GOBIERNO DE MÉXICO | EDUCACIÓN SECRETARÍA DE EDUCACIÓN PÚBLICA | TECNOLÓGICO NACIONAL DE MÉXICO | Instituto Tecnológico de Aguascalientes

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

AUDITORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

UNIDAD 1:

APLICACIÓN DE LA AUDITORÍA IN SITU

TEMA 1:

ÁREAS SUJETAS A AUDITORÍA , IDENTIFICANDO LAS NORMATIVIDADES, PROCEDIMIENTOS Y CONTROLES INTERNOS

Docente

Lic. Juan Carlos Sánchez Gaytán

Participante:

Flores Zavala Jesús Uriel

Semestre: 08

Semestre: enero-junio de 2025

Aguascalientes, Ags. 6 de mayo de 2025

En la era digital, la auditoría ha experimentado una transformación profunda gracias a la integración de las Tecnologías de la Información y la Comunicación (TICs). Estas herramientas no solo han automatizado procesos y mejorado la eficiencia, sino que también han abierto nuevas posibilidades para la detección de fraudes, la gestión de riesgos y la toma de decisiones más informadas. Este artículo explora la influencia de las TICs en la auditoría moderna, analizando sus beneficios, desafíos y el panorama futuro de esta disciplina.

Las TICs se han convertido en herramientas esenciales para la práctica de la auditoría, con aplicaciones específicas en diferentes áreas:

- Auditoría de Sistemas de Información.
- Auditoría de Cumplimiento.
- Auditoría de Gestión. [1]

Auditoría de gestión de TI

Las auditorías de gobernanza de TI son prácticas realizadas por equipos especializados que verifican si los procesos del sector están alineados estratégicamente con los objetivos de la empresa.

La información se volvió el principal activo de las organizaciones y, por ende, necesitan protegerlo. Las auditorías son justamente el proceso especializado responsable de garantizar que eso suceda.

Este procedimiento tiene el objetivo de evaluar la seguridad del sistema de información de las empresas para detectar fallas y vulnerabilidades que pueden comprometer la red y los datos corporativos.

Gracias a la realización de auditorías, las organizaciones logran corregir rápidamente las brechas encontradas en sus sistemas y actualizar procesos e infraestructuras para reforzar la protección de la información.

Procedimiento

Este proceso debe realizarse con cuidado y exige profesionales capacitados para verificar todos los procedimientos de la empresa y garantizar que ninguna fase pase desapercibida.

La auditoría de gobernanza de TI evalúa si los procesos de TI están alineados con las estrategias de la empresa y tiene un enfoque de gerencia. Conozca algunos de los pasos necesarios para realizarla con éxito y auditar la gobernanza de TI de su empresa:

Evaluar los procesos de seguridad

Las ciberamenazas están en constante transformación y, con ello, las empresas se vuelven vulnerables a ataques y robos de datos diariamente. Por lo tan-

to, es crucial contar siempre con herramientas de seguridad de última generación.

La auditoría debe realizar evaluaciones de los procedimientos de seguridad digital usados por la empresa, para verificar si son estructurados y capaces de impedir que los usuarios queden expuestos a amenazas digitales.

Verificar todos los puntos importantes de la empresa

Esto incluye metas, demandas y perfil del negocio. Es importante que la auditoría monitoree si los objetivos de todos los sectores están alineados con las estrategias de la empresa. Esto es fundamental para conquistar mejores retornos en los negocios.

De este modo, en la auditoría, los profesionales deben levantar todos los datos sobre las demandas y los objetivos de cada área de la empresa. Así, la gobernanza de TI se puede mantener actualizada con respecto a lo que sucede en otros departamentos.

Revisar la documentación

La documentación es muy importante para una gobernanza de TI exitosa, pues es por medio de esta que impedimos la repetición de errores pasados, por el hecho de que ya están registrados. De esta forma, los profesionales logran comprender cómo evitar riesgos y optimizar procesos. [2]

Control interno

COBIT (Objetivos de Control para la Información y las Tecnologías Relacionadas) es un marco de referencia desarrollado por ISACA (Information Systems Audit and Control Association) que proporciona una guía completa para la gobernanza, gestión y control de los sistemas de TI. COBIT está diseñado para ser utilizado por una amplia gama de stakeholders, incluyendo ejecutivos, auditores, profesionales de TI y usuarios finales.

Estructura del marco COBIT

COBIT 2019, la última versión del marco, se organiza en 4 dominios que abarcan los aspectos clave de la gobernanza de TI:

1. Evaluación, adquisición y entrega de valor: Este dominio se centra en la planificación estratégica de TI, la alineación con los objetivos del negocio y la gestión de la cartera de proyectos de TI.

2. Creación y soporte de las capacidades: Este dominio se enfoca en la gestión de los recursos de TI, incluyendo la infraestructura, las aplicaciones, los datos y el personal.

3. Entrega de servicios, soporte y protección: Este dominio aborda la gestión de las operaciones de TI, la seguridad de la información y la atención al cliente.

4. Monitoreo, evaluación y mejora: Este dominio se centra en la evaluación del desempeño de TI, la gestión de riesgos y la mejora continua de los procesos. [3]

Auditoría de sistemas de información

La auditoría de seguridad informática (también llamada auditoría de ciberseguridad) es una evaluación que se realiza en las empresas para determinar el estado o nivel de la ciberseguridad de los sistemas informáticos, el acceso a internet, las políticas de seguridad y su cumplimiento por parte del personal.

Estas auditorías pueden ser técnicas, es decir, pruebas realizadas por expertos en ciberseguridad en donde se analizan las vulnerabilidades; pueden ser una revisión de controles ante una autoridad, como por ejemplo para las certificaciones ISO 27001 y PCI-DSS.

También pueden ser una evaluación interna o externa, que busca demostrar que los controles de seguridad están siendo efectivamente implementados, así como también para detectar posibles fallos en los sistemas informáticos.

Procedimiento

1. Objetivos y planificación

Esta fase consiste en definir el alcance, los criterios, la metodología y los objetivos de la auditoría. Se debe determinar qué se va a auditar, cuándo, cómo y por quién. También se debe establecer el marco legal y normativo que se va a aplicar, así como los recursos y herramientas necesarios para realizar la auditoría.

Se debe elaborar un plan de auditoría que contenga los siguientes elementos:

- El propósito y el alcance de la auditoría.
- Los objetivos específicos que se quieren lograr.
- Los criterios o estándares que se van a utilizar para evaluar la seguridad.
- La metodología que se va a emplear para realizar la auditoría.
- El equipo auditor responsable de realizar la auditoría.
- El cronograma, recursos y herramientas necesarias para efectuar la auditoría.

2. Recopilación de información

Esta fase consiste en obtener y analizar la información relevante para la auditoría. Se debe recopilar información sobre los sistemas informáticos, los procesos y las políticas de seguridad de la organización. También se debe identificar y evaluar los riesgos y las amenazas a los que se enfrenta la organización.

En esta fase se debe utilizar diferentes fuentes y métodos de recopilación de información, tales como: la documentación existente sobre los sistemas informáticos, los procesos y las políticas de seguridad, las pruebas o ensayos hechos sobre los sistemas informáticos y evaluaciones de riesgos.

3. Análisis de la información

Esta fase consiste en recopilar y estudiar toda la información relevante sobre la organización y sus sistemas informáticos, como la estructura, los objetivos, los procesos, los recursos, los servicios, el hardware, el software, las redes, los accesos, las bases de datos o las aplicaciones.

Esta información permite conocer el contexto y el alcance de la auditoría, así como identificar los elementos críticos y sensibles que requieren mayor atención.

Para realizar esta fase se pueden utilizar distintas técnicas y herramientas, como entrevistas, cuestionarios, observación directa o análisis documental. El resultado de esta fase es el efecto de las respuestas obtenidas utilizando las técnicas mencionadas anteriormente.

4. Informe de la auditoría

Esta fase consiste en elaborar y presentar un documento que recoja los resultados y las conclusiones de la auditoría, así como las recomendaciones y las acciones correctivas necesarias para mejorar la seguridad informática. A pesar de ser un informe detallado, debe ser claro, preciso, objetivo y fundamentado en evidencias.

El informe debe incluir al menos los siguientes apartados: introducción, objetivos, alcance, metodología, hallazgos, valoración del riesgo, recomendaciones y conclusiones. [4]

Control interno:

Los controles internos de seguridad tienen por finalidad garantizar que todos los activos, sistemas, instalaciones, datos y archivos relacionados con el uso de la Tecnología de Información se encuentran protegidos contra accesos no autorizados, daños eventuales y uso indebido o ilegal que se encentran operables, seguros y protegidos en todo momento.

La seguridad informática tiene el propósito de proteger la información de una amplia gama de amenazas para garantizar la continuidad del negocio, minimizar el costo de posibles daños para el giro del negocio y maximizar el retorno de las inversiones a la par que provee de competitividad para aprovechar oportunidades a través de un mejor posicionamiento competitivo.

Los principales tipos de controles de seguridad son:

- Políticas y planes de seguridad de la Tecnología de la Información.

- Controles de operaciones informáticas.
- Controles de gestión de la seguridad del personal.
- Controles de seguridad en el ámbito del usuario final.
- Asignación de perfiles de acceso y contraseñas u otros mecanismos de validación de identidad.
- Controles organizacionales sobre seguridad. (Por ejemplo, establecimiento de segregación de funciones y rotación de labores).
- Establecimiento y monitoreo de métricas sobre la seguridad de la Tecnología de Información.

El más crítico, y sobre el cual se basan todos los demás, es la Política de Seguridad de la Tecnología de la Información. [5]

Auditoria de cumplimiento de TI

Una auditoría de cumplimiento de TI es una evaluación estructurada que determina si una organización cumple con los requisitos de cumplimiento de TI pertinentes establecidos por organismos reguladores, agencias gubernamentales y estándares del sector. Implica evaluar la eficacia con la que su empresa implementa controles de seguridad, protocolos de gestión de acceso, evaluaciones de riesgos y medidas de protección de datos para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información.

Durante una auditoría de cumplimiento de TI, los auditores examinan cómo su organización almacena, procesa y transmite datos confidenciales. Verifican la existencia de prácticas de cumplimiento clave, como el cifrado, los registros de auditoría y los mecanismos de respuesta a incidentes. Estas auditorías ayudan a detectar deficiencias en su estrategia de cumplimiento de TI y a reducir el riesgo de ciberamenazas, filtraciones de datos y multas regulatorias.

¿Por qué es importante una auditoría de cumplimiento de TI? Porque todas las empresas, independientemente de su tamaño, manejan datos confidenciales como registros de clientes, información de empleados y detalles financieros. Un solo descuido en el cumplimiento puede tener consecuencias devastadoras, como pérdida de datos, acciones legales, sanciones costosas y daño a la reputación. [6]

Ejemplos de Marcos Regulatorios de Cumplimiento de TI

PCI DSS

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) es un estándar de seguridad de la información para organizaciones que manejan tarjetas de crédito, diseñado para proteger los datos del titular de la tarjeta y reducir el fraude. Bajo PCI DSS, las empresas deben cumplir con un nivel mínimo estandarizado de seguridad al almacenar, procesar y transmitir in-

formación del titular de la tarjeta. Como tal, la mayoría de las organizaciones requerirán el cumplimiento de PCI DSS como parte de su auditoría.

SOC 2

SOC 2 (que significa “Controles de Sistemas y Organización”) es un estándar de cumplimiento que especifica cómo las organizaciones de servicios gestionan los datos de los clientes, cubriendo seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad. Las auditorías frecuentemente incluyen informes SOC 2, que están diseñados para detallar cómo las organizaciones gestionan la seguridad de sus datos.

RGPD

RGPD (Reglamento General de Protección de Datos) es un reglamento de la Unión Europea sobre privacidad de la información. Las organizaciones que hacen negocios en la UE querrán mantener el cumplimiento de RGPD al gestionar datos personales e incluirlo en sus auditorías.

Procedimiento

- Prepare documentación para demostrar cómo se gestionan sus datos y seguridad y que está cumpliendo con sus requisitos de seguridad.
- Capacita a tu personal para asegurarte de que entienden tus protocolos de seguridad y siguen las mejores prácticas de seguridad.
- Realiza evaluaciones de riesgos y auditorías internas para identificar cualquier amenaza o vulnerabilidad que debas abordar antes de la auditoría.
- Revise regularmente sus protocolos de seguridad para asegurarse de que está al día y cumpliendo con sus obligaciones.
- Usa software de gestión de cumplimiento para monitorear tus sistemas y controles y asegurar que tus dispositivos cumplan con tus requisitos de cumplimiento. [7]

Referencias

[1] "Auditoría Digital: Tics Para Una Revolución", *Auditoría Group*, 10-ene-2012. [En línea]. Disponible en: https://auditoriagroup.com.ar/tics-en-auditoria/. [Consultado: 08-may-2025].

[2] "Auditoría de gobernanza de TI: ¿qué es y cómo puede ayudar a sus clientes?", *Blog TD SYNNEX*, 29-jun-2023. [En línea]. Disponible en: https://blog.es/auditoria-de-gobernanza-de-ti-que-es-y-como-puede-ayudar-a-sus-clientes/. [Consultado: 08-may-2025].

[3] "Gobernanza de TI y su Relación con el Control Interno: Una guía para la implementación efectiva", *Kcho y Asociados*. [En línea]. Disponible en: https://tuguialegalycontable.blogspot.com/2025/03/gobernanza-de-ti-y-su-relacion-con-el.html. [Consultado: 08-may-2025].

[4] J. A. Gómez, "Auditoría de seguridad informática: Tipos, fases y ventajas", Deltaprotect.com, 04-jul-2023. [En línea]. Disponible en: https://www.deltaprotect.com/blog/auditoria-de-seguridad-informatica. [Consultado: 08-may-2025].

[5] V. Martínez, "¿Qué son los controles de seguridad de TI?", *Auditool.org*, 10-feb-2022. [En línea]. Disponible en: https://www.auditool.org/blog/auditoria-de-ti/que-son-los-controles-de-seguridad-de-ti. [Consultado: 08-may-2025].

[6] *Scalefusion.com*. [En línea]. Disponible en: https://blog.scalefusion.com/es/marcos-de-auditor%C3%ADa-de-cumplimiento-de-TI/. [Consultado: 12-may-2025].

[7] R. Pleasant, "¿Qué es una auditoría de cumplimiento de TI? Asegurando la adherencia regulatoria", *Splashtop Inc*, 03-abr-2025. [En línea]. Disponible en: https://www.splashtop.com/es/blog/it-compliance-audit. [Consultado: 12-may-2025].