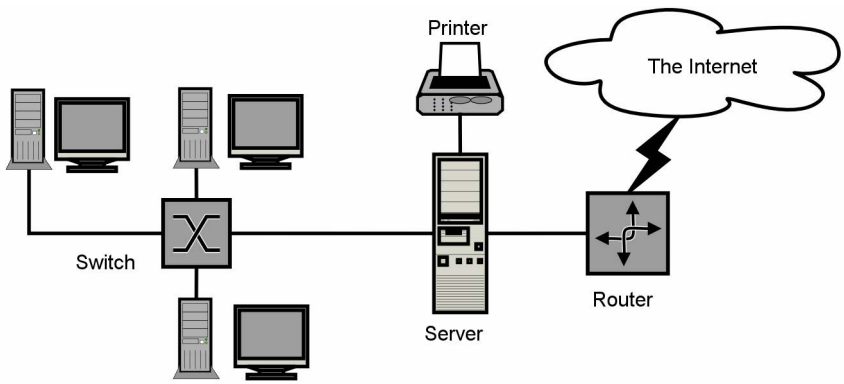
Las redes telemáticas facilitan los componentes específicos y conservan la comunicación de la información que se presenta como datos, video o voz. Para el intercambio de información, los recursos de comunicación pertenecen de forma directa al sistema de software y hardware (red).

Según la extensión geográfica, las redes de datos, las tecnologías y los dispositivos se pueden clasificar de la siguiente forma (Liberatori, 2018):

•Redes de Área Local (LAN, *Local Area Networks*).
•Redes de Área Amplia (WAN, *Wide Area Networks*).

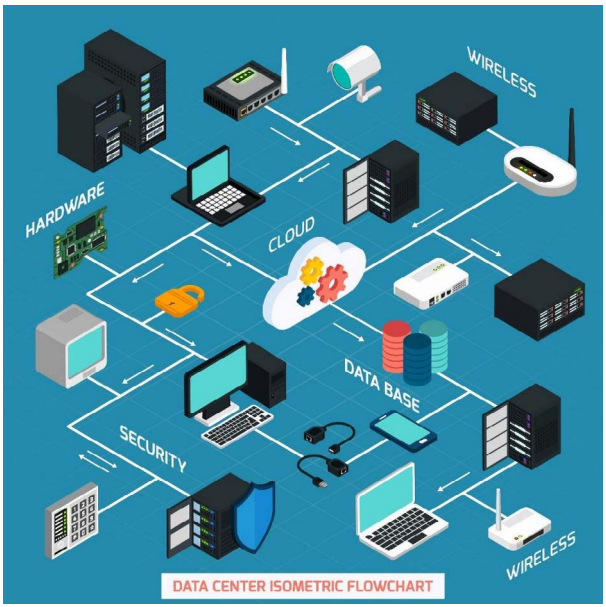
En la figura 13 se describe un ejemplo de una red LAN, y en la figura 14 se muestra una red WAN.

Figura 13. Red LAN



Nota: Imagen con licencia de Creative Commons (2023)

Figura 14. Red WAN



Nota: Imagen de Macrovector en Freepik (2023)

2.4 Seguridad

La seguridad cibernética implica proteger la información y la red de los ciberdelincuentes. Principalmente se enfoca en tres aspectos: los personales, los de la organización, y los de la nación. Lo relacionado a los aspectos personales, la seguridad cibernética requiere resguardar datos, recursos informáticos y las identidades de las y los usuarios. En el aspecto empresarial, la seguridad cibernética debe resguardar los datos generales y los de las y los clientes. Y en el caso de la nación, se protege la seguridad de la ciudadanía y toda la información del estado (Cisco Networking Academy, 2023c).

Las y los ciberdelincuentes son personas o grupos de personas quienes buscan aprovechar las vulnerabilidades para obtener un beneficio personal o económico. Se interesan en todos los datos y en todos los recursos, por ejemplo, tarjetas de crédito, proyectos y diseños de productos con

valor. Todo ataque puede generarse desde el interior o exterior de una organización. Se le conoce como vulnerabilidad de seguridad a las fallas de hardware o software. De forma particular, el vocablo ataque hace referencia a los programas diseñados para acceder y robar información de un sitio que no está protegido (ibid.).

Los ataques se llevan a cabo por medio de software malicioso. Cuando se presenta un robo de datos, se comprometen los sistemas o cuando se efectúa un daño a la información, por medio de un programa, se habla de un malware. Los malware más comunes son (Cisco Networking Academy, 2023c):

- Adware.- son programas que tienen como finalidad el envío automatizado de anuncios publicitarios.
- Spyware.- son programas que se diseñaron para capturar las pulsaciones de la escritura de los datos en los teclados de los equipos de cómputo. En ocasiones cambian los ajustes en la seguridad y también aplican un rastreo de las acciones realizadas por las personas.
- Bot.- de la palabra robot. Los bots son diseñados para realizar acciones automáticas en línea. Los equipos infectados con bots se encuentran a la espera de las instrucciones del ciberdelincuente para realizar el ataque.
- Ransomware.- es un software diseñado con el propósito de encriptar la información y los sistemas de cómputo para inhabilitarlos; de tal forma que, para poder tener un acceso a ellos, se requiere un pago. El ransomware generalmente se encuentra en un archivo descargado por el usuario.
- Rootkit.- es un software que realiza modificaciones a los archivos y a los sistemas operativos de las computadoras para dejarlos vulnerables, así que, los ciberdelincuentes pueden acceder a ellos en cualquier momento.
- Scareware.- este tipo de ataque muestra información en ventanas de diálogo falsas del sistema operativo de un equipo de cómputo. Su propósito es engañar a las y los usuarios para que autoricen o ejecuten programas con los cuales se infecta el sistema operativo.
- Virus.- los virus son códigos que se esconden en otros códigos legítimos,

para causar un daño simple o daños complejos. Su ejecución se da por medio de las y los usuarios finales y pueden ser distribuidos por diferentes medios extraíbles o correo electrónico.

- Troyano.- el troyano opera tras adjuntarse en diferentes tipos de archivos no ejecutables como los juegos, sonidos o imágenes. Su finalidad es acceder y atacar los privilegios de las y los usuarios que sin tener conocimiento de ellos los ejecutan.
- Hombre en el medio.- Así se le llama al tipo de ataque que usualmente es realizado para robar información relacionada a las finanzas. Las personas desconocen que el malware controla sus dispositivos de cómputo y que captura y se apodera de la información antes de que se trasmita al usuario final.
- Hombre en el móvil.- es similar al ataque anterior solo que este se usa para controlar dispositivos móviles. Una vez que el dispositivo móvil es infectado envía información a las o los delincuentes.
- Gusano.- este tipo de ataque tiene como prioridad hacer que las redes trabajen de forma lenta. Una vez que un host de la red es infectado hay una propagación inmediata hacia toda la red (ya que los gusanos suelen ejecutarse sin la participación de las personas).

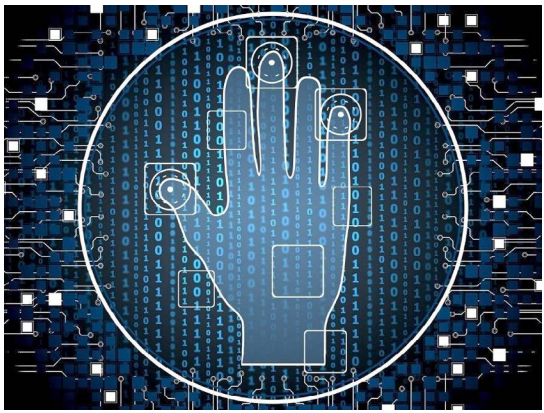
2.4.1 Protección física

La protección física implica proteger (Cisco Networking Academy, 2023b):

- Toda la infraestructura de una red, así como las cuestiones informáticas.
- El acceso a las instalaciones.
- La entrada a las secciones restringidas de la empresa.

Las entradas a los establecimientos de las organizaciones y los espacios exclusivos se protegen a través de dispositivos de bloqueo (eléctricos, tokens, biométricos) (figura 15). Por lo general, las puertas de las instituciones tienen dispositivos de bloqueo automático y cierre.

Figura 15. Seguridad física



Nota: Adaptado de Seguridad Física [Fotografía], por INCIBE, 2018. https://www.incibe.es/ciudadania/blog/seguridad-y-biometria

En la mayoría de las corporaciones, las personas portan credenciales que las identifican como empleado o empleada. En algunos de los casos, las credenciales contienen circuitos integrados para que permitan la entrada a las áreas de mayor seguridad.

Cuando personas externas a la organización desean tener acceso a la empresa deben solicitar permiso y registrarse en el área de control. Y del mismo modo, deberán portar una credencial que las identifique como visitantes.

2.4.2 Protección de datos

Los datos son los activos de mayor relevancia en una institución. Los datos se pueden proteger mediante los siguientes métodos (Cisco Networking Academy, 2023b):

Copia de respaldo de datos

Para resguardar información de las computadoras, es necesario realizar copias seguras de la información y guardarlas en medios extraíbles externos. Cuando exista alguna falla o alguna contingencia en las compu-

tadoras, la información puede ser recuperada a través de las copias de seguridad. Por lo general, los procesos de respaldo están establecidos en la normativa de la empresa.

Permisos de archivos y carpetas

Los permisos son las reglas que se configuran para limitar el acceso a los archivos para una persona o para un grupo de usuarios. Por ende, debe limitarse el acceso de los usuarios solo a los recursos que necesitan de un equipo o red.

Cifrado de archivos y carpetas

Este tipo de protección de datos utiliza software específico para convertir la información de los equipos de cómputo a un formato ilegible. Cuando se requiere utilizar la información, es necesario revertir este proceso, para ello se genera una llave única que se tiene que escribir para obtener la información legible.

Eliminación de datos

Eliminar los archivos de cualquier dispositivo de almacenamiento no es suficiente para proteger su privacidad. Se recomienda utilizar otros métodos como la utilización de un software de eliminación permanente de datos (borrado seguro), la varita desmagnetizadora, o un dispositivo desmagnetizador electromagnético.

2.4.3 Ingeniería social

En este tipo de ataque se engaña a las personas para que ellas mismas proporcionen información confidencial o realicen una actividad específica. Las o los atacantes obtienen la información necesaria para sus fines por medio de engaños, y es así como acceden a los datos y a los dispositivos de una red.

Tipos de ataques mediante ingeniería social (Cisco Networking Academy, 2023c):

- Excusa. - las o los atacantes inventan historias de la empresa o de la red para que las personas entreguen información confidencial o les den acceso a los dispositivos tecnológicos.
- Persecución.- en este caso las o los atacantes siguen a las personas dentro de la organización hasta tener acceso a las áreas restringidas
- Algo por algo.- aquí las o los atacantes piden información a las personas a cambio de "algo", por ejemplo, un regalo o dinero.

Ejercicio: Relación de columnas

Instrucciones: relaciona ambas columnas de manera correcta

1. ( ) ARPANET utilizó conmutación de paquetes para transmitir datos entre computadoras, sentando las bases para la creación de redes globales.	A. Evolución histórica de las TIC en la década de los 2000.
2. ( ) La invención en 1989 de la World Wide Web por parte de Tim Berners-Lee, junto con la creación de navegadores web como Mosaic y Netscape.	B. Evolución histórica de las TIC en la década de 2020.
3. ( ) La proliferación de teléfonos móviles y redes inalámbricas permitió a las personas acceder a Internet desde prácticamente cualquier lugar.	C. Evolución histórica de las TIC en la década de 1960 y 1970.
4. ( ) El big data y los servicios tecnológicos en la nube se hicieron presentes para almacenar y manejar grandes cantidades de datos.	D. El software.
5. ( ) El IoT y las redes 5G están presentes en esta década.	E. Las redes telemáticas.
6. ( ) Es un conjunto de circuitos integrados, dispositivos periféricos y memoria.	F. El hardware.
7. ( ) Son las aplicaciones, paquetes, herramientas y programas de software que se utilizan en un dispositivo tecnológico.	G. La comunicación de datos.
8. ( ) Transmiten y reciben información a través de recursos electrónicos. Toda la representación de los datos se hace con dígitos binarios.	H. Evolución histórica de las TIC en la década de 1990.

9. ( ) Facilitan los componentes específicos y conservan la comunicación de la información que se presenta como datos, video o voz.	I. Inteligencia Artificial y Computación Cuántica.
10. ( ) El futuro de las TIC, estará fuertemente centrado en estos dos grandes avances.	J. Evolución histórica de las TIC en la década de 2010.
11. ( ) Consiste en realizar tareas para proteger datos y sistemas de red contra daños o la no autorización.	K. Ingeniería social.
12. ( ) En este tipo de ataque se engaña a las personas para que ellas mismas proporcionen información confidencial o realicen una actividad específica.	L. Seguridad cibernética.

Capítulo 3

Auditoría en Informática

En un mundo competitivo y globalizado, las TIC han eliminado las barreras geográficas y de tiempo, es necesario contar con el recurso humano y tecnológico que permita obtener ventajas competitivas.

Generalmente todas las áreas de la organización cuentan con recursos tecnológicos (hardware, software y de comunicación), tales recursos son administrados y coordinados por un área de TIC, quien además se asegura de su buen funcionamiento.

Para el logro de un funcionamiento óptimo se requiere establecer procesos y procedimientos, los cuales permiten a los sistemas de información manipular grandes cantidades de datos, generando información oportuna y confiable que ayude a tomar decisiones (Alvarado, et al., 2017).

3.1 El concepto de auditoría en informática

3.1.1 Concepto de Auditoría

La palabra auditoría procede del latín *auditorius* cuyo origen etimológico es auditor "el que escucha", en sus inicios los auditores solo escuchaban, hoy en día los auditores además de escuchar leen, revisan, evalúan y dan sus recomendaciones para la mejora continua.

La Real Academia de la Lengua Española puntualiza que la palabra auditoría es la "revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse" (Real Academia Española, s.f., definición 1).

Piattini y del Peso (2001), definen a la auditoría como un diagnóstico emitido por un profesional con base al análisis de las actividades realizadas por una entidad contra las prescritas en sus procedimientos.

De acuerdo con Enlace SC (2019), la auditoría se lleva a cabo mediante un procedimiento metódico, autónomo y documentado. La finalidad de la auditoría es conseguir evidencias. Dichas evidencias tienen que ser evaluadas de forma objetiva para poder determinar así hasta qué punto se cumple con la normatividad (políticas, requisitos y procesos empleados como referencia en la auditoría). Las evidencias pueden ser cualquier

tipo de información verificable e importante para la normatividad de la auditoría como documentos, hechos o acontecimientos.

3.1.2 Concepto de Informática

La palabra informática es definida por la Real Academia de la Lengua Española de la siguiente forma "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores" (Real Academia Española, s.f., definición 1).

Sánchez (s.f.) menciona que la informática es la sistematización de la información perteneciente a cualquier área de conocimiento, su finalidad es facilitar su usabilidad.

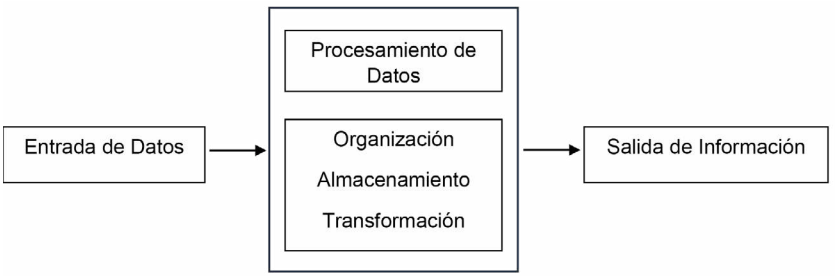
La informática, ha sido considerada como una rama de la cibernética, que responde a la necesidad de las personas por optimizar procesos de producción. Por ende, el incremento en la cantidad de datos exactos y oportunos requeridos en las organizaciones orilló al desarrollo de sistemas informáticos que facilitaron las comunicaciones y la forma en tomar de decisiones entre personas, empresas y países.

Según la UNESCO (2021b) la informática y la tecnología son un núcleo digital que consta de tres elementos: hardware, software e Internet. El hardware son los dispositivos físicos. El software son las aplicaciones y el sistema operativo. Internet es una red de sistemas informáticos interconectados a nivel global.

Se entiende que la informática es una ciencia que a través de los dispositivos tecnológicos efectúa el tratamiento de la información, es decir desde la entrada de datos, su procesamiento y presentación de resultados.

El esquema del tratamiento de la información se representa en la figura 16.

Figura 16. Tratamiento de la Información.



Nota: Elaboración propia.

3.1.3 Concepto de Auditoría en Informática

Para Echenique (2001) y Ramírez (2016) la auditoría en informática comprende dos etapas, la primera es el proceso de evaluar cada sistema de información (procesos, entrada y salida, seguridad, archivos, permisos, procedimientos específicos, entre otros). La segunda etapa consiste en evaluar el equipamiento informático (computadoras, dispositivos de red, servidores, entre otros).

Piattini y del Peso (2001), refieren que la auditoría en informática es una cadena de técnicas y procedimientos para admitir el control y la evaluación parcial o total de un sistema de información. De acuerdo con este concepto, la auditoría en informática deberá revisar si las acciones realizadas se apegan a los planes y a la política organizacional, y si son protegidos los recursos y los activos de la organización.

Hernández (2010), conceptualiza la auditoría en informática como un mecanismo evaluador y de diagnóstico del contexto informático con respecto a estándares internacionales y en modelos que hacen referencia al énfasis para mejorar la gestión. En dicha gestión se involucra a todas las personas que trabajan en el contexto informático: desde el personal técnico, personal administrativo, personal contable, entre otros. Cada uno de ellos, participa en determinadas fases de la auditoría: planificación, hallazgos, análisis, desarrollo de informes, entre otros.

Minaya et al. (2023), plantean que la auditoría en informática es un procedimiento específico para que las organizaciones identifiquen fallas

posibles en el análisis de riesgos y así poder disminuir o neutralizar su impacto. La ejecución de la auditoría permite evaluar y asegurar la efectividad, eficiencia y seguridad en los sistemas y métodos tecnológicos.

Entonces se puede conceptualizar que la auditoría en informática consiste en revisar y evaluar los controles y procesos determinados para el buen funcionamiento de las TIC, para conocer el grado de eficiencia en su utilización, así como las medidas de seguridad física de los recursos tecnológicos, con la finalidad de identificar áreas de oportunidad/mejora para apoyar a una eficaz toma de decisiones en cada organización.

3.2 La historia de la auditoría

3.2.1 La historia de la auditoría

De acuerdo con Hernández (1993), la auditoría en informática es referenciada en los años cuarenta, cuando en Estados Unidos inicia la era de la computación con el uso de sistemas estratégicos para militares; en ese tiempo solo consistía en controles de acceso y uso de las computadoras. Sin embargo, la auditoría se practica desde los intercambios comerciales de la antigüedad, los movimientos se registraban en papel y esto permitía realizar una verificación. En México, los escuchadores de la realeza de España, supervisaban el pago del quinto real de los reyes españoles, su trabajo era confirmar los pagos de dichos impuestos.

A continuación, se describe la línea de tiempo (ibid.):

- 5000 a. de C.: los sumerios practicaban la retroalimentación administrativa.
- 4000 a. de C.: en Egipto practicaban la planeación y organización.
- 1994 a. de C.: en China se aplican técnicas de control.
- 1436: en Venecia, se utilizaron controles de inventario, contables, de costos y de personal.
- 1554: en la Nueva España es creada la Junta Superior de Hacienda.
- 1799: se implementa el sistema de calidad y de control de costos.
- 1800: existe la propuesta para usar la auditoría para evaluar.

•1924: los organismos aplican el gobierno estadístico de la calidad.
•1933: gracias a la auditoría las organizaciones utilizan mayor cantidad de controles, los cuales incrementan la productividad.
•1935: se establecen las bases para la auditoría administrativa.
•1945: es argumento de debate en simposio la importancia de la auditoría interna de operaciones técnicas.
•1955: se describe la auditoría interna como una técnica que permite el control del desempeño total.
•1965: se crea de manera formal una unidad de auditoría, especificando su estructura, funciones y perfil del personal.
•1965: se crean criterios que deben de cumplir las y los aspirantes a integrar un equipo de auditoría.
•1967: se establece un marco metodológico, el alcance y la importancia que debe tener para toda organización la auditoría administrativa.
•1968: la auditoría es establecida como un requerimiento en el proceso de evaluar las responsabilidades sociales y funciones de las organizaciones.
•1971: se realizan auditorías a los recursos humanos y se establece una relación con la auditoría administrativa.
•1975: estructura metodológica que permite definir los elementos de una auditoría de operaciones.
•1978: la certificación de Auditor en Sistemas de Información (CISA) es establecida por parte de la Asociación de Auditoría y Control de Sistemas de Información (ISACA).
•1984: se implementa la evaluación del ambiente laboral y de todos los sistemas de la información.
•1995: se realiza la primera auditoría administrativa mediante una computadora.

3.2.2 Objetivos de la auditoría

En una auditoría, se requiere integrar una guía específica que trace la pauta para el logro de los objetivos. Existe una diversidad de criterios que ayudan a concretar los objetivos de la auditoría como los mencionados por Franklin (2007):

a. De organización

Establecen que el proceso de la auditoría coincida con los procedimientos y las definiciones planteadas. Un ejemplo de ellos son las actividades que se delegan y la colaboración y comunicación entre las personas.

b. De calidad

La auditoría permite aumentar el nivel de calidad de lo servicios o productos que se ofrecen en las empresas. Esto indica que si los resultados de la auditoría son positivos la empresa puede competir con otras empresas.

c. De vinculación

Determinan que la auditoría instituya una unión entre la empresa y un marco globalizado.

d. De control

Orientan el trabajo de la auditoría y permiten aplicar una evaluación en el desarrollo organizacional de acuerdo con modelos establecidos.

e. De productividad

Dirigen las actividades de la auditoría con el objetivo de administrar el tiempo y aprovechar cada recurso de la empresa.

f. De servicio

Incorporan la forma en que la auditoría puede comprobar que la empresa se encuentra integrada en un proceso que la enlaza en todos los aspectos con las perspectivas y preferencias de sus clientes.

g. De cambio

Convierten a la auditoría en una herramienta que permite que la empresa sea más receptiva y adaptable a las circunstancias.

h. De aprendizaje

Aprueban la auditoría como componente de aprendizaje organizacional constituido por experiencias, áreas de mejora, áreas de oportunidad.

i. De toma de decisiones

La obtención de resultados y procesos en el transcurso de la auditoría instituyen una herramienta consolidada y que sirve como un soporte dentro de la empresa.

j. De interacción

Permiten relacionar estratégicamente a la empresa con los clientes, proveedores y competidores potenciales.

3.2.3 Ventajas y limitaciones de la auditoría

De acuerdo con Aguirre (2005), se pueden mencionar las siguientes ventajas de la auditoría:

•Ofrece una evaluación del logro de planes, programas, normas, lineamientos y políticas.
•Reconoce las áreas de mejora.
•Proporciona información de retroalimentación para realizar tareas correctivas y preventivas.
•Informa sobre los resultados de la evaluación obtenidos en la ejecución de sus objetivos y funciones.
•Crea un ambiente interno de confianza con respecto a servicios de TIC.
•Brinda confianza en los clientes.
•Disminuye costos.

En contra parte, se pueden mencionar la existencia de las siguientes limitaciones:

•El tiempo: tiempo insuficiente para realizar la auditoría.
•Presupuesto: la falta de recursos económicos no permite una auditoría externa, por tal motivo se tendrá que realizar una auditoría interna.
•Personal: falta de conocimiento, experiencia y/o disponibilidad.
•Lugar: el tamaño del área supera el presupuesto asignado (Aguirre, 2005).

3.3 Tipos de auditoría

La auditoría se puede clasificar en los siguientes tipos (Piattini, y del Peso, 2001; Franklin, 2007):

3.3.1 Administrativa

Es el proceso de investigación sistemático que se efectúa a los movimientos y acciones de una organización, incluyendo las interacciones entre las personas trabajadoras y la forma en que se cumplen cada una

de las funciones sustantivas y operativas de la empresa.

El propósito de la auditoría en la administración es evaluar y valorar toda la función administrativa que se realiza como proceso: planeación, organización, dirección, integración y el control. Por otra parte, la auditoría en la contabilidad revisa la situación económica en el contexto informático y administrativo. La auditoría administrativa y la contable se integran con la auditoría en la informática por el hecho de que los medios informáticos son el sustento de las actividades que se realizan tanto en la administración como de la contabilidad.

3.3.2 Financiera

Es un análisis basado en los principios de contabilidad que se realiza sobre las finanzas de una institución. La intención es que la o el profesional contable (que deberá ser independiente) elabore un dictamen de las condiciones en que se encuentran las operaciones, las finanzas, los movimientos contables, y en general de los estados financieros de toda la empresa.

3.3.3 Informática

Revisión práctica que se realiza de manera objetiva, crítica y sistémica para evaluar el uso de los medios que se utilizan en la informática dentro de una organización. Los fines de esta auditoría es presentar un juicio o un informe profesional para conocer la relación existente entre el ambiente de la auditoría y las actividades de la organización.

Dentro de los recursos informáticos podemos encontrar: información, aplicaciones, infraestructura, conceptuales y recurso humano.

La aplicación de la auditoría en el área de la informática consiste en revisar que todos los elementos informáticos involucrados, como, por ejemplo, los recursos de software y hardware, los recursos financieros y humanos, y los datos se encuentren debidamente administrados por las personas de la empresa.

La realización de auditorías permite evaluar las fortalezas y debilidades, y mejorar aspectos como el desempeño, fiabilidad, eficacia, rentabilidad, seguridad y privacidad.

La tabla 1 especifica una comparación de las tres auditorías.

Tabla 1.Comparación de los tipos de auditoría

Las propiedades de una auditoría	La auditoría administrativa	La auditoría contable	La auditoría informática
Propósito/objetivo	Evaluación y mejoramiento en la administración	Dictaminación de las finanzas	Evaluación de los medios informáticos
Naturaleza	Técnica de control administrativo	Técnica de control administrativo	Técnica de control administrativo
Metodología	Apoyo en los métodos científicos	Técnicas y procedimientos establecidas	Técnicas y procedimientos establecidas
Alcance	La eficiencia y la productividad en el proceso administrativo	El sistema de contabilidad	Todas las tareas informáticas
Proyección	Hacia el futuro	Hacia el pasado	Hacia el futuro
Fundamento	La ciencia administrativa y la normatividad de la institución	Principios de las normas de auditoría y de contabilidad	Normatividad legal e institucional y los estándares mundiales.
Aplicación	A la organización y las funciones elementales	A las finanzas	A todas las áreas de la organización
Informe	Extenso	Exacto	Extenso y exacto

Nota: Datos tomados de Piattini y del Peso (2001).

3.4 Áreas de aplicación

De acuerdo con Álvarez (1981) y Aguirre (2005), las áreas de aplicación de la auditoría pueden ser:

Sistemas. Evalúa los procedimientos, metodologías, ciclo de vida y el uso de controles en el desarrollo de sistemas de información.

Administración de la función de informática. Revisa la aplicación del proceso administrativo en la informática desde la planeación y control

de actividades, la gestión de los presupuestos, costos y adquisiciones, la capacitación del personal y la administración de estándares de operación.

Auditoría a redes. Evalúa el cumplimiento de estándares en la implementación de redes de video, voz y datos, sus topologías, protocolos y su funcionamiento, así como la administración, configuración y políticas de acceso.

Centros de cómputo. Revisa todas las actividades de administración, políticas de mantenimiento, políticas de respaldo y resguardo, políticas de acceso a fin de evaluar el uso de los recursos informáticos.

Seguridad. Evaluación de las protecciones a la información, aplicaciones e infraestructura, así como a las actividades preventivas y correctivas.

Proyectos. La administración por proyectos consiste en elaborar un plan de trabajo en donde se especifiquen las actividades a realizar, recursos involucrados y tiempo asignado. Esto permite dar un seguimiento periódicamente y evaluar los avances evitando retrasos.

3.5 Tipos de auditores

Para Franklin (2007), existen dos tipos de auditores, los internos y externos. Cada auditor tiene sus ventajas y desventajas, en ocasiones se pueden utilizar ambos para la realización de las auditorías.

3.5.1 Internos

Las o los auditores internos pertenecen a la corporación, su labor consiste en el apoyo de las funciones de la auditoría. La selección de la o el auditor depende de sus características para dicha intervención. En seguida, se muestra una lista de ventajas y desventajas (ibid.):

Ventajas

- Posee amplio conocimiento de los procedimientos internos de la empresa.
- Acepta a todos los y las participantes.

- Tiene conciencia de toda la actividad de la empresa.
- No tiene problema al adaptarse al cambio.
- Percibe un apoyo de todos los y las trabajadoras.
- Encuentra una respuesta rápida a las instrucciones que asigna.
- Se identifica con las y los trabajadores.
- Posee habilidades para una cultura prevaleciente.
- No muestra nerviosismo al solicitar informes de resultados y avances del trabajo.
- Posee amplio conocimiento sobre los recursos de la empresa que pueden usarse en la auditoría.
- Posee amplio conocimiento de la imagen de la empresa.
- Posee habilidades para relacionar las expectativas de los y las clientes con los servicios y/o productos de una organización.

Desventajas

- Manipula los informes de resultados y avances a conveniencia propia.
- Se conforma con informes parciales de los resultados y avances.
- Demuestra preferencias por algunas áreas o personas.
- Asigna menor relevancia a los objetivos de la auditoría y pone mayor atención a los medios.
- Es subjetivo o subjetiva en la realización del análisis de datos.
- No muestra calidad, claridad ni precisión en el trabajo que presenta.
- Muestra confianza excesiva en todos los procesos, en los tiempos en que se responde y en la usabilidad de todos los recursos.
- Demuestra que no tiene un enfoque general de las necesidades de las y los clientes de la empresa.
- Prefiere no causar molestias o afectar a sus compañeras y compañeros de trabajo.

3.5.2 Externos

El auditor externo es un profesional independiente con vasta experiencia y conocimientos en la auditoría. Es una persona con estudios profesionales en el área de la auditoría y control interno posee una percepción global

y objetiva de las funciones; además administra el tiempo para cumplir con las fechas propuestas. El auditor externo cuenta con las siguientes ventajas y desventajas (Franklin, 2007):

Ventajas

- Posee una amplia experiencia y coherencia en la aplicación de las auditorías.
- La empresa le reconoce su labor.
- Tiene un grupo de trabajo para realizar las actividades de la auditoría.
- No tiene dificultades para acceder a los altos niveles donde se toman las decisiones.
- Mantiene una perspectiva imparcial de la empresa.
- Mantiene un criterio independiente al desarrollar las observaciones encontradas.
- Es responsable en el uso de los medios y recursos con el objeto de minimizar los costos de la empresa.
- Es veloz en el trabajo que realiza.
- Tiene confianza al identificar y marcar anomalías sin sentirse con preocupación.
- Proporciona resultados sólidos.

Desventajas

- Se le dificulta adaptarse al cambio.
- Las personas de la empresa la o lo identifican como persona externa.
- Existe un temor frente a lo que se desconoce.
- Mantiene una dureza y severidad al realizar las observaciones.
- Entrega los resultados siguiendo los tiempos en la guía de trabajo, lo que a su vez dificulta que se realice un análisis profundo de las observaciones.
- Muestra una actitud impersonal frente al funcionamiento de la empresa.
- Carece de conocimiento respecto a la cultura de la empresa.
- Carece de conocimiento ante las perspectivas de las y los clientes, y de los proveedores.

3.5.3 Equipo combinado

Al decidir efectuar una auditoría, es recomendable analizar las siguientes variables (Franklin, 2007):

•El periodo de tiempo de realización de la auditoría.
•La armonización que debe predominar frente a la auditoría y la labor ordinaria de la empresa.
•Los medios y recursos que se deberán usar.
•El personal necesario para ejecutar el programa de auditoría.
•La continuidad del trabajo con recursos humanos específicos.

Dependiendo de la respuesta de las finanzas y del análisis de la corporación para efectuar los pagos correspondientes de la o el auditor independiente, se estará en posibilidades de formar un equipo de auditores internos y externos. Las ventajas y desventajas de un equipo combinado son (Franklin, 2007):

Ventajas

- Acelerar la realización de la auditoría.
- Complementar la información desde dos perspectivas.
- Administrar racionalmente todos los recursos.
- Examinar más eficientemente la implementación de la auditoría.
- Aminorar la negativa al cambio.
- Integrar personal diverso de cada una de las áreas de la empresa.
- Reunir de las y los auditores externos toda la experiencia posible.
- Accede de forma más sencilla a las altas jerarquías de decisión.
- Dividir equitativamente con el personal las tareas y actividades referentes a la auditoría.
- Tener la confianza de que, si hace falta personal en determinada área, ésta puede ser cubierta por otro personal.

Desventajas

- Puede resultar una presunción excesiva en el progreso de cada tarea.
- Se pueden generar esperanzas que no se pueden cumplir.
- Es posible que se complique unificar los criterios y los tiempos del trabajo.
- Puede existir una situación conflictiva entre las y los auditores externos y el personal interno.
- Aumento del estrés y tensión entre el recurso humano de la organización.
- Incremento de las finanzas en la organización.
- Generación de inquietud y desconfianza en las instancias que se relacionan con la empresa.
- Inferir recomendaciones que no se ajustan a la realidad de la empresa.

3.6 Característica de los auditores

Las características de los auditores, según Cotaña (2020) son:

3.6.1 Perfil del auditor

La implementación de la auditoría obedece al trabajo profesional que realiza el auditor. Su experiencia, agudeza en las tareas, aplicación de aptitudes, habilidades y conocimientos son componentes necesarios para contribuir en el éxito y la calidad de la auditoría.

3.6.2 Formación académica

Una o un auditor puede contar con una formación académica en las áreas de: contabilidad, administración general, administración pública, ingeniería industrial o de sistemas, derecho, ciencias políticas, informática, diseño gráfico, piscología, pedagogía, relaciones industriales e internacionales o el área de comunicación. Los estudios pueden ser a nivel de posgrado, licenciatura o técnico.

3.6.3 Formación complementaria

Participación en actividades de formación, capacitación, actualización y desarrollo, tales como cursos, congresos, seminarios, talleres, foros, conferencias o encuentros.

3.6.4 Formación empírica

Conocimiento y experiencia obtenida mediante la implementación y ejecución de auditorías o propuestas de mejoras en diferentes organizaciones, manejo de equipo tecnológico.

3.6.5 Habilidades y destrezas

Las particularidades de una o un auditor pueden ser las siguientes:

•Mostrar una actitud efectiva.
•Contar con competencias para negociar, analizar y observar.
•Tener destrezas para la comunicación en forma escrita y oral.
•Poseer conducta ética.
•Aplicar técnicas de concentración.
•Practicar valores.
•Mostrar un patrón de comportamiento estable.
•Tener creatividad e imaginación.
•Poseer iniciativa y una escucha activa.
•Tener habilidades para trabajar en equipo y una empatía por las opiniones de los o las otras participantes.
•Aplicar la objetividad y la discreción.
•Contar con sentido de pertenencia.

También las o los auditores en informática deben contar con conocimientos básicos de (Piattini, y del Peso, 2001):

•Técnicas de telecomunicación.
•Análisis de riesgos y vulnerabilidades de la red.

•Seguridad de datos, física, del medio ambiente y de las personas.
•Software ofimático.
•Administración de bases de datos.
•Los sistemas operativos.
•Progreso de proyectos informáticos.
•Desarrollo de planes de contingencia y amenazas para proteger la información.
•Actividad económica digital.
•Cifrado de datos.
•Control y dirección del departamento de sistemas.
•Administración de cambios.
•Redes de Área Local y Área Amplia.

3.7 Principios del auditor

3.7.1 Principios que deben regir a una persona que audita

Franklin (2007), refiere que un buen auditor o auditora debe afrontar su responsabilidad alcanzando y cumpliendo con las siguientes políticas:

•Integridad. - preservar sus valores sobre las presiones.
•Honestidad. - realizar las tareas con ética y evitar actos inmorales o tratos corruptos.
•Imparcialidad. - mostrar una actitud objetiva sobre los hechos y no involucrarse de forma personal.
•Responsabilidad. - llevar un seguimiento de cada una de las tareas y cumplirlas en el tiempo establecido.
•Iniciativa. - mantener y ejecutar respuestas rápidas y mantener una actitud positiva.
•Creatividad. - conservar la innovación en el progreso de las actividades.
•Equilibrio. - nivelar el contexto con los hechos.
•Integridad. - salvaguardar valores y practicar la honestidad.
•Confidencialidad. - mantener en privado las acciones que se ejecutan y los datos de la institución.

•Compromiso. - perseguir las obligaciones, deberes y acuerdos relacionados con las funciones y acciones de la empresa.
•Criterio. - implementar aptitudes de discernimiento.
•Institucionalidad. - seguir y practicar la normatividad y la reglamentación de la empresa.

Piattini y del Peso (2001), mencionan que todas las acciones del auditor deben sustentarse en la ética y siguiendo los siguientes principios:

•Cautela.- la persona que audita recomendará de acuerdo con su experiencia y dejara de lado suposiciones, sobre todo en temas de innovación donde se involucran las tecnologías de información y comunicación. Dicha persona no tiene que pensar que, gracias a sus conocimientos y experiencias, puede propiciar al personal auditado a crear nuevos proyectos garantizando su éxito futuro.
•Calidad.- la persona que audita revisará que existan los recursos imprescindibles para la ejecución de la auditoría, de lo contrario deberá solicitar lo que se necesita para poder empezar y llevar a cabo un buen trabajo. Es importante considerar que, si no se encuentran disponibles todos los medios, la persona que audita tiene la obligación de cancelar el trabajo de la auditoría. También es relevante discurrir en el tema de solicitar que otras personas cualificadas participen en los temas con mayor nivel de especialidad.
•Capacidad.- la o el auditor debe poseer habilidades y destrezas suficientes y especializadas para crear un ambiente de trabajo favorable. Todas las personas involucradas deberán sentir armonía para trabajar de forma colaborativa al revisar y evaluar la información.
•Beneficio del auditado.- todas las acciones que realiza el o la auditora en la evolución de la auditoría deberán de estar orientadas al cliente. En ningún caso dichas actividades deberán beneficiar a la o el auditor.
•Economía.- en la aplicación de la auditoría la o el auditor deberá cuidar las finanzas de la empresa, el propósito es no causar costos adicionales. Deberá procurar evitar dilaciones innecesarias en la realización de la auditoría. Gastos no justificados.
•Comportamiento profesional.- la persona que audita deberá mantener

un comportamiento ético en su relación con las y los participantes en el proceso de la auditoría. Es recomendable buscar un equilibrio al emitir las observaciones y las opiniones para no causar confusiones o malentendidos; en este sentido debe de brindar confianza y seguridad. De la misma forma, es necesario que las y los clientes perciban una imagen profesional y de respeto por parte de la o el auditor.

- Concentración en el trabajo.- es pertinente que la o el auditor establezca prioridades y desarrolle un trabajo de calidad y con sentido de responsabilidad. No podrá realizar actividades extras o innecesarias para la auditoría.
- Información suficiente.- la o el auditor tiene la responsabilidad de proporcionar a las o lo clientes todos los datos derivados de los resultados y del proceso de la auditoría. Dichos datos deberán ser concreta, clara e inteligible, evitando proporcionar datos irrelevantes.
- Confianza.- la o el auditor deberá ser transparente y garantizar el secreto profesional en el desarrollo de su actividad, de tal forma, que el personal auditado se sienta en confianza y se pueda establecer un diálogo cordial. Del mismo modo, se deberá crear un ambiente de aclaración de dudas durante todo el proceso de la auditoría, para evitar de este modo cualquier situación problemática o de desconfianza.
- Criterio propio.- toda actuación de la o el auditor tendrá que ser con un criterio propio y no deberá estar influenciado por criterios de otras personas.
- Discreción.- la información que se maneja en la auditoría es confidencial, por ende, la o el auditor deberá mantener en total discreción todos los datos revisados en la misma.
- Formación continua.- debe ser un compromiso de una o un auditor, se requieren conocimientos nuevos y actuales para hacer frente a los requerimientos que se exige la competencia.
- Fortalecimiento y respeto de la profesión.- es importante que las o los auditores respeten los costos de sus servicios. Aunque exista mucha competencia no deberán rebajar los precios ni portarse desleales con otros profesionales; sino que por el contrario deberán actuar con ética para que se valore su trabajo y puedan mantener su prestigio.
- Independencia.- puesto que los resultados deberán ser objetivos, la o el

auditor solicitará una posición de independencia para que los resultados se generen con profesionalidad. Se deberá actuar con total libertad al emitir los juicios, la información analizada y la realización de todas las acciones inmersas en la auditoría.

- Principio de integridad moral.- la o el auditor deberá comportarse moralmente y con sumisión a la normatividad. Así también, deberá ser imparcial en todo acto y hecho y sobre todo evadir la participación en sucesos de corrupción. Por ninguna razón tratará de utilizar la información para otro efecto que no sea el de la auditoría.
- Principio de legalidad.- la o el auditor deberá considerar y garantizar todos los derechos de protección de la información establecidos en cada organización como los secretos profesionales, propiedad intelectual, cuestiones personales, entre otros. Por tal razón, no intentará sobrepasar los límites de seguridad físicos y digitales.
- Libre competencia.- la o el auditor deberá evitar frenar la posible participación de cualquier competencia; de ser así se estaría incurriendo en un acto ilegítimo.
- Principio de no discriminación.- la o el auditor evadirá excluir cualquier situación que de forma personal no le beneficie a él o ella o al proceso de la auditoría. Dicho proceso se someterá con igualdad de condiciones.
- Principio de no injerencia.- la o el auditor evitará en todo momento intervenir en las acciones de otras personas y respetar el trabajo que cada profesional realiza. Del mismo modo, evadirá mencionar o hacer comentarios despectivos para descalificar sus actuaciones; al menos, que, por alguna razón de la actividad de la auditoría, sea necesario expresar ciertas competencias que pudieran perjudicar a las conclusiones de los dictámenes.
- Principio de precisión.- la evaluación será estrictamente lo que la o el auditor señale o lo que sus colaborares o colaboradores hayan indicado y comprobado específicamente. Se deberá evitar especificar como propias las observaciones de terceras personas u observaciones parciales o inconclusas.
- Publicidad adecuada.- las o los auditores deberán detener cualquier tipo de publicidad que de acuerdo con su contexto falsifique las formas de

trabajo o la realidad de sus acciones o el cumplimento de objetivos que no se puedan alcanzar.

- Principio de responsabilidad.- todo auditor o auditora tiene la obligación de remunerar cualquier daño ocasionado por actos negligentes comprobados; por los que tendrá que hacer una compensación. Dicha compensación debe estar estipulada con anticipación.
- Veracidad.- este principio explica que toda información que se dé a conocer como resultado de la auditoría será con rigurosa veracidad; es decir que ya con anterioridad fue verificada con los objetivos. Esto significa que no incluirá información basada en suposiciones o creencias.
- Secreto profesional.- la o el auditor está obligado a no difundir a terceras personas información que haya indagado durante el progreso de sus actividades y que pudiera perjudicar al cliente.
- Servicio público.- la o el auditor deberá informar cualquier situación riesgosa o de vulnerabilidad que pueda dañar a la organización y que ha sido descubierta durante la ejecución de la auditoría, como, por ejemplo, la propagación de un programa maligno (malware). Siempre deberá contar con una actitud de servicio.

Ejercicio: Relación de columnas

Instrucciones: Relaciona ambas columnas de manera correcta

1. ( ) Consiste en revisar y evaluar controles y procesos determinados para el buen funcionamiento de las TIC	A. Objetivo de productividad.
2. ( ) Es el propósito de la auditoría en informática, destinado a orientar el trabajo de la auditoría y permiten aplicar una evaluación en el desarrollo organizacional de acuerdo con modelos establecidos.	B. Auditor interno.
3. ( ) Es el objetivo de la auditoría en informática, que dirige las actividades de la auditoría con el objetivo de administrar el tiempo y aprovechar cada recurso de la empresa	C. Identificar áreas de mejora, disminuir costos.

4. ( ) Es el objetivo de la auditoría en informática en donde los resultados y procesos de la implementación de la auditoría instituyen una herramienta consolidada y que sirve como un soporte dentro de la empresa.	D. Administrativa, financiera, informática.
5. ( ) Es alguna de las ventajas de la auditoría en informática.	E. Auditor externo.
6. ( ) Son los diferentes tipos de auditoría.	F. Principio de confidencialidad.
7. ( ) Es un profesional que es parte de la organización, su función puede ser considerada viable y pertinente en la auditoría.	G. Objetivo de control.
8. ( ) Es un profesional independiente con conocimientos y experiencia en auditoría, es una persona capacitada para cumplir con dicha función de forma específica, posee una percepción global y objetiva de las funciones.	H. Principio de responsabilidad
9. ( ) Es el principio de la auditoría que permite observar una conducta profesional, en otras palabras, cumplir con las actividades de manera adecuada y eficiente.	I. Auditoría en informática
10. ( ) Es el principio de la auditoría que mantiene en privado las acciones que se ejecutan y los datos de la institución.	J. Objetivo de toma de decisiones

Fuente: Aguirre (2005), Álvarez (1981), Cotaña (2020), Franklin (2007), Hernández (1993), Piattini y del Peso (2001) y Ramírez, (2016).

Capítulo 4

Control Interno y Seguridad

4.1 Concepto

4.1.1 Control interno

Echenique (2001), conceptualiza al control interno como aquellas acciones o actividades ejecutadas de forma manual o de manera automatizada para enmendar cualquier irregularidad o para evitar errores que como consecuencia puedan afectar los sistemas para alcanzar sus propósitos. Todos los lineamientos y normativas se trazan para dar facilidades en la observancia de los propósitos de la organización y también para evitar situaciones no deseadas.

Pinilla (1997) menciona que el control interno informático tiene su definición a través un sistema inmerso al procedimiento de administración, el organizativo, el de planeación, y en los procesos de control y dirección de todas las acciones que se efectúan para proteger los medios de informática y para optimar los temas económicos y desarrollar la eficiencia y eficacia de las técnicas de operación automatizadas.

En la informática, el control interno tiene la encomienda de inspeccionar que las acciones de los sistemas relacionados con la información se realicen bajo los estándares, procesos y normativas especificadas legalmente, por la empresa y el departamento o el área de informática.

4.1.2 Importancia

Principales objetivos según Echenique (2001) y Piattini y del Peso (2001):

- Apoyar y favorecer las tareas de la auditoría en informática externa e interna.
- Inspección de las acciones para conocer si fueron realizadas bajo el cumplimiento de pautas y procesos plasmados, evaluando sus bondades y asegurar el desempeño de la normativa legal.
- Concretar, establecer y elaborar controles y mecanismos para evidenciar la consecución de los objetivos determinados en el servicio de la informática.

•Aconsejar sobre el conocimiento de las normas.
•Adoptar y transferir la cultura del riesgo y vulnerabilidades informáticas.
•Poner en práctica controles en las comunicaciones a través de las redes.
•Aplicar control de eficiencia y calidad del mantenimiento y progreso del *software* y de la prestación informática.
•Aplicar el control microinformático.
•Ejecutar controles sobre el *software* de base.
•Administrar relaciones y licenciamiento contractual con terceras personas.
•Implementar vigilancia en el control de cambios y versiones del *software.*
•Implementar controles diarios de la producción.

4.1.3 Tipos de control interno

Trascendentalmente, la finalidad de los controles en informática se ha catalogado con las categorías descritas a continuación (Echenique, 2001 y Piattini, y del Peso, 2001):

•Controles automáticos. se integran en el *software*; ya que pueden ser de comunicación, de operación, de dirección de base de datos y de software de aplicación.
•Controles preventivos. este tipo de controles impide los accesos no autorizados a los sistemas.
•Controles manuales. estos controles se ejecutan sin utilizar recursos computacionales y son hechos por personas del departamento de informática.
•Controles detectivos. son utilizados cuando fallan los controles preventivos y tratan de indagar sobre lo sucedido (omisiones y errores).
•Controles correctivos. este tipo de controles corrige las incidencias permitiendo que los sistemas vuelvan a funcionar. Un ejemplo puede ser el restablecimiento de un documento afectado por medio de una copia respaldada.

4.2 Los componentes del control interno

Los elementos que integran el control interno pueden ser (Piattini, y del Peso, 2001):

•Entorno general en el control.
•La información y la comunicación.
•La supervisión.
•La evaluación de riesgos.
•Las tareas de control.

4.3 Las actividades de control

Para las actividades de control se proponen las siguientes funciones (Piattini, y del Peso, 2001):

•Gobernar toda información sensible y comprometida.
•Ejecutar control de soportes magnéticos de acuerdo con la categorización de los datos.
•Conexiones externas con áreas concernientes con la seguridad de la información.
•Administración de los recursos técnicos y humanos.
•Fijar propietarios y perfiles de acuerdo con la clasificación de 1a información.
•Responsabilidad en el desarrollo del plan de contingencias y su actualización.
•Responsabilidad en los manuales de procedimientos y plan de seguridad.
•Promoción del plan de seguridad informática al comité de seguridad.
•Fijación de las operaciones de control.
•Definición de normas de seguridad informática.
•Implementar control del entorno de desarrollo.
•Implementar el control de la calidad de software.
•Implementar control para los apoyos físicos.
•Implementar control de costes.
•Establecer el control de calidad del servicio de informática.

•Definir el control de usuarios y microinformática.
•Implementar control de licencias y relaciones contractuales con terceros.
•Implementar controles de medidas de la seguridad física o colectiva en la informática.
•Ejecutar control de cambios y versiones.
•Definición de manejo y control de claves de cifrado.
•Definición de requerimientos de seguridad en nuevos planes.
•Implementar supervisión para el cumplimiento de las normas y controles.
•Responsabilidad de datos personales.
•Implementar la dirección delegada en control dual (dos personas intervienen en una actividad como régimen de control) en la seguridad lógica.
•Implementar control de información sensible o comprometida.

4.4 Riesgos

4.4.1 Concepto de riesgo

Todo riesgo implica la contingencia de ocurrencia de un suceso, consecuencia o impacto adverso. Del mismo modo, el riesgo puede ser definido como la magnitud y la probabilidad de los impactos desfavorables, que se relaciona con la repetición de la presencia del evento (Echenique, 2001).

Cotaña (2020), plantea que el riesgo en una auditoría figura la posibilidad de que la persona que audita diga una opinión equivocada en el reporte final debido a que la operatividad de los sistemas de información entregada a ella esté influenciada por la alteración material o por la normativa.

4.4.2 Tipo de riesgos

Los tipos de riesgos según Cotaña (2020) pueden ser:

•Riesgo de detección. es la amenaza de que las instrucciones aplicadas por la persona que audita para minimizar el riesgo de la auditoría a un aceptable nivel no manifiesten la existencia de una falta material, considerada individual o de forma agregada con otra sin correcciones.

•El riesgo de control. se relaciona con la probabilidad de que los controles internos imperantes no descubran errores en los sistemas y que se deben corregir con revisiones internas más seguros.
•El riesgo inherente. es la probabilidad de la existencia de errores importantes en la información que se audita, siguiendo la garantía del control interno que se relaciona con ello. Se trata de un tipo de errores que no pueden ser precedidos.

4.4.3 Medición

La medición de análisis de riesgos se encuentra desplegada para reconocer la inexistencia de controles y la ejecución de un procedimiento de contramedidas. En este sentido, hay dos tipos de metodologías: las cuantitativas y las cualitativas.

4.4.4 Manejo de los riesgos

Los autores Álvarez (1981) y Gaitán (2007) recomiendan las siguientes cuestiones para manejar cada riesgo:

•Es presentada cuando el riesgo aparece por tener problemas de tipo operacional, por lo que se recomienda llevar a cabo una reducción al nivel más bajo. Esta recomendación es la más fácil y económica. Se logra mejorando los procedimientos, el monitoreo constante y la implementación de los controles.
•La no exposición. Se lleva a cabo cuando hay un compromiso de no realizar la acción que origina dicho riesgo. La técnica de no exposición tiene desventajas, ya que la organización se puede abstener de explotar oportunidades.
•Respaldo y buscar compartir el riesgo con otras áreas. Consiste en alejar o transferir un riesgo de un lugar a otro, o para reducirlo, compartiéndolo con otras áreas.
•La aceptación total del riesgo. La aceptación se puede presentar de forma involuntaria o voluntaria. La involuntaria se presenta cuando el riesgo es obstaculizado de forma inconsciente; la aceptación vo-

luntaria se identifica al reconocer la existencia del riesgo y el acuerdo de reconocer las perdidas implicadas, dicha decisión es presentada por falta de elecciones.

4.4.5 Riesgos por área de TIC

Los posibles riesgos por área de TIC, de acuerdo con Álvarez (1981) y Gaitán (2007) son:

•Los incendios.
•El aire de ventilación o renovación.
•Los terremotos.
•Las inundaciones.
•Iluminación.
•Los factores humanos.
•Los factores del medio ambiente.
•Las fuentes de alimentación.
•La humedad.
•Los robos.
•Los actos vandálicos contra la red.
•Terrorismo.
•Los factores físicos.
•Fraude.
•Acciones deliberadas.
•El cableado.

Ejercicio: Reactivos de verdadero o falso

Instrucciones: Leer de forma comprensiva cada una de las oraciones e indica con una “V”, si es verdadero, o una “F”, si es falso.

1. _____ El control interno informático tiene la encomienda de inspeccionar que las acciones de los sistemas de información se realicen bajo los procesos, estándares y normativas especificadas legalmente, a través de una empresa y el departamento o el área de informática.

2. _____En el control interno informático, merece resaltar la vigilancia sobre las versiones del *software* y el control del cambio.
3. _____El riesgo de control se relaciona con la probabilidad de que los controles internos imperantes no descubran errores en los sistemas y que se deben corregir con revisiones internas más seguros.
4. _____ Los controles preventivos y detectivos, son 2 tipos de control interno informático.
5. _____ El riesgo es la probabilidad de que ocurra un impacto, evento o consecuencia adversa.
6. _____ Los controles correctivos se utilizan como un software de seguridad que no permite el acceso o los accesos no acreditados a dicho sistema.
7. _____ El riesgo en auditoría representa la posibilidad de que la persona que audita no exprese una opinión equivocada en su informe.

Fuente: Alvarez (1981), Cotaña (2020), Echenique (2001), Gaitán (2007), Piattini y del Peso (2001), (Pinilla, 1997).

Capítulo 5

Metodologías y buenas prácticas para realizar una auditoría

5.1 Metodología

5.1.1 Concepto

De acuerdo con Echenique (2001), para efectuar una auditoría informática adecuada es pertinente seguir una consecución de pasos ordenados. Piattini y del Peso (2001), mencionan que para cualquier proceso científico se requiere un método o en su caso una metodología conveniente para cumplir los objetivos planteados.

El diccionario de la lengua española, indica que la palabra método significa el "modo de decir o hacer con orden" (Real Academia Española, s.f., definición 1) y la palabra metodología significa "conjunto de métodos que se siguen en una investigación científica o una exposición doctrinal" (Real Academia Española, s.f., definición 2).

Una metodología en el contexto de la auditoría informática, indica las fases a seguir para realizar las actividades de la auditoría de manera fluida y sistemática en los espacios correspondientes de las tecnologías de información.

Varios autores han planteado diferentes metodologías de acuerdo con sus experiencias y habilidades, como es el caso de Davis, et al. (2011), que proponen las siguientes etapas:

a) Planeación.
b) Trabajo de campo y documentación.
c) Descubrimiento de problemas y validación de problemas.
d) Desarrollo de soluciones.
e) Redacción y emisión de informes.
f) Seguimiento de problemas.

Echenique (2001), sugiere las siguientes fases:

a) La planeación.
b) La revisión preliminar.
c) La revisión detallada.

d) La evaluación de la información y el examen.
e) Las pruebas de control de las y los usuarios.
f) Las pruebas individuales.
g) Y las pruebas de consentimiento.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2016), señala tres fases en el marco de la auditoría:

a) La planeación.
b) El monitoreo de una auditoría.
c) La ejecución de una auditoría.

Y Hernández (1993), plantea las siguientes etapas:

a) Preliminar.
b) Justificación.
c) Adecuación.
d) Formalización.
e) Desarrollo

En general una metodología para una auditoría integra fases, que definen a las personas involucradas, las revisiones y el avance de acuerdo con el proceso y los medios que se necesitan para su realización.

5.2 Etapas de una auditoría

Para este marco de referencia, se toma como sustento las fases que menciona Davis, et al. (2011):

a) Planeación.
b) Trabajo de campo y documentación.
c) Descubrimiento de problemas y validación de problemas.
d) Desarrollo de soluciones.
e) Redacción y emisión de informes.
f) Seguimiento de problemas.

a) Etapa de planeación

La etapa de planeación consiste en determinar el alcance y el o los objetivos de una auditoría.

La realización de la planeación debe considerar lo siguiente:

- El auditor deberá notificar la programación de la auditoría al personal que participará.
- El personal involucrado en la realización de la auditoría deberá realizar una encuesta preliminar para obtener información básica y comprender el área a revisar. Para ello se deberá entrevistar a los clientes.
- Tener en cuenta las peticiones de la clientela respecto a las áreas que les preocupan y creen debería tener mayor atención y de esta manera mantener la comunicación abierta y honesta.
- Realizar un listado verificable estándar para los procedimientos y sistemas de una institución.
- Realizar un mecanismo de investigación en la red de Internet, libros y materiales de capacitación para obtener información adicional del área a auditar.

Una vez referenciados estos recursos, el auditor debe realizar una evaluación de los riesgos en el área que se está revisando para identificar los pasos que deben llevarse a cabo durante la auditoría.

El resultado debe ser una determinación del alcance de la auditoría, incluida la determinación y comunicación específicas de lo que está fuera del alcance y compilar una lista de pasos a realizar para lograr ese alcance.

Posteriormente se deberá programar la auditoría considerando la disponibilidad de los clientes.

Finalmente se deberá realizar una reunión inicial de la auditoría con los clientes para que se pueda comunicar lo que está dentro y fuera del alcance del proyecto de auditoría y también recibir sus opiniones finales. En esta reunión también se establecerán los contactos principales para cada paso de la auditoría y determinar un cronograma y metodología (como reuniones o correos electrónicos) para mantener a los clientes informados del estado de la auditoría. Una vez que se completa la reunión

inicial, los pasos de la auditoría deben distribuirse entre los miembros del equipo de auditoría y puede comenzar la siguiente etapa de la auditoría.

b) Etapa del trabajo de campo y documentación

En el trabajo de campo, las personas autorizadas realizarán las entrevistas para obtener la información correspondiente.

La información ayudará a cada integrante del grupo a revisar los riesgos destacados y la determinación de los riesgos que no mitigados de forma oportuna. En este punto, el auditor validará la información proporcionada.

La documentación también es una parte fundamental del trabajo de campo. Todo el trabajo que realizan los auditores debe documentarse. El objetivo es documentar el trabajo con suficiente detalle para que una persona razonablemente informada pueda entender lo que se hizo y obtener la igualdad en las conclusiones.

Básicamente existen 3 fundamentos para la documentación:

1) La documentación se necesita para cumplir con los estándares de la profesión.
2) En el futuro, existe la posibilidad de que los resultados de la auditoría sean cuestionados o impugnados, y el auditor que realizó la auditoría ya no puede ser empleado por la empresa o el departamento en ese momento. Será esencial que exista documentación para explicar el proceso realizado durante una auditoría y fundamentar las pertinentes conclusiones.
3) Si una auditoría se vuelve a realizar, conservar la documentación detallada permitirá que otro grupo de auditoría aprenda de la experiencia del grupo que auditó con anterioridad, lo que permitirá una mejora continua.

c) Etapa de descubrimiento de problemas y validación de problemas

En esta etapa, mientras los auditores llevan a cabo el trabajo de campo, deberán de ir realizando una lista de problemas descubiertos.

Los problemas descubiertos deberán ser discutidos con los clientes, de tal forma que los clientes trabajen de manera conjunta en la validación del problema y tomen posesión de la temática a tratar.

El auditor se asegurará de que los problemas tratados sean significativos y potenciales. También se asegurará que se desarrollen las soluciones adecuadas para abordarlos.

d) Etapa de desarrollo de soluciones

En esta etapa, una vez que se hayan identificado los problemas potenciales en el área que está auditando y se hayan validado los hechos y los riesgos, se puede trabajar con los clientes para desarrollar un plan de acción para abordar cada problema.

Se utilizan tres enfoques comunes para desarrollar y asignar elementos de acción para abordar cada problema, los cuales se describen a continuación:

1. El enfoque de respuesta de gestión.- el personal que audita desarrolla un listado sobre problemáticas, los cuales son enviados al cliente para que él le dé una respuesta o realice plan de acción. Los clientes brindan ideas para resoluciones basadas en su conocimiento operativo de la vida real.
2. El enfoque de recomendación.- aquí el personal que audita plantea los problemas y proporciona las recomendaciones para su resolución con base a su conocimiento de control.
3. El enfoque de solución.- en este enfoque, las personas que auditan trabajan con los clientes para elaborar de forma conjunta una solución que simboliza un método de acción para abordar los problemas trazados en el transcurso de la auditoría. Se compone de los dos enfoques anteriores.

e) Etapa de redacción y emisión de informes

El informe de auditoría es el medio que hace referencia a los resultados de la auditoría. En esta etapa se redacta y se emite el informe.

El informe de la auditoría cumple con dos funciones principales:

- Para el auditor y el cliente, es un registro de la auditoría, los resultados, y los planes de acción que se derivaron.
- Para las y los directivos organizaciones y el comité de la auditoría, es un seguimiento de calificaciones del área que fue auditada.

Los componentes elementales en un informe de auditoría pueden ser:

- El listado de las problemáticas, y las acciones para su resolución.– describe los problemas significativos descubiertos durante la auditoría y la acción que se seguirá para solucionarlos.
- La manifestación del alcance de la auditoría.- se describe lo que se incluyó y no se incluyó en la auditoría.
- El resumen ejecutivo.- deberá ser un documento independiente que contenga información relevante sobre el resultado de la auditoría, asumiendo que el lector no lee ninguna otra parte del informe.

También se pueden considerar los siguientes elementos adiciones en el informe de la auditoría:

- Controles clave.– describir los controles que se están llevando a cabo de manera correcta.
- Elementos cerrados.– mencionar y reconocer los problemas que fueron resueltos durante el proceso de la auditoría.
- Problemas menores.– mencionar aquellos problemas menores que fueron detectados durante la auditoría para que los clientes tomen medidas para mejorar.

El último paso es en esta etapa es distribuir el informe de la auditoría. Una vez que el informe ha sido redactado y revisado por los clientes, es el momento de distribuirlo.

f) Etapa de seguimiento de problemas

En esta etapa, la auditoría no está realmente completa hasta que se solucionen los problemas planteados en dicha auditoría.

El departamento de la auditoría deberá desarrollar un procedimiento mediante el cual sus miembros puedan rastrear y seguir los problemas hasta que se resuelvan. Esto probablemente implicará el trabajo de una base de datos que integra todos los puntos de la auditoría y sus fechas de vencimiento, junto con un mecanismo para marcar como cerrados, vencidos, etc.

El auditor que realizó la auditoría estará en contacto con los responsables de la empresa hasta que se resuelvan los problemas. Si resulta que un problema no se está abordando según lo acordado, los auditores son responsables de iniciar los procedimientos de escalamiento con el comité de la auditoría.

5.2.1 Ejemplo de una auditoría en informática

De acuerdo con Echenique (2001), se ejemplifica una plan de una auditoría en informática:

I. *Los antecedentes.*
Se deberán especificar los antecedentes particulares en el trabajo de la auditoría.
II. *Los objetivos de la auditoría en informática.*
Se anotarán los objetivos determinados de dicha auditoría.
III. *Los alcances en el proyecto*
Escribir los alcances del trabajo, el cuál comprenderá:

1. La evaluación de la trayectoria informática en relación con:
   a. Condiciones de trabajo.
   b. Funciones.
   c. Objetivos.
   d. Estructura.
   e. Capacitación.
   f. Planes de trabajo.
   g. Controles.
   h. Organización.
   i. Situación presupuestal y financiera.

j. Estándares.
k. Normas y políticas.
l. Los recursos humanos.

2. Las evaluaciones de todos los sistemas:
a. La seguridad en la lógica de los respaldos, sistemas y en la confidencialidad.
b. La evaluación en el avance de los sistemas en progreso y coherencia con la perspectiva general, modularidad y el control de proyectos.
c. Derechos de autor y secretos empresariales de todos los sistemas de la institución.
d. La evaluación de las bases de datos.
e. La evaluación de los diversos sistemas que se encuentran en operación (documentación, opiniones de las personas, la organización de los archivos, el flujo, los estándares de programación, uso de los sistemas, los controles y procedimientos).

3. La evaluación del equipamiento:
a. Redes.
b. Estandarización.
c. Los equipos adicionales.
d. Almacenamiento.
e. Controles.
f. La comunicación.
g. Adquisición.
h. Los proyectos de adquisición nuevos.

4. La evaluación de la seguridad:
a. Seguridad contra virus.
b. Los seguros.
c. Plan de procedimientos en caso de desastre y de contingencia.
d. Seguridad en la restauración de los sistemas y equipos
e. Seguridad personal.
f. Seguridad en lo físico.
g. Seguridad confidencialidad y lógica.
h. Seguridad en el uso de los equipos.

IV. *Metodología*

1. En la evaluación del área de informática se realizarán las acciones siguientes:

a. Petición de programas de trabajo, manuales administrativos, organización, función, planes, políticas y estándares utilizados.

b. Implementación del cuestionario a las personas, y ejecución de entrevistas.

c. Discusiones con personas clave del área de informática y con líderes de proyectos.

d. Desarrollo de un cuestionario evaluativo de la dirección.

e. Evaluación y análisis de la información.

f. Realización de un informe.

g. Petición de presupuestos y costos de informática.

2. En la evaluación de sistemas de operación y desarrollo se realizarán las acciones siguientes:

a. Petición del diseño y análisis de los sistemas en desarrollo y en operación.

b. La evaluación de la participación de auditoría interna.

c. La petición de los contratos de renta o de compra de software.

d. Petición del plan de trabajo.

e. Petición de estudios de costo-beneficio y de viabilidad.

f. Recopilación y análisis de los procedimientos administrativos de cada sistema.

g. Examen de la seguridad lógica y confidencial.

h. Análisis de base de datos.

i. Evaluación de los proyectos en desarrollo, prioridades y personal asignado.

j. Evaluación de las licencias, la obtención de la confidencialidad de la información y los derechos de autor.

k. Entrevistas con las y los usuarios de los sistemas.

l. La petición de licenciamiento y derechos de autor.

m. Petición de documentos de los sistemas en operación (manuales de usuario, técnicos, de operación y de diseños).

n. Evaluación directa de la información obtenida contra las necesidades y especificaciones de los y las usuarias.

o. La evaluación en el control.

p. Análisis objetivo de la estructuración y flujo de los programas.

q. La evaluación y el análisis de la información recolectada.

r. La planeación de contingencia y recuperación en los casos de catástrofes.

s. Preparación del informe.

3. En la evaluación de los equipos se realizarán las consecutivas acciones:

a. Petición de los contratos de renta o compra de los equipos.

b. Petición del convenio de respaldo y contratos.

c. Petición de los contratos de mantenimiento de los equipos.

d. Petición de los contratos de seguros.

e. Petición de las bitácoras de los equipos.

f. Realización de un cuestionario para el uso del equipamiento, unidades de entrada/salida, archivos, seguridad y dispositivos periféricos.

g. Visita a las instalaciones y a las áreas donde se almacenan los archivos magnéticos.

h. Evaluación de los sistemas de la seguridad en la entrada.

i. Petición de los estudios de costo-beneficio, de viabilidad y tipologías de los actuales equipos, proyectos de ampliación y adquisición del equipo.

j. Evaluación técnica ambiental del equipamiento y del sistema eléctrico del edificio utilizado y en general de las instalaciones.

k. Análisis de la información que se recopilo, justificación, realización de gráficas y porcentajes de uso del equipamiento.

l. Producción del informe.

4. Preparación final del informe, discusión y presentación de este, y exposición de las recomendaciones y conclusiones.

V. *El tiempo y el costo*

Aquí se agregará:

a) Tiempo estimado de cada una de las fases en que se realizará el proyecto.

b) El costo y las especificaciones del modo de pago.

5.2.2 Ejemplo de formato para un programa de auditoría en informática

La tabla 2 muestra un ejemplo de formato para desarrollar un programa para la auditoría en informática.

Tabla 2. Formato Programa para una Auditoría en Informática.

Programa de Auditoría en Informática						
Corporación_____				**Hoja No. _____De _____**		
Fecha de formulación_____						
Fase	**Descripción**	**Actividad**	**No. personal participante**	**Periodo estimado**		**Días**
				inicio	**término**	

Nota: Elaborado a partir de http://auditoríasistemasucb.pbworks.com/f/ANEXOS.pdf

5.2.3 Ejemplo de formato para avance de cumplimiento del programa de la auditoría en informática

La tabla 3 muestra un ejemplo de formato para el seguimiento del programa de auditoría en la informática.

Tabla 3. Formato Avance de Cumplimiento del Programa de Auditoría en la Informática.

Avance del Cumplimiento del Programa de Auditoría en Informática									
Organismo_____						**Hoja No. _____ De _____**			
Periodo que reporta_____									
Fase	**Situación de la auditoría**			**Periodo de la auditoría**		**Días reales utilizados**	**Avance**		**Observaciones**
	No iniciada	**En proceso**	**Terminada**	**Inicio**	**Termino**		**%**	**Días**	

Nota: Elaborado a partir de http://auditoríasistemasucb.pbworks.com/f/ANEXOS.pdf

5.3 Buenas prácticas en la auditoría en informática

Albarrán et al. (2020), en el estudio realizado de las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares, muestran tres ejemplos de buenas prácticas que ayudan a las instituciones a lograr un manejo adecuado de la información. Las mejores prácticas se resumen a continuación:

5.3.1 COBIT

COBIT (por sus siglas en inglés, Objetivos de Control para la Información y Tecnología Relacionada), es el marco aprobado en el contexto internacional para una buena práctica de control de la información, tecnologías de información (TI) y el riesgo. Esta práctica es utilizada para efectuar auditorías de informática y el gobierno de TI (estructura de procesos y relaciones propuestos a controlar y dirigir la organización, el propósito de lograr sus propósitos y sumar valor en tanto se nivela el retorno sobre TI, los riesgos y sus procedimientos) y optimizar los controles de TI.

COBIT permite a las instituciones evaluar el desempeño de su estructura, estimando en primera instancia el rendimiento individual, para después determinar lo que está funcionado de forma general. Puede ser aplicado en organizaciones del sector público o privado, y en instituciones sin fines de lucro.

Este marco se integra de cinco principios (ILIXUM, 2021): a) acreditar un enfoque holístico (significa que la organización está integrada para ayudar a que la administración y el gobierno de TI funcione de forma efectiva); b) cubrir la empresa de punta a punta (significa que la gestión y el gobierno de TI soportan las necesidades de tecnología de toda la organización); c) satisfacción de necesidades (representa la optimización de los recursos y que los objetivos de la organización se encuentran alineados con los de los socios y los de TI); d) priorizar toma de decisiones (representa el monitoreo del desempeño y el cumplimiento de los objetivos mediante la evaluación de las necesidades); y e) marco integrado (significa que la organización puede emitir reportes de sus recursos y activos de tecnología).

Los componentes principales de COBIT son (AUDITOOL, 2024):

a) El sistema de objetivos. representa un enlace entre los aspectos técnicos de TI y las necesidades de la organización. Aquí se identifican los objetivos de gestión y gobierno que son la llave para la gestión de riesgos de TI y la implementación de estrategias de TI.
b) El modelo de evaluación de desempeño. integra un método para medir y evaluar el desempeño de las capacidades en una organización de TI.

c) Los componentes de gestión y gobierno. detalla los objetivos de gobierno y gestión que son fundamentales para las tareas de TI. Cada objetivo es respaldado por un grupo de prácticas, procesos y entradas/salidas establecidas.
d) Las descripciones de relaciones, actividades y roles. precisa las relaciones y responsabilidades de las partes interesadas en el gobierno y la gestión de TI.
e) La guía de diseño de sistema de gobierno. enseña la forma de cómo diseñar un sistema de gobierno específico de TI para una organización.

COBIT es una práctica muy útil para las o los auditores de TI, ya que permite (AUDITOOL, 2024):

•Establecer controles de TI para administrar de manera eficaz los sistemas de TI y mitigar los riesgos asociados.
•Evaluar la eficacia del control de TI mediante la medición del desempeño de las capacidades de TI, identificando áreas débiles y haciendo recomendaciones para mejorar.
•Asegurar la alineación de TI con los objetivos de la organización.
•Cumplimiento normativo, porque COBIT está diseñado para estar en conformidad con otras normas y marcos, como ISO 27001 y el Reglamento General de Protección de Datos (GDPR), entre otros.
•Soporte para la mejora continua, proporcionando directrices para la identificación de áreas de mejora en la gobernabilidad y gestión de TI.

5.3.2 COSO

COSO (por sus siglas en inglés, Comité de Organizaciones Patrocinadoras de la Comisión Treadway) su finalidad es llevar a cabo una evaluación en la administración del riesgo organizacional, el control interno, las finanzas y los fraudes. Del mismo modo, busca proveer liderazgo intelectual por medio del desarrollo de orientaciones y contextos generales de la administración de control interno, riesgo y retractación del fraude, delineado en la perfección del desempeño de la empresa y minimizar el alcance de los fraudes de las instituciones.

Este modelo se integra de cinco componentes, los cuáles se encuentran interrelacionados entre sí (Worldsys, 2023):

a) Generación de un ambiente de control. proporciona estructura y disciplina entre el personal de la organización.
b) Las actividades de control. son los procedimientos y las políticas que consienten el aseguramiento de las acciones pertinentes para enfrentar los riesgos que puedan obstaculizar el cumplimiento de los objetivos de la organización.
c) La evaluación de riesgos. lleva a cabo la evaluación de los riesgos internos y externos de todas las áreas de la organización, en función de los objetivos y de la planeación.
d) La comunicación efectiva y la información. hace referencia al análisis e intercambio de información entre las y los responsables de cada área para evaluar de forma apropiada los riesgos generales de la organización. Del mismo modo, significa garantizar una comunicación efectiva donde la información fluya hacia arriba y hacia abajo dentro de la organización.
e) El monitoreo. implica monitorear o evaluar de forma continua la calidad del desempeño de los sistemas de control interno. Los resultados ayudarán a tomar las medidas correctivas necesarias para asegurar la mejora continua del sistema.

El control interno facilita el cumplimiento de los objetivos de las organizaciones ya que permite comprender cómo funciona la gestión de riesgos, facilita fijar los objetivos de acuerdo con el rendimiento, brinda seguridad en la aplicación de la gestión de riesgos, permite que la información fluya entre las todas las personas involucradas, y fija actividades de monitoreo para la mejora continua del sistema de control interno (Delta Exponential Technologies, 2024).

5.3.3 ITIL

ITIL (por sus siglas en inglés, la Biblioteca de Infraestructura de Tecnologías de Información), tiene como propósito definir las prácticas

mejores en las responsabilidades y los métodos que se establecen para administrar los servicios de TI de la organización. Estas prácticas incluyen cinco disciplinas: gestión de cambios, de versiones, de configuración, de incidencias, y la gestión de problemas.

Este modelo se integra de cinco componentes, los cuáles se encuentran interrelacionados entre sí (Worldsys, 2023):

a) Generación de un ambiente de control. – proporciona estructura y disciplina entre el personal de la organización.
b) Las actividades de control. - son los procedimientos y las políticas que consienten el aseguramiento de las acciones pertinentes para enfrentar los riesgos que puedan obstaculizar el cumplimiento de los objetivos de la organización.
c) La evaluación de riesgos. – lleva a cabo la evaluación de los riesgos internos y externos de todas las áreas de la organización, en función de los objetivos y de la planeación.
d) La comunicación efectiva y la información. – hace referencia al análisis e intercambio de información entre las y los responsables de cada área para evaluar de forma apropiada los riesgos generales de la organización. Del mismo modo, significa garantizar una comunicación efectiva donde la información fluya hacia arriba y hacia abajo dentro de la organización.
e) El monitoreo. – implica monitorear o evaluar de forma continua la calidad del desempeño de los sistemas de control interno. Los resultados ayudarán a tomar las medidas correctivas necesarias para asegurar la mejora continua del sistema.

El control interno facilita el cumplimiento de los objetivos de las organizaciones ya que permite comprender cómo funciona la gestión de riesgos, facilita fijar los objetivos de acuerdo con el rendimiento, brinda seguridad en la aplicación de la gestión de riesgos, permite que la información fluya entre las todas las personas involucradas, y fija actividades de monitoreo para la mejora continua del sistema de control interno (Delta Exponential Technologies, 2024).

5.3.3 ITIL

ITIL (por sus siglas en inglés, la Biblioteca de Infraestructura de Tecnologías de Información), tiene como propósito definir las prácticas mejores en las responsabilidades y los métodos que se establecen para administrar los servicios de TI de la organización. Estas prácticas incluyen cinco disciplinas: gestión de cambios, de versiones, de configuración, de incidencias, y la gestión de problemas.

ITIL integra un modelo de cuatro dimensiones relacionado con la gestión de servicios para exponer lo relevante para los componentes del Sistema de Valor de Servicio (SVS) (ITIL 4, s.f.):

a) La tecnología y la información. – contempla los componentes técnicos pertenecientes a la oferta de los servicios en la organización.
b) Las organizaciones y las personas. – comprende la cultura de la organización y todo lo referente a los recursos humanos.
c) Los flujos y procesos de valor. – integra la realización de las acciones y actividades suficientes para alcanzar los resultados esperados de la organización.
d) Los proveedores y socios. – corresponde a las relaciones que maneja la organización con otras organizaciones y que de forma conjunta agrupan el valor de la organización.

El contexto de ITIL permite la mejora continua de la calidad en los servicios de TI y la productividad y eficiencia de los mismos servicios.

Proceso de la auditoría mediante ITIL

Los pasos para llevar a cabo el proceso de la auditoría con ITIL son (Ingenio Learning, s.f.):

1. Establecer los objetivos de la auditoría. – en este paso la organización determina su alcance y cómo es que sus sistemas apoyan a cumplirlo.
2. Realizar un inventario. – aquí se integra una lista de los factores más importantes a auditar de acuerdo con la organización.

3. Registrar incidencias. – en este paso se lleva a cabo el registro de incidencias encontradas en el proceso de la auditoría, estas pueden ser: malas prácticas de TI, ineficiencias, o actitudes negativas de las personas.
4. Corregir errores. – aquí se realizan todas las correcciones posibles para alcanzar los objetivos y aportar valor a la organización.

Ejercicio: Reactivos de verdadero o falso

Instrucciones: Leer de forma comprensiva cada una de las oraciones e indica con una "V", si es verdadero, o una "F", si es falso.

1. _____Una metodología en el contexto de la auditoría informática, indica las fases a seguir para efectuar las tareas de la auditoría de forma fluida y sistemática en las áreas correspondientes de las tecnologías de información.
2. _____La etapa de planeación en una auditoría informática, consiste en determinar el alcance y los propósitos de la auditoría.
3. _____En la etapa del trabajo de campo de una auditoría informática, el equipo de la auditoría no realizará las entrevistas para obtener la información correspondiente.
4. _____En la etapa de descubrimiento y validación de problemas en una auditoría informática, los problemas descubiertos deberán ser discutidos con los clientes, de tal forma que los clientes trabajen de manera conjunta en la validación del problema y tomen posesión de la temática a tratar.
5. _____En la etapa de desarrollo de soluciones en una auditoría informática, se utilizan los enfoques de recomendación, de respuesta de gestión y de solución para descubrir problemas.
6. _____El informe de la auditoría informática es el medio para documentar lo resultante de una auditoría.
7. _____El auditor que realizó la auditoría estará en contacto con los responsables de la empresa hasta que se resuelvan los problemas.

Fuente: Davis, et al. (2011), Echenique (2001), Piattini y del Peso (2001).

Capítulo **6**

Norma ISO

“La mejor manera de hacer algo”
(ISO)

6.1 Historia de ISO

De acuerdo con Moeller (2010), la Organización Internacional para la Estandarización (ISO), es responsable de desarrollar y publicar normas internacionales correspondientes a diversas áreas comerciales y de procesos. Las normas, adquieren importancia a nivel mundial, ya que las empresas que se rigen por dichos estándares obtienen un lenguaje común en la calidad de los productos y servicios que brindan.

Dado que la institución tendría diferentes acrónimos en diferentes idiomas, los iniciadores tomaron la decisión de proporcionar la abreviación de ISO. La palabra ISO se origina del griego 'isos', que tiene el significado de igual. No importa el idioma o la nación, la Organización Internacional para la Estandarización se identifica como ISO (ISO, s.f.).

El surgimiento de ISO data de 1946 y se derivó por la unión de 2 organizaciones: la primera de ellas nombrada la Federación Internacional de Asociaciones Nacionales de Normalización (ISA, por sus siglas en inglés, *International Federation of the National Standarizing Association*), instituida en 1926 en Nueva York y administrada en Suiza; la cual tenía el objetivo de regular las áreas de Europa Occidental que no estaban dentro de la normativa de la electrónica, que en ese entonces estaba reglamentada por la Comisión Internacional de Electrónica (IEC, por sus siglas en inglés, *International Electrotechnical Commission*), fundada en 1906. La ISA, suspendió sus actividades al cerrarse las comunicaciones internacionales durante la segunda guerra mundial. La siguiente organización fue el Comité Coordinador de Normas de las Naciones Unidas (UNSCC, por sus siglas en inglés, United Nations Standards Coordinating Commitee), establecida en 1944 y administrada en Londres en las oficinas de la IEC, su finalidad era reconstruir y normalizar los estándares entre los países fecha posterior a la segunda guerra mundial (ISO, 1997).

En octubre de 1945, las personas de las delegaciones de la UNSCC tuvieron una reunión en Nueva York en la que se discutió el futuro de la estandarización. En esta reunión se acordó integrar fuerzas con los miembros de la ISA y así crear un organismo único de normalización. Después de las negociaciones, el 14 de octubre de 1946, se desarrolló la conferencia en el Instituto de Ingenieros Civiles en Londres con la

participación de 65 delegados como representantes de 25 países, donde se acordó crear ISO, siendo Ginebra la sede para la organización. Oficialmente ISO empezó sus actividades en 1947 y para finales de ese mismo año ya había recibido el estatuto consultivo por parte de las Naciones Unidas. En los años 50´s, los Comités Técnicos comenzaban a producir lo que entonces se conocía como "Recomendaciones", y en 1951 se publicó la primera norma denominada "ISO/R 1:1951", en la cual se deducía la temperatura de referencia estándar para mediciones de longitudes organizacionales (ibid.).

A continuación, se describe la línea de tiempo de la historia de ISO (ISO, s.f.):

- **1946:** en Londres, se reúnen 65 delegados de veinticinco naciones para discernir el futuro de la normalización a nivel internacional.
- **1947**: nace oficialmente ISO con 67 comités técnicos.
- **1949:** se establecen las primeras oficinas de ISO.
- **1950**: la secretaría principal es integrada por cinco personas.
- **1951:** se difunde la primera norma ISO (llamadas recomendaciones), ISO/R 1:1951.
- **1952**: se lanza la revista ISO.
- **1955:** ISO es integrada por treinta y cinco miembros y sesenta y ocho normas (lque fueron denominadas como recomendaciones).
- **1960**: ISO publica la norma ISO 31 sobre cantidades y unidades, que se apoya en el Sistema Internacional de Unidades. ISO busca la integración de otras naciones en desarrollo en su trabajo de la normalización internacional.
- **1961**: se instituye DEVCO, un comité para cuestiones de países en desarrollo.
- **1968:** introduce la membresía correspondiente para DEVCO.
- **1969**: Olle Sturen es nombrado secretario general de ISO. En sus discursos iniciales menciona que la normalización internacional es el fin del nacionalismo técnico.
- **1971**: ISO crea dos comités técnicos en el área ambiental: calidad del agua y calidad del aire.
- **1975:** Olle Sturen, secretario general de ISO tiene la intención de convertir a ISO en una institución internacional.

•**1986**: Lawrence D. Eicher obtiene el puesto de secretario general.
•**1987:** ISO divulga la norma de gestión de calidad: ISO 9000.
•**1995:** ISO publica su primer sitio web.
•**1996:** ISO emite el estándar de sistema de gestión ambiental, ISO 14001. Dicho estándar otorga recursos a las organizaciones de toda índole para ayudarlas a identificar e inspeccionar su impacto ambiental.
•**2003**: ISO agranda su labor para integrar tecnologías nuevas como los biocombustibles y la nanotecnología. En este año, Bryden Alan es nombrado secretario general.
•**2005:** es presentado ISO/IEC 27001 por el comité técnico JTC1 de ISO e IEC. Es un estándar de sistema de gestión sobre seguridad de la información. Puesto que las instituciones usan las TIC en cada actividad, se vuelve más imprescindible proteger los sistemas y minimizar o erradicar las vulnerabilidades.
•**2008**: es recibido un Emmy, lo cual se deriva del trabajo realizado en la producción del estándar de codificación de video avanzado. Dicho estándar consiente que las imágenes en movimiento y el sonido se compriman en gran medida, para la transmisión por la red de Internet con una mayor calidad.
•**2009**: ISO instituye a Rob Steele como secretario general. Durante su administración, la empresa acoge un conocimiento ágil, que minimiza el tiempo de desarrollo de los estándares y apoya el desempeño de los estándares a nivel global.
•**2010:** es proyectada la primera norma internacional que provee pautas en la responsabilidad social, la cual es denominada "ISO 26000".
•**2011**: ISO lanza la norma de gestión de la energía ISO 5001. Esta norma brinda a las empresas privadas y públicas estrategias administrativas para incrementar la eficacia energética, disminuir costos y perfeccionar el desempeño energético.
•**2012:** se establece la coordinación para fundar un espacio consistente para estufas limpias. La coordinación es dirigida por la alianza global para estufas limpias (asociación pública privada, organizada por la Fundación de las Naciones Unidas), que está integrada por 1, 300 socios.
•**2015**: Kevin Mckinley, siendo secretario general interino, adopta la

última tecnología de publicación, concentrándose en el valor para las naciones miembro y la visión a largo plazo de "normas ISO utilizadas en todas partes".

- **2016:** ISO publica ISO 37001. Este es un estándar internacional de sistema de gestión antisoborno que ha sido pactado para apoyar a las empresas a combatir las vulnerabilidades de soborno en sus propias sistematizaciones y en sus cadenas de valor.
- **2017**: ISO celebra 70 años con 163 miembros y más de 21000 estándares. Se designa a Sergio Mujica, de la nación de Chile, como secretario general de ISO, integrando experiencia amplia de sus funciones en la Organización Mundial de Aduanas (OMA) y el Gobierno de su país.
- **2018**: ISO publica la norma internacional de salud y seguridad en el trabajo ISO 45001:2018. Esta norma se platea con el objetivo de apoyar a las empresas a eviar las enfermedades y lesiones en las áreas de trabajo.
- **2019:** se implementó ISO 56002 el Sistema de Gestión de la Innovación, para mantener a las instituciones robustas para enfrentarse a los desafíos futuros y actuales. Se lanza el plan de acción de género de ISO, que refiere cinco campos: la sensibilización sobre los estándares en apoyo al empoderamiento de las mujeres y la igualdad de género, la creación de una red para compartir mejores prácticas y la recopilación de datos.
- **2020**: se extiende el estándar ISO/PAS 45005 en el transcurso de la contingencia por la pandemia de COVID-19. Este estándar absorbe los lineamientos de vida segura y saludable en todas las áreas de trabajo.
- **2021**: Se publica la Declaración de Londres como una respuesta de transformación por la acción climática y el progreso en el compromiso internacional para alcanzar los objetivos net-zero.

Actualmente, ISO, en su página web (https://www.iso.org/standards.html), alude que se han integrado más de 24,449 normas internacionales, tiene 167 miembros, y hay 808 comités y subcomités técnicos encargados para el desarrollo de las normas. Entre los principales estándares se encuentran:

- **Estándares de seguridad y salud** para apoyar a minimizar o erradicar los accidentes en las áreas de trabajo.

- **Estándares de gestión de energía** para apoyar a minimizar el gasto energético.
- **Estándares de gestión de calidad** para apoyar el trabajo eficiente y la erradicación o disminución de las fallas del producto o servicio.
- **Normas de seguridad alimentaria** en el apoyo para que los alimentos no resulten contaminados.
- **Estándares de seguridad de Tecnologías de la Información** para contribuir a mantener segura la información confidencial.
- **Y estándares de gestión ambiental** para apoyar a disminuir los impactos en el medio ambiente, minimizar los desechos, y ayudar a que las organizaciones sean sostenibles.

De manera generalizada los estándares de ISO refieren la mejor manera de hacer las cosas (productos o servicios), es decir con calidad y seguridad.

6.2 Certificación ISO

6.2.1 ¿Qué es?

A palabras del diccionario de la lengua española, la palabra certificación significa "un documento en que se asegura la verdad de un hecho" (Real Academia Española, s.f., definición 2).

Para la norma ISO, una certificación comprueba el establecimiento de un sistema de gestión en una institución para avalar que se emplean las prácticas mejores en las diferentes divisiones de su especialización. La certificación refleja una ventaja competitiva, confianza del mercado, una mejora de los servicios y productos, y un positivo impacto en la imagen y valoración de las instituciones. Las principales certificaciones se relacionan con la calidad de los productos y procesos, seguridad en la información, el comportamiento ambiental responsable, la utilización adecuada de los recursos y la energía, el desempeño en seguridad y salud laboral, gestión de activos y riesgos, seguridad alimentaria, persistencia del negocio, cumplimiento legal, entre otros aspectos (Normas ISO, s.f.).

6.2.2 Requisitos

Se recomiendan los siguientes requisitos para alcanzar una certificación ISO:

a) Identificar los requisitos normativos y legales para la implantación del sistema de gestión correspondiente. Esta tarea puede ser efectuada por personas internas de la organización, por una institución consultora externa a la organización o por ambas.
b) Analizar la situación de la organización. Se requiere realizar una evaluación inicial de la organización para conocer el contexto del cumplimiento para la certificación.
c) Fundar el sistema de gestión ISO a partir de una acción de implantación. Es recomendable una implementación del sistema con un plan de acción y de manera estructurada.
d) Documentar los procesos del estándar ISO. Es recomendable documentar las políticas, instrucciones, registros, análisis, procesos, planes, funciones, entre otros documentos.
e) Formar y sensibilizar a las personas de la empresa. De los directivos o directivas para asentar las bases del liderazgo y la ayuda y a los empleados o empleadas para obtener el apoyo que se requiere.
f) Realizar auditorías internas. Este proceso se lleva a cabo para verificar que la institución cumpla todos los requisitos que indica la norma.
g) Utilizar y trabajar con el sistema de gestión. Se implementa para conocer si las políticas y procesos son claros, si la forma de operación de la institución incluye los procedimientos que se necesitan y se ejecutan de manera integrada.
h) Solicitar la auditoría de certificación. Este proceso lo realiza una empresa certificadora independiente que expide el certificado posterior a un proceso de auditoría de certificación (Normas ISO, s.f.).

6.2.3 Ventajas

Las principales ventajas que incluye la certificación ISO son:
•Reconocimiento de la empresa a nivel internacional.

•Mayor eficiencia en los procedimientos.
•Proporcionar herramientas para la medición de los resultados.
•Acceso a nuevos mercados y escenarios de negocio.
•Auxiliar en la toma de decisiones.
•Mejorar la administración interna.
•Habilidad de integrar diferentes sistemas de gestión (calidad, legal, seguridad en la información, ambiental, entre otros) (Normas ISO, s.f.).

6.3 ISO y las TIC

6.3.1 Aplicación de la norma ISO en las TIC

En esta época, todas las empresas cuentan con tecnologías de las información, sistemas y redes de comunicación de apoyo, depósitos de datos y, en general componentes de estructura de las tecnologías de información para mantener sus operaciones continuas. ISO ha desarrollado una diversidad de estándares las áreas de las Tecnologías de Información, como los estándares para el vocabulario, procesamiento de la información, inteligencia artificial, computación cuántica, computación en la nube, gestor de servicios, Big Data, calidad del producto del software, la Internet de las Cosas, centros de datos, biometría, seguridad de la información, entre otros.

Dado que todos los recursos tecnológicos pueden estar sujetos a diversas fallas (ataques, errores, situaciones naturales como incendios, inundaciones) las empresas necesitan tener los mecanismos adecuados para recuperar y restaurar sus operaciones de forma rápida y ordenada (Moeller, 2010). Para efectos de este manual, se tomará como referencia la norma ISO/IEC 25000 y la Norma ISO/IEC 27000.

6.3.2 Norma ISO/IEC 25000

La norma ISO/IEC 25000, es un conjunto de normativas que tiene el propósito de crear un ambiente de trabajo favorable en la evaluación de la calidad del producto del software. Se conoce como Evaluación y Re-

quisitos de Calidad del Software y del Sistema (SQuaRE, por sus siglas en inglés, *System and Software Quality Requirements and Evaluation*), (ISO 25000, s.f.).

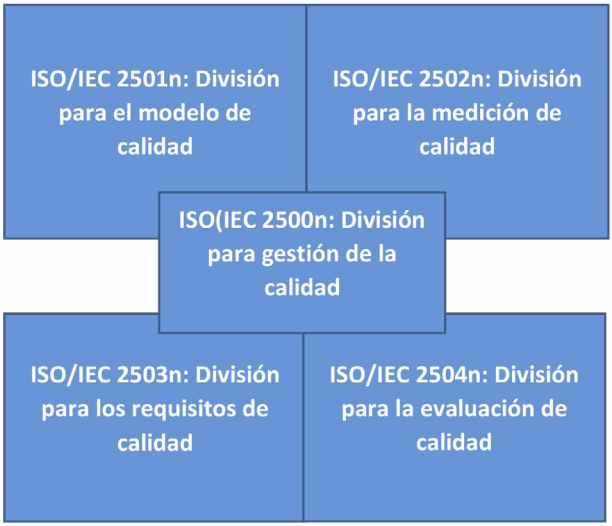
La certificación de la norma ISO/IEC 25000 consiente a las organizaciones que se dedican a estar al tanto de la calidad de los productos y desarrollo de software, y a las organizaciones que compran software a tomar la decisión de un recurso de software de acuerdo con sus necesidades (AENOR, s.f.).

Entre los principales beneficios de esta certificación, se encuentran:

- Definir parámetros de la calidad del producto de software, antes de su entrega.
- Averiguar y eliminar los desperfectos en el producto de software, y a la vez ahorrar costes por un posterior mantenimiento.
- Hay que avalar que el producto del software desarrollado respete las categorías de seguridad de autenticidad, confidencialidad, integridad, entre otros.
- Controlar y evaluar el rendimiento del producto de software, afirmando que podrá generar los resultados a pesar de las restricciones de recursos y tiempos determinados.
- Demostrar que el producto que se desarrolló se pondrá en producción sin poner en riesgo los otros sistemas.
- Reducir fallas en los productos durante su establecimiento en la producción.
- Demostrar que el producto desarrollado mantiene la coincidencia con las interfaces específicas para su operación (ibid.).

La familia de normas ISO/IEC 25000 se compone por cinco divisiones, que se describen en la figura 17:

Figura 17. Divisiones de ISO/IEC 25000.



Nota: Elaboración propia a partir de datos tomados de ISO 25000 (s.f.).

La descripción de las divisiones se describe a continuación (ISO 25000, s.f.):

ISO/IEC 2500n: división para la gestión de calidad.

Las normas que constituyen esta división precisan los términos, modelos y las comunes definiciones especificados por las siguientes normas de la familia 25000:

- ISO/IEC 25000 – Guía de SQuaRE: incorpora el modelo de la arquitectura de SQuaRE, un resumen de las partes, la terminología de la familia, los modelos de referencia, las y los usuarios conocidos y las partes que se asocian.
- ISO/IEC 25001 – Planificación y gestión: instituye las orientaciones y los requisitos para administrar la especificación y evaluación de los requerimientos del producto software.

ISO/IEC 2501n: división de modelo de calidad.

Este tipo de normas muestran modelos de calidad minuciosos que integran tipologías para calidad externa e interna y en uso del producto software:

- ISO/IEC 25010 – Modelos de calidad de sistemas y software: representa el modelo de calidad para el producto de software y su uso.
- ISO/IEC 25012 – Modelo de calidad de datos: precisa un modelo general para la calidad de los datos. Este modelo se emplea a aquella información almacenada estructuradamente y forman parte de un sistema de información.

ISO/IEC 2502n: división para la medición de calidad.

Las normas integran un modelo que referencia la medición de calidad del producto y las definiciones de las medidas de calidad: externa e interna y en uso. Así también las guías prácticas para su implementación:

- ISO/IEC 25020 – guía y modelo de referencia de medición: muestra una introducción y un modelo de referencia común a los factores de medición de la calidad. Del mismo modo, emite un manual para que las y los usuarios elijan y empleen medidas planteadas por las normas ISO.
- ISO/IEC 25021 – elementos de medida de calidad: precisa y detalla un grupo de métricas base y derivadas que puedan ser usadas en el ciclo de vida del desarrollo software.
- ISO/IEC 25022 – medición de calidad en uso: precisa las métricas para llevar a cabo la medición de la calidad en uso de un producto.
- ISO/IEC 25023 – medición de la calidad del sistema y del producto del software: delimita las métricas en la realización de la medición de la calidad de sistemas software y productos.
- ISO/IEC 25024 – medición de la calidad de datos: precisa las métricas para efectuar la comprobación de la calidad de los datos.

ISO/IEC 2503n: división para los requisitos de calidad.

Las normas especifican los requisitos de calidad que se utilizan en las tareas de incitación del producto software a desplegar o a través de un acceso en la evaluación:

•ISO/IEC 25030. Requerimientos de calidad: suministra recomendaciones para llevar a cabo la especificación de los requisitos de calidad del producto software.

ISO/IEC 2504n: división de la evaluación de calidad.

Se forma de normas que suministran sugerencias, guías y requisitos para efectuar el procedimiento de la evaluación del producto software:

•ISO/IEC 25040. es la guía y modelo de referencia de evaluación: presenta una referencia como un modelo general para una evaluación (tima en cuenta las entradas al procedimiento de evaluación, recursos y restricciones en la obtención de las salidas).
•ISO/IEC 2504. la guía de evaluación para adquirientes, personal evaluador independiente, personal desarrollador: muestra las recomendaciones y los requisitos para la práctica evaluativa del producto software.
•ISO/IEC 25042. los módulos de evaluación: presenta la evaluación, contenido, la documentación y estructura para precisar las unidades.
•ISO/IEC 25045. el módulo de evaluación de la recuperabilidad: precisa un módulo evaluativo que se deriva de la particularidad de recuperación.

6.3.3 Norma ISO/IEC 27000

La Norma ISO/IEC 27000 (Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, Descripción General y Vocabulario), aporta una perspectiva general del Sistema de Gestión de Seguridad de la Información (SGSI).

Los términos y definiciones de ISO/IEC 27000 sobre seguridad de la información se describen a continuación (Noma ISO 27001, s.f.):

Control de acceso. se refiere a los medios que garantizan el acceso autorizado a los activos y restringe de acuerdo con los requerimientos de seguridad y comerciales.

Auditoría. hace referencia al tratamiento independiente, documentado y sistemático para conseguir evidencia de la auditoría y su evaluación de forma objetiva decretando el nivel en que se efectúan los principios de la auditoría.

Ataque. es un intento por arruinar, alterar, exponer, deshabilitar, robar o conseguir el acceso sin autorización o usar los activos sin autorización.

Alcance de auditoría. integra la descripción de las unidades institucionales, las áreas físicas, procesos y actividades, y el periodo de tiempo cubierto.

Autenticación. es la garantía de que una particularidad reivindicada de un área es adecuada.

Autenticidad. se refiere a la propiedad que una entidad es lo que dice ser.

Disponibilidad. se refiere a la propiedad de ser utilizable y accesible para atender un área acreditada.

Medida base. se define en términos de una particularidad y el método para cuantificarla.

Información documentada. es la información que se controla y mantiene por la institución.

Consecuencia. representa los resultados de un suceso que altera a los objetivos.

Confidencialidad. es el dominio representado para que la información no sea publicada o divulgada a procesos sin autorización, áreas o personas.

Competencia. es la capacidad de usar habilidades y conocimientos para lograr resultados que se esperan.

Conformidad. es la propiedad que da cumplimiento a un requisito.

Control. es la medida que modifica un riesgo.

Corrección. se refiere a la tarea de suprimir una no conformidad descubierta.

La acción correctiva. hace referencia a la actividad para descartar el origen de una no conformidad y para advertir algo recurrente.

Sistema de información. es el grupo de servicios, aplicaciones y activos TIC y diversidad de dispositivos que manejan información.

Medida derivada. se refiere a la medida de más de dos valores de las medidas base.

Contexto externo. es el medio externo en el que una institución busca alcanzar los propósitos.

Órgano rector. hace referencia a la persona o al equipo de personas que tienen la responsabilidad del buen funcionamiento de la institución.

Medida. hace referencia a la variable fijada a un valor que resulta de una medición.

Objetivo de control. muestra los resultados de los cumplimientos de los controles.

Indicador. es la medida que suministra una evaluación o estimación.

No desprecio. habilidad que señala la ocurrencia de hechos reclamados y las áreas donde se originó.

Seguridad de información. hace referencia a aspectos confidenciales, preservación de la integridad y disposición de la información.

Continuidad de la seguridad de la información. se refiere a los procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad de la información.

Mejora continua. se refiere a las tareas periódicas en la optimización de la productividad.

Efectividad. se refiere en qué medida se efectúan las acciones planeadas y se alcanzan los resultados estipulados.

Gestión de incidentes de seguridad de la información. es el compuesto de procedimientos para, evaluar, detectar, tratar, informar, aprender y responder a las incidencias de seguridad de la información.

Necesidad de información. hace referencia a las capacidades específicas para administrar problemas, objetivos, riesgos.

Integridad. hace referencia a la propiedad de la exactitud y la integridad.

Evento. es el cambio u ocurrencia de un grupo específico de situaciones.

Contexto interno. es el ambiente interior en el que la empresa busca cumplir todos los propósitos.

Riesgo residual. es el riesgo innecesario posterior al tratamiento de un riesgo.

Gobernanza de la seguridad de la información. es la forma de dirigir y controlar todas las acciones de seguridad de la información de una institución.

Probabilidad. hace referencia a la posibilidad de que algo suceda.

Medición. es el proceso para determinar un valor.

Parte interesada. es la empresa o persona que puede perjudicar, verse perjudicada o detectarse afectada por una acción o decisión.

El Nivel de riesgo. es la dimensión de un riesgo representada en aspectos de la probabilidad y consecuencias combinadas.

Monitoreo. establecer el estado de un procedimiento, proceso o una acción.

Incidente de seguridad de la información. hace referencia a un suceso o un conjunto de hechos sobre seguridad inesperados o no deseados que posibilitan comprometer la seguridad informática y los trabajos comerciales.

No conformidad. Incumplimiento de un requerimiento.

Función de medición. cálculo o algoritmo efectuado en la armonización de más de una medida base.

Comunidad de intercambio de información.- hace referencia al conjunto de empresas o personas que admiten compartir información.

Objetivo de revisión. es lo que se declara en una descripción: lo que se debería lograr como resultado en el análisis.

Método de medida. es la serie lógica de operaciones explicada genéricamente, y usada para cuantificar una característica con referencia a una escala determinada.

El evento de seguridad de información. es la coyuntura que se ha reconocido de un sistema, estado de red o servicio que manifiesta una falla de los controles, una falta de cumplimiento de la normativa de seguridad de la información o un escenario desconocido que es importante para la seguridad.

Externalizar. crear un convenio para que empresa externa efectúe parte de las funciones de una institución.

Criterios del riesgo. se refiere a los requisitos evaluadores de la relevancia de un riesgo.

Instalaciones para procesar datos. es todo tipo de sistema de transformación de la información, infraestructura, ubicación física o servicio que lo aloja.

Desempeño. resulto medible.

Política. propósitos de una organización, de acuerdo con lo expresado de manera formal por su alta dirección.

La entidad de comunicación de información confiable. empresa con autonomía que ayuda en el intercambio de información en un área.

Confiabilidad. es la característica de las conductas y los resultados esperados confiables.

Organización. conjunto de personas o persona que define sus ocupaciones con responsabilidades, relaciones y autoridades para alcanzar sus objetivos.

Objeto de revisión. Artículo específico a revisar.

Proceso. grupo de acciones conectadas o interactivas que permiten la transformación de las entradas en salidas.

Riesgo. efecto de la incertidumbre sobre los propósitos establecidos.

Aceptación del riesgo. toma de decisiones informadas de tomar un riesgo específico.

Evaluación de riesgos. proceso general de reconocimiento de riesgos, análisis y evaluación de riesgos.

Revisión. acción en el establecimiento de la adecuación, idoneidad, y la eficacia en la revisión para lograr los propósitos planteados.

Comunicación y consulta de riesgos. grupo de procedimientos continuos e iterativos que una empresa realiza para compartir, proporcionar y efectuar el proceso de recibir la información, así mismo mantiene un diálogo para la administración del riesgo.

La evaluación del riesgo. proceso de cotejar los resultados del análisis de riesgo con los criterios de riesgo para establecer si el riesgo es admisible.

Identificación de riesgo.- es el procedimiento para el reconocimiento, búsqueda y la descripción de un riesgo.

Vulnerabilidad.- debilidad de activos que son explotados por más de un riesgo.

Objetivo. es lo que se busca lograr (el o los resultados).

El proceso de gestión de riesgos. hace referencia a la práctica metódica de políticas de gestión procesos y aplicación de consulta, comunicación, establecimiento del contexto, evaluación, tratamiento, análisis, revisión y seguimiento de riesgos.

El tratamiento del riesgo. se refiere a la modificación de un riesgo.
Estándar de implementación de seguridad. son los documentos que especifican las maneras autorizadas en la ejecución de la seguridad.
El propietario del riesgo. entidad y/o persona que tiene autoridad y responsabilidad de administrar un riesgo.
La amenaza. causa deliberada de un caso imprevisto, que genera deterioros a una institución.
Requisito. es la expectativa que se presenta de forma obligatoria o implícita.
Alta dirección. persona o grupo de personas que manejan y controlan una institución en primer nivel.
Sistema de gestión de seguridad de la información (SGSI) profesional. personal que tiene la responsabilidad de conservar, establecer, mejorar y realizar de forma continua uno o más procedimientos del sistema de administración de seguridad de la información.
Sistema de gestión. es el grupo de componentes interactivos o interrelacionados de una empresa para el establecimiento de políticas, objetivos y procesos para lograr dichos objetivos.
Análisis de riesgo. procedimiento que comprende el ambiente del riesgo y que establece el nivel del riesgo.
Gestión de riesgos. acciones organizadas en el control y dirección de empresas relacionadas con el riesgo.

6.3.3.1 Elementos para la certificación

La norma ISO 27001 es la norma que referencia la certificación de la seguridad de la información en las instituciones. Las instituciones requieren evaluar y monitorear la eficiencia de los procedimientos y controles que se implementan, identificar los riesgos emergentes a tratar, y seleccionar, implementar y mejorar los controles apropiados según sea necesario mediante políticas y propósitos para la seguridad de la información y alcanzar esos propósitos de forma efectiva mediante el uso de un sistema de gestión. La norma ISO 27001 contiene las especificaciones para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI). El SGSI se compone de un conjunto de instrucciones, procedi-

mientos y políticas, sustantivas para las tareas o sistema de información que buscan como finalidad protejer los activos de información en una institución (Noma ISO 27001, s.f.).

Los objetivos que identifican un SGSI son (ISO 27000, 2005):

1. La confidencialidad de la información.
2. La integridad de la información y sus métodos de proceso.
3. La disponibilidad y acceso a la información.

6.3.3.2 Estructura de los elementos

Para implementar un SGSI se requiere seguir los siguientes pasos (Norma ISO 27001, s.f.).:

1. Identifica y caracterizar los activos de información de la empresa de acuerdo con sus especificaciones para la seguridad de la información que se relacionan al tipo de información que manejan.
2. Realizar un método de tratamiento de riesgos de forma ponderada tomando en cuenta el o los resultados de una evaluación de riesgos.
3. Plantear proyectos de mejora para los riesgos nuevos que se han identificado.
4. Efectuar los controles elegidos para disminuir los riesgos que no son aceptados.
5. Llevar a cabo la evaluación de riesgos para la seguridad de la información reconocidos para cada tipo de información.
6. Efectuar la medición de los resultados en la aplicación de los controles.
7. Valorar la pertinencia de los controles efectuados referentes a los activos de la información.

Se recomienda que este proceso esté sistematizado y se mantenga durante todo el tiempo con el propósito de optimar continuamente la seguridad de la información en cada institución.

6.4 Situaciones en las auditorías

De acuerdo con la Entidad Latinoamericana de Consultoría Educativa SC (ENLACE SC, 2019), para implementar el proceso de la auditoría, se debe aplicar la norma ISO 19011. La norma presenta las líneas para llevar a cabo las auditorías, así como también los términos y definiciones:

•Auditor. es la persona competente para formalizar una auditoría.
•Expertise técnico. es la persona que contribuye con conocimientos especializados o experiencia al equipo que trabajará con la auditoría.
•La planeación de la auditoría. es la explicación de las acciones in situ y las disposiciones de una auditoría.
•Los criterios de auditoría. es el grupo de requerimientos y políticas usados como una referencia.
•Las evidencias una auditoría. se relaciona con las declaraciones de hechos, los registros y otra información que son importantes para las especificaciones de la auditoría.
•El programa de auditoría. es la planeación de una o varias auditorías en un lapso de tiempo específico y encaminadas hacia un objetivo determinado.
•El equipo auditor. se refiere a uno o a un grupo de auditores o auditoras que realizan la auditoría.

6.4.1 Responsabilidades

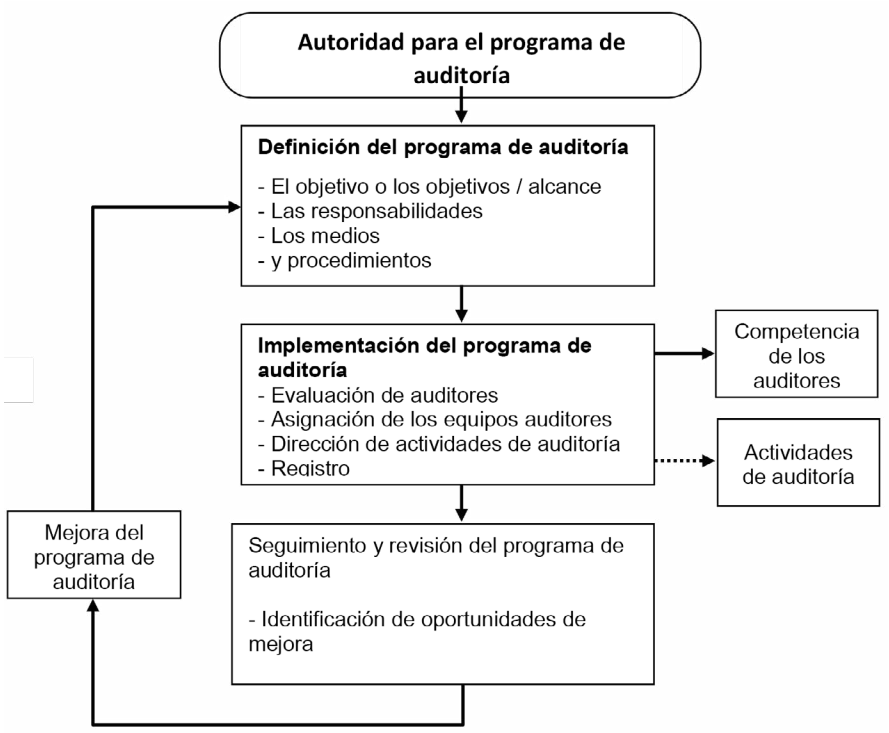
Las personas que tienen responsabilidades en la gestión del programa de la auditoría deberán asumir los siguientes compromisos (ENLACE SC, 2019):

a) Crear objetivos y describir un alcance para el programa de auditoría.
b) Mejorar, inspeccionar y analizar el programa de auditoría.
c) Instaurar las obligaciones, procedimientos y medios.
d) Consolidación al implementar el programa de la auditoría.
e) Certificar que se mantengan las exploraciones en el programa de la auditoría.

6.4.2 Aplicación del ciclo Planificar-Hacer-Verificar-Actuar a la administración de un programa

La aplicación del ciclo Planificar-Hacer-Verificar-Actuar a la gestión de un programa, se especifica en la figura 18.

Figura 18. Ciclo Planificar-Hacer-Verificar-Actuar.



Nota: Datos tomados de ENLACE SC (2019).

6.4.3 Actividades de la auditoría

6.4.3.1 Inicio de la auditoría

Para iniciar la auditoría es necesario realizar las siguientes acciones (ENLACE SC, 2019):

- Designar al auditor líder.
- Definir los criterios, el alcance y objetivos de la auditoría, basados en el objetivo global del programa de auditoría.
- Determinar la viabilidad de la auditoría en cuanto a la información, cooperación, tiempo y recursos adecuados.
- Instituir los contactos de inicio con el auditado para establecer los canales de acceso a la información y comunicación.

6.4.3.2 Preparación de las actividades de visita al emplazamiento.

La preparación de las actividades consiste en (ENLACE SC, 2019):

- Examinar los documentos para establecer la conformidad del sistema.
- Habilitar el plan de la auditoría, incluyendo los criterios y documentos de referencia, el alcance, el calendario de fechas y el lugar, la duración de las actividades, y las funciones y responsabilidades del equipo que audita y el de las personas que los acompañe.
- Asignar los trabajos y responsabilidades específicas que deberá realizar el equipo auditor.
- El equipo auditor tiene la función de recoger, analizar y verificar la información correspondiente en las actividades planeadas y organizar la documentación del trabajo pertinentes, así como registrar el progreso de la auditoría, entre ellos, la lista de comprobación y la planeación del muestreo de la auditoría y los formularios para recabar evidencias de soporte, hechos encontrados y los registros.

6.4.3.3 Realización de actividades de auditoría.

Actividades y las tareas de la auditoría se deberán efectuar mediante pasos secuenciados (ENLACE SC, 2019):

- Realizar una reunión de apertura con el personal responsable de funciones y procesos auditables.
- Revisar la documentación relevante del auditado.
- Intercambiar información durante la auditoría, evaluar el seguimiento de la auditoría y asignar tareas entre el personal que audita, si es necesario.
- Recolectar y verificar información.
- Generar los descubrimientos de la auditoría (que podrán ser de conformidad o de no conformidad) con los aspectos de la auditoría y distinguir una oportunidad para el mejoramiento.
- Preparar las conclusiones de la auditoría, considerando los hallazgos y recomendaciones.
- Llevar a cabo la reunión de cierre, presentando las recomendaciones de mejora, la conclusión y estableciendo el tiempo para que el auditado realice las acciones correctivas.

6.4.3.4 La reparación, aprobación y distribución del informe.

El auditor líder debe ser responsable de distribuir el informe final, de preparar el contenido, el cual deberá incluir (ENLACE SC, 2019):

- El alcance de la auditoría.
- El objetivo o los objetivos.
- El reconocimiento de las y los integrantes del equipo auditor.
- Las áreas físicas y las fechas donde se llevaron a cabo todas las actividades de la auditoría.
- Las pautas y hallazgos.
- Los resultados y conclusiones de la auditoría.

Nota: Los hallazgos pueden clasificarse de la siguiente forma:

a) Debilidad. es el incumplimiento de algunos de los criterios especificados en la norma.
b) Riesgo. es la no aplicación o la ausencia parcial de un criterio de la norma en una o dos áreas de la organización.
c) No conformidad. es la no aplicación o la ausencia de un criterio de la norma en toda la organización.

6.4.4 Finalización de la auditoría

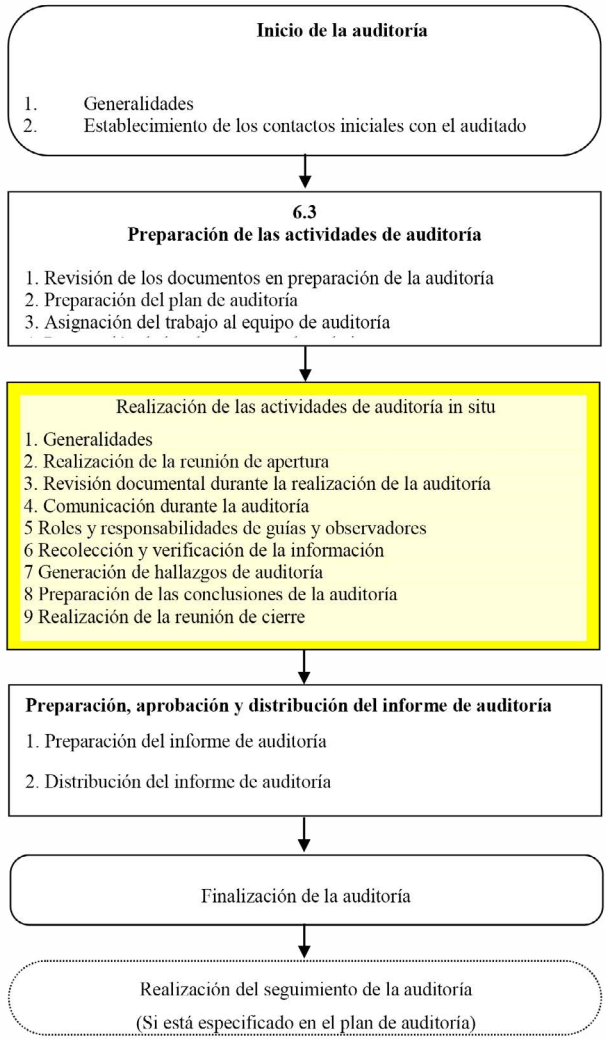
Al finalizar todas las acciones y actividades establecidas en la planeación y el informe de la auditoría se aprobó y se compartió, en este punto se puede decir que la auditoría ha sido completada. Posterior a ello, todos los escritos elaborados para este fin deberán deshacerse o preservarse por común acuerdo entre las y los participantes y según lo especificado en el programa de la auditoría y con los obligaciones contractuales y legales aplicables (ENLACE SC, 2019).

6.4.5 El seguimiento de la auditoría

La conclusión de la auditoría refleja todas las necesidades de medidas correctivas y preventivas y las actividades para el mejoramiento. Dichas actividades no forman parte de la auditoría y especialmente son iniciadas por la persona que audita en un período de tiempo estipulado (ENLACE SC, 2019).

En la figura 19 se presenta la visión general de las actividades de la auditoría.

Figura 19. Visión general de las actividades de la auditoría.



Nota: Datos tomados de ENLACE SC (2019)

Ejercicio: Relación de columnas

Instrucciones: relaciona ambas columnas de manera correcta

1. ( ) Es el significado de las iniciales ISO	A. Estándar de gestión ambiental.
2. ( ) Es el estándar que ayuda a minimizar los desechos, impactos ambientales y ayuda en la sostenibilidad.	B. Identificar los requisitos normativos y legales para la implantación del sistema de gestión correspondiente, formar y sensibilizar a las personas de la empresa.
3. ( ) Es el estándar que ayuda a trabajar de forma eficiente y apoya en la reducción de las fallas del producto.	C. La norma ISO/IEC 25000
4. ( ) Es el estándar que ayuda a mantener segura la información confidencial	D. La certificación en una norma ISO
5. ( ) Es la norma que se encarga de la certificación de la seguridad de la informa*ción en las instituciones.	E. La integridad, confidencialidad y disponibilidad de la información.
6. ( ) Es la norma que tiene el objetivo de crear un ambiente de trabajo común para la evaluación de la calidad del producto del software.	F. Estándar de gestión de calidad
7. ( ) Son algunos de los requisitos para obtener una certificación ISO	G. Mejorar la gestión interna, favorecer la toma de decisiones.
8. ( ) Son algunas de las ventajas que incluye la certificación ISO	H. Organización Internacional para la Estandarización
9. ( ) Son los objetivos que identifican un Sistema de Gestión de la Seguridad de la Información (SGSI).	I. Estándar de Seguridad de Tecnologías de la Información
10. ( ) Manifiesta que se ha implementado un sistema de gestión en una institución garantizando que fueron implementadas las mejores prácticas en los diferentes sectores de especialización.	J. La norma ISO/IEC 27001

Fuente: AENOR (s.f.), ENLACE SC (2019), Moeller (2010), Normas ISO (s.f.), Noma ISO 27001 s.f.), ISO, (s.f.), ISO, (1997), ISO 25000 (s.f.), ISO 27000 (2005).

Capítulo 7

La auditoría en informática en la nube

La auditoría en informática en la nube es un proceso fundamental para garantizar la seguridad, el cumplimiento y la gestión eficiente de los recursos en entornos de computación en la nube. A medida que las organizaciones migran a la nube para aprovechar sus beneficios de escalabilidad y flexibilidad, la necesidad de una auditoría adecuada se vuelve esencial.

7.1 Auditoría de Sistemas en la Nube utilizando Inteligencia Artificial

El auge de la computación en la nube ha transformado la gestión y almacenamiento de datos, introduciendo riesgos adicionales en términos de seguridad y privacidad de la información. En este contexto, la auditoría de sistemas en la nube es esencial para garantizar la seguridad, integridad y cumplimiento de los servicios. La inteligencia artificial (IA), con sus capacidades avanzadas de análisis de datos y aprendizaje automático, se ha convertido en una herramienta clave para optimizar y automatizar estos procesos, mejorando la detección de anomalías y la gestión de riesgos en tiempo real (Qureshi, 2020).

7.2 Ventajas del uso de IA en Auditoría de Sistemas en la Nube

La IA aplicada a la auditoría en la nube permite una revisión continua y profunda de los datos, facilitando la identificación de patrones inusuales y comportamientos sospechosos sin intervención humana constante (Rodríguez, 2024). El aprendizaje automático permite desarrollar modelos predictivos que anticipan posibles vulnerabilidades o brechas de seguridad, mejorando la eficiencia de las auditorías y reduciendo los tiempos de respuesta ante incidentes (Auditoría y Co, 2024). Además, los algoritmos de procesamiento de lenguaje natural (PLN) permiten analizar rápidamente grandes volúmenes de registros de actividad, identificando posibles incumplimientos o áreas de riesgo (Sayid, 2023).

7.3 Aspectos Clave de la Auditoría en la Nube

1. **Seguridad y protección de datos:** La auditoría revisa los mecanismos de seguridad para proteger los datos sensibles y garantizar la confidencialidad, integridad y disponibilidad de la información. Esto incluye verificar el cifrado de datos, la autenticación de usuarios y la gestión de accesos, así como la detección y respuesta a incidentes de seguridad.
2. **Cumplimiento normativo**: Las empresas deben cumplir con normativas específicas, como GDPR, HIPAA o PCI DSS, según la industria. La auditoría revisa que los servicios en la nube estén configurados para cumplir con estos requisitos, garantizando que los datos se manejen de acuerdo con la regulación vigente y que se implementen controles necesarios para evitar sanciones.
3. **Gestión de identidades y accesos (IAM):** La auditoría revisa los sistemas de administración de identidades y accesos para asegurarse de que solo las personas autorizadas tengan acceso a los datos y recursos críticos. También se evalúa el uso de roles y permisos y la implementación de la autenticación multifactor (MFA) para proteger contra accesos no autorizados.
4. **Evaluación de la infraestructura y configuración de seguridad**: La auditoría evalúa la infraestructura en la nube, verificando que esté configurada adecuadamente. Esto incluye revisar la configuración de redes, firewalls, y las políticas de seguridad. Los errores de configuración son una de las principales causas de brechas de seguridad en la nube, y una auditoría busca identificar y corregir estos problemas.
5. **Control de costos y optimización de recursos:** La computación en la nube puede ser costosa si no se administra adecuadamente. La auditoría también revisa el uso y los costos asociados a los recursos en la nube, asegurándose de que se utilicen de manera eficiente y que no se incurra en gastos innecesarios. Esto incluye monitorear los recursos infrautilizados y proponer estrategias para optimizar costos.
6. **Monitoreo y detección de incidentes:** Es esencial contar con sistemas que permitan detectar actividades sospechosas o inusuales en tiempo real. La auditoría revisa las herramientas de monitoreo de seguridad

y gestión de eventos (SIEM), que permiten a las empresas responder rápidamente a amenazas y proteger sus activos.

7. **Planes de recuperación ante desastres:** Una auditoría en la nube también evalúa los planes de recuperación ante desastres (DR) para asegurar que la organización pueda recuperar sus datos y servicios rápidamente en caso de un fallo o ataque. Esto incluye probar y verificar los mecanismos de backup y recuperación.

7.4 Desafíos de implementar IA en Auditoría de la Nube

En entornos de nube, el personal auditor debe abordar desafíos únicos, como la falta de control directo sobre los servidores físicos, la dependencia de los proveedores de servicios en cuanto a políticas de seguridad, y la complejidad de asegurar que las configuraciones de infraestructura cumplan con estándares como ISO 27001 y GDPR. Según estudios recientes, la implementación de controles de auditoría efectivos en la nube requiere la combinación de herramientas de monitoreo en tiempo real y evaluaciones regulares que pueden detectar actividades anómalas y potenciales vulnerabilidades de seguridad (Oyinkansola, 2022). Además, es crítico que las auditorías en la nube incluyan la revisión de los acuerdos de nivel de servicio (SLA), asegurando que estos reflejen las responsabilidades de seguridad tanto del proveedor como del cliente. Sin embargo, la capacidad para realizar auditorías exhaustivas puede estar limitada por la falta de transparencia en algunos proveedores de nube, lo que plantea un obstáculo significativo en términos de visibilidad y acceso a registros críticos. Con la rápida evolución de las tecnologías y servicios en la nube, la auditoría en este ámbito requiere de métodos dinámicos y adaptativos, apoyados en tecnologías como la inteligencia artificial para predecir y mitigar riesgos de forma proactiva.

Del mismo modo, la IA enfrenta desafíos éticos y técnicos. Uno de los problemas más discutidos es la falta de transparencia en algunos algoritmos de IA, lo que genera una "caja negra" que dificulta la comprensión de cómo se toman las decisiones en los procesos de auditoría. Este aspecto es crucial en auditorías de cumplimiento, donde la trazabilidad es esencial. Además, el manejo de datos sensibles en entornos de IA requiere

prácticas robustas de seguridad y privacidad para evitar el mal uso o la filtración de información crítica (Laine, et al. 2024).

7.5 Aplicaciones comunes de IA en Auditoría de la Nube

1. Detección de Anomalías: A través de algoritmos de aprendizaje profundo, es posible monitorear el tráfico de red en tiempo real, identificando comportamientos inusuales que podrían indicar accesos no autorizados o amenazas internas (Hagemann y Katsarou, 2021).
2. Automatización del Cumplimiento Normativo: La IA permite auditar de manera automática y continua la conformidad con normativas como GDPR, CCPA o HIPAA, gracias a sistemas que procesan y evalúan grandes volúmenes de datos de manera eficiente (Mestari et al., 2024).
3. Análisis de Registros: Las técnicas de PLN son ampliamente utilizadas para analizar registros de actividades y notificaciones de seguridad, facilitando la detección temprana de posibles amenazas o infracciones de políticas (Mestari et al., 2024).

7.6 Herramientas para la Auditoría en la Nube

Existen herramientas específicas que facilitan la auditoría de entornos en la nube, entre ellas:

- AWS CloudTrail y AWS Config para auditorías en Amazon Web Services.
- Google Cloud Audit Logs para registros y monitoreo en Google Cloud Platform.
- Microsoft Azure Security Center para análisis y reportes de seguridad en Azure.
- Cloud Security Posture Management (CSPM), que permite gestionar la postura de seguridad general de la infraestructura en la nube.

Capítulo 8

Consideraciones éticas y legales en el proceso de la auditoría en informática

8.1 Consideraciones éticas

En el área profesional, la ética es una reflexión sobre el actuar propio o corporativa ante la toma de acciones o decisiones. Por otro lado, la profesión se determina en una acción o tarea de la sociedad cooperativa, cuyo fin consiste en proveer a la sociedad un bien específico y éste lo constituyen los productos y servicios concernientes a los sistemas de información. Fijar los elementos éticos y legales en las decisiones de la profesión es un componente que considerar en las actividades y sus consecuencias, porque afectan indirecta o directamente a instituciones y personas (Cohen y Asín, 2014).

Al trabajar con personas y sus equipos informáticos, existen normas legales y costumbres éticas que se deben considerar. Las computadoras personales y los dispositivos tecnológicos son propiedad, pero también se considera propiedad a los datos y a la información a la que se puede acceder, entre ella (Cisco Networking Academy, 2023b):

•Listas de contactos y números telefónicos.
•Mensajes de correo electrónico.
•Impresión de documentos o información expuesta en los escritorios de trabajo.
•Registros o información en la computadora personal.

Para trabajar con las computadoras personales, se debe de obtener la aprobación y el permiso de la persona. Es posible que durante el proceso de la auditoría se haya recopilado información privada, como claves, contraseñas y cuentas de usuario. Si hay un registro de este tipo de datos, se recomienda mantenerla confidencial; ya que su divulgación es antiético e ilegal. Además, la información de identificación personal también es confidencial, algunos ejemplos de ella pueden ser (Cisco Networking Academy, 2023b):

•Nombres o cuentas.
•Claves de identificación personal: número de seguridad social, de pasaporte, de cuenta de banco o tarjeta de débito crédito, de licencia de

conducir, de identificación de contribuyente; o direcciones como el domicilio del hogar.
•Características personales: Características personales: imágenes fotográficas, huellas digitales, datos biométricos (escaneo de firma de voz, la retina, geometría facial, entre otras).

8.2 Consideraciones legales

La normativa global y las competencias legales son distintas; aunque existen acciones que se estiman ilegales alrededor del mundo (Cisco Networking Academy, 2023b):

•Entrar a las cuentas, leer los mensajes de correo electrónico o archivos privados de las personas sin su permiso.
•Copiar, compartir o instalar contenido digital como música, software, imágenes, video o texto; ya que esto infringe los convenios de la ley aplicable o de copyright y de software.
•Permitir recursos de TI a usuarios no autorizados.
•Manejar los recursos de TI de la institución con propósitos comerciales.
•Compartir información confidencial de las personas.
•Usar de manera intencional los medios de la institución para actividades ilícitas como la pornografía infantil, obscenidad, infracción de copyright ,acorralamiento, amenazas, violación de marca comercial, robo, calumnia, accesos no autorizados y el robo de identidad.
•Realizar modificaciones en las configuraciones de software o hardware o del sistema sin que las personas lo autoricen.

8.3 Código de ética y conducta profesional

Los códigos de ética son compromisos de un profesional o de una empresa que incluyen acciones, valores y responsabilidades para el bien común. Ejemplo de ello, es el código de ética y conducta profesional de la Association for Computing Machinery (2023), el cual apoya a la toma de decisiones. La tabla 4, muestra la información:

Tabla 4. Código de ética y conducta profesional

Principios Éticos Generales	
Reconocer que las personas son partes interesadas en la informática y que se contribuye a la sociedad y al bienestar humano.	Se relaciona con la promoción de los derechos humanos fundamentales y la protección de la autonomía de cada persona. Subraya la obligación de utilizar las destrezas en favor de la sociedad.
Evitar el daño.	Las acciones con buena intención, abarcando el cumplimiento de funciones adheridas, pueden causar daños. Cuando el daño es involuntario, el personal responsable está obligado a mitigar o deshacer el daño tanto como este a su alcance.
Honestidad y ser confiable.	La honestidad es un mecanismo fundamental de la confiabilidad. Mantener afirmaciones premeditadamente falsas o engañosas, falsificar o fabricar información, aceptar conductas deshonestas o el soborno son infracciones al Código.
Aplicar la justicia y tomar medidas de no discriminación.	Está relacionado con los valores de tolerancia, igualdad, respeto por las demás personas y la justicia. Dicha justicia involucra que, se proporcione alguna vía razonable en la reparación de los daños.
Respetar el trabajo necesario para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos.	Este principio se relaciona con el respeto a la autoría de los inventores de ideas, creadores, trabajos y artefactos, las patentes, los derechos de autor, el secreto comercial, los acuerdos de licencias y otros métodos para proteger el trabajo de la autoría.
Respeto a la privacidad.	El principio se relaciona con las distintas definiciones de privacidad y la comprensión de los derechos y responsabilidades relacionados a la usabilidad de datos personales y su recopilación.
Respeto a la confidencialidad.	Este principio se relaciona con la protección de la confidencialidad de la información, datos de clientes y de investigación, secretos comerciales, información financiera, estrategias comerciales privadas, solicitud de patentes y documentos académicos que no han sido publicados.

Nota: Datos tomados de Association for Computing Machinery (2023)

Ejercicio: Reactivos de verdadero o falso

Instrucciones: Lee detenidamente cada uno de los enunciados e indica con una "V", si es verdadero, o una "F", si es falso.

1. _____ En el área profesional, la ética es una reflexión sobre el actuar propio o corporativa ante la toma de decisiones o acciones.
2. _____ Cuando trabaja con personas y sus equipos tecnológicos, existen costumbres éticas y normas legales que se deben tener en cuenta.
3. _____ Es posible que durante el proceso de la auditoría se haya recopilado información privada, como nombres de usuario y contraseñas; esta información se puede mantener pública.
4. _____ Antes de acceder a cuentas de las computadoras personales, incluida la cuenta de administrador, se debe de obtener el consentimiento de la persona.
5. _____Números de identificación personal, como el número de seguridad social, número de pasaporte, número de licencia de conducir, número de identificación de contribuyente y número de cuenta financiera o tarjeta de crédito, o direcciones, como la dirección del hogar o la de correo electrónico; son ejemplos de información de identificación personal, la cual debe mantenerse confidencial.
6. _____ Divulgar la información de las personas no es solo antiético, sino que también puede ser ilegal.
7. _____ De acuerdo con la ley, se permite instalar, copiar o compartir contenido digital (incluso software, música, texto, imágenes y video), en cualquier trabajo de auditoría.
8. _____ Los códigos de ética son compromisos de un profesional o de una empresa que incluyen acciones, valores y responsabilidades para el bien común.
9. _____ Mantener afirmaciones deliberadamente falsas o engañosas, fabricar o falsificar datos, ofrecer o aceptar sobornos y otras conductas deshonestas son infracciones al Código de Ética y Conducta.
10. _____ El respeto a la privacidad significa comprender los derechos y responsabilidades asociados con la recopilación y el uso de datos públicos.

Fuente: (Cohen y Asín, 2014), (Cisco Networking Academy, 2023b), Association for Computing Machinery (2023).

Ejercicio Integrador

Objetivo:

Realizar una investigación en una empresa sobre el área de TIC para conocer su estructura.

Instrucciones:

Responder las siguientes preguntas.

1. Conociendo las áreas de TIC. Investigar cuáles son los posibles departamentos que conforman un área de TIC, identificando los objetivos de cada departamento.

2. Funciones de las áreas de las TIC. Realizar el manual de puestos y funciones de los departamentos que conforman un área de TIC.

3. Procesos de las áreas de TIC. Identificar los diferentes procesos en los que participa un área de TIC.

4. Creación de procedimientos. Utilizando la estructura de la norma ISO, realizar el procedimiento para algún proceso en los que participen las TIC.

Ejercicio Final: Caso Práctico

Objetivo:

Realizar una auditoría de las tecnologías de la información y comunicación en una empresa, con el propósito de aplicar los conocimientos adquiridos y proporcionar información valiosa a la alta gerencia que permita incrementar la eficiencia de sus procesos y/o actividades.

Instrucciones:

- Visita una empresa pública o privada.
- Elige el área de Tecnologías o un departamento específico de la misma área para llevar a cabo la auditoría.
- Efectúa las etapas de una auditoría y elabora el informe final, cómo se muestra en la siguiente guía.

Guía

Nombre de la Empresa:
Área:
Tipo de auditoría:

Fase I: Definición de alcance y objetivos	
Alcance:	
Objetivo:	
Fase II: Estudio Inicial	
Estructura organizativa del área a auditar	
Aplicaciones informáticas	
Organigrama	
Funciones de los departamentos y sus relaciones jerárquicas	
Flujos de información	
Número de puestos de trabajo y personas por puesto de trabajo	

Fase III: Entorno operacional	
Hardware	
Software	
Seguridad	
Fase IV: Determinación de los recursos	
Materiales	
Humanos	
Fase V: Actividades de la auditoría	
Técnicas	
Métodos	
Herramientas	
Lista de Verificación	
Fase VI: Informe Final	
Titulo o Identificación del Informe	
Fecha de inicio	
Equipo auditor	
Nombre del área auditada	
Personas que reciben el informe	
Objetivos y alcance de la auditoría	
Limitaciones encontradas y objetivos no auditados	
Situación actual: hechos importantes y consolidados	
Hallazgos	
Tendencias de situación futura	
Puntos débiles y amenazas	
Recomendaciones	
Conclusiones	
Nombre y firma del auditor	
Fecha de emisión del informe	

Referencias

AENOR (s.f.). ISO 25000: Certificación de la calidad del software. https://www.aenor.com/certificacion/tecnologias-de-la-informacion/producto-software

Aguirre, J.J, (2005). Auditoría en Informática. http://fcasua.contad.unam.mx/apuntes/interiores/docs/2005/informatica/6/1664.pdf

Albarrán, S. E., Pérez, J. C., Salgado, M. y Valero, L. L. (2020). *Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares. Ideas en Ciencias de la Ingeniería*, *1*(1), 47-70. https://hemeroteca.uaemex.mx/index.php/ideasingenieria/article/view/14591

Alvarado, R., Acosta, K., Mata de Buonaffina, Y. (2018). Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones. https://www.redalyc.org/journal/666/66658188002/html/

Alvarez, L. (1981). Seguridad en Informática (Auditoría de Sistemas). Recuperado el 10 de octubre de 2021 de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Arimetrics. (2022). Qué es software. https://www.arimetrics.com/glosario-digital/software

Association for Computing Machinery. (2023). Código de Ética y Conducta Profesional de ACM. https://www.acm.org/about-acm/code-of-ethics-in-spanish#:~:text=Los%20profesionales%20de%20la%20Inform%C3%A1tica%20deben%20ser%20honestos%20acerca%20de,ya%20sean%20reales%20o%20percibidos.

AUDITOOL. (2024). Auditoría de TI. https://www.auditool.org/blog/auditoría-de-ti/entendiendo-el-marco-de-cobit-para-auditores-de-ti

Auditoría y Co. (8 de Marzo de 2024). El futuro de la Auditoría: integrando tecnología e inteligencia artificial. https://auditoría-auditores.com/articulos/articulo-auditoría-el-futuro-de-la-auditor-a-integrando-tecnolog-a-e-inteligencia-artificial/

Cisco Networking Academy (2023a). Introduction to IoT. Cisco

Cisco Networking Academy (2023b). ITE 7.01. Cisco

Cisco Networking Academy (2023c). Introducción a la ciberseguridad. Cisco

Cisco Systems, Inc. (2023). ¿Qué es 5G? https://www.cisco.com/c/es_mx/solutions/what-is-5g.html

Cohen, D. y Asín, E. (2014). *Tecnologías de la Información, Estrategias y Transformación en los Negocios.* McGrawHill.

Comunicare. (2019). Cómo era la comunicación antes y ahora: descúbrelo. https://www.comunicare.es/como-era-la-comunicacion-antes-y-ahora-descubrelo/#:~:text=En%20la%20comunicaci%C3%B3n%20antigua%2C%20los,de%20la%20distancia%20y%20el

Cotaña, M. (2020). Auditoría Informática. Recuperado el 10 de octubre de 2021 de http://cotana.informatica.edu.bo/downloads/PROGRAMA%20ANALISIS%20Y%20DISENO2-2020.pdf

Creative Commons (21 de noviembre de 2023). Imagen bajo licencia CC BY-NC 3.0 DEED. https://creativecommons.org/licenses/by-nc/3.0/

Davis, C., Schiller, M. y Wheeler, K. (2011). IT Auditing: Using Controls to Protect Information Assets. (2ª ed.) Mc Graw Hill.

Delta Exponential Technologies. (2024). Modelo COSO: características, beneficios e implementación. https://www.deltaprotect.com/blog/que-es-modelo-coso#:~:text=El%20Comit%C3%A9%20de%20Organizaciones%20Patrocinadoras,fraude%20financiero%20en%20las%20empresas.

Echenique, J. A. (2001). *Auditoría en Informática*. (2ª ed.), Mc Graw Hill.

EcuRed. (s.f.) Computadora Personal (PC) [Fotografía]. Https://www.ecured.cu/Computadora_personal

ETSINF-UPV. (2021). El UNIVAC, el primer computador comercial de Estados Unidos [Fotografía]. https://museo.inf.upv.es/univac2/

Entidad Latinoamericana de Consultoría Educativa SC. (ENLACE SC, 2019). Manual de Trabajo. Formación y Desarrollo de Auditores Institucionales, ISO 27001:2013, ISO 19011:2018.

Espitia, P. (2023). ¿Quién inventó el computador? Historia y generaciones de la computadora. https://pcsystemcolombia.com/quien-invento-el-computador-historia-y-generaciones-de-la-computadora/#:~:text=Los%20inicios%20de%20la%20computadora,Mesopotamia%20hace%20unos%205.000%20a%C3%B1os.

Franklin, E. (2007). Auditoría Administrativa – Gestión estratégica del cambio. Pearson.

Gaitan, R. (2007). Administración o Gestión de Riesgos E.R.M y la Auditoría Interna. ECOE EDICIONES.

Hagemann, T., y Katsarou, K. (2021). A Systematic Review on Anomaly Detection for Cloud Computing Environments. AICCC '20: Proceedings of the 2020 3rd Artificial Intelligence and Cloud Computing Conference, 83-96.

Hernández, E. (1993). *Auditoría en informática, un enfoque metodológico.* Compañía editorial continental, S.A de C. V.

Hernández, A. (2010). Auditoría Informática y Gestión de las Tecnologías de Información y Comunicación (TIC´s). *Compendium*, 13(25), 3-4. https://www.redalyc.org/articulo.oa?id=88019355001

Home Computer Museum. (s.f.). Apple Macintosh [Fotografía]. https://www.homecomputermuseum.nl/collectie/apple/apple-macintosh/

IBM. (s.f.). IBM's ASCC introduction [Fotografía]. https://www.ibm.com/ibm/history/exhibits/markI/markI_intro.html

IBM. (s.f.). Data Processing System [Fotografía]. https://www.ibm.com/ibm/history/exhibits/mainframe/mainframe_PP7094.html

ILIXUM. (2021). COBIT, ¿Qué es y para qué sirve? https://ilixum.com/cobit-que-es-y-para-que-sirve/

Ingenio Learning (s.f.) ITIL ¿Cómo hacer una auditoría informatica? https://ingenio.edu.pe/blog/itil-como-hacer-una-auditoría-informatica/

ISO. (s.f.). ABOUT US. Recuperado el 01 de septiembre de 2022 de https://www.iso.org/about-us.html

ISO (1997). *Friendship Among Equals, Recollections from ISO,s first fifty years*. ISO CENTRAL SECRETARIAT. https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/docs/en/Friendship_among_equals.pdf

ISO 25000. (s.f.). ISO 25000 calidad de software y datos. https://iso25000.com/index.php/normas-iso-25000

ISO 27000. (2005). SGSI. Recuperado el día 31 de agosto de 2022 de https://www.iso27000.es/sgsi.html

ITIL 4. (s.f.) ¿Qué es ITIL? https://www.itil.com.mx/

ITU. (2010). La evolución hacia los sistemas móviles – balance. https://www.itu.int/itunews/issue/2003/06/thirdgeneration-es.html

Kaspersky Daily. (2015). Telegraph [Fotografía]. https://latam.kaspersky.com/blog/telegraph-grandpa-of-internet/5641/

Laine, J., Minkkinen, M. y Mäntymäki, M. (2024). Ethics-based AI auditing: A systematic literature review on conceptualizations of ethical principles and knowledge contributions to stakeholders. Information & Management.

Liberatori, M. C. (2018). Redes de datos y sus protocolos. Eudem.

Macrovector (21 de noviembre de 2023). Freepik. Imagen de licencia libre. **https://www.freepik.com/free-vector/data-center-isometric-flowchart_4267665.htm#query=red%20wan&position=30&-from_view=search&track=ais&uuid=aff126de-c550-48a6-a751-16c91c16d069**

Mestari, S. Z., Lenzini, G. y Demirci, H. (2024). Preserving data privacy in machine learning systems. Computers & Security.

Microsoft. (2023). ¿Qué es la computación cuántica? https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-quantum-computing

Minaya. M. M., Minaya, R. W., Intriago, M. L., Intriago, J. A. (2023). Normas y Estándares en Auditoría: Una Revisión de su Utilidad en la Seguridad Informática. *PENTACIENCIAS*, 5(4), 584-59. https://www.editorialalema.org/index.php/pentaciencias/article/view/700/975

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía de Auditoría, Seguridad y Privacidad de la Información. https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoría.pdf

Moeller, R. (2010). It Audit, Control and Security. John Wiley & Sons, Inc.

Museo de Informática García Santesmase. (2021). *IMB System 360/65* [Fotografía]. https://www.fdi.ucm.es/migs/catalogo/ibm_system_360_65/

Museo de Informática García Santesmase. (2021). Apple II plus [Fotografía]. https://www.fdi.ucm.es/migs/catalogo/apple_ii_plus/

Normas ISO (s.f.). *Obtener un certificado ISO*. Recuperado el día 31 de agosto de 2022 de https://www.normas-iso.com/certificacion-iso/

Norma ISO 27001 (s.f.). *Referencias Normativas ISO 27000*. Recuperado el día 31 de agosto de 2022 de https://normaiso27001.es/referencias-normativas-iso-27000/#ISO27000

Piattini, M. G. y del Peso E. (2001). *Auditoría en Informática, un enfoque práctico*. Alfaomega Grupo Editor, S.A de C.V.

Pinilla, J. D. (1997). Auditoría informática: Aplicaciones en producción. Ecoe.

Oficina de Información Científica y Tecnológica para el Congreso de la Unión. (2018). Los Datos Masivos (Big Data). https://www.forocon-sultivo.org.mx/INCyTU/documentos/Completa/INCYTU_16-001.pdf

Oracle. (2023). ¿Qué es el Big Data? https://www.oracle.com/mx/big-data/what-is-big-data/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2023). La Inteligencia Artificial. https://unesdoc.unesco.org/ark:/48223/pf0000386262

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2021a). Las TIC y las sociedades del conocimiento. https://es.unesco.org/indigenous-peoples/icts

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2021b). La tecnología en la educación. https://unesdoc.unesco.org/ark:/48223/pf0000378951_spa

Oyinkansola, B. (2022). The impact of AI on Cloud Auditing, transforming practices and ensuring compliance. Finance & Accounting Research Journal, 4(6), 350-370. https://doi.org/10.51594/farj.v4i6.1316

Qureshi, M. A. (2020). Auditoría de tecnologías emergentes: Afrontar los desafíos de la nueva era. ISACA.

Ramírez, L. (2016). Auditoría Informática. Recuperado el 10 de octubre de 2021 de https://es.scribd.com/document/473062757/Auditoría-Informatica-pdf

Ranchal, J. (2018). 25 años de Mosaic, el navegador que iluminó la Web. https://www.muycomputer.com/2018/04/24/25-anos-de-mosaic/#:~:text=Mosaic%2C%20el%20primer%20navegador%20web,la%20web%20era%20principalmente%20texto.

Real Academia Española. (s.f.). Auditoría. En *Diccionario de la lengua española.* Recuperado el 04 de diciembre de 2022, de https://dle.rae.es/auditor%C3%ADa

Real Academia Española. (s.f.). Certificación. En *Diccionario de la lengua española*. Recuperado el 21 de agosto de 2022, de https://dle.rae.es/certificaci%C3%B3n?m=form

Real Academia Española. (s.f.). Hardware. En *Diccionario de la lengua española*. Recuperado en 10 de julio de 2023, de https://dle.rae.es/hardware

Real Academia Española. (s.f.). Informática. En *Diccionario de la lengua española*. Recuperado en 05 de julio de 2023, de https://www.rae.es/drae2001/inform%C3%A1tica

Real Academia Española. (s.f.). Internet. En *Diccionario de la lengua española*. Recuperado en 05 de julio de 2023, de https://dle.rae.es/internet?m=form

Real Academia Española. (s.f.). Método. En *Diccionario de la lengua española*. Recuperado en 03 de septiembre de 2022, de https://dle.rae.es/m%C3%A9todo?m=form

Real Academia Española. (s.f.). Metodología. En Diccionario de la lengua española. Recuperado en 03 de septiembre de 2022, de https://dle.rae.es/metodolog%C3%ADa?m=form

Real Academia Española. (s.f.). Software. En Diccionario de la lengua española. Recuperado en 10 de julio de 2023, de https://dle.rae.es/software?m=form

Real Academia Española. (s.f.). Teléfono. En Diccionario de la lengua española. Recuperado en 05 de octubre de 2023, de https://dle.rae.es/tel%C3%A9fono?m=form

Real Academia Española. (s.f.). Telégrafo. En Diccionario de la lengua española. Recuperado en 05 de octubre de 2023, de https://dle.rae.es/tel%C3%A9grafo

Rodríguez, I. (17 de Mayo de 2024). Inteligencia Artificial: Un catalizador para la innovación en la auditoría. https://www.auditool.org/blog/auditoría-de-ti/inteligencia-artificial-un-catalizador-para-la-innovacion-en-auditoría

Sayid, H. (3 de Febrero de 2023). Cómo realizar una auditoría de IA en 2023. Obtenido de https://www.unite.ai/es/c%C3%B3mo-realizar-una-auditor%C3%ADa-de-inteligencia-artificial-en-2023/

Sánchez, L. R. (s.f.). El derecho informático: protector de nuevos derechos. http://www.ordenjuridico.gob.mx/Congreso/pdf/85.pdf

Tanenbaum, A. (2000). Organización de computadoras un enfoque estructurado. México. Pearson Educación.

TecnoMagazine (2023). Tipos de software. https://tecnomagazine.net/tipos-de-software/

Tecnología + informática. (s.f.). Historia de la Computadora: ENIAC [Fotografía]. https://www.tecnologia-informatica.com/historia-de-la-computadora-eniac/

Trigo, V. (s.f.). Historia y evolución de Internet. **https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf**

Worldsys. (2023). ¿Qué es el modelo COSO? https://www.worldsys.co/que-es-el-modelo-coso/

Anexos

Respuestas Ejercicio Capítulo 2.

1. (C).
2. (H).
3. (A).
4. (J).
5. (B).
6. (F).
7. (D).
8. (G).
9. (E).
10. (I).
11. (L).
12. (K)

Respuestas Ejercicio Capítulo 3.

1. (I).
2. (G).
3. (A).
4. (J).
5. (C).
6. (D).

7. (B).
8. (E).
9. (H).
10. (F).

Respuestas Ejercicio Capítulo 4.

1. V
2. V
3. F
4. V
5. V
6. V
7. F

Respuestas Ejercicio Capítulo 5.

1. V
2. V
3. F
4. V
5. F
6. V
7. V

Respuestas Ejercicio Capítulo 6.

1. (H).
2. (A).
3. (F).
4. (I).
5. (J).
6. (C).
7. (B).
8. (G).

9. (E).
10. (D).

Respuestas Ejercicio Capítulo 8.

1. V
2. V
3. F
4. V
5. V
6. V
7. F
8. V
9. V
10. F

Un estudio contemporáneo de la auditoría en informática
Se terminó de editar en diciembre de 2024
en los talleres de Astra Ediciones
Av. Acueducto No. 829
Colonia Santa Margarita, C. P. 45140
Zapopan, Jalisco, México.
33 38 34 82 36
E-mail: edicion@astraeditorial.com.mx
www.astraeditorialshop.com

Estudiar esta disciplina del conocimiento de la auditoría del uso de las TIC, es asimilar e indagar el conocimiento y operación de una práctica esencial que se orienta a la evaluación de la eficacia, la administración y el desempeño de riesgos en los sistemas de la información implementados mediante las TIC. Implica afrontar el reto que representa describir las complejidades de la auditoría en el contexto de las TIC y brindar información valiosa para profesionales, auditores y tomadores de decisiones que buscan navegar con confianza en los cambiantes paisajes digitales.

ISBN: 979-13-87631-35-2

Consulta y descarga

astra editorial