UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"PLANIFICACIÓN DE AUDITORÍA DE SISTEMAS APLICABLES A LA EVALUACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN EN LOS ENCARGOS DE AUDITORÍA"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

ALFARO, MANUEL DE JESÚS

ANTILLÓN MORAN, EMANUEL ARMANDO

CARRILLO CENTENO, SERGIO GIOVANNI

PARA OPTAR AL GRADO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA

ABRIL, 2021

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:	Msc. Roger Armando Arias Alvarado
Secretario General	:	Ing. Francisco Antonio Alarcón Sandoval
Decano de la Facultad de Ciencias Económicas	:	Msc. Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas	:	Licda. Vilma Marisol Mejía Trujillo
Director de la Escuela de Contaduría Pública	:	Lic. Gilberto Díaz Alfaro
Coordinador General de Seminario De Graduación	:	Lic. Mauricio Ernesto Magaña Menéndez
Coordinación de Seminario De Procesos de Graduación de la Escuela de Contaduría Pública	:	Lic. Daniel Nehemías Reyes López
Docente Director	:	Lic. Carlos Ernesto Ramírez
Jurado Evaluador	:	Lic. Daniel Nehemías Reyes López
	:	Lic. Abraham de Jesús Ortega Chacón
	:	Lic. Carlos Ernesto Ramírez

ABRIL, 2021

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AGRADECIMIENTOS

Agradezco a Dios por la fortaleza y acompañarme en mi camino para poder culminar mis estudios y por bendecirme de salud y empleo para continuar avanzando cada día, a mi familia por ese ánimo que me dieron durante los años de estudio, por la paciencia y comprensión, gracias por sus oraciones, en especial a mi esposa Martha Alicia Trejos de Alfaro, a mi hija Alexia Elizabeth Alfaro Trejos y a mi abuela María Delfina de Aguilar, amigos y compañeros por ese apoyo y ánimo que me dieron para que terminara mis estudios.

"Alfaro, Manuel de Jesús"

Agradezco a Dios por darme la bendición de celebrar este logro de mi vida profesional junto a mi familia y amigos, y dedico este triunfo a mis padres que estuvieron conmigo en los momentos más difíciles apoyándome en cada decisión que he tomado para forjar mi camino hasta este momento de mi vida. A mi esposa que me motivó y me dio las palabras de aliento necesarias para seguir adelante y dar todo de mí. A mi hijo que me ha inspirado a ser un hombre de bien y darle el mejor ejemplo a seguir, a todos que en mis años estudios conocí muchas gracias.

"Antillón Moran, Emanuel Armando"

La gloria sea para Dios; quien representa todo en mi vida y que sin él no hubiese sido posible lograr este objetivo en mi vida profesional, dedico este triunfo a mi abuela Santos Miranda de Carillo, quien junto a mi esposa Griselda Yaneth Andrés Vásquez, mis hermanos me brindan todo su amor, apoyo moral y espiritual. A mis hijas Alison Carillo y Yanci Carillo; quienes son la inspiración de mi vida y razón por la cual proyecto metas y objetivos. A la Universidad de El Salvador; agradeciendo a maestros, asesores y a mis compañeros de trabajo de investigación por el apoyo y conocimiento brindado.

"Carillo Centeno, Sergio Giovanni"

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ANEXOS

RESUMEN EJECUTIVO

La presente investigación se desarrolló en la firma de auditoría L GROUP, S. A. de C. V. la cual presta sus servicios de auditoría de sistemas, financiera, fiscal y asesorías, las auditorías de sistemas representan un aumento significativo en la complejidad de las operaciones y registros a los que el encargado de auditoría debe prestarles mayor atención y revisar. Debido a lo anterior, se tomó a bien realizar un memorándum de planificación de auditoría de sistemas basada en la evaluación de las tecnologías de información y comunicación, considerando identificar las áreas de mayor riesgo en las revisiones realizadas y disminuirlos a un nivel aceptablemente bajo, se proporcionará al auditor de sistemas un instrumento que facilite su labor en la realización de encargos de esta naturaleza.

La auditoría a las tecnologías de información y comunicaciones, consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos.

La investigación desarrollada permite afirmar que existen diferentes problemas a los que se enfrentan al desarrollar las auditorías de sistemas para evaluar las tecnologías de información y comunicación, así como también los problemas a los que se enfrentan con el control interno que están desarrollados actualmente enfocados en las TICs.

Dentro de las áreas críticas para este tipo de encargos están las relacionadas con el rubro de hardware, software, seguridad lógica, seguridad física, redes, telecomunicaciones y procesamiento electrónico de datos, y aquellas referentes a los aspectos de integridad, confidencialidad y disponibilidad de la información; ya que los sistemas electrónicos y la

infraestructura que da soporte son susceptibles de situación de abuso, mal uso y fallas en muchas formas debido a lo complejo de su naturaleza.

Para la recolección de datos en la investigación se utilizó como instrumento la entrevista estructurada, cuestionario de preguntas abiertas las cuales fueron hechas a la socia directora y a la gerente de tecnologías de información y comunicación de la firma L GROUP, S.A. DE C.V., con el objetivo de obtener información sobre el uso de las tecnologías de la información en los encargos de auditoría de sistemas, lo que permitió concluir que la población en estudio está interesada en los procedimientos de auditoría de sistemas para evaluar las tecnologías de información y comunicación en sus encargos; ya que además pretende ser un instrumento útil y novedoso para la población de auditores y para el enriquecimiento de la profesión de la Contaduría Pública.

Por tal razón se considera importante proporcionar una guía de lineamientos y procedimientos en la ejecución de auditoría de sistemas a las tecnologías de información y comunicación.

INTRODUCCIÓN

La auditoría de sistemas ha cobrado mayor relevancia y demanda en la actualidad, y es necesario el resguardo de las tecnologías que poseen las entidades, pero su control y su resguardo es cada vez más compleja. Es por ello que la presente investigación se sustenta en la presentación de una propuesta que sirva de guía para la aplicación en el área de auditoría de sistemas, con base a normativa técnica aplicable en las tecnologías de información y comunicación (TICs), los cuales se espera sean aplicados en la ejecución de auditorías de sistemas, y que este memorándum de planificación facilite su ejecución.

Por lo anterior se desarrolla en tres capítulos. En el capítulo I se detalla el marco teórico, que comprende una descripción de la situación actual de la problemática, las principales definiciones, la legislación aplicable y la normativa técnica correspondiente al área investigada.

El siguiente apartado, el capítulo II, desarrolla el diseño metodológico de la investigación en el cual se puntualiza el enfoque y tipo de investigación, la unidad de análisis, así como también el universo y la población, se especifica además los instrumentos y técnicas a utilizar, el análisis e interpretación de los datos, y finalmente el diagnóstico de la investigación.

En el capítulo III, se desarrolla la propuesta de solución, en donde se presenta un memorándum de planificación de auditorías de sistemas basadas en la evaluación de las tecnologías de información y comunicación, el cual está bajo marco de referencia COBIT® 2019 y las normas ISO 27000, en él se describen los procedimientos para la planificación de auditoría de sistemas.

Finalmente se presentan las conclusiones y recomendaciones necesarias para aplicar y fortalecer la propuesta de solución desarrollada. Cabe mencionar que se presenta una bibliografía utilizada y anexos que sustentan el desarrollo de la problemática en estudio.

CAPÍTULO I. MARCO TEÓRICO, CONCEPTUAL, TÉCNICO LEGAL

1.1. SITUACIÓN ACTUAL DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

En la actualidad la tecnología se ha convertido en un activo muy importante, sobre todo cuando crece la dependencia hacia ellos, ha potenciado la aparición de la auditoría de sistemas como un servicio orientado a garantizar, no solo la salvaguarda de estos activos sino también la utilidad que estos reportan.

Los servicios de auditoría de sistemas, hoy en día no se encuentran excesivamente difundidos, el éxito demostrado en las experiencias obtenidas, va repercutiendo en una mayor proliferación de estos servicios.

El auditor externo ha de velar por la correcta utilización de los amplios recursos para disponer de un eficiente y eficaz sistema de información.

Las condiciones actuales en las que se desempeña un auditor externo y el contexto normativo que regula la profesión, exigen que haya un grado de conocimiento en el ámbito de las tecnologías de información, considerando a estas como un componente de un sistema de información dentro de las empresas; en tal sentido, resulta importante tomar en cuenta aspectos generales como el concepto, componentes, tipos, fases y técnicas de evaluación de los sistemas de información, para relacionar la teoría de todos estos temas con los requerimientos normativos de la práctica de auditoría de estados financieros.

Como parte de su trabajo de auditoría es responsabilidad del auditor externo determinar la posible existencia de riesgos generados por incumplimiento de normativas legales de la entidad auditada y evaluar su posible impacto a fin de diseñar los procedimientos adicionales en respuesta a tales riesgos.

1.1.1. Antecedentes

- **De las tecnologías de información y comunicación**

A nadie sorprende estar informado minuto a minuto, comunicarse con personas del otro lado del planeta, ver el video de una canción o trabajar en equipo sin estar en un mismo sitio. Las TICs se han convertido, a una gran velocidad, en parte importante de nuestras vidas. Este concepto que también se llama sociedad de la información se debe principalmente a un invento que apareció en 1969: el internet se gestó como parte de la red de la agencia de proyectos de investigación avanzada, creada por el departamento de defensa de Estados Unidos y se diseñó para comunicar a los diferentes organismos del país

Sus principios básicos eran: ser una red descentralizada con múltiples caminos entre dos puntos y que los mensajes estuvieran divididos en partes que serían enviadas por caminos diferentes. La presencia de diversas universidades e institutos en el desarrollo del proyecto hizo que se fueran encontrando más posibilidades de intercambiar información. Posteriormente se crearon los correos electrónicos, los servicios de mensajería y las páginas web. Pero no es hasta mediados de la década de los noventa -en una etapa en la que ya había dejado de ser un proyecto militar- cuando se da la verdadera explosión de internet. Y a su alrededor todo lo que conocemos como TICs.

El desarrollo de Internet ha significado que la información esté ahora en muchos sitios. Antes la información estaba concentrada, la transmitía la familia, los maestros, los libros. La escuela y la universidad eran los ámbitos que concentraban el conocimiento. Hoy se han roto estas barreras y con Internet hay más acceso a la información. El principal problema es la calidad de esta información. También se ha agilizado el contacto entre personas con fines sociales y de negocios. No hace falta desplazarse para cerrar negocios en diferentes ciudades del mundo o para realizar transacciones en cualquier lugar con un sencillo clic.

En parte, estas nuevas tecnologías son inmateriales, ya que la materia principal es la información; permiten la interconexión y la interactividad; estas son instantáneas; tienen elevados parámetros de imagen y sonido. Al mismo tiempo, las nuevas tecnologías suponen la aparición de nuevos códigos y lenguajes, la especialización progresiva de los contenidos sobre la base de la cuota de pantalla (diferenciándose de la cultura de masas) y dando lugar a la realización de múltiples actividades en poco tiempo.

La adopción de TICs en las empresas se ha sucedido en etapas. Si bien con altas y bajas, en general las grandes empresas han mantenido las inversiones en sistemas de soporte a sus funciones empresariales desde hace varias décadas, por ejemplo, en sistemas de intercambio electrónico de datos (EDI – Electronic Data Interchange).

En cierta medida las grandes empresas han señalado (y lo siguen haciendo) el camino a las empresas de menor tamaño. Con la simplificación y reducción de los costes de la tecnología, los servicios que antes estaban al alcance de las grandes empresas- poco a poco se han difundido a medianas y hasta pequeñas empresas. Es verdad que también hubo fracasos en las estrategias de grandes empresas, especialmente durante el boom de Internet de los años 90’s, pero los errores (y las pérdidas) fueron rápidamente absorbidos y sus lecciones incorporadas en mejores prácticas.

Los avances científicos en el campo de la electrónica tuvieron dos resultados inmediatos: la caída vertiginosa de los precios de las materias primas y la preponderancia de las tecnologías de la información, que combinaban esencialmente la electrónica y el software.

Pero, las investigaciones desarrolladas a principios de los años 80 han permitido la convergencia de la electrónica, la informática y las telecomunicaciones, posibilitando la interconexión entre redes. De esta forma, las TICs se han convertido en un sector estratégico para la "Nueva economía".

Desde entonces, los criterios de éxito para una organización o empresa dependen cada vez en gran medida de su capacidad para adaptarse a las innovaciones tecnológicas y de su habilidad para saber explotarlas en su propio beneficio empresarial.

- **De la asociación de auditoría y control de sistemas de la información (ISACA)**

Information Systems Audit and Control Association (ISACA) es una asociación profesional internacional cuyo objetivo principal es la promoción de la capacitación profesional para el desarrollo y la optimización del conocimiento y las habilidades relacionadas con la auditoría y la seguridad en el campo de las Tecnologías de la Información y las Comunicaciones (TICs).

ISACA comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares de auditar controles en los sistemas computacionales que se estaban haciendo cada vez más críticos para las operaciones de sus respectivas organizaciones se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TICs.

Hoy, los miembros de ISACA son más de 95,000 en todo el mundo se caracterizan por su diversidad. Los miembros viven y trabajan en más de 160 países y cubren una variedad de puestos profesionales relacionados con TICs sólo por nombrar algunos ejemplos, auditor de Sistemas de Información, consultor, profesional de la educación, profesional de seguridad de Sistemas de Información, regulador, director ejecutivo de información y auditor interno. Algunos son nuevos en el campo, otros están en niveles medios de la gerencia y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias,

incluyendo finanzas y banca, firmas de auditoría y consultoría, gobierno y sector público, servicios públicos y manufactura. Esta diversidad permite que los miembros aprendan unos de otros, e intercambien puntos de vista comunes sobre una variedad de tópicos profesionales. Esta ha sido considerada durante mucho tiempo como una de las fortalezas de ISACA. Previamente conocida como la asociación de auditoría y control de sistemas de la información, ISACA ahora identificada ya por su acrónimo, para reflejar el amplio rango de profesionales del gobierno de las TICs a los que sirve.

1.1.2. Importancia

- **En las empresas**

En las empresas, las TIC aumentan la productividad de los trabajadores, optimizan la toma de decisiones, mejoran la colaboración en equipos y realizan tareas de riesgo. Por ejemplo: los empleados pueden trabajar desde cualquier lugar (en un autobús o avión, en su hogar, en la oficina de los clientes) mediante computadoras portátiles. Los gerentes pueden dictar mensajes directamente a su computadora personal y enviarlos por correo electrónico a sus colegas o jefes en segundos.

- **En la contabilidad**

El impacto que ha tenido la tecnología en el área de la contabilidad, está fuera de toda duda. Las tecnologías de información operan como motor de cambio que permite dar respuestas a las nuevas necesidades de información actualmente el área de contabilidad y fiscal ha dado un giro importante en el uso de la tecnología de información, debido a que anteriormente se realizaba la contabilidad sin ningún tipo de paquete computacional, y ahora podemos encontrar paquetes contables desarrollados especialmente para estas áreas.

La aparición de la informática ha supuesto una revolución en la contabilidad. La creación de programas contables específicos en un entorno Windows, acercó las aplicaciones informáticas al usuario, haciendo que fueran más fáciles de utilizar y más versátiles.

El siguiente paso, fue la revolución de las comunicaciones, especialmente de Internet, así como la ampliación del abanico de posibilidades de la contabilidad a actividades tales como la banca electrónica y el envío de declaraciones fiscales por Internet (que por otro lado se han convertido recientemente en obligatorios para las grandes empresas en algunas declaraciones), que facilitaron el intercambio de datos con mayor facilidad, fiabilidad y rapidez. Hay que señalar, además, que el nacimiento y posterior regulación de la firma electrónica reconocida como medio de autenticar los mensajes enviados haciendo muy difícil su falsificación, incrementa en gran medida el interés de las nuevas TIC.

- **En la contaduría pública**

En el pasado la información contable de interés para la organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, informes financieros, procesos u operaciones contables quedaban registrados en papel, con todos los problemas que luego acarrea su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesamiento. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación.

Es por ello que se determina el uso de las TICs para los procedimientos y salvaguardas de las operaciones contables enfocadas a empresas de comercio, por lo que se verá el impacto que generó la implementación de éstas en la contabilidad, y la trascendencia que marcó para el manejo de la información financiera.

1.1.3. De la auditoría de sistemas

La palabra auditoría viene del latín “auditorius” y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

La mayor preocupación de los auditores hoy en día, en especial los que no son auditores de sistemas de información, y algunos de éstos también, es poder utilizar el computador para realizar las auditorías "por dentro del mismo", en la revisión de los datos que contiene; y no se han dado cuenta todavía, (a pesar de estar tan avanzada esta especialización, tanto en métodos, técnicas, pronunciamientos, tecnología, y herramientas, así como en el tiempo), que ésta tarea es muy sencilla y que, más que todo es parte sustancial de la auditoría financiera.

1.2. MARCO CONCEPTUAL

Se ha considerado de suma importancia el establecimiento de sus definiciones que ayuden a comprender el desarrollo de la presente investigación:

- **Auditoría a las tecnologías de información y comunicación:** consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos.

- **Delito informático:** se considerará la comisión de este delito, cuando se haga uso de las tecnologías de la información y la comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información.

- **Datos informáticos:** es cualquier representación de hechos, información o conceptos en un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los datos.

- **Marco de referencia COBIT® 2019:** es un marco de referencia de Gobierno de TICs y un conjunto de herramientas de soporte que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Además, permite el desarrollo de una política clara y una buena práctica para el control de TICs en las organizaciones. El marco acentúa el cumplimiento regulatorio, ayuda a las organizaciones a incrementar el valor asociado al área de TICs, habilita la alineación y simplifica la puesta en práctica del marco de referencia.

- **Procedimiento de auditoría de sistemas:** se le da el nombre de procedimientos de auditoría en sistemas. El conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que sirven para fundamentar la opinión del auditor dentro un encargo de auditoría.

- **Riesgos de tecnología:** se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la institución y soporten el cumplimiento de la misión.

- **Sistemas de información:** cuando se habla de un sistema de información (SI) se refiere a un conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente.

- **Tecnologías de información y comunicación:** son el conjunto de tecnologías desarrolladas en la actualidad para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas, TIC es la abreviatura de tecnologías de la información y la comunicación.

1.3. MARCO TÉCNICO

En la tabla 1 se muestra los aspectos técnicos relacionados a las prácticas para auditoría y aseguramiento de las tecnologías de información.

Tabla No.1

Marco de Prácticas Profesionales para Auditoría y Aseguramiento de Tecnologías de Información ITAF

Referencia	Descripción
Estándar 1003 Lineamiento 2003	Los profesionales de auditoria y aseguramiento de SI deben ser independientes y objetivos, tanto en actitud como en apariencia.
Estándar 1004 Lineamiento 2004	Expectativa Razonable: los profesionales de auditoria y aseguramiento de SI deben tener una expectativa razonable de que la asignación puede ser realizada de conformidad con los estándares de auditoria y aseguramiento de SI y, cuando se requiera, otros estándares adecuados o regulaciones aplicables, y brindar una conclusión u opinión profesional. - Opinión no Calificada. - Opinión Calificada. - Opinión adversa.
Estándar 1006 Lineamiento 2006	Los profesionales de auditoria y aseguramiento de SI, junto con otras personas que ayudan en la asignación, deben poseer las habilidades y competencias adecuadas para realizar las asignaciones de auditoria y aseguramiento de SI y ser profesionalmente aptos para realizar el trabajo requerido.
Estándar 1201 Lineamiento 2201	Los profesionales de auditoria y aseguramiento de SI, deben tener el nivel mínimo de desempeño para planificar cada asignación abordada. - Objetivo, alcance, cronograma. - Cumplimiento con los estándares de auditoria profesional y la ley aplicable para este tipo de empresas. - Uso de un enfoque basado en riesgos que sea apropiado al sector. - Problemas específicos a la asignación del personal con conocimiento del rubro. - Requerimientos de reportes y documentación.

Estándar 1202 Lineamiento 1202	Al planificar una asignación individual, los profesionales en auditoria en SI deben: - Identificar una vez al año riesgos relevantes para facilitar el desarrollo del plan de auditoria. - Realizar una evaluación preliminar de los riesgos, objetivos, planes estratégicos organizacionales a nivel aceptable. - Considerar las áreas de riesgo y planificar una acción específica para cada tipo de servicio. - Intentar reducir el riesgo a un nivel aceptable y cumplir con los objetivos de la auditoria.
Estándar 1204 Lineamiento 2204	Los profesionales de auditoria y aseguramiento de SI deben considerar las debilidades potenciales o ausencia de controles mientras planifican una asignación y si esas debilidades o ausencias de controles pudieran resultar en una deficiencia significativa o una debilidad material. También deben de considerar la materialidad de la auditoria y su relación con el riesgo de auditoria, determinando a su vez, la naturaleza, los plazos y el alcance de los procedimientos.
Evaluación de riesgo	Un proceso utilizado para identificar y evaluar riesgos y sus posibles efectos. Las evaluaciones de riesgo se utilizan para identificar aquellos temas o áreas de mayor riesgo.
	Obtención de pruebas de auditoria de sistemas sobre la integridad, exactitud o existencias de actividades o transacciones durante el periodo de la ejecución.
	Fases de la planificación de auditoria de sistemas. - Objetivos de la planificación de auditoria de SI. - Evaluación de control interno. - Identificación de áreas críticas del sector. - Evaluación de riesgo informático. - Programas de auditoria. - Personal asignado.

Nota: Comité de gestión de carreras y estándares profesionales de ISACA

En la tabla 2 se muestra los aspectos importantes de la normativa internacional de formación para contadores profesionales.

Tabla No. 2

Normas Internacionales de Formación

Marco de referencia	Descripción	Comentarios
IES 1:	Requisitos de ingreso a un programa de formación profesional en contaduría.	Establece los requisitos para el ingreso a un programa de formación profesional en contaduría y experiencia práctica que debe ser exigido por un organismo miembro de IFAC.
IES 2:	Contenido de los programas profesionales de formación en contaduría	Prescribe el contenido de los programas profesionales de formación en contaduría que los aspirantes deben adquirir para ser calificados como contadores profesionales.
IES 3:	Habilidades profesionales y formación general	Prescribe el conjunto de destrezas que los aspirantes necesitan adquirir para ser reconocidos como contadores profesionales.
IES 4:	Valores, ética y actitud profesionales	Prescribe los valores, ética y actitudes profesionales que los futuros contadores profesionales deberán adquirir antes de finalizar su programa de calificación profesional.
IES 5:	Requisitos de experiencia práctica	Prescribe la experiencia práctica que los organismos miembros de IFAC deben requerir a sus asociados para poder ser contadores profesionales.
IES 6:	Evaluación de las capacidades y competencia profesional	Establece los requisitos para una evaluación final de las capacidades y la competencia de un pasante antes de la calificación como contador profesional.
IES 7:	Desarrollo profesional continuo: Un programa de aprendizaje permanente y desarrollo continuo de la competencia profesional	Fomentar el compromiso de aprendizaje permanente entre los contadores profesionales, facilitar el acceso a oportunidades de desarrollo profesional continuo (DPC), Controlar y hacer cumplir el desarrollo profesional continuo y mantenimiento de las competencias profesionales por los contadores profesionales.

IES 8:	Requisitos de la competencia que deben reunir los auditores profesionales	Establece requisitos de competencia para los auditores profesionales, incluyendo aquellos que trabajan en entornos e industrias específicas. Los organismos miembros de IFAC necesitan establecer políticas y procedimientos que permitan a sus asociados satisfacer los requerimientos de esta IES antes de desempeñar el papel de auditor profesional.

Nota: Consejo de Normas Internacionales de Formación en Contaduría (IAESB) de la Federación Internacional de Contadores (IFAC)

En la tabla 3 se muestra los aspectos importantes de la normativa internacional de auditoria NIA.

Tabla No. 3

Normas Internacionales de Auditoría NIA

Marco de referencia	Descripción	Comentarios
Norma Internacional de Control de Calidad	NICC 1 - Control de calidad en las firmas de auditoría que realizan auditorías y revisiones de estados financieros, así como otros encargos de que proporcionan un grado de seguridad y servicio relacionado	Se considerará en lo que corresponde a la responsabilidad de adoptar un sistema de control de calidad para las auditoría y revisiones
Normas Internacionales de Auditoría	NIA 210 - Términos de los trabajos de auditoría	Se tomará como referencia para los acuerdos y responsabilidades de los encargos de auditoría durante la etapa de planeación
	NIA 260 - Comunicación con los responsables del gobierno de la entidad	El criterio a aplicar corresponde a la comunicación recíproca y eficaz en la medida en que las circunstancias lo requieran durante el transcurso de la auditoría
	NIA 265 - Comunicación de las deficiencias en el control interno a los responsables del gobierno y a la dirección de la entidad	Se utilizarán las vías de comunicación de las inconsistencias y errores identificados durante la auditoría y de control de calidad, de forma adecuada a los responsables del gobierno de la entidad
	NIA 300 - Planificación de la auditoría de estados financieros	Se identificarán las áreas importantes a evaluar para resolver problemas de forma oportuna, con el fin de facilitar la selección de los miembros del equipo de auditoría
	NIA 315 - Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno	Se aplicará procedimientos, en la etapa de planificación, para conocer a la entidad y su entorno, con el fin de prever y proporcionar respuestas acordes a las necesidades de cada cliente

NIA 330 - Respuesta del auditor a los riesgos valorados	Se aplicarán procedimientos de controles y procedimientos sustantivos acorde a los riesgos valorados previamente, para la obtención de evidencia suficiente y adecuada, y otorgar respuestas precisas a los riesgos identificados
NIA 620 - Utilización del trabajo de un experto del auditor	Identificando los riesgos, y tener un entendimiento de la entidad y su entorno, el auditor considerará si es necesario la utilización de un experto para el cumplimiento de los objetivos del encargo de auditoría.

Nota: Normas Internacionales de Auditoría (NIA) emitidas por la Federación Internacional de Contadores (IFAC).

En la tabla 4 se muestra los aspectos éticos que un auditor debe de cumplir para los encargos de una auditoria de sistemas para evaluar las TICS

Tabla No. 4

Código de Ética Profesional para Auditores y Contadores

Marco de referencia	Descripción	Comentarios
Código de Ética Profesional para Auditores y Contadores	Art.	El auditor debe de regir su conducta con ética, con el fin de proporcionar un servicio de calidad y manteniendo la independencia profesional. Los auditores y contadores en el ejercicio de sus funciones, implementarán las normas y principios éticos contenidos en el presente código, debiendo cumplir con las obligaciones, atribuciones y funciones que el mismo les establece, así como las de las Leyes y normativa técnica aplicable. Cuando se haga referencia a auditor o contador, se entenderá que la obligación es para ambos dentro del límite de sus funciones; si es un auditor ejerciendo como contador, se entenderá como obligado hasta el límite de las funciones para las que ha sido contratado. En el ejercicio de sus funciones, los contadores públicos deberán observar el cumplimiento de los principios siguientes: I. Independencia II. Preparación del profesional III. Calidad profesional de los servicios IV. Responsabilidad personal V. Secreto profesional VI. Faltará al honor y dignidad profesional todo auditor o contador VII. El auditor o contador debe evitar actuaciones que puedan perjudicar a quien haya contratado sus servicios. VIII. Retribución económica

Nota: Diario oficial, tomo N. 422, San Salvador, miércoles 27 de febrero de 2019

En la tabla 5 se muestra el marco de referencia COBIT 2019 para evaluar las TICS.

Tabla No. 5

Marco de referencia COBIT 2019

Marco de referencia	Descripción	Comentarios
COBIT 2019	Marco de referencia: introducción y metodología	Es el marco de referencia a aplicar para la evaluación y distinción del gobierno de una entidad y la gerencia, desarrollando procedimiento de auditoría para elementos de TI enfocado en ambas áreas
	Marco de referencia: objetivos de gobierno y gestión	Es el marco de referencia para la ejecución de procedimientos de evaluación de procesos, estructuras organizacionales, políticas, PED, infraestructura y servicios relacionados con las TICs de la entidad.
COBIT 2019	Principios de Covid 2019:	1- Satisfacer las necesidades de las partes interesadas. 2- Cubrir la empresa extrema a extremo. 3- Aplicar un marco de referencia único integrado. 4- Hacer posible un enfoque holístico 5- Separar el gobierno de la gestión

Nota: ISACA, antes conocida como la Asociación de Control y Auditoría de Sistemas de Información.

En la tabla 6 se muestra el marco normativo ISO 27001 Y 27002 para evaluar las TICS.

Tabla No. 6

ISO 27001 e ISO 27002

Marco de referencia	Descripción	Comentarios
ISO 27001	Sistema de gestión de seguridad informática	Al aplicar la ISO 27001 se tiene en consideración para la seguridad de un cargo: 1- Planificar: Definir políticas de seguridad 2- Hacer: Implantar el plan de gestión de riesgos 3 - Controlar: Realizar auditorías internas 4- Actuar: Adoptar acciones correctivas. El eje central de esta norma es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. La filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar donde están los riesgos y luego tratarlos sistemáticamente. Hay cuatro ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información: - Cumplir con los requerimientos legales. - Obtener una ventaja comercial. - Menores costos. - Una mejor Organización. El sistema de gestión de seguridad de la información está formado por cuatro fases que se deben implementar en forma constante. Las fases son las siguientes: - Fase de planificación. - Fase de Implementación. - Fase de revisión. - Fase de mantenimiento y mejora.
ISO 27002	Seguridad de la Información	Es una guía que sirve para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la Información. La seguridad de la información se define como la preservación de confidencialidad, integridad y disponibilidad. El estándar describe los dominios principales, 35 objetivos de control y 114 controles de ISO / IEC 27002. Por ejemplo:

1- Políticas de seguridad
2- Control de acceso
3- Gestión de activos
4- Seguridad física y ambiental

Nota: Organización Internacional de Normalización (ISO)

1.4. MARCO LEGAL

En la tabla 7 se muestra el marco legal relacionado a la evaluación de las tecnologías de información y comunicación.

Tabla No. 7

Normativa legal

Normativa	Artículo	Comentarios
Código Penal	184-185	El que por descubrir secretos vulnere la intimidad de otro, se apodera de comunicación escrita, soporte informático será sancionado con multas que van desde treinta hasta doscientos días multa.
	186-187	El que, con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiera una comunicación telefónica, grabación del sonido, la imagen o cualquier otra señal de comunicación, será sancionado con prisión.
	226-227	Será sancionado con prisión quien: usurpe la condición de autor sobre una obra o parte de ella, modificando sustancialmente la integridad de la obra, si la cantidad o el valor de la copia ilícita fuere de especial trascendencia económica.
	238	El que utilizare cualquier otro medio fraudulento capaz de ocasionar grave perjuicio a un competidor, con el fin de obtener para sí o para un tercero una ventaja indebida.
Ley Especial Contra los Delitos Informáticos y Conexos	1	La ley contra delitos informáticos y conexos fue creada con el propósito de proteger de forma jurídica las acciones consideradas como conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación.
	4	Acceso indebido a sistemas informáticos: será toda acción sin autorización acceda, intercepte total o parcialmente un sistema informático que utilice las tecnologías de información, será sancionado con prisión.
	7	El que destruya, dañe o realice cualquier otro acto que altere parcial o totalmente un sistema informático que utilice las tecnologías de información.

	13	El que se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, por medio del uso de las tecnologías de la información y la comunicación.
	15	Los administradores de las plataformas tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilice en todo o en parte cualquier información, dato contenido en un registro de acceso.
Ley de Regulación del Teletrabajo	1	El objeto de la ley es promover, armonizar, regular e implementar el teletrabajo como instrumento para generar empleo y modernización a través de la utilización de tecnologías de la información y comunicación.
	3	Se entenderá por teletrabajo una forma de desempeñar la relación de trabajo, fuera del centro de trabajo y utilizando como soporte las tecnologías de la información y la comunicación.
	6	La implementación del teletrabajo es estrictamente voluntaria tanto para el trabajador como para el patrono y debe existir un acuerdo entre las partes.
	9	Desempeñar el trabajo convenido, de acuerdo a las instrucciones que reciba del empleador, en la forma, tiempo y lugar autorizado.
Ley Especial Contra Actos de Terrorismo	12	Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley.

Nota: Ley Reguladora del Ejercicio de la Contaduría Pública, Recopilación de Leyes en Materia Tributaria, 28ª Edición, Lic. Luis Vásquez López.

En la tabla 8 se muestra el marco legal relacionado a la evaluación de las tecnologías de información y comunicación.

Tabla No.8

Ley Reguladora del Ejercicio de la Contaduría

Marco de referencia	Descripción	Comentarios
Art. 1 – Art. 6	Requisitos y sujeto de regulación	La ley estable quien o quienes se encuentran sujetos a la regulación de la ley y los requisitos para ejercer la profesión
Art. 7 – Art. 11	Requisitos formales	Detalla los requisitos de los registros, expediente y tramites de solicitud
Art. 12 – Art. 16	Autorizaciones, acreditaciones y restricciones	Se describe la inscripción en el consejo, emisión de sello para ejercer el ejercicio y la restricción de ejercer de forma ilegal
Art. 17 – Art. 23	Responsabilidad de los contadores públicos	Describe los trabajos que el auditor está obligado de ejercer su función, firma del responsable, honorarios, prohibiciones y tiempo de almacenamiento de los documentos

Nota: Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria (CVPCPA)

CAPÍTULO II. METODOLOGÍA DE LA INVESTIGACIÓN

2.1. ENFOQUE Y TIPO DE INVESTIGACIÓN

2.1.1. Enfoque de investigación

Por los medios utilizados para la obtención de información se consideró el enfoque cualitativo, la información se obtuvo de fuentes documentales, electrónicas y la aplicación de la técnica de recolección de información: la entrevista de la cual se retomaron los datos para hacer la respectiva tabulación.

En el enfoque de la investigación se evaluaron características en relación a las tecnologías de la información y comunicación en los encargos de auditoría, por ello se elaboraron procedimientos de auditoría de sistemas para que permita mitigar los problemas en los cuales se enfrenta el auditor externo, y que le ayude detectar hallazgo, minimizando así riesgos a niveles aceptables.

2.1.2. Tipo de investigación

La investigación se realizó mediante un estudio de tipo analítico descriptivo, que, a su vez, permitió analizar la problemática que enfrentan los profesionales en los encargos de la auditoría de sistemas, especialmente aplicable a la evaluación de las tecnologías de información y comunicación.

Se aplicó el método hipotético deductivo, el cual permitió estudiar los aspectos generales que fueron verificados a través de instrumentos confiables y llegar a conocimientos específicos por ello se estudiaron las deficiencias existentes en los encargos de auditoría para evaluar las tecnologías de información y comunicación, permitiendo detectar hallazgos y minimizar riesgos a niveles aceptables y plantear una alternativa de solución.

2.2. DELIMITACIÓN ESPACIAL Y TEMPORAL

2.2.1. Espacial

El estudio se realizó en la firma de auditoría L GROUP, S.A. DE C.V. la cual está ubicada en la colonia Escalón, municipio de San Salvador departamento de San Salvador, El Salvador.

2.2.2. Temporal

La investigación se realizó a partir de marzo de 2019 y finalizando el 12 de diciembre de 2020, fecha en el cual la firma de auditoría L GROUP, S.A. DE C.V. amplio e incursionó en sus encargos de auditoría de sistemas para evaluar las tecnologías de información y comunicación.

2.3. SUJETOS Y OBJETO DE ESTUDIO

2.3.1. Unidades de análisis

Las unidades de análisis considerada en la investigación, la conforma el socio director y el auditor de sistemas de la firma L GROUP, S.A. DE C.V., el cual está ubicado en la colonia Escalón, municipio de San Salvador departamento de San Salvador, El Salvador.

2.3.2. Población y marco muestral

La población de estudio considerada en la investigación estuvo conformada por la firma de auditoría L GROUP, S.A. DE C.V., cuya actividad económica consiste en el servicio de auditoría, impuestos, consultoría, asesoría entre otros; debido a que únicamente es una unidad de estudio no fue necesario calcular muestra.

2.3.3. Variables e indicadores

En la tabla 9 se muestra la matriz de congruencia realizada para la investigación.

Tabla No. 9

Matriz de congruencia

Formulación del problema:	Objetivo general:	Hipótesis del trabajo	Elementos de la hipótesis	Variables	Medición de variables
¿En qué medida la falta de experiencia en el área de auditoría de sistemas y evaluación de las tecnologías de la información y comunicación, incide en la oferta de nuevos servicios y aceptación de los encargos de auditoría por parte del auditor externo?	Elaborar la planificación aplicable a la evaluación de las tecnologías de información y comunicación, que contribuya al auditor externo que no cuenta con conocimientos especializados en la auditoría de sistemas a incursionar o ampliar el campo de sus servicios.	La elaboración de la planificación de auditoría de sistemas aplicable a la evaluación de las tecnologías de información y comunicación, contribuirá al auditor externo a ampliar la oferta de servicios y aceptación de los encargos de auditoría	Planificación de auditoría de sistemas	**Independiente** Planeación de auditoría de sistemas	a) Entrevista b) Existencia de controles de auditoría c) Documentación
			Oferta de servicio y aceptación de encargos de auditoría	**Dependiente** Oferta de servicio y aceptación de encargos de auditoría	a) Conocimiento del área técnica b) Desarrollo de procedimientos de auditoría

Nota: Lineamientos de guía del informe final seminario de graduación ciclo I-2020

2.4. TÉCNICAS, MATERIALES E INSTRUMENTOS

2.4.1. Técnicas e instrumentos utilizados en la investigación

Las técnicas utilizadas para la compilación de la información fueron:

- **Bibliográfica:** se obtuvo de trabajos de investigación, libros digitales, revistas, boletines entre otros.
- **Entrevista estructurada:** se llevó a cabo al socio director y al auditor de sistemas, ambas entrevistas se realizaron por separado, lo cual nos permitió recopilar información mediante una conversación profesional, se utilizó la aplicación zoom para realizar las reuniones virtuales para documentar las entrevistas que facilitó la obtención de una información más precisa.

2.4.2. Instrumento de medición

Se utilizó una guía de preguntas para la recolección de información la cual fue dirigida al socio director y al auditor de sistemas, el cual contiene preguntas abiertas enfocadas a la planificación y auditoría de sistemas aplicables a la evaluación de las tecnologías de información y comunicación. (Ver Anexo 1 y 2).

2.5. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

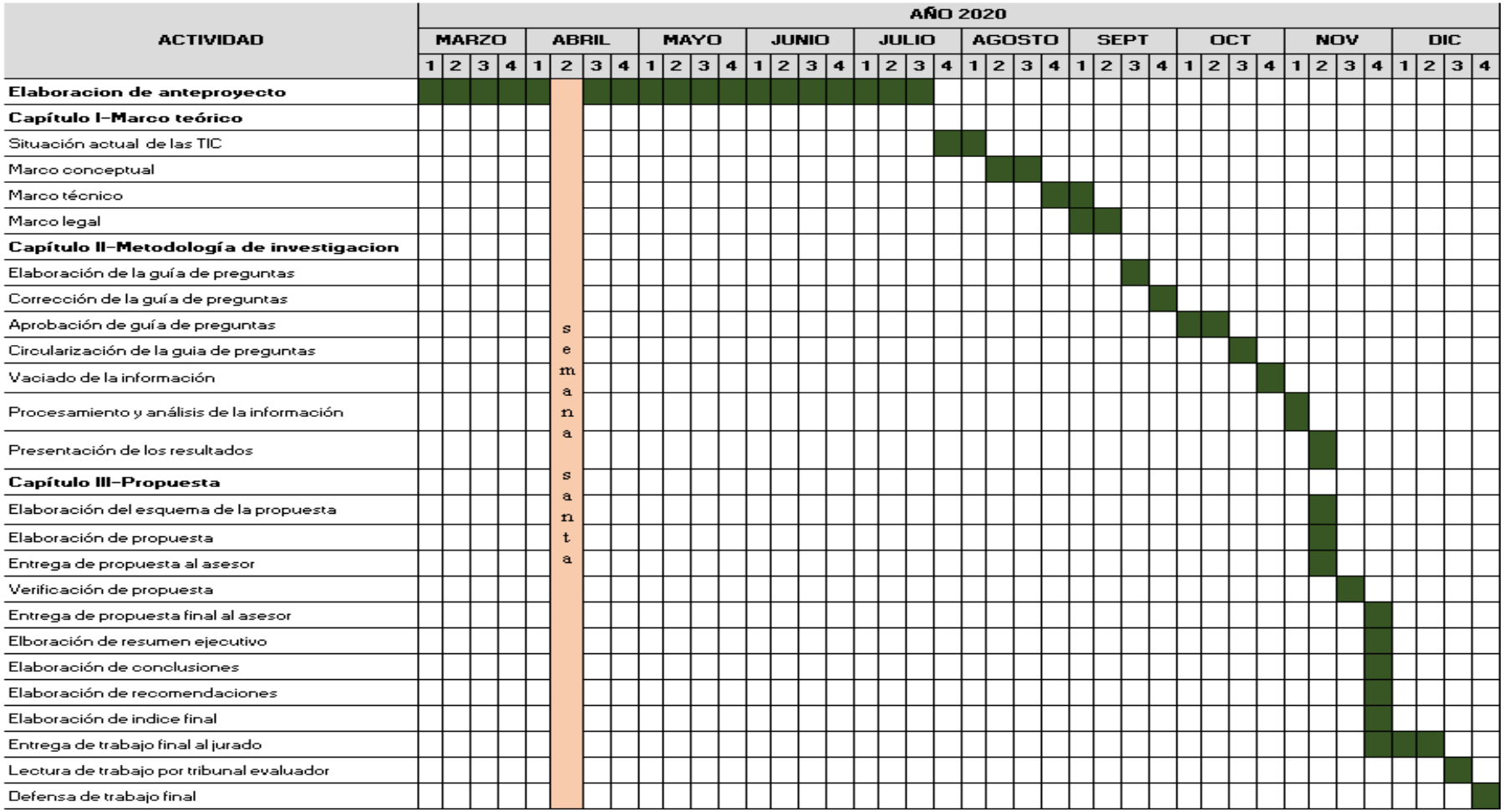
Para el procesamiento de la información se utilizaron una serie de herramientas informáticas, Microsoft Word y que permiten el vaciado de los datos obtenidos y la utilización de grabaciones audiovisuales, sobre los puntos relevantes durante dicho proceso; mediante la cual se prepararon y expusieron los resultados obtenidos de la investigación de campo; mismos que fueron analizados e interpretados para la formulación y presentación del correspondiente diagnóstico y las conclusiones a las cuales se llegó sobre éstos.

2.6. CRONOGRAMA DE ACTIVIDADES

Todas las actividades desarrolladas y las que aún se encuentran pendientes de ejecución se resume en la tabla 10 siguiente.

Tabla N. 10

Cronograma de actividades.



Nota: Lineamientos de guía del informe final seminario de graduación ciclo I-2020

2.7. PRESENTACIÓN DE LOS RESULTADOS

2.7.1. Tabulación y análisis de resultados

Se presenta la tabulación y análisis de la información obtenida; como resultado del instrumento de la entrevista realizada, y con la información recolectada por medio de la herramienta de registro de audio-grabación, con los cuales dieron lugar a un mejor análisis y diagnóstico respectivo de la problemática en estudio.

2.7.2. Diagnóstico

Al obtener los resultados suministrados de la población de estudio se pudieron identificar diferentes problemas a lo que se enfrentan al desarrollar las auditorías de sistemas para evaluar las tecnologías de información y comunicación, así como también los problemas a los que se enfrentan con el control interno que están desarrollando actualmente, es importante mencionar que el marco de referencia utilizado actualmente son las normas internacionales de auditoría (NIA) y no el marco de referencia COBIT 2019 emitido por ISACA y las ISO 27000 emitida por el organismo internacional de estandarización.

Pocas firmas a nivel nacional prestan servicios de auditoría de sistemas a entidades, esto se debe a diferentes factores, tales como la poca demanda de estos tipos de encargos, certificación y capacitación en seminarios que abordan esta temática son costosas. Retomando lo antes mencionado, la formación brindada por universidades no existe una actualización en maya curricular en las tecnologías de información y comunicación y los gremios dedicados al desarrollo de la profesión de Contaduría Pública no incluyen este tipo de capacitaciones, lo cual no es suficiente para cumplir con los requisitos de preparación que

demanda el marco de referencia COBIT 2019 y las normas ISO para enfrentar la complejidad de este tipo de encargo.

A pesar de estar conscientes de lo anterior, muy pocos auditores han considerado los aspectos que requiere la norma de educación continuada emitida por el consejo de vigilancia de la profesión de contaduría pública y auditoría, la que establece en la temática o área número 17 puntos sobre otras materias relacionadas con el trabajo del auditor, entre ella en materia de tecnologías de la información y las competencias necesarias que debe de poseer un contador en su formación profesional.

Se debe mencionar que las instituciones enfocadas al desarrollo de la carrera en contaduría y auditoría no están a la vanguardia en el área de la tecnología de información y comunicación, dejando vacíos en el mejoramiento de la profesión, siendo uno de los principales la inexistencia de seminarios, charlas o diplomados enfocados a las áreas de tecnología de información y comunicación; tomando en cuenta este factor, la modernización de los mercados económicos dará paso a que la mayor parte de las auditorías de sistemas incluyan la revisión de operaciones en tecnologías de información y comunicación, lo cual implica una mayor complejidad en la realización de este tipo de encargos dejando claramente establecido que el profesional debe contar con la competencia suficiente para cumplir con su labor especializada.

Dentro de las áreas críticas para este tipo de encargos están las relacionadas con el rubro de hardware, software, seguridad lógica, seguridad física, redes, telecomunicaciones y procesamiento electrónico de datos, y aquellas referentes a los aspectos de integridad, confidencialidad y disponibilidad de la información; ya que los sistemas electrónicos y la infraestructura que da soporte son susceptibles de situación de abuso, mal uso y fallas en muchas formas debido a lo complejo de su naturaleza.

Para el caso de los aspectos de tratamiento de la información, estos se vuelven muy delicados debido a que se manejan datos confidenciales de los clientes, proveedores y de la entidad, todos estos en una base de datos en la nube; con lo que las auditorías de sistemas se pudiesen ver afectadas si los clientes modifican sus registros a conveniencia o racionalizan la información, con el propósito de desviar la atención del auditor de sistemas hacia áreas distintas a las que en realidad poseen problemas, estas pueden disminuir su vulnerabilidad con adecuados procedimientos de auditoría de sistemas para evaluar las tecnologías información y comunicación de la organización, además se deben establecer políticas eficaces para este tipo de operaciones.

A partir de las inseguridades existentes en este tipo de encargo, se determinó que los procedimientos más efectivos para disminuir los niveles de riesgo a un nivel aceptable en una auditoría de sistemas es que contengan procedimientos de auditoría de sistemas para evaluar las tecnologías de información y comunicación, que puedan ser realizadas por medio de pruebas sustantivas que son programas diseñados para detectar errores materiales a nivel de aseveración y pruebas analíticas, que consisten en evaluaciones de información realizadas mediante el análisis de las relaciones plausibles entre datos financieros y no financieros.

Cabe destacar que, para realizar este tipo de encargos, toda firma busca el apoyo de un experto en tecnología de información y comunicación, aunque muchas de estas posean un departamento en tecnologías de información dentro de su equipo de colaboradores; esto demuestra evidentemente la falta de preparación que poseen los auditores en el mencionado tema de estudio, así como la poca confianza que se le da a los gremios encargados de capacitar a los profesionales de la contaduría pública. A esto se le suma la inexistencia de material de apoyo e información bibliográfica que aborde esta temática con claridad.

La población en estudio está interesada en los procedimientos de auditoría de sistemas para evaluar las tecnologías de información y comunicación en sus encargos; ya que además pretende ser un instrumento útil y novedoso para la población de auditores y para el enriquecimiento de la profesión de la contaduría pública.

CAPÍTULO III. PROCEDIMIENTOS DE AUDITORÍA DE SISTEMAS PARA EVALUAR LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

3.1. PLANTEAMIENTO DEL CASO

L GROUP, S.A. de C.V. es una compañía que ofrece servicios de auditoría de impuestos, auditoría financiera, consultoría y asesoría, ubicada en la colonia Escalón, municipio de San Salvador, departamento de San Salvador. El propósito principal es brindar un servicio integral de alta calidad y de manera personalizada a cada uno de sus clientes, incursionar y ampliar sus encargos de auditoría de sistemas para evaluar las tecnologías de información y comunicación.

La propuesta de la investigación plantea diseñar un modelo de planeación que describa los lineamientos necesarios que minimice el riesgo en los encargos de auditoría de sistemas a un nivel aceptable y los procedimientos de auditoría que sean posibles someterlos a una evaluación de control interno acorde a los requerimientos del marco de referencia COBIT 2019 y la normativa ISO 27000.

El auditor externo debe de contar con procedimientos de auditorías de sistemas que le permita ampliar o incursionar sus encargos para evaluar de manera confiable las tecnologías de información y comunicación.

La importancia de diseñar y proponer procedimientos de auditoría de sistemas para evaluar las tecnologías de información y comunicación en los encargos de auditoría en L GROUP, S.A. DE C.V. es que resultará un instrumento que será de utilidad social porque servirá como guía para evaluar aspectos que midan las deficiencias en el desarrollo de las actividades normales de la entidad.

3.2. ESTRUCTURA DEL PLAN DE SOLUCIÓN

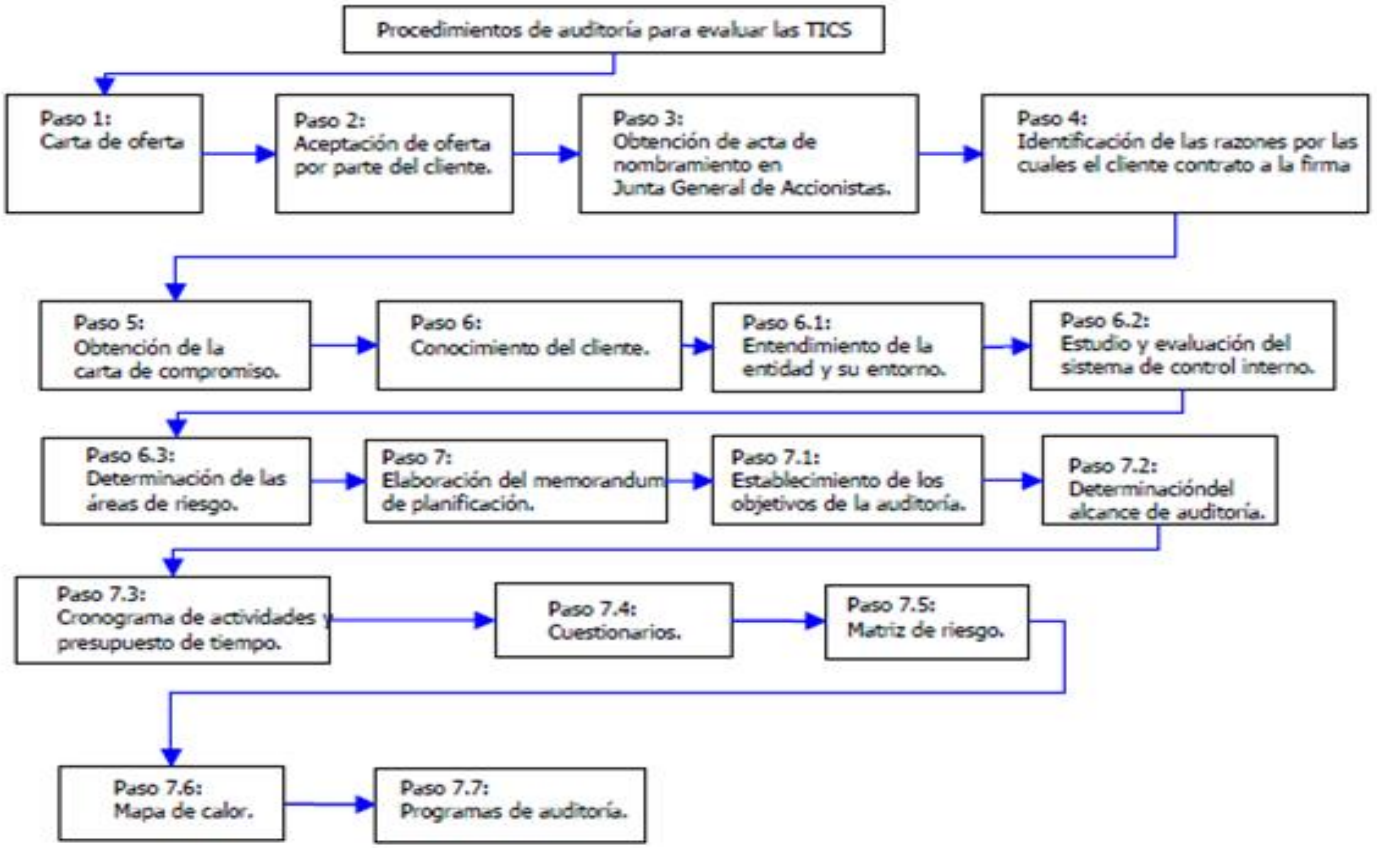


Figura N. 1 mapa mental de la propuesta de solución.

3.3. BENEFICIOS Y LIMITANTES

3.3.1. Beneficios

En el desarrollo de la presente propuesta de solución se determinaron los siguientes beneficios:

- Es una auditoría de sistemas especializada para evaluar las tecnologías de información y comunicación.
- Será de apoyo a L GROUP, S.A. de C.V., para que amplíe o incursione en sus encargos de auditoría de sistemas.
- L GROUP, S.A. de C.V. podrá aplicar los procedimientos de auditoría de sistemas para evaluar las tecnologías de información y comunicación de acuerdo al marco de referencia COBIT 2019 emitido por ISACA y la norma ISO 27001 y 27002 emitida por el organismo internacional de estandarización.

3.3.2. Limitantes

En el desarrollo de la presente propuesta de solución se determinaron las siguientes limitantes:

- La normativa ISO 27001 y 27002 emitida por el organismo internacional de estandarización actualmente no son muy utilizadas, por tal razón obtenerlas de forma gratuita y digital fue difícil, la cual es de aplicación para los procedimientos de auditoría de sistemas para evaluar las tecnologías de información y comunicación.

- Las normativas ITAF y COBIT 2019 no son utilizadas en L GROUP, S.A. DE C.V., la cual es de aplicación para realizar los procedimientos de auditoria de sistemas para evaluar las TICs.

3.4. DESARROLLO DEL CASO PRÁCTICO

3.4.1. Memorándum de planeación para la auditoría de sistemas

A continuación, se presenta el contenido de una planificación de auditoría de sistemas para evaluar las tecnologías de información y comunicación, aplicable a L GROUP, S. A. de C. V., mediante la cual se pretende aplicar procedimientos de auditoría de sistemas para mitigarlos y obtener evidencia suficiente y adecuada:

MEMORÀNDUM DE PLANEACIÓN

PROCEDIMIENTOS DE AUDITORÍA DE SISTEMAS PARA EVALUAR LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

PARA:

L GROUP, S.A. DE C.V.

L Group
S.A. de C.V.

SAN SALVADOR, FEBRERO DE 2021

A. Memorándum

Es el documento por medio del cual se expone de manera breve el trabajo de planificación de la auditoría de sistemas para el equipo de auditores en L GROUP, S. A. de C. V., que se dedica a prestar servicio de auditoría, impuestos, consultoría y asesoría. Se realizará un resumen de los factores, consideraciones y decisiones significativas pertinentes al enfoque y al alcance de auditoría de sistemas.

A.1. Objetivos de la auditoría

A.1.1. Objetivo general

Realizar procedimientos de auditoría para evaluar las tecnologías de información y comunicación en L GROUP, S.A. DE C.V. con el fin de brindar, proponer recomendaciones sobre el funcionamiento y seguridad del mismo, que permitan el logro de los objetivos organizacionales, llevaremos a cabo una auditoría de sistemas cumpliendo con el marco de referencia COBIT 2019 y normas ISO 27000.

A.1.2. Objetivos específicos

- Revisar las políticas aplicadas por la firma L GROUP, S.A. de C.V. en el uso de las tecnologías de información y comunicación.
- Evaluación de suficiencia en los planes de contingencia
- Evaluación de la seguridad de la información en el área de las TICS.
- Evaluar el control de riesgos que posee L GROUP, S.A. DE C.V. para el manejo de las auditorías de sistemas realizadas.

B. Determinación del alcance de la auditoría

El equipo de auditores es responsable de realizar una auditoría de sistemas para evaluar las tecnologías de información y comunicación basada en el marco de referencia COBIT 2019 y las ISO 27000, las cuales requieren que esta se ejecute con el propósito de obtener una seguridad razonable, Es por ello, que nuestro principal compromiso en la

revisión, análisis, evaluación y emisión de informe de la estructura de control informático en lo relacionado a áreas como hardware, software, procesamiento electrónico de datos, seguridad física y lógicas, leyes y reglamentos.

La auditoría de sistemas comprende el presente periodo marzo de 2019 y finalizando el 30 de noviembre de 2020 y se ha realizado especialmente al departamento de tecnología de información y comunicación de la firma L GROUP, S.A. de C.V.

C. Responsabilidad de la firma

Se llevará a cabo la auditoría de sistemas de acuerdo al marco de referencia COBIT 2019 y la normativa internacional ISO 27000. Dichas normas exigen que cumplamos los requisitos de ética, así como que planifiquemos y ejecutemos la auditoría con el fin de obtener una seguridad razonable de que no existan errores en los sistemas utilizados por L GROUP, S.A. DE C.V. Una auditoría conlleva la aplicación de procedimientos para obtener evidencia de auditoría sobre los sistemas utilizados y la información que se encuentra en ellos. Los procedimientos seleccionados dependen del juicio del auditor, incluida la valoración de los riesgos de los sistemas.

Para la evaluación de los controles mantenidos por la entidad, la entidad se basará en el enfoque COBIT 2019 ya que éste es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir administradores de TI, usuarios y por supuesto, los auditores involucrados en el proceso.

COBIT 2019 es un modelo de evaluación y monitoreo que enfatiza en el control del negocio y la seguridad del mismo.

D. Personal clave de la firma L GROUP, S.A. de C.V.

El personal clave para efectos de ejecución de auditoría de sistemas, es el siguiente:

1. Directora de la firma: Flor de Carmen Fabián

2. Gerente de las TICS: María José Trejos de Roche

E. Estudio del control interno informático

La evaluación de los riesgos deberá de tomar como base la normativa que COBIT 2019 como marco de referencia y evaluar los riesgos inherentes sobre la aplicación del sistema informático que la compañía haya adoptado, así como la resistencia de los usuarios directos e indirectos frente al correcto manejo la tecnología en sus procesos operacionales, con ello el auditor debe de ser capaz evaluar que el sistema informático cumpla con 2 grandes rasgos:

1. Adaptabilidad: el sistema debe de ser flexible a los cambios del avance tecnológico, así como al ritmo de las estrategias del negocio.

Se deberá de determinar si el sistema informático, o elementos del sistema, parcial o total, es apto para ser modificado, sustituido, a hacer adiciones o retiros, con el fin de expandir su gama de aplicación y funcionalidad según los requerimientos de la compañía.

2. Funcionalidad: el sistema debe de ser eficiente para los requerimientos del negocio, cada elemento debe de otorgar a la compañía una ventaja estratégica ante la competencia.

Se debe de evaluar si las inversiones realizadas o futuras inversiones por la compañía, posee elementos no funcionales o en elementos con limitantes, así como determinar si la compañía y los usuarios, se encuentran preparados para la adopción de los nuevos elementos.

Para ello el auditor de bebe de considerar que las tecnologías de la información y comunicaciones poseen una serie características y factores para cada categoría de riesgo identificables.

En la tabla11 se muestra los riesgos y factores claves para cada categoría de riesgo identificables.

Tabla No.11

Riesgos y factores claves asociados

Tipo de riesgo de TI	Fuente de riesgo	Factores claves
Operacional y riesgos técnicos asociados	- Perdida de activos informáticos - Riesgo inexacto de datos - Aumento del riesgo de fraude - Pérdida o robo de datos - Interrupción del negocio - Violaciones de privacidad - Brechas informáticas - Protección insuficiente de la información o los sistemas - Roles y responsabilidades pocos claros - Falta técnica y humanas - Vulnerabilidad de sistemas - Fraude o eventos externos	- Gestión de activos - Gestión del recurso humano - Gestión de seguridad de la información - Gestión de tecnología de información
Estratégicos	- Falta de estrategia - Falta de gestión específica para riesgos de TI - La naturaleza de la perspectiva de gestión - Fallos en los procesos de gestión - La responsabilidad de la auditoría y el control de las TI - La complejidad de los sistemas - Plan estratégico poco claro - Plan operativo poco claro - Fallos en la gestión de proyectos de TI	- Estrategia organizacional - Política organizacional - Planificación en relación con planes estratégicos y planes operativos

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

La evaluación de las áreas de las tecnologías de información y comunicación, debe de considerar que existen diferentes tipos de amenazas, vulnerabilidades y riesgos asociados, provenientes de factores externos, incidentes operativos, procesos inadecuados, normativa y otros factores controlables:

En la tabla 12 se muestran las amenazas, vulnerabilidades y riesgos asociados provenientes de diversos factores.

Tabla No. 12

Amenazas, vulnerabilidades y riesgos asociados

Amenaza	Vulnerabilidad	Riesgo
Maliciosa	Falencias en capacitaciones del personal respecto a la adopción de los métodos utilizados para el procesamiento y resguardo de la información	Información sensible sea revelada o sustraída sin autorización
Natural	Ubicación incorrecta de servidores, ausencia de copias de seguridad, ubicación incorrecta de información sensible	Destrucción de la infraestructura informática y de la información
Falla	Ausencia de un plan de continuidad de aquellos procesos críticos para la entidad	Interrupción de servicios y del negocio
Accidental	Ineficiencia en los controles interno para el manejo de dispositivos proporcionados al personal de la compañía	Pérdida de un dispositivo y accesos no autorizados al dispositivo

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

Para el análisis integral de los riesgos de las tecnologías de la información y comunicación, es posible separar las diferentes áreas y ordenarlas en un modelo por capas, que se encuentran interrelacionadas directa o indirectamente, con lo que, al identificar y solventar un riesgo de una de las capas, logre corregir o superar una falla en otra de las capas:

1. Procesos del negocio
2. Servicios de TI
3. Datos e información
4. Sistemas de información transaccionales
5. Sistemas de información de soporte
6. Gestores de base de datos
7. Sistemas operativos
8. Computadores, dispositivos, impresoras y cualquier tipo de dispositivo conectado a la red

9. Servidores
10. Centro de redes
11. Sistemas de energía

3.4.2 Cuestionario del control interno informático

El objetivo general del cuestionario es la evaluación del control interno en las áreas de tecnologías de información y comunicación, y los factores de riesgo y determinación de las vulnerabilidades en la eficiencia de las operaciones y confiabilidad de la información.

Dentro de los objetivos específicos, los cuestionarios deben de proporcionar información suficiente para poder determinar los procedimientos de auditoría de sistemas a ejecutar de forma más eficiente para cada área.

Cada pregunta debe de considerar múltiples factores de riesgo para el cumplimiento de la auditoría, que deben estar claramente identificados, como se indica a continuación:

En la tabla 13 se muestran los factores de riesgos asociados a una auditoría de sistemas.

Tabla No. 13

Factores de riesgos de una auditoría de sistemas

Evaluación de riesgo de TICs	Fuente de riesgo	Código	Descripción
Funcionalidad	Operacional	IN	Interrupción del negocio
Adaptabilidad	Operacional	VI	Vulnerabilidad informática
Funcionalidad	Operacional	VF	Vulnerabilidad física
Adaptabilidad	Operacional	PS	Protocolos de seguridad
Funcionalidad	Operacional	RH	Recurso humano
Funcionalidad	Estratégico	CI	Control interno

Adaptabilidad	Estratégico	PO	Política organizacional
Adaptabilidad	Estratégico	PL	Planificación a corto y largo plazo
Adaptabilidad	Estratégico	RA	Responsabilidad de la administración

Nota: memorándum de planeación de una auditoría de sistemas.

Se presenta el cuestionario que se utilizó en la empresa modelo S.O.S. CRÉDIT, S. A. de C.V. para evaluar las áreas críticas relacionadas con las tecnologías de información y comunicación, con el propósito de identificar las debilidades existentes en las operaciones de la entidad.

S.O.S. CRÉDIT, S.A. DE C.V.

ÀREA DE LAS TÈCNOLOGIAS DE INFORMACIÒN Y COMUNICACIÒN

CUESTIONARIO DE CONTROL INTERNO

PROCESO: Aplicación de Marco de Referencia COBIT 2019

DEPENDENCIA: Departamento de TICs

DIRIGIDO A: Gerencia de TICs

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a hardware**, **software, seguridad lógica, seguridad física, redes, telecomunicaciones, procesamiento electrónico de datos y aspectos legales de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**

2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en las áreas de software, hardware, seguridad física, seguridad lógica, PED, redes, telecomunicaciones y leyes y reglamentos de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

CUESTIONARIO DE CONTROL INTERNO

PROCESO: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Hardware

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a hardware de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en las áreas de hardware de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para el hardware de la empresa?		X					
2.	RH	¿El equipo o dispositivo le es asignado a un responsable y se emite documento que la responsable	X						

		firma de aceptación?							
3.	PL	¿Realiza evaluación a los equipos informáticos de forma periódica para la adquisición de nuevas flotas de equipos y dispositivos informáticos?		X					
4.	PO	¿Posee contrato con proveedores de forma exclusiva para la adquisición de equipos y/o dispositivos?		X					Se adquieren nuevos equipos informáticos a base de cotizaciones con diferentes proveedores
5.	CI	¿Se imparte capacitación al personal para el uso adecuado de los equipos o dispositivos?		X					
6.	PS	¿Clasifican, etiquetan y codifican los equipos para control de inventario?	X						

7.	PS	¿El área de oficina, área operativa y área de almacenamiento de equipo y dispositivos se encuentran adecuadas para el resguardo físico?		X					
8.	VF	¿Cuentas con un área resguardada de accesos no autorizados, para el inventario de equipos, dispositivos, repuestos y periféricos?		X					
9.	PS	¿Se autoriza el uso de los equipos y dispositivos fuera del área de la empresa, y se controla a través de notas de remisión o algún otro documento?	X						
10.	PO	¿Posee algún plan o procedimiento para la disposición final, venta, destrucción, donación, etc., de los equipos dados de baja, obsoletos o daños?	X						

11.	VI	¿La empresa posee sus propios servidores dedicados para correos, almacenamiento, procesamiento de datos, comunicaciones, etc.?		X					En la empresa solo se cuenta con un solo servidor que realiza todas esas funciones
12.	PL	¿Posee bitácora de errores o sucesos relevantes con el hardware?	X						

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Software

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a software de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en las áreas de software de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para el hardware de la empresa?		X					

2.	RH	¿El equipo o dispositivo le es asignado a un responsable y se emite documento que la responsable firma de aceptación?	X						
3.	PL	¿Realiza evaluación a los equipos informáticos de forma periódica para la adquisición de nuevas flotas de equipos y dispositivos informáticos?		X					
4.	PO	¿Posee contrato con proveedores de forma exclusiva para la adquisición de equipos y/o dispositivos?		X					Se adquieren nuevos equipos informáticos a base de cotizaciones con diferentes proveedores
5.	CI	¿Se imparte capacitación al personal para el uso adecuado de los equipos o dispositivos?		X					

6.	PS	¿Clasifican, etiquetan y codifican los equipos para control de inventario?	X						
7.	PS	¿El área de oficina, área operativa y área de almacenamiento de equipo y dispositivos se encuentran adecuadas para el resguardo físico?		X					
8.	VF	¿Cuentas con un área resguardada de accesos no autorizados, para el inventario de equipos, dispositivos, repuestos y periféricos?		X					
9.	PS	¿Se autoriza el uso de los equipos y dispositivos fuera del área de la empresa, y se controla a través de notas de remisión o algún otro documento?	X						

10.	PO	¿Posee algún plan o procedimiento para la disposición final, venta, destrucción, donación, etc., de los equipos dados de baja, obsoletos o daños?	X						
11.	VI	¿La empresa posee sus propios servidores dedicados para correos, almacenamiento, procesamiento de datos, comunicaciones, etc.?		X					En la empresa solo se cuenta con un solo servidor que realiza todas esas funciones
12.	PL	¿Posee bitácora de errores o sucesos relevantes con el hardware?	X						

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Seguridad lógica

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en

las diferentes áreas y actividades **delimitadas a seguridad lógica de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en las áreas de seguridad lógica de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para el software de la empresa?	X						
2.	IN	¿Se cuenta con licencia, para el uso o concesión de uso del software que la compañía utiliza?	X						
3.	VI	¿Existe protocolo para la actualización del software y el antivirus?	X						
4.	VI	¿El antivirus se encuentra actualizado y posee licencia que cubra todos los requerimientos que la empresa necesite?	X						
5.	PS	¿Existe procedimiento para la eliminación de aplicaciones, archivos, documentos, etc.,		X					

		no utilizados o no deseados?							
6.	PO	¿La compañía utiliza sistemas informáticos ERP es open source, con licencia, a la medida o freeware?	X						Sistemas ERP con licencia
7.	VI	¿Existe un programa especializado para la generación de backup o recuperación de la información?		X					
8.	CI	¿Existe protocolos para la creación y parametrización de las cuentas de usuarios?	X						
9.	CI	¿Existe una verificación o feedback de los derechos de los accesos de los usuarios creados?	X						
10.	CI	¿Existe una política para la disposición de los usuarios dados de	X						

		baja?							
11.	IN	¿La empresa posee un sistema de gestión de base de datos?	X						
12.	RH	¿Existe personal interno u outsourcing para el mantenimiento de los softwares de la empresa?		X					
13.	RH	¿Existe políticas para la capacitación de los usuarios de los programas informáticos?		X					
14.	PO	¿Posee contrato con proveedores de forma exclusiva para la adquisición de software o mantenimiento?	X						
15.	PS	¿Posee póliza de seguro para las contingencias derivadas de los softwares?		X					
16.	PL	¿Posee bitácora de errores o sucesos	X						

		relevantes con el software?							

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Seguridad física.

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a seguridad física de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en el área de seguridad física de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para los protocolos de seguridad, firmware, conexión a internet, etc.?	X						
2.	PS	¿Cuenta con un sistema de monitoreo para los accesos a la internet de los usuarios?	X						
3.	PS	¿Cuenta con un sistema de monitoreo de los registros realizados en las computadoras	X						

		personales de los empleados?							
4.	PS	¿Las computadoras o dispositivos proporcionados a los empleados, poseen un sistema de bloqueo para evitar inicio de sesión no autorizada?	X						
5.	PS	¿Las computadoras o dispositivos poseen un sistema de seguridad para evitar la instalación de programas no autorizados?	X						
6.	CI	¿Existen protocolos de seguridad para los equipos y usuarios, para el acceso de la información resguardada en los servidores o dispositivos de almacenamiento?	X						

7.	PS	¿Existe protocolos de seguridad para la conexión remota a los programas, servidores e información de la empresa?	X						
8.	PS	¿Existe protocolo para el cambio de contraseña de forma periódica?	X						
9.	CI	¿Se realizan backup de la información de forma periódica?	X						
10.	PS	¿Al momento de guardar la información confidencial, se encuentra encriptada?	X						
11.	VI	¿El antivirus utilizado, cuenta con protección firewall, spyware, malware y spam?	X						
12.	PS	¿Se cuenta con protocolos para la restricción al acceso a internet, redes sociales, páginas pornográficas y páginas	X						

		maliciosas?							
13.	PS	¿Existe protocolo de seguridad y/o restricción para la conexión de dispositivos de almacenamiento flash en los equipos y dispositivos?		X					
14.	PS	¿Posee póliza de seguro para las contingencias derivadas de la vulnerabilidad informática?		X					
15.	PL	¿Posee bitácora de errores o sucesos relevantes de las vulnerabilidades?		X					

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Redes

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a redes, de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en el área de redes de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para los protocolos y utilización de las redes?		X					
2.	PS	¿Cuenta con protocolos de acceso, restricciones de IP o restricciones de usuario que se conectan a una red wifi o alámbrica dentro de la compañía?	X						
3.	VI	¿Cuentan con métodos de autenticación o validación de los usuarios que se conectan a la red de la compañía?	X						
4.	PS	¿Se ha implementado una	X						

		segregación de redes?							
5.	PS	¿Se ha designado un servidor para las directivas de redes?	X						
6.	PO	¿Posee contrato con proveedores de forma exclusiva para el suministro y mantenimiento de la red de la compañía?	X						
7.	PO	¿Posee contrato con proveedores de forma exclusiva para servicio de redes?	X						
8.	RH	¿Cuenta con personal capacitado dentro de la compañía u outsourcing, para el monitoreo de las redes?	X						
9.	RA	¿Posee un diagrama de red definido para la compañía?	X						
10.	CI	¿Cuenta con un firewall para redes?	X						

11.	VI	¿Cuenta con un sistema de filtrado de paquetes salientes y entrantes?	X						
12.	PL	¿Posee bitácora de errores o sucesos relevantes de las vulnerabilidades?	X						

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Telecomunicaciones

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a telecomunicaciones de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**

2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en el área de telecomunicaciones de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para la instalación, mantenimiento y uso de las telecomunicaciones de las TICs?		X					
2.	VI	¿Cuenta la compañía con una red de telefonía IP?	X						
3.	PO	¿Cuenta con servicio satelital para el internet?		X					

4.	VI	¿Posee conexión Wireless para la transmisión de la información dentro de la compañía?	X						
5.	PS	¿Cuenta con un sistema de Edge Data Center, para el procesamiento de la información?		X					
6.	VI	¿Cuenta con dispositivos y plataformas Lot en la compañía?		X					
7.	PO	¿Cuenta con un servidor de correo electrónico local?	X						
8.	PO	¿Cuenta con servicio de cloud computing?		X					
9.	PS	¿Cuenta con un servidor DNS?	X						
10.	PO	¿Cuenta con diferentes tipos de servidores locales?		X					Solo se cuenta con un tan solo servidor
11.	PL	¿Posee bitácora de errores o sucesos relevantes de las vulnerabilidades?		X					

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Procesamiento electrónico de datos.

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a procesamiento electrónico de datos de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en el área de Procesamiento electrónico de datos de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno general o específicos para la instalación, mantenimiento y uso de las telecomunicaciones de las TICs?		X					
2.	VI	¿Cuenta la compañía con una red de telefonía IP?	X						
3.	PO	¿Cuenta con servicio satelital para el internet?		X					
4.	VI	¿Posee conexión Wireless para la transmisión de la información dentro de la compañía?	X						
5.	PS	¿Cuenta con un sistema de Edge Data Center, para el procesamiento de la información?		X					
6.	VI	¿Cuenta con dispositivos y plataformas IoT en la compañía?		X					

7.	PO	¿Cuenta con un servidor de correo electrónico local?	X						
8.	PO	¿Cuenta con servicio de cloud computing?		X					
9.	PS	¿Cuenta con un servidor DNS?	X						
10.	PO	¿Cuenta con diferentes tipos de servidores locales?		X					Solo se cuenta con un tan solo servidor
11.	PL	¿Posee bitácora de errores o sucesos relevantes de las vulnerabilidades?		X					

CUESTIONARIO DE CONTROL INTERNO

PROCES: Aplicación de marco de referencia COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Aspectos legales

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar el control interno en base al enfoque **COBIT 2019** sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA e identificar en las diferentes áreas y actividades **delimitadas a aspectos legales de S.O.S. CRÉDIT, S.A. de C.V.** los factores de riesgo que ponen en peligro el logro de los objetivos: A) efectividad y eficiencia de las operaciones; B) confiabilidad de la información y documentos que se generan en el proceso; C) cumplimiento de leyes y regulaciones aplicables. Todo con el propósito de elaborar una efectiva planeación y programa de auditoría.

OBJETIVOS ESPECÍFICOS:

1. Conocer el entorno en el cual se desarrolla, con el fin de evaluar la eficiencia y eficacia del control interno informático de **S.O.S. CRÉDIT, S.A. de C.V.**
2. Identificar los riesgos asociados a cada uno de las actividades en base a COBIT 2019 en cuanto a los procesos informáticos, en el área de aspectos legales de **S.O.S. CRÉDIT, S.A. de C.V.**

INSTRUCCIONES PARA EL LLENADO: Por favor conteste a cada pregunta con: **SI o NO** colocando una "**X**" en la casilla respectiva; y si es necesario explicar algo sobre la respuesta utilice la columna de la derecha: "Comentarios…". **N/A** Significa No Aplica, y debe marcar esa casilla cuando no le compete hacer lo que se le pregunta.

Se advierte que las respuestas que emita en este cuestionario **deben ser veraces**, ya que estarán sujetas a ser comprobadas por esta auditoría.

Corr.	Riesgo	Descripción	Si	No	N/A	Nivel de riesgo	Nivel de impacto	Prob. e impacto	Comentario
1.	CI	¿Cuenta con manual de control interno de las principales leyes aplicables relacionadas con las TICs?		X					
2.	RH	¿Existe personal asignado para el cumplimiento de las leyes aplicables a las TICs?		X					
3.	IN	¿Los contratos de servicio cumplen con los aspectos legales para su validación jurídica?		X					
4.	IN	¿Existen sub contratos de servicio o conexos, derivados de los contratos principales con otras entidades?		X					

5.	IN	¿Los protocolos de seguridad aplicados en su sistema informático lo protegen de los delitos informáticos?		X					
6.	IN	¿Existen políticas que protejan a la compañía contra el fraude?		X					
7.	IN	¿Posee protocolos para minimizar el riesgo de la falsificación de la información?		X					
8.	PL	¿Posee bitácora de errores o sucesos relevantes de las vulnerabilidades?		X					

3.4.3. Matriz de Riesgo

Los niveles de aceptabilidad o tolerancia de los riesgos identificados en la evaluación de riesgos, son definidos por el auditor de sistemas con base a la valoración de cada riesgo, donde cada riesgo es categorizado como aceptable y no aceptable. Los riesgos aceptables para la auditoría, son calificados con riesgo bajo y moderado, en cambio los riesgos no aceptables son calificados con un nivel de riesgo alto:

En la tabla 14 se muestran los niveles de aceptabilidad de los riesgos identificados.

Tabla No. 14

Niveles de aceptabilidad aceptables

Categoría	Nivel de riesgo
No Aceptable	Muy Alto
	Alto
	Medio
Aceptable	Moderado
	Bajo

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

La categoría de aceptabilidad de un riesgo puede designarse por su frecuencia y su factibilidad donde se define:

- **Frecuencia:** Es la cantidad de veces que el suceso un evento de riesgo en un periodo determinado, diario, semanal, mensual o anual

- **Impacto:** corresponde a la consecuencia de la intervención de factores internos y externos

Para determinar el impacto de la frecuencia y factibilidad, se debe de consignar valores que faciliten su valoración según se muestra en la tabla 15.

Tabla No. 15

Escala de probabilidad por frecuencia

Periodo	Calificación cuantitativa	Riesgo
Diario	**5**	**Muy Alto**
Semanal	**4**	**Alto**
Mensual	**3**	**Medio**
Anual	**2**	**Moderado**
Más de un año	**1**	**Bajo**

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

En la tabla 16 se muestran las escalas de impacto de los riesgos identificados.

Tabla No. 16

Escala de impacto

Impacto	Calificación cuantitativa	Riesgo
Interrupción de total o parcial del negocio	5	Muy alto
Pérdida de información sensible y confidencial	4	Alto
Accesos no autorizados a dispositivos	3	Medio
Interrupción y problemas con la conectividad entre los dispositivos sin afectar el negocio	2	Moderado
Errores y problemas en los dispositivos operativos y administrativos y usuarios de los dispositivos	1	Bajo

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

Nivel de riesgo y mapa de calor

El nivel de riesgo es el valor que se determina a partir del análisis de la probabilidad de ocurrencia del evento y del impacto de sus consecuencias potenciales, para cada encargo de auditoría se necesario definir que la escala de medición sea apropiada, según los requerimientos del negocio, por lo que la valorización debe de ser ajustada.

En la tabla 17 se muestran los niveles de los riesgos identificados.

Tabla No. 17

Niveles de riesgo

Nivel de riesgo	Probabilidad e Impacto
Muy alto	15 – 25
Alto	10 - 14
Medio	5 - 9
Moderado	3 – 4
Bajo	1 – 2

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

El cálculo matemático para el nivel de riesgo está dado por la fórmula ER = PF x I; donde:

- ER = Exposición al riesgo
- PF = Probabilidad de frecuencia
- I = Impacto

Al determinar el nivel de riesgo, es necesario ubicar cada riesgo en un mapa de calor o matriz de riesgo, tal como se muestra en la tabla 18, gráficamente se pueda asignar la importancia del riesgo inherente, y considerar y enfocar los métodos de evaluación y pruebas.

Tabla No. 18

Mapa de calor

Mapa de Calor			Impacto				
			Bajo		Medio	Alto	
		valor	1	2	3	4	5
Frecuencia	Bajo	1					
		2					
	Medio	3					
	Alto	4					
		5					

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

Universo de la auditoría de sistemas

- Para el desarrollo de las pruebas de auditoría de sistemas se sugiere la evaluación de las áreas de las tecnologías de información y comunicación siguiente: Hardware, software, seguridad lógica, seguridad física, redes, telecomunicaciones, procesamiento electrónico de datos, leyes y reglamento

En la tabla 19 se tabulará la ponderación de la probabilidad de impacto de los cuestionarios de evaluación del control interno, y se determinará la proporcionalidad de cada área calculando el total del área entre total de puntos de probabilidad de impacto

Tabla No. 19

Materialidad

RIESGO DE PROBABILIDAD DE IMPACTO											
Área de evaluación	**IN**	**VI**	**VF**	**PS**	**RH**	**CI**	**PO**	**PL**	**RA**	**Total**	**Proporcionalidad**
Hardware											
Software											
Seguridad Lógica											
Seguridad Física											
Redes											
Telecomunicaciones											
Procesamiento electrónico de datos											
Total punto de probabilidad de impacto											

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

En la tabla 20 se muestran el orden de importancia de la auditoria a partir del cuadro de la materialidad, consignando en primer lugar el área que posea el mayor porcentaje de la probabilidad de impacto en ultimo el que posea la menor ponderación

Tabla No. 20

Orden de relevancia de auditoria

Orden de importancia	Área de evaluación	Proporcionalidad
1	Hardware	
2	Software	
3	Seguridad lógica	
4	Seguridad física	
5	Redes	
6	Telecomunicaciones	
7	Procesamiento electrónico de datos	

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas.

En la tabla 21 se muestran los niveles de los riesgos porcentualmente.

Tabla No. 21

Niveles de los riesgos evaluados

Nivel	Proporcionalidad	
Alto	80.01%	100.00%
	60.01%	80.00%
Medio	40.01%	60.00%
Bajo	20.01%	40.00%
	0.00 %	20.00%

Nota: trabajo de investigación memorándum de planeación de una auditoría de sistemas

3.4.4. Programas de auditoría de sistemas

S.O.S. CRÉDIT, S.A. DE C.V.

ÀREA DE LAS TÈCNOLOGIAS DE INFORMACIÒN Y COMUNICACIÒN

PROGRAMA DE AUDITORÌA DE SISTEMAS

PROCESO: Evaluar TICs con enfoque COBIT 2019

DIRIGIDO A: Gerencia de TICs

DEPENDENCIA: Departamento de TICs

OBJETIVOS DE LA AUDITORÍA

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de TICs en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.

2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Hardware

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de redes en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
1.	**PROCEDIMIENTO DE CUMPLIMIENTO: REDES**			
1.1.	**Verifique si la entidad cuenta con un mantenimiento preventivo y correctivo de hardware.**			
1.2.	Revise el equipo de cómputo con el fin de evaluar su estado físico y deterioro de los componentes.			
1.3.	Valide que las instalaciones y puestos de trabajo donde se encuentran los equipos de cómputo cumplan con las condiciones mínimas de temperatura.			
1.4.	Compruebe que el código asignado al hardware coincide con el que les corresponde según detalle de propiedad planta y equipo.			
1.5.	Revise que cada computadora cuente con una adecuada protección de terminales tanto como protectores de voltaje y UPS.			

1.6.	Verifique que la infraestructura donde está ubicado el equipo, es capaz de proveer un adecuado nivel de seguridad, en cuanto a paredes, ventanas y techos, etc.			
1.7.	Obtuve confirmación de si existe personal externo que efectúe mantenimiento a los equipos de cómputo (hardware).			
1.8.	Evalúe el sistema de backups utilizado para los archivos de datos y que estos estén actualizados y resguardados de manera segura.			
1.9.	Valide la existencia o respaldo, con análisis de costo-beneficio, de las solicitudes de compra de equipos.			
1.10.	Evalúe la capacidad de almacenamiento y memoria RAM del servidor, considerando el número de equipos clientes que se conectan a él y la cantidad de información a almacenar.			
1.11.	Verifique la existencia de registro de los números seriales de los equipos y sus partes más relevantes.			
1.12.	Compruebe si se efectúan comparaciones periódicas entre el inventario físico y el registro de los equipos.			
1.13.	Corrobore que exista un plan de mantenimiento de los equipos de cómputo (hardware).			
1.14.	Verifique si existe un procedimiento o norma de registro y custodia de los equipos de cómputo (hardware).			
1.15.	Observe si existen procedimientos y requisitos establecidos para la salida de los equipos (hardware) y para el traslado del mismo.			
1.16.	Valide si los usuarios cumplen las indicaciones que los fabricantes de los equipos (hardware) recomiendan en cuanto a instalación y almacenamiento del mismo.			

1.17.	Verifique cual es el proceso de notificación de las fallas del equipo informático y como se documenta dicho proceso.			
1.18.	Compruebe si existe un plan de mantenimiento y si este cubre la totalidad del equipo de cómputo o no.			
1.19.	Confirme si el proveedor tiene la capacidad de ofrecer la sustitución temporal del equipo principal como servidores en caso de retiro por reparación y otro tipo de mantenimiento.			

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Software

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de software en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
2.	**PROCEDIMIENTO DE CUMPLIMIENTO: SOFTWARE**			
2.1.	Compruebe si existen medidas de seguridad como contraseña para el ingreso del personal autorizado al sistema y los diferentes sistemas informáticos de la entidad.			
2.2.	Identifique con qué frecuencia se dan los cambios de clave de los usuarios en los diferentes sistemas informáticos.			
2.3.	Investigue si la entidad cuenta con un departamento de TI y/o posee personal autorizado para el manejo del software.			
2.4.	Compruebe si el sistema administrativo/contable cuenta con manual de usuario, manual técnico.			
2.5.	Evalúe la administración y control de los accesos de los usuarios al sistema de acuerdo a la estructura jerárquica de la entidad.			
2.6.	Revise la existencia de políticas de capacitación al personal en cuanto a la seguridad del sistema.			
2.7.	Verifique que los equipos informáticos cuenten con software antivirus actualizado.			
2.8.	Identifique si las transacciones que realizan el sistema son fáciles de rastrear.			
2.9.	Compruebe si el sistema administrativo/contable cuenta con un módulo de consultas para ser usado por la entidad.			
2.10.	Verifique si el sistema administrativo/contable cuenta con los reportes necesarios para ser usados por la entidad.			

2.11.	Revise que el sistema cuente con el módulo de ventas y que este cumpla con los requisitos mínimos para poder emitir facturas.			
2.12.	Valide que el sistema cuente con el módulo de inventario y que este cumpla con los requisitos mínimos para poder llevar el control de inventarios.			
2.13.	Compruebe si el módulo de ventas genera la reportería mínima legal (libros de IVA).			
2.14.	Revise que el sistema cuente con el módulo de compras y que este cumpla con los requisitos mínimos para poder llevar el control de compras.			
2.15.	Verifique que el módulo de compras genere la reportería necesaria para dar seguimiento necesario a las compras realizadas.			

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Seguridad lógica

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de seguridad lógica en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

3. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
4. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
3.	**PROCEDIMIENTO DE CUMPLIMIENTO: SEGURIDAD LÓGICA**			
3.1.	Compruebe que el sistema administrativo contable (ERP) exija un código de usuario y contraseña para su acceso.			
3.2.	Verifique las restricciones en los registros que se realizan en los módulos del sistema administrativo contable.			
3.3.	Valide si al crearle la contraseña al usuario el sistema permite menos caracteres de los establecidos por el.			
3.4.	Realice prueba de verificación de que contraseña no pueda ser leída.			
3.5.	Identifique cual es el límite de intentos para entrar al sistema, y comprobar si este se bloquea al sobrepasar.			
3.6.	Identifique si al usuario se le puede restringir el acceso a los diferentes módulos del sistema administrativo/contable.			
3.7.	Comprobé si se ha implementado una política de respaldo de la información y cada cuanto se realiza esta acción.			
3.8.	a) Instalación y actualización diaria de software antivirus.			
3.9.	b) Implementación de mecanismos de filtrado de red, tales como cortafuegos y software de detección de intrusos.			
3.10.	c) Verificar que solo los dispositivos autorizados tengan acceso a la información y red de la empresa.			
3.11.	Solicite el listado de los usuarios que tienen acceso al sistema, según los roles y responsabilidades definidas en el manual de organización de la empresa.			

3.12.	Verifique si en los manuales y procedimientos existen políticas para el acceso al sistema en horas inhábiles para desarrollar el trabajo.			
3.13.	Identifique si los usuarios pueden modificar la fecha y hora de las computadoras.			
3.14.	Verifique si al imprimir los reportes en ellos se identifica la hora y el día en que se han impreso.			
3.15.	Valide que los procedimientos realizados en el sistema queden registro del usuario que los elaboró.			
3.16.	Compruebe los accesos que tienen los usuarios para la instalación de software en los equipos.			
3.17.	Solicite al Proveedor una carta de autenticidad del programa implementado en los equipos.			
3.18.	Valide que las licencias de Microsoft estén vigentes a la fecha.			
3.19.	Identifique si los usuarios tienen acceso a páginas de entretenimiento como redes sociales.			
3.20.	Revise si existen registros documentales que respalden todas las modificaciones realizadas a los valores parametrizables.			

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Seguridad física.

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de seguridad física en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
4.	**PROCEDIMIENTO DE CUMPLIMIENTO: SEGURIDAD FÍSICA**			
4.1.	Compruebe si existen contratos de seguros para proteger las instalaciones y edificaciones de la entidad.			
4.2.	Valide si existe contratos de seguros para proteger el equipo cómputo de la entidad.			
4.3.	Verifique si existe contrato de seguros contra incendios.			
4.4.	Revise si existen detectores de fuego y humo dentro de las instalaciones de la empresa.			

4.5.	Observe si los extintores han sido ubicados en lugares estratégicos.			
4.6.	Capacite a los empleados sobre el uso de los extintores.			
4.7.	Verifique actividades de mantenimiento periódicas al equipo de cómputo de preferencia no mayor a las 1000 hora de uso.			
4.8.	Compruebe la ventilación adecuada para los equipos.			
4.9.	Valide la instalación de polarizado para los equipos eléctricos con los que cuenta la entidad.			
4.10.	Revise si las instalaciones cuentan con antena para rayos.			
4.11.	Verifique si existe equipo de vigilancia de manera interna y externa.			
4.12.	Revise si la empresa cuenta con un panel de control de alarmas.			
4.13.	Verifique si existe un control sobre la entrada del personal interno y externo al centro de cómputo.			
4.14.	Valide el uso de marcación biométrica para el acceso al centro de cómputo.			
4.15.	Revise la marcación digital en los horarios de trabajo.			
4.16.	Realice pruebas mensuales para verificar que el equipo de almacenamiento del backup esté en óptimas condiciones.			
4.17.	Elabore un control numérico de copias de respaldo (backups).			

4.18.	Realice controles de seguridad preventivos contra fallas técnicas, red de usuario y el uso indebido de información por parte de los empleados.			
4.19.	Verifique el cableado adecuado dentro de las instalaciones.			
4.20.	Establecí periodos de vida útil para el cableado de redes y equipo informático.			
4.21.	Revise los paneles y ductos de cableado resistentes al fuego.			
4.22.	Valide que el material de oficina sea resistente al fuego.			
4.23.	Realice la inspección periódica de parte del cuerpo de bomberos.			
4.24.	Verifique los avisos de prohibido comer, beber y fumar cerca del equipo de cómputo de la entidad.			
4.25.	Valide los carnets de identificación diferentes para empleados y visitantes.			
4.26.	Establezca barreras físicas como medidas de prevención en lugares estratégicos para evitar daños a las instalaciones de la entidad.			
4.27.	Realice la asignación de un responsable para cada equipo informático.			
4.28.	Valide la infraestructura de forma mensual de terremotos o sismos sucedidos.			
4.29.	Verifique que la entidad cuente con escaleras de emergencia y que estas sean las adecuadas.			

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Redes

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de redes en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
5.1.	**PROCEDIMIENTO DE CUMPLIMIENTO: REDES**			
5.1.1.	Realice entrevista con la gerencia o máxima autoridad de la compañía y determine las inquietudes y las principales fortalezas, oportunidades, debilidades y amenazas, entorno a las Instalaciones y conectividad de las Redes.			
5.1.2.	Obtenga y clasifiqué los contratos de suministros y servicio de mantenimiento que la compañía posee con los proveedores.			

5.1.3.	Realice entrevista con el personal de mantenimiento de las redes, e identifique si el personal se encuentra debidamente capacitado y posee experiencia para desempeñar sus funciones y pueda responder de forma eficaz y eficiente ante problemas relacionados a las redes y conectividad de la empresa.			
5.1.4.	Realice entrevista con los usuarios de las redes informáticas, e identifique si el personal ha sido capacitado para que tome las medidas pertinentes en caso existan problemas de conectividad, interrupción del servicio o problemas de configuración.			
5.2.	**MANUALES DE PROCEDIMIENTOS Y CONTROLES INTERNOS**			
5.2.1.	Determine la existencia de los Manuales de Procedimientos para la instalación las Redes de Intra, extra e internet.			
5.2.2.	Identifique manuales de procedimientos para la adquisición, cambio y reparación de los componentes de las redes Intra, extra e Internet.			
5.2.3.	Determine la existencia de controles internos, escritos o verbales, sobre el uso de las Redes, accesos a la Intra, extra e internet.			
5.3.	**FUNCIONALIDAD, SERVICIOS Y CONECTIVIDAD DE EQUIPOS E INSUMOS.**			
5.3.1.	Identifique si el personal interno y externos poseen usuarios y contraseña para conectarse a la Red Inalámbrica.			
5.3.2.	Valide si los equipos se encuentran debidamente conectados a la red de la compañía, ya sea de forma alámbrica e inalámbrica.			
5.3.3.	Determine si la conectividad alámbrica e inalámbrica se encuentra en óptimas condiciones, calidad de los insumos utilizados y durabilidad.			

5.3.4.	Compruebe si la compañía cuenta un inventario de repuestos en caso problemas de conectividad, daño o desperfectos en los equipos e insumos utilizados.			
5.3.5.	Identifique el correcto funcionamiento de la conectividad entre equipos y el servidor, el rendimiento es el mismo que el contratado o previsto por la empresa.			
5.4.	**ADICIONES DE EQUIPOS E INSUMOS**			
5.4.1.	Determine la muestra a evaluar de las adiciones de los equipos e insumos que se encuentran actualmente utilizando.			
5.4.2.	Verifique la documentación existente, tales como facturas, créditos fiscales, escrituras y contrato, sobre los equipos, servicios e insumos, amparando el costo de adquisición, flete y traslados, costo de instalación.			
5.4.3.	Revise el adecuado registro de las adiciones y/o altas de equipos e insumos, en contabilidad y controles extra contables.			
	Compruebe si los equipos e insumos poseen codificación de activos, detalle de los equipos e insumos en inventario y en uso.			
5.4.4.	Revise el adecuado tratamiento de la recepción de equipos e insumos de redes: quien es el personal autorizado, procedimiento de verificación física, etc.			
5.4.5.	Examine la integridad del proceso de adición o solicitud de equipo e insumo, documento y/o solicitud de adición o alta, orden de compra, quien solicita, quien autoriza, requerimiento para inventario o para uso directo.			
5.4.6.	Verifique el acceso a los equipos e insumos (incluido las herramientas), se encuentran debidamente resguardados de daños físicos y climáticos, se encuentran bajo llave, personal autorizado para retirar y utilizar.			

5.5.	**BAJAS DE EQUIPOS E INSUMOS**			
5.5.1.	Determine la muestra a evaluar de las bajas de los equipos e insumos que se hayan realizado dentro del periodo de la auditoría.			
5.5.2.	Examine la integridad de la documentación tal como, requerimiento y/o solicitud de baja, usuario que solicita, quien autoriza, quien desinstala o retira el equipo o insumo.			
5.5.3.	Verifique la disposición final de los equipos e insumos dados de baja, se encuentran resguardados dentro o fuera de las instalaciones de la empresa, se desechan, se venden partes como repuestos, quién autoriza la disposición final.			

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: Telecomunicaciones

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de telecomunicaciones en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
6.	**PROCEDIMIENTO DE CUMPLIMIENTO: TELECOMUNICACIONES**			
6.1.	Identifique los Tipos de Medios de telecomunicación que utilizan sus colaboradores en la entidad para la prestación de sus servicios.			
6.2.	Valide si el equipo de comunicaciones está en un lugar cerrado y con acceso Limitado.			
6.3.	Verifique la existencia de procedimientos de autorización para conectar un nuevo equipo a la red.			
6.4.	Compruebe el tipo de topología de red que tiene la empresa.			
6.5.	Verifique el ancho de banda con el que cuenta la empresa.			
6.6.	Verifique el acceso de internet de la empresa.			
6.7.	Valide como está definida la política del perímetro de los firewalls para el uso de internet.			
6.8.	Revise la existencia de controles y procedimientos de la administración en las telecomunicaciones.			
6.9.	Verifique que las medidas de respaldo sean adecuadas.			
6.10.	Compruebe que el software de comunicación sea efectivo y controlado.			
6.11.	Verifique las pruebas de seguridad y control de acceso a cada uno de los roles.			
6.12.	Revise que existan parámetros de medición del desempeño de la red: bitácoras, gráficas, estadísticas.			

6.13.	Compruebe la distribución de las bases de datos en la red sea segura.			
6.14.	Valide cómo se realiza la administración de la red de telecomunicaciones.			
6.15.	Revise cuántos usuarios ingresan a la red de la empresa.			
6.16.	Verifique si disponen de reportes de incidentes y contingencias que afecten el funcionamiento de la red.			
6.17.	Revise el plano de red de comunicaciones para poder establecer riesgos que puedan existir.			
6.18.	Valide el aseguramiento del mecanismo de cifrado en las telecomunicaciones.			
6.19.	Compruebe la implementación de políticas de prohibición para instalar programas dentro de los equipos.			
6.20.	Verifique que cuentas alternativas tiene la entidad para la comunicación.			

PROGRAMA DE AUDITORIA DE SISTEMAS

PROCES: Evaluar TICs con enfoque COBIT 2019

DEPENDENCIA: Departamento de TICs.

DIRIGIDO: Gerencia de TICs

ÀREA: PED

Preparò		
Revisò		
Supervisò		

OBJETIVO GENERAL: Evaluar las tecnologías de información y comunicación en el área de PED en S.O.S. CREDIT, S.A. de C.V., con base en el enfoque COBIT 2019 sobre el "Marco de referencia objetivos de gobierno y gestión" emitido por ISACA.

ESPECÍFICOS:

1. Evaluar el sistema de control interno, concretamente para obtener un conocimiento preliminar del ambiente informático y de los procedimientos de control implementados.
2. Presentar recomendaciones preventivas o correctivas a los responsables del área o proceso, cuando se determinen desviaciones con relación a la eficiencia de las operaciones, confiabilidad de la información y disposiciones legales y administrativas.

No	PROCEDIMIENTO	RE. P/T	ELABORO	FECHA
7.	**PROCEDIMIENTO DE CUMPLIMIENTO: PED**			
7.1.	Identifique donde se inicia las operaciones los usuarios y verifique el seguimiento cronológico de las operaciones que realizan los usuarios.			
7.2.	Examine la validez de los cálculos realizados en operaciones importantes con base a los datos ingresados en el sistema.			
7.3.	Corrobore manualmente los cálculos que han sido solicitados al sistema en el punto anterior y que estos posean los niveles mínimos de seguridad.			
7.4.	Solicite una muestra de datos del módulo de facturación, revise el documento físico y realizar un recalculo de las operaciones diarias, auxiliándose de hojas electrónicas para verificar el atributo de totalidad de saldos en función del procesamiento de datos y la emisión de los reportes.			
7.5.	Realice una prueba para verificar que el sistema posea una rutina de indexamiento, mantenimiento preventivo de datos y validación de datos.			
7.6.	Evalué la existencia y aplicación de estándares para el procesamiento de datos del sistema en la empresa.			

7.7.	Valide la existencia y la aplicación de procedimientos para la corrección y recaptura de datos que fueron ingresados de manera incorrecta.			
7.8.	Verifique la existencia de políticas de capacitación al personal en cuanto a la seguridad del sistema.			
7.9.	Realice la exportación de una base de datos, para efectuar un procedimiento de recalculo de las operaciones generadas en un módulo determinado y verificar los niveles de aproximación de los datos numéricos.			
7.10.	Examine una muestra de datos ingresados al sistema y verificar que estos cumplan con los parámetros mínimos de seguridad para su ingreso.			
7.11.	Obtenga una muestra de datos procesados y compare uno por uno contra documentos físicos.			
7.12.	Evalúe la aplicación de las políticas en ingreso de datos, que estén de acuerdo a las necesidades de los usuarios en cuanto a: - Tiempo - Integridad - Responsabilidad de su elaboración - Mantenimiento.			
7.13.	Describa mediante una narrativa los niveles de conocimiento académico que tienen los empleados del área de informática y específicamente del programa utilizado en la empresa.			
7.14.	Evalúe el manejo que los usuarios poseen del sistema, así como la capacidad de resolver errores leves que no requieran de un profesional técnico.			
7.15.	Identifique los riesgos asociados y su impacto, por la falta de comprensión de los usuarios al sistema.			

7.16.	Verifique que los módulos no efectúen duplicidad de información.			
7.17.	Valide que las claves de acceso sean aplicadas correspondientemente.			
7.18.	Identifique los procedimientos y políticas establecidas para evitar el uso indebido de la información generada por el sistema y su respectivo cumplimiento por cada usuario.			
7.19.	Evalúe mediante la observación e inspección, la utilidad y funcionamiento del sistema de contabilidad.			
7.20.	Verifique el funcionamiento del sistema cuando hay más de dos usuarios ingresando datos.			
7.21.	Seleccione una muestra y verificar los cálculos y completitud de la información.			
7.22.	Compruebe que la información transferida al departamento de contabilidad es recibida sin distorsiones.			
7.23.	Elabore una cédula de detalle que contiene las ventajas y desventajas del sistema de contabilidad utilizado por la empresa, a fin de determinar si este es adecuado para el procesamiento de datos en sus operaciones.			
7.24.	Verifique si se poseen políticas para la tiempo y recuperación de la información contenida en los back ups.			
7.25.	Valide que toda la información que se ingresa al sistema sea totalmente veraz y cumpla con los requerimientos mínimos aceptables.			

CONCLUSIONES

Tomando como base el análisis de la información obtenida en la investigación realizada, se exponen las siguientes conclusiones:

I. Las instituciones que tienen como propósito la formación de los profesionales, no están capacitando adecuadamente en tecnología y comunicación a los auditores estos no buscan educación continua en TICs, mediante cursos de enseñanzas en los cuales se puedan especializar acerca de esta temática.

II. Actualmente las firmas de auditoría no cuentan con una guía en la cual puedan apoyarse si se les presentará la oportunidad de desarrollar un encargo de esta naturaleza; además no se cuenta con información bibliográfica suficiente que esté enfocada específicamente a este tema.

III. Las firmas denotan poco conocimiento sobre el modelo de gestión COBIT 2019, y el marco normativo ISO 27000 y a la vez muestran interés por conocerlos para implementarlo.

RECOMENDACIONES

I. Al consejo de vigilancia de la profesión de contaduría pública y auditoría, red de contadores, instituto salvadoreño de contadores públicos y otras gremiales afines, para que brinden cursos de especialización en tecnologías de la información, los cuales tengan como objetivo a corto plazo la capacitación técnica del auditor para ejercer la auditoría de sistemas en el campo de las TICs.

II. Se les recomienda a los auditores el uso de esta herramienta, la cual describe los elementos mínimos que deben considerarse en el proceso de planificación de auditoría de sistemas para evaluar las tecnologías de información y comunicación.

III. Las firmas deberán implementar una auditoría de sistemas que incluya las áreas y elementos que retoma COBIT 2019 y las ISO 27000; que no han sido cubiertos por las auditorías tradicionales, con el objetivo de alcanzar metas y minimizar los riesgos a un nivel aceptable.

BIBLIOGRAFÍA

Mario G. Piattini Emilio del Peso, (2001), Auditoría informática Un enfoque práctico, 2ª edición ampliada y revisada.

Alonso Tamayo Alzate, (2001), Auditoría de sistemas una visión práctica, Universidad Nacional de Colombia Sede Manizales, I.S.B.N. 958-9322-66-2

Ricardo J. Castello, (2006), Auditoría en entornos informáticos, Segunda edición, I.S.B.N. 950-33-0199-8, e-mail: castello@eco.unc.edu.ar

Marco de referencia COBIT 2019 Objetivos de gobierno y gestión, ©2018 ISACA. Todos los derechos reservados. Para acceder a las instrucciones de uso, visite www.isaca.org/COBITuse

Cuervo Álvarez Sara (2017), ¨Implementación ISO 27001¨, Trabajo fin de máster.

Calderón Trinidad, Osbaldo Antonio, (2007), ¨Manual de auditoría de sistemas para la evaluación de la tecnología de información-MASTI¨, trabajo de graduación UFG, El Salvador. ¨

Raúl Ponce San Juan, (2016), ¨ Auditoría de sistemas de información¨, trabajo en ingeniería administrativa.

Revista digital Universidad Modular Abierta Facultad de Ciencias Económicas, (junio de 2017), ¨auditoría a las tecnologías de información y comunicación¨, información@uma.edu.sv

ANEXOS

Anexo No. 1 guía de preguntas para entrevistar al socio director de la firma

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

Guía de preguntas para entrevista sobre "planificación de auditoría de sistemas aplicables a la evaluación de las tecnologías de información y comunicación"

Solicitud:

Reciba un cordial saludo, somos estudiantes de la Universidad de El Salvador, licenciatura en contaduría pública, que actualmente estamos realizando nuestro trabajo de graduación respecto a la temática antes descrita, para lo cual, es de vital importancia conocer su punto de vista y aspectos de la experiencia profesional que contribuirán con la calidad de la investigación, por lo que solicitamos de su amable colaboración para la realización de la presente entrevista.

Dirigida al: Socio director

Objetivo:

Obtener información precisa y relevante, sobre la evaluación de las tecnologías de información y comunicación en los encargos de auditoría de sistemas, a efecto de la identificación, medición, valoración y análisis de los riesgos relacionados, que permita elaborar propuestas de mejora y fortalecimiento en la firma.

Nombre del entrevistado: _____

Cargo que posee: _____

1. ¿Cuál considera que es la importancia de realizar auditoría a las tecnologías de información y comunicación?

2. ¿Qué diferencias podría resaltar entre la auditoría financiera y auditoría de TI?

3. ¿Qué tipo de encargos de auditoría a las tecnologías de la información y comunicación, se han ejecutado en firma?

4. Mencione si la firma de auditoría cuenta con un equipo especializado en las tecnologías de la información y comunicación

5. Explique si el equipo de trabajo recibe capacitaciones relacionadas a las tecnologías de la información y comunicación de forma periódica

6. Explique si cuentan con políticas y procedimientos en caso de contingencias al momento de la ejecución de las auditorías de sistemas

7. ¿Mencione los puntos o áreas de mejora en la ejecución y evaluación de una auditoría de sistemas?

8. ¿De qué manera se realiza el monitoreo sobre los encargos de auditoría orientados a la evaluación de las tecnologías de información y comunicación?

9. Para la ejecución de la auditoría de sistemas ¿Cuál es la normativa técnica aplicada?

10. Según la nueva realidad y contexto que atraviesa el país, comente ¿considera que la auditoría de sistemas debe de replantearse el enfoque de aplicación y adecuarse a los cambios actuales?

11. ¿Por qué considera que es importante la elaboración de una herramienta de planificación de auditoría de sistemas enfocada en la evaluación de las tecnologías de información y comunicación?

12. ¿La firma de auditoría estaría interesada en implementar una herramienta o propuesta para el fortalecimiento y mejora de los encargos de auditoría, relacionados con evaluación de las tecnologías de información?

¡Muchas gracias!

Anexo No. **2** guía de preguntas para entrevistar al auditor de sistemas

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

Guía de preguntas para entrevista sobre "planificación de auditoría de sistemas aplicables a la evaluación de las tecnologías de información y comunicación"

Solicitud:

Reciba un cordial saludo, somos estudiantes de la Universidad de El Salvador, licenciatura en contaduría pública, que actualmente estamos realizando nuestro trabajo de graduación respecto a la temática antes descrita, para lo cual, es de vital importancia conocer su punto de vista y aspectos de la experiencia profesional que contribuirán con la calidad de la investigación, por lo que solicitamos de su amable colaboración para la realización de la presente entrevista.

Dirigida al: Auditor de sistemas

Objetivo:

Obtener información precisa y relevante, sobre la evaluación de las tecnologías de información y comunicación en los encargos de auditoría de sistemas, a efecto de la identificación, medición, valoración y análisis de los riesgos relacionados, que permita elaborar propuestas de mejora y fortalecimiento en la firma.

Nombre del entrevistado: _____

Cargo que posee: _____

1. Comente si ha recibido certificación en evaluación de las tecnologías de la información y comunicación para realizar las auditorías de sistemas

2. Explique cuáles son las áreas de las tecnologías de información y comunicación con mayor riesgo al ejecutar las auditorías de sistemas

3. Comente si el equipo asignado cuenta con un plan estratégico y sistemático para la ejecución de las pruebas de auditorías de sistemas

4. Detalle cuales son las áreas de tecnologías de información y comunicación evaluadas en la ejecución de la auditoría de sistemas

5. ¿Explique cuál ha sido el mayor reto que se ha presentado a raíz de la pandemia Covid-19, en la planificación y ejecución de la auditoría de sistemas a las tecnologías de información y comunicación?

6. Describa la forma de evidenciar los hallazgos informáticos obtenidos en la auditoría de sistemas.

7. Para la ejecución de la auditoría de sistemas ¿Cuál es la normativa aplicada?

8. Describa si el equipo cuenta con los elementos y herramientas tecnológicas necesarias para una ejecución de los procedimientos de la auditoría de sistemas eficientes

9. Comente si existen áreas de mejora (herramientas, recurso humano, procedimientos, etc.), en la ejecución y evaluación de auditoría de sistemas que considere necesarios

10. ¿Estaría interesado en implementar una herramienta o propuesta para el fortalecimiento y mejora de los encargos de auditoría, relacionados con evaluación de las tecnologías de información?

¡Muchas gracias!

Anexo No. **3** análisis de entrevista a la gerente de auditoría en sistemas

NÚMERO	PREGUNTA	RESPUESTA	COMENTARIO
1	Comente si ha recibido certificación en evaluación de las tecnologías de la información y comunicación para realizar las auditorías de sistemas	He recibido capacitación de los módulos de COBIT para auditorías de TI (Univ. Don Bosco), Actualmente estudiante de maestría en dirección Estratégica de tecnologías de Información con una especialización en evaluación de riesgo TI, Diplomado en capítulo ISACA El Salvador: Auditoría de sistemas.	La gerente de tecnología de información y comunicación está en constante capacitación, por ejemplo: COBIT, dirección estratégica para evaluar riesgos en TI y diplomado en capítulo ISACA, en auditoría de sistemas.
2	Explique cuáles son las áreas de las tecnologías de información y comunicación con mayor riesgo al ejecutar las auditorías de sistemas	Se debe de indagar el Gobierno TI de la organización. Conocer los planes estratégicos de TI, planes operativos, planes de contingencia y/o continuidad del negocio, personal técnico informático que conforma la dirección, con la competencia y debida capacitación, el entorno de la entidad apoyado con tecnologías informáticas y del Área de Tecnologías de la Información, bases de datos, la infraestructura tecnológica. Determinar el enfoque basado en riesgos para evaluar la función de TI, el ambiente de control de la organización y líneas de autoridad y responsabilidad y definición clara de las funciones de las áreas que conforman la TI. La distribución de los	Las políticas que ha adoptado, estándares y procedimientos que sirven de base para la administración, control y evaluación de sus actividades, aseguramiento de calidad de los servicios de información, la seguridad y confiabilidad de la información. El entorno de la entidad apoyado con tecnologías informática y del área de tecnologías de la Información, bases de datos, la infraestructura tecnológica, calidad y efectividad de los servicios y soporte informático, planes de mantenimiento preventivo y correctivo de la plataforma tecnológica, teniendo presente que la ubicación y estructura organizacional del área de informática le permita brindar el apoyo a todas las unidades de la entidad.

		recursos de TI y el desempeño de los procesos administrativos, funciones desarrolladas por el capital humano de la TI y seguridad física e instalaciones de cuartos de servidores, (Data Center).	Analizar el nivel jerárquico de la TIC dentro de la pirámide administrativa para el cumplimiento de sus objetivos y el apoyo de la máxima autoridad.
3	Comente si el equipo asignado cuenta con un plan estratégico y sistemático para la ejecución de las pruebas de auditorías de sistemas	TI cuenta con el plan de contingencia, continuación de negocio, capas de seguridad con las que se gobierna el área de TI. Anualmente se realiza la auditoría de sistemas, se reciben las recomendaciones las cuales de manera anual se incorpora en el presupuesto de TI para ir fortaleciendo cualquier hallazgo.	Los servidores de desarrollo cuentan con todas las actualizaciones de los servidores de producción lo que ha permitido que las auditorías realicen pruebas preliminares para luego realizarlas en los ambientes de producción.
4	Detalle cuales son las áreas de tecnologías de información y comunicación evaluadas en la ejecución de la auditoría de sistemas	Gestión del Gobierno TI de la organización. Evaluación de los planes estratégicos de TIC, planes operativos, planes de contingencia y/o continuidad del negocio, planes de mantenimiento preventivo y correctivo de la infraestructura tecnológica Evaluación de la formación técnica del recurso humano de TI Enfoque basado en riesgos para evaluar la función de TI, integridad y seguridad de la información.	El área de TI cuenta con: Políticas, control y evaluación de actividades, aseguramiento de calidad de los servicios de información, la seguridad y confiabilidad de la información. Planes operativos, planes de contingencia y/o continuidad del negocio, planes de mantenimiento preventivo y correctivo de la infraestructura tecnológica.
5	¿Explique cuál ha sido el mayor	Actualmente se	El área de TI

	reto que se ha presentado a raíz de la pandemia Covid-19, en la planificación y ejecución de las auditorías de sistemas a las tecnologías de información y comunicación?	administra un modelo hibrido tanto en el iCloud como de infraestructura TI propia, por lo tanto, los servicios principales están en la nube lo que no ha complicado la ejecución de dicha evaluación, pues llevamos 3 años en este proceso, las auditorías de sistemas en pandemia han sido efectuadas sin problemas. El Teletrabajo fue posible porque el 90% de servicios están desarrollados para operar tanto interna como externamente, se activó una política de TI para brindar los accesos con las autorizaciones del nivel ejecutivo correspondiente y brindar la seguridad tanto de la computadora del cliente hacia nuestros servidores.	estableció criterios de seguridad para garantizar integridad en la conectividad, pero en sí mismo la pandemia no ha concebido un inconveniente para ejecutar tal actividad.
6	Describa la forma de evidenciar los hallazgos informáticos obtenidos en las auditorías de sistemas	Elaboración de un Informe con una estructura similar a: - Hallazgos de Auditoría El auditor deberá elaborar los hallazgos cuando haya confirmado la observación -Condición de observación; Describe o relata lo que sucedió, debe ser puntual y específica. -Criterio o normativa incumplida - Causa - Efecto -Comentarios de la Administración de TI -Comentarios del	Para evidenciar los hallazgos informáticos el auditor de sistemas debe de hacerlo con un informe de hallazgos. El informe de hallazgos debe de elaborarse siempre y cuando este se haya confirmado. Y debe de cumplir con los apartados siguientes: condición de observación, criterio o normativa incumplida, causa, efecto, comentarios de la administración de TI, comentario de auditor, recomendaciones de auditoría.

		Auditor -Recomendaciones de auditoría.	
7	Para la ejecución de la auditoría de sistemas ¿Cuál es la normativa aplicada?	Para las organizaciones gubernamentales están estipuladas en los artículos 30 y 31 de la Ley de la Corte de Cuentas de la República y al Reglamento de las Normas Técnicas de Control Interno Específicas del CNR. Para las empresas privadas están contempladas en el sistema de gestión de la calidad que se rigen, en sus políticas o reglamentos internos.	Dependiendo de la institución, entidad gubernamental, empresa privada, cada una puede aplicar la normativa que por ley se establece o la normativa contemplada en el sistema de gestión de calidad, según políticas o reglamentos internos.
8	Describa si el equipo cuenta con los elementos y herramientas tecnológicas necesarias para una ejecución de los procedimientos de la auditoría de sistemas eficientes	Si se cuenta con los elementos necesarios para que se desarrolle una auditoría de sistemas: se cuenta con el marco legal de TI, políticas, planes de contingencia, etc.…las herramientas tecnológicas, cualquier información que se ha requerido se ha brindado si es sistemas de información, análisis de seguridad perimetral de la red, firewall, etc.	El equipo de auditoría si cuenta con los elementos necesarios para ejecutar la auditoría, por ejemplo: marco legal de TI, políticas, planes de contingencia, etc. Además, cuenta con las herramientas tecnológicas, entre ellas equipos informáticos, hardware, software, entre otros.
9	Comente si existen áreas de mejora (herramientas, recurso humano, procedimientos, etc.), en la ejecución y evaluación de auditoría de sistemas que considere necesarios	Creo que la mayoría de auditores fallan en los procedimientos de su ejecución, primero no lo conocen todo, porque el área de TI tiene muchas especialidades, tendría que ser un especialista en todas las áreas algo difícil, pero puede haber excepciones. Que cuenten con la formación en COBIT, ISACA pueden apoyar a desarrollar una auditoría de sistemas más ad hoc.	El área de las TI es muy amplia, con muchas especialidades es complicado que un solo auditor se especialice en todas ellas, pero con la formación y especialización en COBIT e ISACA, se pueden desarrollar auditorías de sistemas más ad hoc.
10	¿Estaría	El interés estaría en	Se habla de una

	interesado en implementar una herramienta o propuesta para el fortalecimiento y mejora de los encargos de auditoría, relacionados con evaluación de las tecnologías de información?	conocer la propuesta de fortalecimiento de los encargados de auditoría. No sé si se habla de una herramienta informática o técnico/metodología.	herramienta técnica/metodológica la cual pretende ser una guía al momento de realizar la planificación de la auditoría de sistemas.

Nota: entrevista realizada en la plataforma zoom a la gerente de auditoría en sistemas.

Anexo No. **4** análisis de entrevista a la directora de la firma

NÚMERO	PREGUNTA	RESPUESTA	COMENTARIO
1	¿Cuál considera que es la importancia de realizar auditoría a las tecnologías de información y comunicación?	La importancia es que la información viaje de forma íntegra y que se fiable, para efectuar los procedimientos y poder pronunciar una opinión	La opinión a la que se refiere el entrevistado corresponde a la opinión sobre auditorías fiscal y auditoría financiera exclusivamente
2	¿Qué diferencias podría resaltar entre la auditoría financiera y auditoría de TI?	La auditoría financiera busca dar una razonabilidad en las cifras de los Estados Financieros, y la auditoría de TI busca evaluar que la información sea integral e identificar la vulnerabilidad del sistema	Para la firma, los resultados de la auditoría TI es complementaria a la auditoría financieras y fiscales
3	¿Qué tipo de encargos de auditoría a las tecnologías de la información y comunicación, se han ejecutado en firma?	La evaluación se realiza a través de la auditoría financiera o auditoría fiscal, donde se evalúa los rubros importantes, ingresos, inventario, planilla, costos; así como entrevista con los usuarios que alimentan la información, pero no se realiza una auditoría de TI como un servicio independiente.	La firma no ejecuta una auditoría de TI de forma independiente de otros servicios
4	Mencione si la firma de auditoría cuenta con un equipo especializado en las tecnologías de la información y comunicación.	La firma de auditoría cuenta con un equipo conformado por 2 personas, sin embargo, se cuenta con un especialista contratado como outsourcing que apoya en los clientes más representativos y áreas específicas.	La utilización del especialista corresponde a la confidencialidad y hermetismo que los clientes exigen

5	Explique si el equipo de trabajo recibe capacitaciones relacionadas a las tecnologías de la información y comunicación de forma periódica	El personal de TI recibe entre una o dos capacitaciones al año especializadas, junto con otras capacitaciones cumpliendo un aproximado de 40 horas anuales	El equipo de TI cuenta con capacitaciones adicionales al área de informática
6	Explique si cuentan con políticas y procedimientos en caso de contingencias al momento de la ejecución de las auditorías de sistemas	La firma no posee un manual de procedimientos para contingencias, pero al encontrar inconveniente se realizan procedimientos analíticos, narrativas, preguntas claves y print screen para respaldar lo más posible	Al no tener un servicio de auditoría de TI no ha sido necesario tener un manual o políticas de forma escrita
7	¿Mencione los puntos o áreas de mejora en la ejecución y evaluación de una auditoría de sistemas?	Que los clientes tomen una mayor importancia al área de las tecnologías, y realizar una evaluación inicial al sistema para poder desarrollar una planificación para las futuras pruebas	Para una empresa maximizar sus ganancias es primordial, por lo que no incurrirán en gastos que no sean necesario o gastos
8	¿De qué manera se realiza el monitoreo sobre los encargos de auditoría orientados a la evaluación de las tecnologías de información y comunicación?	En la firma de auditoría, el personal de TI es la única área que posee la experticia suficiente para evaluar los procedimientos, por lo que no existe un monitoreo de forma independiente del área, el departamento únicamente se retroalimenta con un informe al final de sus procedimientos.	La firma de auditoría no cuenta con personal capacitado fuera del área de TI para monitorear el su desempeño
9	Para la ejecución de la auditoría de sistemas ¿Cuál es la normativa técnica aplicada?	Se utiliza las NIAS como marco de referencia	No posee conocimiento respecto a la normativa técnica aplicada en una auditoría de sistemas

10	Según la nueva realidad y contexto que atraviesa el país, comente ¿considera que la auditoría de sistemas debe de replantearse el enfoque de aplicación y adecuarse a los cambios actuales?	La auditoría de sistema debe de realizar evaluaciones incluyendo el home office, la información virtual, y facturación electrónica, se debe de considerar la vulnerabilidad del internet residencial y accesos a personal no autorizado al equipo de trabajo de los empleados en modalidad home office	Con el home office será importante que las empresas consideren proteger su información, desde los puntos de conexión ya que la seguridad informática en las residencias de los colaboradores es muy vulnerable
11	¿Por qué considera que es importante la elaboración de una herramienta de planificación de auditoría de sistemas enfocada en la evaluación de las tecnologías de información y comunicación?	Es importante porque hace más eficiente el trabajo de las auditorías en general, los especialistas en el área de TI pueden evaluar información específica, ya que, por su naturaleza, cantidad de información y procesos que los sistemas informáticos ejecutan, no pueden ser evaluados de forma manual.	La opinión del socio de la firma está enfocada en que la auditoría de TI es una herramienta de apoyo para las auditorías financieras y fiscales, y no como una auditoría independiente que debe de tener su procedimiento bien estructurado de planeación, ejecución y revisión.
12	¿La firma de auditoría estaría interesada en implementar una herramienta o propuesta para el fortalecimiento y mejora de los encargos de auditoría, relacionados con evaluación de las tecnologías de información?	Si estamos interesados, ya que hoy por hoy, las compañías le han dado importancia al tema digital, y esto va de la mano con la auditoría	El documento que será entregado será un apoyo muy importante en las futuras auditorías, así como de cubrir áreas que a la fecha no se encuentren contemplados evaluar

Nota: entrevista realizada en la plataforma zoom a la directora de la firma.