Maestría en Seguridad Informática
Curso de Auditoría Informática

PROYECTO FINAL

La Auditoría es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

En virtud de lo anterior, los equipos de trabajo del curso de Auditoría Informática habrán de realizar práctica de auditoría como proyecto final, enfocada en alguna de las áreas listadas a continuación:

- Gobierno y Gestión de IT (COBIT 2019, ISO 38500)
- Adquisición, Desarrollo e Implementación de Sistemas de Información (OWASP, ISO/IEC 15504, ISO/IEC 33000, ISO 55000, CMMI)
- Operaciones, Mantenimiento y Soporte de los sistemas de información (ITIL, CMMI Servicios, ISO 20000)
- Plan de BCP/DRP (ISO 22301, ISO 24752, ISO 31000)
- Protección de los Activos de Información (Clasificación de los activos de la información, ISO 27001)
- Otra que el catedrático asigne

La auditoría deberá ser desarrollada considerando los aspectos sobre la gestión de un programa de auditoría, su planificación y realización como por ejemplo "ISO19011 Directrices para la Auditoría de Sistemas de Gestión", entre otras, combinado con el estándar, buenas prácticas y/o cuerpo de conocimientos que apoya el área a auditar.

I. ENTREGABLES DEL PROYECTO

Para su efectivo avance, la auditoría de sistemas de información deberá presentarse mediante entregables cuyo contenido mínimo se describe a continuación.

Primer entregable: Conocimiento y comprensión del área a auditar

Previo a la elaboración del plan de auditoría, se debe investigar todo lo relacionado con el área a auditar, para poder elaborar el plan en forma objetiva. Este análisis debe contemplar: el período a evaluar, dónde se identificó el riesgo, su descripción, responsables, las disposiciones legales que la rigen, características del sistema que utiliza, y todo aquello que sirva para comprender exactamente cómo funciona el área de la empresa a auditar.

El equipo de auditoría habrá de identificar el área específica a auditar y priorizar los riesgos según el análisis realizado. Se recomienda considerar la metodología COSO ERM u otras herramientas consideradas por el catedrático. El equipo deberá presentar al menos:

a. Identificación del área a auditar
b. Cuestionario de control interno
c. Matriz de evaluación de riesgos y controles

VISIÓN													
VALORES													
OBJETIVO GENERAL													
PROCESO DE LA EMPRESA	COMPONENTE TI	IDENTIFICACIÓN DE RIESGO				EVALUACIÓN DEL RIESGO		TRATAMIENTO DEL RIESGO			Control Implementado		
Nombre del Proceso	Nombre del Componente	ID Riesgo	Nombre del Riesgo	Causa	Consecuencia	Probabilidad	Impacto	Respuesta al Riesgo	Responsable	Prioridad			
						3	4						

Ilustración 1 - Matriz de evaluación de riesgos (Propuesta)

d. Mapa de calor

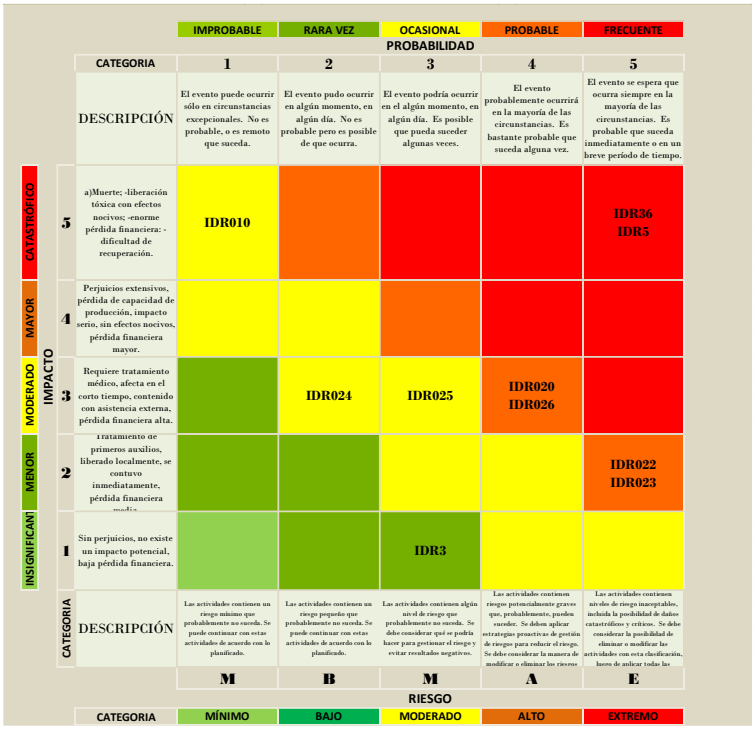

Ilustración 2 - Mapa de calor (Propuesta)

Primer entregable: Planificación de la auditoría

En esta fase se debe tener un entendimiento del área a ser auditada y delimitar el trabajo que se va a realizar para cumplir en tiempo y contar con el personal idóneo en la ejecución de esta. El equipo de auditoría deberá presentar al menos:

a. Fundamento de la auditoría (leyes, normas, resoluciones, reglamentos, acuerdos, etc. que justifican y permiten la evaluación)
b. Objetivos de la auditoría (general y específicos)
c. Alcance de la auditoria
d. Recursos (RRHH, mobiliario, herramientas, etc.)
e. Programa de auditoría (actividades a realizar, cronograma específico)

Segundo entregable: Ejecución de la auditoría

La ejecución de la auditoría involucra una variedad de actividades, que incluyen: realizar evaluaciones de riesgo, ejecutar procedimientos, revisar y analizar evidencia, entre otras. Por lo anterior, el equipo de auditoría deberá presentar al menos lo siguiente:

a. Definición de herramientas y metodologías (CAATs, buenas prácticas, BoK, estándares, marcos de trabajo)
b. Pruebas sustantivas (cuestionarios, entrevistas, check list, diagramas, etc.)
c. Pruebas de cumplimiento (basado en los criterios de auditoria)
d. Pruebas de consentimiento (escenarios, hacking, etc.)

Esta fase deberá de acreditarse con los papeles de trabajo pertinentes que evidencien la realización de esta. Los papeles de trabajo de la auditoría son la principal evidencia documental de las pruebas de auditoría, las discusiones y las observaciones. La administración de los papeles de trabajo debe estar centralizada, automatizada y disponible en tiempo real, de modo que la supervisión que ejerza el catedrático sea transparente.

Segundo entregable: Informe de auditoría

El informe de auditoría es la expresión de una opinión profesional, en el que se materializa el resultado del ejercicio de auditoría y contiene además del dictamen, la evaluación del control interno, el cumplimiento de las normas y procedimientos y otros aspectos relacionados con la gestión y el periodo examinado. En esta fase, el equipo de auditoría habrá de presentar el informe de sus actividades bajo la estructura siguiente:

a. Carátula de la auditoria
b. Carta de presentación
c. Informe ejecutivo (máximo de dos páginas)
d. Hallazgos (tipo de hallazgo, título del hallazgo, área de mejora, condición, criterio, causa, efecto, recomendación)
e. Comentarios de la administración

Fechas de entregables (sugeridas)

Actividad	Detalle	Fecha
Entrega de enunciado del Proyecto Final		06- de Diciembre
Primer entregable	Identificar el área a ser auditada	29 de Noviembre
	Planeación de auditoría	
Segundo entregable	Ejecución de auditoría	06- de Diciembre
	Informe final	

Tabla 1 - Detalle de entregables y fechas de recepción sugeridas

II. PRESENTACIÓN DE LA DOCUMENTACIÓN DEL PROYECTO FINAL

La estructura del documento final a presentar por cada uno de los equipos de auditoría es la siguiente:

1. Caratula
2. Introducción
3. Desarrollo de la auditoría (entregables)
   a. Conocimiento y comprensión del área a auditar
   b. Planeación de auditoría
   c. Ejecución de auditoría
   d. Informe final de auditoría
4. Conclusiones y recomendaciones
5. Referencias bibliográficas
6. Anexos

Adicionales:

- El tipo de hoja que se emplea en cuanto al tamaño son las denominadas "tamaño carta".
- El tipo de letra es Arial, tamaño 12 normal.
- El interlineado es de 1,5 para todo el texto.
- Las sangrías en el primer renglón de cada párrafo cumplen la función de destacarlos visualmente. Se expresan con un número de 5 espacios.
- Los márgenes son de: 3,5 cm para el margen izquierdo y 2,5 cm para el derecho; y 3 cm para los márgenes superior e inferior.
- Todas las páginas del trabajo deben estar numeradas, excepto la portada y el índice. La numeración que se usa es la arábiga y la posición es el ángulo superior derecho.

Nota: donde realice alguna cita, inserte o cree alguna tabla o imagen y para referencias bibliográficas utilice el estándar APA 7.

III. CALIFICACIÓN

A continuación, se describen los puntos a evaluar con su respectiva escala de calificación:

- Las calificaciones posibles por cada elemento a ser evaluado dentro del proyecto son:
  - EXCELENTE (100% del Punteo): El Cumple a un 100% con la solución debidamente aplicada.
  - BUENO (80% del Punteo): El Cumple a un 80% con la solución debidamente aplicada.
  - ACEPTABLE (60% del Punteo): Cumple a un 60% con la solución debidamente aplicada.
  - DEFICIENTE (40% del Punteo): Cumple a un 40% con la solución debidamente aplicada.

- NO ACEPTABLE (10% del Punteo): Cumple con menos del 40% con la solución debidamente aplicada.

- El proyecto final será evaluado sobre 40 puntos.