RIESGOS Y AUDITORIA DE LA TECNOLOGIA DE INFORMACION, EN LA NUEVA ERA DE LA DIGITALIZACION.

BOXLER Lilian Inés

Contadora Pública

Especialista en Docencia Universitaria

Especialista en Contabilidad Superior y Auditoria

M.P. Nº 2973 C.P.C.E.

liliboxler@gmail.com

RESUMEN

En el panorama digital actual en rápida evolución, las organizaciones dependen en gran medida de la tecnología para impulsar la eficiencia operativa y obtener una ventaja competitiva. Sin embargo, esta mayor dependencia de la tecnología también expone a las empresas a una amplia gama de riesgos, incluidas amenazas a la ciberseguridad, filtraciones de datos, fallas del sistema, y problemas de cumplimiento (compliance).

Las organizaciones deben realizar evaluaciones periódicas de riesgos de auditoría de Tecnología de Información (TI) para garantizar la integridad y seguridad de su entorno de TI, brindando información sobre el proceso de identificación, evaluación y gestión de riesgos en las auditorias de TI.

Los riesgos de auditoría de TI se refieren a las posibles amenazas y vulnerabilidades que podrían afectar los sistemas de información, la integridad de los datos y la infraestructura general de TI de una organización, comprometiendo la toma de decisiones de las organizaciones. La mitigación de riesgos de auditoría de TI es un proceso fundamental que permite a las empresas tomar medidas proactivas para controlar las amenazas y proteger sus intereses.

Las Auditorias de Tecnología de la Información desempeñan un papel vital para garantizar la seguridad y eficacia de la infraestructura de TI de una empresa.

PALABRAS CLAVES

Tecnología de Información – Auditoria – Riesgos – Mitigar.

1. AUDITORIA DE TECNOLOGIA DE INFORMACION

La automatización de los procesos en las organizaciones hace que la inteligencia artificial este exigiendo a los Auditores, analizar un gran volumen de datos en menor tiempo, estar mejor equipados para identificar vulnerabilidades en los sistemas de TI, comprender mejor el negocio con escepticismo profesional y obtener mejores resultados en su trabajo.

El auditor debe tener una amplia comprensión del sistema de información del ente que es relevante para la preparación de los estados financieros, incluido el entorno de TI que se requiera para procesar las transacciones y los flujos de datos que permiten generar la información financiera de la entidad. Comprender la relevancia del sistema de información del cliente es importante porque el uso de aplicaciones de

TI y otros aspectos en el entorno dan lugar a los riesgos derivados de su uso.

Para comprender mejor las Auditorias de TI, es importante explorar sus diferentes tipos y los procesos involucrados. Las Auditorias de TI se pueden clasificar en términos generales en dos tipos principales: auditorias generales y auditorias de controles de aplicaciones. Las Auditorias de controles generales evalúan la eficacia general de la infraestructura de TI de una organización, centrándose en áreas como controles de acceso, gestión de cambios, seguridad operativa y seguridad física. Por otro lado, las auditorias de controles de aplicaciones evalúan los sistemas y aplicaciones de TI específicos utilizados dentro de una organización, evaluando su funcionalidad, seguridad y cumplimiento.

Planificar una auditoría de tecnología de información de manera eficiente es esencial para asegurar un proceso efectivo y completo. Aquí hay una guía paso a paso para comenzar rápidamente con la planificación de una auditoría de TI:

1. Definir el Alcance:

Identifica claramente el alcance de la auditoría. Esto puede incluir sistemas específicos, procesos, áreas funcionales o toda la infraestructura de tecnología de información.

2. Establecer Objetivos y Metas:

Define claramente los objetivos y metas de la auditoría. ¿Qué quieres lograr con la auditoría? Esto podría incluir evaluar la seguridad de la información, revisar la eficiencia de los controles internos, o asegurarse de que la organización cumple con los estándares y regulaciones.

3. Recopilar Información Preliminar:

Revisa la documentación existente, como políticas de seguridad de la información, procedimientos operativos, inventarios de activos de TI, informes de auditorías anteriores, etc.

4. Identificar Partes Interesadas:

Identifica a todas las partes interesadas en la auditoría, incluyendo a los propietarios de procesos, equipos de TI, gestión sénior y cualquier otra persona clave relacionada con la tecnología de la información.

5. Evaluar Riesgos Preliminares:

Realiza una evaluación inicial de los riesgos asociados con la tecnología de información. Esto puede ayudar a determinar las áreas críticas que requieren una atención especial durante la auditoría.

6. Seleccionar el Equipo de Auditoría:

Forma un equipo de auditoría con las habilidades y conocimientos necesarios para abordar los aspectos técnicos y de gestión de la auditoría de TI.

7. Desarrollar un Plan de Auditoría:

Elabora un plan detallado que incluya los pasos a seguir, los recursos necesarios, el calendario de la auditoría y los resultados esperados.

8. Revisar y Aprobar el Plan:

Comparte el plan de auditoría con las partes interesadas relevantes y obtén su revisión y aprobación. Esto asegura que todos estén alineados y comprometidos con el proceso.

9. Realizar Reuniones Iniciales:

Programa reuniones iniciales con el equipo de auditoría y las partes interesadas para discutir el alcance, objetivos y plan de la auditoría

10. Obtener Acceso y Autorización:

Asegúrate de que el equipo de auditoría tenga acceso a la información y sistemas necesarios. Obtén la autorización necesaria para llevar a cabo la auditoría.

11. Ejecutar la Auditoría:

Sigue el plan de auditoría, recopila evidencia, realiza entrevistas, y evalúa los controles y procesos de TI de acuerdo con los objetivos establecidos.

12. Comunicar Resultados Preliminares:

Durante la auditoría, comunica los hallazgos preliminares a las partes interesadas para abordar cualquier problema crítico de manera oportuna.

13. Finalizar el Informe de Auditoría:

Una vez completada la auditoría, elabora un informe detallado que incluya los hallazgos, recomendaciones y un resumen ejecutivo.

14. Presentar los Resultados:

Programa una presentación de los resultados a la dirección y otras partes

interesadas. Discute las conclusiones, recomendaciones y planes de acción.

15. Realizar Seguimiento:

Monitorea la implementación de las recomendaciones y realiza un seguimiento para asegurarte de que se aborden los problemas identificados durante la auditoría.

Este enfoque paso a paso ayudará a iniciar rápidamente la planificación de una auditoría de tecnología de información y garantizar un proceso efectivo y eficiente.

2. RIESGOS DE AUDITORIA DE TI

Los riesgos de auditoría de TI, es esencial conocer sus implicancias, se refieren a las posibles amenazas y vulnerabilidades que podrían afectar los sistemas de información, la integridad de los datos y la infraestructura general de TI de una organización, comprometiendo la toma de decisiones de las organizaciones.

El conocimiento del control interno incluye el modo en que el ente ha respondido a los riesgos derivados de la tecnología de la información. Si el Ente utilizase una organización de servicios, es necesario considerar la obtención de un conocimiento del control interno en relación con dicha organización de servicios relevante para la auditoria (F.A.C.P.C.E. R.T. 53 – 3.5).

Algunos de los riesgos de TI más frecuentes y explicación de cómo pueden ser auditados eficazmente:

1. Acceso no autorizado

Descripción del riesgo:

El acceso no autorizado ocurre cuando individuos no autorizados logran acceder a sistemas, datos o recursos de la red. Esto puede llevar a la pérdida o manipulación de

datos sensibles, interrupciones en las operaciones del negocio, y potenciales brechas de seguridad.

Estrategias para auditar:

Revisar políticas de seguridad: Asegurarse de que las políticas de seguridad de la información estén actualizadas y sean adecuadas.

Auditar controles de acceso: Evaluar los mecanismos de control de acceso, como autenticación y autorización, para verificar su efectividad.

Pruebas de penetración: Realizar pruebas de penetración para identificar vulnerabilidades en los sistemas que podrían permitir accesos no autorizados.

2. Pérdida de datos

Descripción del riesgo:

La pérdida de datos puede ser el resultado de errores humanos, fallas de software o hardware, ataques cibernéticos o desastres naturales. Este riesgo afecta la integridad y disponibilidad de la información, con consecuencias potencialmente devastadoras para la empresa.

Estrategias para auditar:

Revisión de backups y recuperación de datos: Comprobar la frecuencia y efectividad de las políticas y procedimientos de backup y recuperación de datos.

Auditoría de controles físicos y ambientales: Inspeccionar las medidas de protección física y ambiental en los centros de datos y otras instalaciones críticas.

Análisis de impacto de negocio: Realizar un análisis de impacto en el negocio para entender las consecuencias de la pérdida de datos en las operaciones del negocio.

3. Malware

Descripción del riesgo:

El malware, que incluye virus, gusanos, troyanos, ransomware, entre otros, siendo un software malicioso diseñado para infiltrarse o dañar un sistema de computadora sin el consentimiento del usuario. El malware es una de las amenazas más comunes y perjudiciales en el ambiente de TI.

Estrategias para auditar:

Evaluación de sistemas antimalware: Verificar que se cuenten con soluciones antimalware actualizadas y operando efectivamente.

Revisión de parches y actualizaciones de seguridad: Asegurarse de que todos los sistemas operativos y aplicaciones estén al día con las últimas actualizaciones de seguridad.

Auditoría de respuesta a incidentes: Examinar la capacidad de la organización para detectar y responder a incidentes relacionados con malware

3. MITIGAR LOS RIESGOS DE AUDITORIA DE TI

Hay distintas estrategias para responder a los riesgos como:

• Evitar: eliminar el riesgo eliminando la causa

• Transferir: trasladar las consecuencias del riesgo a una tercera parte.

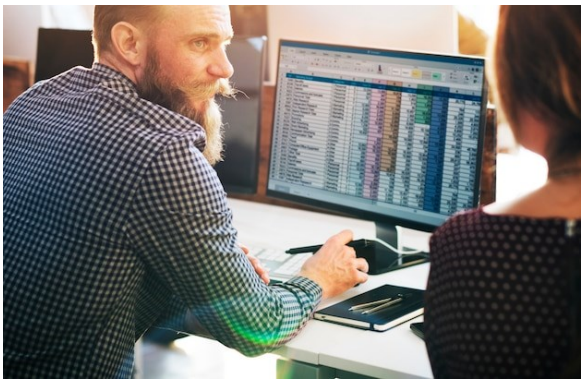
Se transfiere la responsabilidad de la gestión, pero no elimina el riesgo.

• Mitigar: Reducir la probabilidad o el impacto del evento

• Aceptar:

Plan de Contingencia: plan de mitigación en caso que surjan riesgos no previstos

Reservas: fondos o plazos adicionales para usar en caso que se produzca el evento.



En esta oportunidad nos centraremos en la estrategia de mitigar el riesgo en los sistemas de información en general de la organización. En el ámbito de la auditoria, la palabra mitigar juega un papel crucial. Se refiere a la acción de reducir, minimizar o eliminar los riesgos que pueden afectar a una organización. La mitigación de riesgos es un proceso fundamental que permite a las empresas tomar medidas proactivas para controlar las amenazas y proteger sus intereses. El primer paso para desarrollar una estrategia eficaz de mitigación de riesgos de auditoría de TI es identificar los riesgos comunes a los que se enfrentan las organizaciones, estos riesgos pueden incluir acceso no autorizado a datos confidenciales, tiempo de inactividad del sistema, violaciones de datos, incumplimiento de las regulaciones de la industria, controles inadecuados del sistema y planes de recuperación ante desastres inadecuados, entre otros.

Una vez que los riesgos han sido identificados, es crucial implementar controles de ciberseguridad adecuados para proteger los sistemas de información contra amenazas internas y externas. Esto puede incluir la instalación de firewalls, antivirus, sistemas de detección de intrusos y políticas de acceso y contraseña robustas.

El factor humano sigue siendo uno de los eslabones más débiles en la seguridad de la información. Por lo tanto, es fundamental proporcionar formación y concienciación adecuadas al personal sobre las mejores prácticas de seguridad de TI. Esto incluye la sensibilización sobre las amenazas comunes, la importancia de proteger la información confidencial y los procedimientos para manejar incidentes de seguridad de manera efectiva..

4. CONCLUSIÓN

Una auditoría es una investigación o inspección de un sistema, entidad o informe. En este caso, una auditoría de TI es una revisión de los sistemas, aplicaciones, gestiones, operaciones, el uso de datos y otros procesos relacionados con las

tecnologías de la información de una empresa. Auditar el entorno de TI y los sistemas de información, por lo general, sigue el mismo procedimiento que una auditoría de estados financieros. De esta manera, como la mayoría de los tipos de auditoría, consta de cuatro fases principales, que son:

- Planificación;
- Pruebas de controles;
- Pruebas sustantivas;
- Finalización de la auditoría y redacción del informe.

La evaluación de riesgos y vulnerabilidades de un sistema operativo o la seguridad de la información en general es parte del punto de vista con el cual se aborda un proceso de auditoría de TI. De esta manera, este tipo de auditoría informática reduce las posibilidades y los riesgos que ocurren en una organización en relación con su sistema de TI.

5. BIBLIOGRAFÍA

BARA, M. (, 2017). Estrategias para las Amenazas y Oportunidades en Proyectos. OBS Business School. Recuperado de https://www.obsbusiness.school/blog/7-estrategias-para-las-amenazas-y-oportunidades-en-proyectos

CASAL, A. M. (2022). Cuestiones de Auditoria. Tecnología digital e Inteligencia artificial en la Auditoria y el Aseguramiento. Profesional y Empresaria D&G.

EQUIPO AUDITOOL. (2024). Gestión de riesgos de TI: Cómo identificar y evaluar riesgos efectivamente. Auditoria de TI. Recuperado de https://www.auditool.org/blog/auditoria-de-ti/gestion-de-riesgos-de-ti-como-identificar-y-evaluar-riesgos-efectivamente

EQUIPO AUDITOOL. (2024). Riesgos comunes en TI y cómo auditarlos. Recuperado de https://www.auditool.org/blog/auditoria-de-ti/riesgos-comunes-en-ti-y-como-auditarlos

PAREDES, G. (2023). Si tuvieras que realizar una auditoría de tecnología de información, por donde comienzo y obtengo resultados a la vena. Linked in. Recuperado de https://es.linkedin.com/pulse/si-tuvieses-que-realizar-una-auditor%C3%ADa-de-tecnolog%C3%ADa-por-paredes--mlmee

RODRIGUEZ, I. (2022). El Auditor y los Controles Generales de Tecnología de la Información. Auditool. Recuperado de https://www.auditool.org/blog/auditoria-externa/el-auditor-y-los-controles-generales-de-tecnologia-de-la-informacion