LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA	NOMBRE DEL CURSO: AUDITORIA INFORMÁTICA UNIDAD: I
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ	FIRMA DEL DOCENTE

DATOS GENERALES DEL PROCESO DE EVALUACIÓN

NOMBRE DEL ALUMNO: DOMINGUEZ CRUZ DANIELA	No. DE CONTROL: 21140371	FIRMA DEL ALUMNO:
PRODUCTO: RESUMEN	FECHA: 28/09/2023	PERIODO ESCOLAR: SEPT 2023 - ENE 2024

INSTRUCCIONES DE APLICACIÓN

Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.

VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
5	Material a utilizar: Se apegó a los criterios previamente establecidos.	X		
5	Creatividad: Plasmó los temas con ingenio.	X		
0	Originalidad: El producto es único.	X		
5	Contiene todos los temas relacionados a la unidad.	X		
5	Claridad y Estructura: Se da a entender el tema que se está tratando.	X		
0	Responsabilidad: Entregó el producto en la fecha y hora señalada.	X		
20 '/.	**CALIFICACIÓN**	20 '/.		

LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA	NOMBRE DEL CURSO: AUDITORIA INFORMÁTICA UNIDAD: I
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ	FIRMA DEL DOCENTE

DATOS GENERALES DEL PROCESO DE EVALUACIÓN		
NOMBRE DEL ALUMNO: DOMINGUEZ CRUZ DANIELA	No. DE CONTROL: 21140371	FIRMA DEL ALUMNO:
PRODUCTO: REPORTE TÉCNICO	FECHA: 28/09/2023	PERIODO ESCOLAR: SEPT 2023 - ENE 2024

INSTRUCCIONES DE APLICACIÓN

Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.

VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
10	Material a utilizar: Se apegó a los criterios previamente establecidos.	X		
0	Creatividad: Plasmó los temas con ingenio.	X		
0	Originalidad: El producto es único.	X		
10	Contiene todos los temas relacionados a la unidad.	X		
10	Claridad y Estructura: Se da a entender el tema que se está tratando.	X		
0	Responsabilidad: Entregó el producto en la fecha y hora señalada.	X		
30%	**CALIFICACIÓN**	30%		

LISTA DE COTEJO

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA	NOMBRE DEL CURSO: AUDITORIA INFORMATICA UNIDAD: I
NOMBRE DEL DOCENTE: ROSARIO CARVAJAL HERNÁNDEZ	FIRMA DEL DOCENTE

DATOS GENERALES DEL PROCESO DE EVALUACIÓN

NOMBRE DEL ALUMNO: DOMINGUEZ CRUZ DANIELA	No. DE CONTROL: 21140371	FIRMA DEL ALUMNO:
PRODUCTO: AVANCE DE PROYECTO	FECHA: 28/09/2023	PERIODO ESCOLAR: SEPT 2023 - ENE 2024

INSTRUCCIONES DE APLICACIÓN

Revisar las actividades que se solicitan y marque con una X en los apartados "SI" cuando la evidencia se cumple; en caso contrario marque "NO". En la columna "OBSERVACIONES" escriba indicaciones que puedan ayudar al alumno a saber cuáles son las condiciones no cumplidas, si fuese necesario.

VALOR DEL REACTIVO	CARACTERÍSTICA A CUMPLIR (REACTIVO)	CUMPLE		OBSERVACIONES
		SI	NO	
10	Material a utilizar: Se apegó a los criterios previamente establecidos.	X		
10	Creatividad: Plasmó los temas con ingenio.	X		
5	Originalidad: El producto es único.	X		
10	Contiene todos los temas relacionados a la unidad.	X		
10	Claridad y Estructura: Se da a entender el tema que se está tratando.	X		
5	Responsabilidad: Entregó el producto en la fecha y hora señalada.	X		
50'1.	**CALIFICACIÓN**	50'1.		

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA.

“RESUMEN UNIDAD 1”

INGENIERÍA INFORMÁTICA

Materia:

AUDITORIA INFORMÁTICA

Profesora:

ROSARIO CARVAJAL HERNÁNDEZ

Por:

DANIELA DOMÍNGUEZ CRUZ

Fecha: 28/Septiembre/2023

CONCEPTO

Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

CLASES DE AUDITORÍA

1. Auditoría Financiera: Presenta la realidad
2. Auditoría Informática: Operatividad eficiente y según normas establecidas
3. Auditoría de Gestión: Eficacia, eficiencia, economicidad
4. Auditoria de Cumplimiento: Las operaciones se adecuan a estas normas.

La opinión profesional, elemento esencial de la auditoría, se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma.

Como es natural, cada una de las clases o tipos de auditoría posee sus propios procedimientos para alcanzar el fin previsto aun cuando puedan en muchos casos coincidir. El alcance de la auditoría, concepto de vital importancia, nos viene dado por los procedimientos. La amplitud y profundidad de los procedimientos que se apliquen nos definen su alcance.

Para ello se establecen unas normas y procedimientos que en cuanto a la ejecución de la auditoría se resumen en que:

1. El trabajo se planificará apropiadamente y se supervisará adecuadamente.
2. Se estudiará y evaluará el sistema de control interno.
3. Se obtendrá evidencia suficiente y adecuada

Estas tres normas se deducen claramente de la situación real actual de los riesgos que ha de afrontar el auditor.

Sin embargo, cuando llegó la llamada revolución cuantitativa, que trajo consigo la creación de sociedades con importantes medios, que las operaciones se

multiplicaran enormemente y que la gestión y propiedad se diferenciaran cada vez más claramente, el método tradicional resultó laborioso, tedioso, largo, ineficaz y económicamente inviable.

No era posible verificar la totalidad de las muy cuantiosas operaciones y, por tanto, había que reducir el campo de acción del auditor a parte de la numerosa información.

Este nuevo planteamiento, sin embargo, traía implícito un riesgo evidente, al no verificarse la totalidad de los movimientos.

Los controles establecidos por la entidad auditada pudieran permitir que se produjeran irregularidades, potencialmente significativas, casuales o voluntarias.

VARIACIÓN DEL OBJETO

Por añadidura es innegable, que con mayor o menor profundidad la gestión de las entidades ha experimentado un cambio sustancial y hoy, salvo casos dignos del Guinness, se utiliza la TI (Tecnología de la Información) en todo proceso contable.

Se ha introducido un nuevo elemento cualitativo en el objeto de la auditoría, el uso de la informática como factor consustancial a la gestión, con la introducción de la Tecnología de la Información (TI) en los sistemas, muy probablemente basada en las ventajas que aporta la informatización con respecto al trabajo manual, entre las que, según C. Martin, se podrían distinguir:

1. Costo de explotación
2. Costo de operación
3. Rendimiento continuado
4. Consistencia
5. Capacidad de cálculo
6. Reacción ante lo inesperado
7. Sentido común
8. Lenguaje

Este nuevo elemento (TI), puede estar y de hecho tiende a estar en todos los niveles del sistema.

Este hecho impone un nuevo condicionante al auditor: ha de trabajar ante y con los elementos de TI. Dado que según las propias Normas Técnicas de auditoría que regulan su actuación el auditor debe tener en cuenta todos los elementos de la entidad incluso los informáticos.

La consultoría consiste en “dar asesoramiento o consejo sobre lo que se ha de hacer o cómo llevar adecuadamente una determinada actividad para obtener los fines deseados”.

Los elementos de consultoría podrían resumirse en:

- Contenido: Dar asesoramiento o consejo
- Condición: De carácter especializado
- Justificación: En base a un examen o análisis
- Objeto: La actividad o cuestión sometida a consideración
- Finalidad: Establecer la manera de llevarla a cabo adecuadamente

El Control Interno Informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la Organización y/o Dirección Informática, así como los requerimientos legales.

La misión del Control Interno Informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.

- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al Grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informática.

AUDITORÍA INFORMÁTICA

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por computador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección,

requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.

- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

EL plan de auditor Informático es el esquema más importante del auditor informático. En este documento se debe describir todo sobre la función y el trabajo que se realiza en la entidad.

Las partes de un plan auditor informático deben ser al menos las siguientes:

- **Funciones:** Debe existir una clara segregación de funciones con la Informática y de control interno informático, y éste debe ser auditado también. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.
- **Procedimientos para las distintas tareas de las auditorías:** Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.
- **Tipos de auditoría que realiza.**
- **Sistema de evaluación y los distintos aspectos que evalúa.**
- **Nivel de exposición:** El nivel de exposición en este caso un número del 1 al 10 definido subjetivamente y que me permite en base a la evaluación final de la auditoría realizada sobre ese tema.
- **Lista de distribución de informes**
- **Seguimiento de las acciones correctoras**
- **Plan quinquenal**: Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartirse en cuatro o cinco años de trabajo. Esta planificación, además de las repeticiones y añadido de las auditorías no programadas que se estimen oportunas, deberá componer anualmente el plan de trabajo anual.

- **Plan de trabajo anual:** Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado nos dé un resultado de horas de trabajo previstas y, por tanto, de los recursos que se necesitarán. [1]

En general, el auditor debe utilizar la computadora en la ejecución de la auditoría, ya que esta herramienta permitirá ampliar la cobertura del examen, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente. Existen paquetes de computadora que permiten elaborar auditorías a sistemas financieros y contables que se encuentran en medios informáticos. Además, el empleo de la computadora por el auditor le permite familiarizarse con la operación del equipo en el centro de cómputo de la institución.

Con fines de auditoría, el auditor interno puede emplear la computadora para:

- Utilización de paquetes para auditoría; por ejemplo, paquetes provenientes del fabricante de equipos, firmas de contenedores públicos o compañías de software
- Supervisar la elaboración de programas que permitan el desarrollo de la auditoría interna
- Utilización de programas de auditoría desarrollados por proveedores de equipo, que básicamente verifican la eficiencia en el empleo del computador o miden la eficiencia de los programas, su operación o ambas cosas.

PLANEACIÓN DE LOS PROCEDIMIENTOS DE AUDITORÍA CON INFORMÁTICA

El propósito principal de la planeación de las medidas de auditoría es incluir dentro de las aplicaciones las facilidades que permitan realizar las actividades de auditoría de la manera más fluida.

La planeación de los servicios establece las facilidades tanto actuales como futuras que ofrece la dirección de informática. El auditor debe examinar este plan para establecer los requerimientos de auditoría necesarios.

El poder planear y realizar estas tareas implica un trabajo complicado pero que es necesario hacer. La computarización de las organizaciones ha dado por resultado una concentración de datos y funciones, que son seleccionados, correlacionados, resumidos y diseminados.

Es necesario que el auditor cuente con las herramientas adecuadas para poder seguir el rastro del mismo y también verificar que el sistema esté realizando las funciones que supuestamente debe ejecutar; estas herramientas computarizadas le deben permitir detectar errores y corregirlos.

Es comprensible que el auditor no es un programador especializado, por lo que es obligación de este grupo planear el desarrollo de estas herramientas de cómputo, atendiendo las solicitudes y recomendaciones de los auditores y aportando su propia experiencia.

También debe participar en las pruebas en paralelo y en la implantación del sistema, para asegurarse de que todos los procedimientos, entradas y salidas son los solicitados por el usuario en el momento del diseño detallado.

La participación del auditor interno en el diseño e implementación de un sistema es de suma importancia. El auditor interno debe estar presente en el desarrollo del sistema para evaluar que la información requerida por el usuario quede cubierta y se cumpla con el grado de control que necesita la información procesada del sistema, de acuerdo con los objetivos y políticas de la organización.

Existen ciertas habilidades fundamentales que deber ser consideradas como las mínimas que todo auditor de informática debe tener:

- Habilidad para manejar paquetes de procesadores de texto
- Habilidades para el manejo de hojas de cálculo
- Habilidad para el uso de E-mail y conocimiento de Internet
- Habilidad para el manejo de bases de datos
- Habilidad para el uso de al menos un paquete básico de contabilidad

Como evaluador, el auditor de informática debe ser capaz de distinguir entre los procesos de evaluación de sistemas y las aproximaciones que son apropiadas para encauzar los propósitos específicos de evaluación relevante para el área de trabajo. En este caso, el auditor en informática debe tener los conocimientos de los pasos requeridos para aplicar una evaluación particular en el contexto de la tecnología de información.

Las habilidades técnicas requeridas por el auditor en informática son las de implantar, ejecutar y comunicar los resultados de la evaluación en el contexto de la tecnología de información, de acuerdo con estándares profesionales que gobiernen el objetivo de la auditoría. [2]

Referencias

[1] M. d. Clase, 19 Agosto 2016. [En línea]. Available: https://classroom.google.com/c/NjIxMDMxMzgyMzY2/m/NjIyODM2NzgyOTkw/details. [Último acceso: 16 Septiembre 2023].

[2] M. d. clase, 19 Agosto 2016. [En línea]. Available: https://classroom.google.com/c/NjIxMDMxMzgyMzY2/m/NjIyODM2NzgyOTkw/details. [Último acceso: 16 Septiembre 2023].

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA.

REPORTE TÉCNICO: ROL Y RESPONSABILIDAD DEL AUDITOR EN EL PROCESO DE AUDITORÍA

INGENIERÍA INFORMÁTICA

Materia:

AUDITORIA INFORMÁTICA

Profesora:

ROSARIO CARVAJAL HERNÁNDEZ

Por:

DANIELA DOMÍNGUEZ CRUZ

Fecha: 28/Septiembre/2023

INTRODUCCIÓN

El presente reporte tiene como objetivo detallar el rol y las responsabilidades del auditor, así como proporcionar ejemplos de cómo se desarrolla este proceso de auditoría.

Cuando hablamos de auditoria nos referimos a un proceso crítico donde el auditor es el encargado de evaluar la seguridad y el cumplimiento del proyecto que se esté realizando asegurando que los procesos digitales cumplan los requisitos legales y brindando confianza a los clientes, inversores, etc. de una empresa u organización.

ROL DEL AUDITOR

1. **Evaluación de riesgos**

El auditor comenzará evaluando los riesgos en el entorno de la empresa, esto incluye entender todo el entorno de la empresa, las políticas y los procesos internos, de igual forma se encarga de evaluar los riesgos y las posibles amenazas cibernéticas, las vulnerabilidades del sistema, etc.

2. **Planificación de la Auditoría**

Con base a la evaluación de riesgos, los auditores deberán desarrollar un plan de auditoría. Debe incluir la identificación de los sistemas, aplicaciones y los procesos que se van a auditar, así mismo deberá definir los objetivos específicos de la auditoría. Esto también deberá incluir la extensión de pruebas necesarias, los recursos que requeridos y el cronograma de actividades de trabajo.

3. **Acciones de optimización**

El principal propósito de un auditor es mejorar la producción de las empresas, entonces, al trabajar junto a los distintos departamentos, ya sean; Dirección General y Finanzas, los auditores deberán identificar productor y servicios que sean eficientes y competitivos.

4. **Recopilación de Evidencia**

El auditor deberá recopilar evidencia para evaluar la seguridad y el cumplimiento de los sistemas, también deberá revisar documentos, hacer entrevistas con el personal, hacer pruebas de control y técnicas de vulnerabilidades. Este rol se basa principalmente en evaluar la exactitud de la información financiera y detectar posibles errores.

5. **Evaluación de Controles de Seguridad**

El auditor deberá evaluar los controles de seguridad implementados por la empresa u organización, como son: Firewalls, sistemas de detección de intrusos, encriptación, etc. Esto ayuda a determinar si los controles internos utilizados son confiables. En caso de ocurrir un error mediante la evaluación el auditor deberá renovar y actualizar los controles para mejorar.

6. **Comunicación de hallazgos**

Una vez haya finalizado la auditoría, el auditor deberá presentar sus resultados a la dirección de la empresa. Esto debe incluir las debilidades identificadas, las vulnerabilidades y las deficiencias de seguridad, así mismo, proporcionar ideas de mejora.

7. **Entregar un Informe de Auditoría**

El resultado final de la Auditoría deberá ser la entrega de un informe. Este informe deberá detallar los hallazgos, las recomendaciones y una opinión personal del auditor sobre la seguridad y el manejo de la empresa. Así como opciones para poder alcanzar los objetivos de la empresa.

RESPONSABILIDADES DEL AUDITOR

1. Cumplir con los requisitos de la Auditoría
2. Independencia: Es decir, debe evitar cualquier conflicto que puede afectar su imparcialidad en la evaluación de los estados de la empresa

3. Informar los requisitos según el motivo de la auditoría y aclarar las dudas que surjan
4. Planear y desarrollar las responsabilidades que se le hayan asignado
5. Competencia y profesionalidad: El auditor debe poseer conocimiento, experiencia y habilidades para realizar con éxito la auditoría que está llevando a cabo.
6. Confidencialidad
7. Documentación precisa de los hallazgos
8. Analizar las evidencias relevantes para llegar a las conclusiones
9. Alertar posibles errores que puedan afectar el rendimiento y los resultados de la auditoría
10. Elaborar un informe de auditoría
11. Trabajar y colaborar en equipo
12. Regresar la información que haya examinado
13. Ser objetivo
14. Seguir principios éticos y profesionales.

EJEMPLO DEL PROCESO

1. Reunión inicial

Es un paso obligatorio y, más allá de eso, esencial para una auditoría. En esta reunión debe estar presente los representantes o directores de la organización auditada, en el momento que sea más apropiado para todas las partes, así como los colaboradores de la empresa que están a cargo de los procesos auditables. La importancia de ello radica en el hecho, de brindarle a las partes involucradas en el proceso una guía inicial pero breve de las actividades siguientes. Para evitar la mayoría de los malentendidos o conflictos que puedan surgir en esta actividad.

2. Abrir los canales de comunicación

El segundo paso es establecer claridad en el hecho de que el auditado o auditados pueden expresar en todo momento sus preocupaciones y dudas al

equipo responsable para eliminar todas las interrogantes o confusiones del proceso. Asimismo, los auditores deben comunicarle al equipo de la empresa o a los involucrados en la reunión inicial de los progresos de la actividad y tenerlos al tanto de los avances y descubrimientos con el objetivo de brindar transparencia en todo momento.

3. Establecer las responsabilidades del equipo auditor

Ya sea que sea una sola persona o un equipo de auditores, es fundamental determinar el papel de cada uno durante el proceso de auditoría para facilitar todo su desarrollo. Dentro de esta actividad, existen observadores que su tarea se resume en el registro visual de las actividades y procesos dentro de la productividad rutinaria de la compañía y, de esta manera, determinar posibles malas prácticas o incumplimientos de la normativa. Por otra parte, están los guías que ya se encargan de dar dirección mucho más técnica a los auditados en cuestiones que corresponden al proceso en sí. Es decir, son expertos en el área que intervienen en las actividades diarias de la organización y ajustan las prácticas para garantizar la total legalidad y calidad de los procesos.

4. Recopilación y verificación de la información

Para los estándares internacionales, solo la información verificable es válida como evidencia en un proceso de auditoría. En este sentido, es necesario registrar cada hallazgo en forma de muestra y determinar que cumpla con los estándares para ser guardada como prueba. Algunos de los métodos más tradicionales son las entrevistas y la observación de las tareas diarias, así como de la revisión de los documentos de gestión interna.

5. Generación de incumplimientos

El siguiente paso es determinar qué proceso o documento no cumple con las normas, estándares o la legislación actual. Asimismo, también pueden ser considerados procesos fuertes o positivos en esta etapa, previa a la generación de las conclusiones.

6. Conclusiones finales de la auditoría

Nuevamente se debe conformar una reunión con los guías y observadores del proceso de auditoría para compartir las conclusiones de la misma. Aquí, se muestran los hallazgos y la información relevante durante la observación, revisión y verificación. Esto con el objetivo de debatir y acordar las conclusiones en un documento que será transmitido a las partes involucradas o auditados que forma parte del proceso de preparación y distribución que sirve como la última etapa. [1]

Para concluir el auditor desempeña un papel importante en la evaluación de la seguridad y el cumplimiento de los sistemas de información de una empresa. El proceso de auditoría se compone por muchas etapas e involucra la evaluación de riesgos, la planificación, la recopilación de datos y evidencia, evaluación de controles de seguridad y la emisión de conclusiones finales al proceso de auditoría, todo ello con el objetivo de garantizar la optimización de las empresas cumpliendo con sus responsabilidades y principios éticos.

Referencias

[1] D. Contributor, «DocuSign,» 10 Diciembre 2020. [En línea]. Available: https://www.docusign.mx/blog/proceso-de-auditoria. [Último acceso: 23 Septiembre 2023].

[2] M. d. Clase. [En línea]. Available: https://classroom.google.com/c/NjIxMDMxMzgyMzY2/m/NjIyODM2NzgyOTkw/details. [Último acceso: 9 Septiembre 2023].

[3] «Material de clase,» [En línea]. Available: https://drive.google.com/file/d/1YqLqE6WkwmuubT9xSVBx36hcQDlkcl84/view. [Último acceso: 23 Septiembre 2023].

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA.

INGENIERÍA INFORMÁTICA

MATERIA:

AUDITORÍA INFORMÁTICA

PROYECTO:

AUDITORÍA INFORMÁTICA DEL LABORATORIO DE CÓMPUTO LC2

PROFESORA:

ROSARIO CARVAJAL HERNÁNDEZ

ALUMNAS:

SCARLET DEL CARMEN IGNOT MARTINEZ

DANIELA DOMÍNGUEZ CRUZ

Fecha: 28/Septiembre/2023

Índice

Índice de imágenes

Índice de Tablas

Capítulo 1. Introducción

1.1. Estudio inicial del entorno auditable

El entorno auditable que vamos a utilizar será el laboratorio LC2. Este laboratorio cuenta con 24 máquinas funcionales las cuales todas son utilizadas y una de ellas es utilizada como servidor.

Las características del laboratorio son las siguientes:

- Es de gran espacio
- Tiene escritorios donde están colocadas las computadoras
- Cuenta con sillas
- Una cámara de seguridad
- Extintor
- Aire acondicionado
- Servidor
- Computadoras

Las computadoras del laboratorio cuentan con un sistema operativo basado en Windows y son de marca Dell.

El laboratorio tiene una segmentación de red de 193.168.2.254 y la topología de la red es en malla. El laboratorio se administra por medio de cables Ethernet.

El laboratorio LC2 surgió por el envío de computadoras con mejor capacidad y al ser este, un salón con una instalación de cableado completo se dio la idea de que sería un buen lugar para estos ordenadores y estarían seguros.

El laboratorio mencionado brinda un servicio a estudiantes para la realización de trabajos y proyectos encargados por los docentes, cada computador cuenta con internet y cada una de ellas funciona en su totalidad.

Estos computadores cuentan con un procesador Intel Core i5 6500, procesador de 3,2 G, así como también 8 GB de RAM y un disco duro de 2TB.

Imagen 1. Laboratorio LC2

1.2. Objetivos

1.2.1. Objetivo general

Aplicar auditorías y consultorías utilizando técnicas y herramientas para la evaluación de las áreas relacionadas con la informática en el laboratorio LC2.

1.2.2. Objetivos específicos

1-Estudiar y analizar el entorno auditable de la empresa...
2-Realizar la planeación y el programa de auditoría
3-Determinar los instrumentos para medir el nivel de aplicación de la normatividad
4-Aplicar la normatividad a la auditoría informática
5-Realizar la auditoría de hw
6-Realizar la auditoria de redes
7-Realizar la auditoria en telecomunicaciones
8-Documentar los resultados obtenidos

1.3. Plan y programa de auditoría (Apéndice C)

1.3.1. Tareas

1.3.2. Calendarios

1.3.3. Responsables

Objetivos de la Auditoría	1. Valorar la situación actual de cada una de las áreas de la organización 2. Realizar una comparación de la situación actual de la organización con respecto a los requisitos de la norma ISO 9001:2000 3. Poder implementar un Sistema de Calidad basado en la norma ISO 9001:2000 4. Identificar las No conformidades encontradas en cada una de las áreas de la organización 5. Proponer acciones correctivas para las no conformidades
Alcance de la Auditoría	El área a auditar es el siguiente: ● Laboratorio de cómputo 2 (LC2) Al terminar la auditoría se le entregarán los resultados del reporte final a los encargados del laboratorio, el reporte contiene: ● Plan de auditoría ● Observaciones obtenidas ● Las no conformidades detectadas ● Propuestas de acciones correctivas
Personas Involucradas	Daniela Dominguez Cruz Scarlet del Carmen Ignot Martinez
Documentos de Referencia	Se tomará como documento de

	referencia la Norma ISO 9001:2000 NMX-CC-9001-IMNC-2000 (Se encuentra ampliamente desarrollado en el Capítulo II)
Miembros Equipo Auditor	Las personas encargadas de realizar la auditoría son: Scarlet del Carmen Ignot Martinez y Daniela Dominguez Cruz. Ellas serán las encargadas de realizar el plan de auditoría, aplicar las listas de verificación y finalmente realizar el reporte final
Idioma Auditoría	El idioma utilizado será el español
Unidades Organizacionales Auditadas	La unidad a auditar es el: Laboratorio de Cómputo (LC2)
Fecha Estimada y duración de las actividades	Las fechas estimadas para la aplicación de la lista serán Laboratorio de Cómputo (LC2): 24, 25, 26, 27 de Noviembre
Programar las reuniones con la Administración	Las reuniones con la administración serán dos, una al principio de la auditoría y otra al finalizar la misma.
Requisitos de confidencialidad	La organización Divulga ha solicitado un cuidado especial de la documentación sobre todo aquella que implica los procedimientos para la realización del servicio.
Distribución del informe de auditoría y fecha de emisión	La entrega del reporte final estará estimada para principios de diciembre. El reporte incluye las no conformidades detectadas, así como también la propuesta a las acciones correctivas.

Tabla 1. Responsables

1.3.4. Organigrama

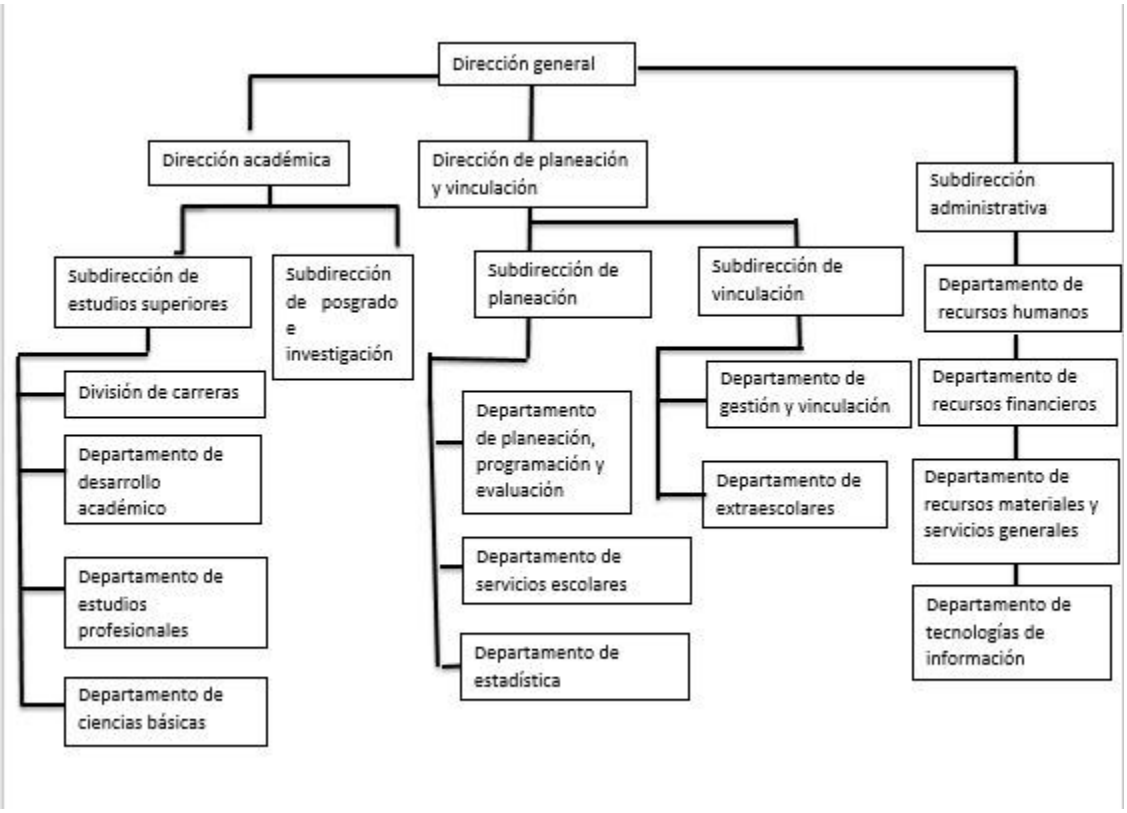

Imagen 2 Organigrama

1.4 Instrumentos para medir el nivel de aplicación de la normatividad

1.4.1. Personal

Preguntas	**SI**	**NO**	**N/A**
¿Existe personal con conocimiento y experiencia suficiente que organiza el trabajo para que resulte lo más eficaz posible?			
¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?			

¿Se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?			
¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?			
¿Existen procedimientos adecuados para mantener la documentación al día?			
¿Tienen manuales todas las aplicaciones?			
¿Existen controles que garanticen el uso adecuado de discos y cintas?			
¿Existen procedimientos adecuados para conectarse y desconectarse de los equipos remotos?			
¿Se aprueban los programas nuevos y los que se revisan antes de ponerlos en funcionamiento?			
¿Revisan y evalúan los departamentos de usuario los resultados de las pruebas finales dando su aprobación antes de poner en funcionamiento las aplicaciones?			
Al poner en funcionamiento nuevas aplicaciones o versiones actualizadas ¿funcionan en paralelo las existentes durante un cierto tiempo?			

Tabla 2. personal

1.4.2 Administración

PREGUNTAS	**SI**	**NO**	**N/A**
¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio?			
¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación?			
¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales?			

¿Se cuenta con software de oficina?			
¿Se han efectuado las acciones necesarias para una mayor participación de proveedores?			
¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?			
¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado?			
¿Se han implantado claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado?			
¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: ¿incendio, vandalismo, robo y uso indebido, intentos de violación?			
¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?			
¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos?			
¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos?			
¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso?			
¿Todas las actividades del Centro de Cómputo están normadas mediante manuales, instructivos, normas, reglamentos, etc.?			
¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras?			
¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores picos, UPS, generadores de energía?			
¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación?			
¿Se han adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo?			

Tabla 3. Administración

1.4.3. Instalación

Pregunta	SI	NO	S/N
¿Se cuenta con la instalación con tierra física para todos los equipos?			
¿La instalación eléctrica se realizó específicamente para el centro de cómputo?			
¿Se cuenta con otra Instalación dentro del centro de cómputo, diferente de la que alimenta a los equipos de cómputo?			
¿La Instalación es independiente para el centro de cómputo?			
¿La misma instalación con tierra física se ocupa en otras partes del edificio?			
¿La iluminación está alimentada de la misma acometida que los equipos?			
¿Las reactancias (balastros de las lámparas) están ubicadas dentro de la sala?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a la planta de emergencia?			

¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a los no-break?			
¿Se cuenta con interruptores generales?			
¿Se cuenta con interruptores de emergencia en serie al interruptor general?			
¿Se cuenta con interruptores por secciones o aulas?			
¿Se tienen los interruptores rotulados adecuadamente?			
¿Se tienen protecciones contra corto circuito?			
¿Se tiene implementado algún tipo de equipo de energía auxiliar?			
¿Se cuenta con Planta de emergencia?			
¿Se tienen conectadas algunas lámparas del centro de cómputo a la planta de emergencia?			
¿Las instalaciones (aulas, cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un laboratorio de cómputo?			
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?			
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?			
¿Existen lugares de acceso restringido?			
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?			
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de sensores?			

¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?			
¿Se tienen medios adecuados para extinción de fuego en el centro de cómputo?			
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?			
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?			
¿Son funcionales los muebles instalados dentro del centro de cómputo: Discoteca, archiveros, mesas de trabajo, etc.?			
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?			
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?			
¿Se limpian las instalaciones?			

Tabla 4. Instalación

1.4.4. Operación

Pregunta	**SI**	**NO**	**N/A**
Existe un contrato de mantenimiento			
¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?			
¿Se lleva a cabo tal programa?			
¿Existen tiempos de respuesta y de compostura estipulados en los contratos?			
Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?			

¿Existe plan de mantenimiento preventivo?			
¿Este plan es proporcionado por el proveedor?			
¿Se notifican las fallas?			
¿Se les da seguimiento?			
Tiene un plan logístico para dar soporte al producto software?			
Los requerimientos de mantenibilidad se incluyen en la actividad de Iniciación durante el Proceso de Adquisición (ISO 12207) y se evalúan durante el Proceso de Desarrollo?			
¿El desarrollador prepara un Plan de Mantenibilidad que establece prácticas específicas de mantenibilidad, así como recursos y secuencias relevantes de actividades?			
¿Durante el análisis de requerimientos, los siguientes aspectos que afectan a la mantenibilidad, son tomados en cuenta? ● Identificación y definición de funciones, especialmente las opcionales. ● Exactitud y organización lógica de los datos ● Los Interfaces (de máquina y de usuario). ● Requerimientos de rendimiento. ● Requerimientos impuestos por el entorno (presupuestos ● Granularidad (detalle) de los requerimientos y su impacto sobre la trazabilidad ● Énfasis del Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de documentación			
¿La transición del software consiste en una secuencia controlada y coordinada de acciones para trasladar un			

producto software desde la organización que inicialmente ha realizado el desarrollo a la encargada del mantenimiento?			
¿La responsabilidad del mantenimiento se transfiere a una organización distinta, se elabora un Plan de Transición? ¿Qué es lo que incluye este plan? ● La transferencia de hardware, software, datos y experiencia desde el desarrollador al mantenedor. ● Las tareas necesarias para que el mantenedor pueda implementar una estrategia de mantenimiento del software. ¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuario o guías de instalación pueden ser modificados o creados, si fuese necesario?			
El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software.			
¿Los elementos software reflejan la documentación de diseño?			
¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas?			
¿Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas?			
¿La documentación de usuario cumple los estándares especificados?			
¿Los costes y calendarios se ajustan a los planes establecidos?			

Tabla 5. Operación

1.4.5. Seguridad

Pregunta	**SI**	**NO**	**N/A**
¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?			

¿Existe un documento donde esté especificado la relación de las funciones y obligaciones del personal?			
¿Existen procedimientos de notificación y gestión de incidencias?			
¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?			
¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?			
¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?			
¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado? ¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?			
¿Existe una relación de personal autorizado a acceder a los soportes de datos?			
¿Existe un periodo máximo de vida de las contraseñas?			
¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?			
¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado?			
¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?			
¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?			

Tabla 6. Seguridad