REVISTA MULTIDISCIPLINARIA
ISSN: 3006-1393
ISSN-L: 3006-1393
Perioricida: Semestral
Vol. 5. N° 8.
Febrero –Julio 2025

Plan de auditoría informática para la gestión tecnológica en la Cámara de diputados de Bolivia

Computer audit plan for technological management in the Chamber of Deputies of Bolivia

Kimberly Luz Velarde Flores
https://orcid.org/0009-0003-5192-7818
Universidad Autónoma Tomás Frías, Bolivia

http://doi.org/10.62349/revistauno.v.5i8.31

ARTÍCULO DE INVESTIGACIÓN

https://revistauno.org

Correspondencia del autor
kimberly2619994@gmail.com

- **Recibido**: 19 de agosto de 2024
- **Arbitrado:** 17 de septiembre de 2024
- **Aceptado:** 25 de enero de 2025
- **Publicado:** 03 de febrero de 2025

RESUMEN

El desarrollo de las Tecnologías de la Información y Comunicación es fundamental para las organizaciones, enfrentando constantes amenazas por la información sensible que manejan El presente trabajo tiene como objetivo diseñar un plan de auditoria informática para mejorar la gestión tecnológica en la Cámara de Diputados de Bolivia. Se trabajo un enfoque cualitativo, de tipo explicativo. La población estuvo conformada por 30 personas del personal Administrativo, se determinó una muestra de 5 personas con el muestreo no probabilístico. Los resultados destacan que fue efectivo el plan de auditoría al verificar las políticas de control de acceso en la Cámara de Diputados, asegurando procesos de autenticación adecuados y documentación correcta para prevenir la fuga de información y proteger los datos institucionales. Se concluye que la implementación de un plan de auditoría basado en COBIT es esencial para mejorar la gestión de las TIC en la Cámara de Diputados y mitigar riesgos.

Palabras clave: Auditoría informática; Gestión tecnológica; Cámara de diputados; Bolivia, Evaluación de sistemas.

ABSTRACT

The development of Information and Communication Technologies is fundamental for organizations, facing constant threats due to the sensitive information they handle. The objective of this work is to design a computer audit plan to improve technological management in the Chamber of Deputies of Bolivia. A qualitative, explanatory approach was used. The population was made up of 30 people from the Administrative staff, a sample of 5 people was determined with non-probabilistic sampling. The results highlight that the audit plan was effective in verifying the access control policies in the Chamber of Deputies, ensuring adequate authentication processes and correct documentation to prevent information leakage and protect institutional data. It is concluded that the implementation of an audit plan based on COBIT is essential to improve ICT management in the Chamber of Deputies and mitigate risks.

Keywords: IT audit; Technology management; Chamber of Deputies; Bolivia; Systems evaluation.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

INTRODUCCIÓN

Las áreas funcionales de las instituciones dependen cada vez más de los servicios de las Tecnologías de la Información y la Comunicación (TIC), lo que facilita la automatización y el desarrollo de procesos productivos basados en tecnología. La implementación de nuevos servicios ha convertido la información y la tecnología en activos valiosos para muchas instituciones (Salgado et al. 2024). Estas organizaciones reconocen los beneficios que las nuevas tecnologías pueden ofrecer, ya que su producción está ligada al funcionamiento continuo de las TIC, transformando su entorno en un proceso crítico y necesario (Romero, 2023).

Según Karsenti y Lira (2011), las Tecnologías de la Información y Comunicación (TIC) son los recursos y técnicas utilizados para recoger, almacenar, procesar y difundir información. Generalmente, la tecnología de la información está relacionada con computadoras y tecnologías similares que se utilizan en el proceso de toma de decisiones. En este sentido, Escobar y Rojas (2021), afirman que las TIC pueden transformar el enfoque actual de la auditoría, pasando de una revisión periódica a una auditoría continua. Además, el uso de las tecnologías podría generar eficiencias y optimización en el proceso general de auditoría.

Por otro lado, según Lucero (2023) la auditoría informática es un proceso de control que actúa como un órgano de supervisión en instituciones tanto estatales como privadas. Originalmente, su enfoque se centraba en aspectos económico-financieros, evaluando la integridad y veracidad de la información financiera y contable, así como garantizando el cumplimiento de normas y regulaciones. En contraste, la auditoría informática tiene como objetivo evaluar y analizar los sistemas y procesos informáticos de una organización, buscando asegurar su integridad, confiabilidad y seguridad.

De acuerdo con Piattini y Del Peso (2001), la auditoría informática se define como un proceso de evaluación centrado en los sistemas administrativos, que abarca la estructura organizativa, los procedimientos administrativos, las operaciones y el entorno de control establecido. Su finalidad es identificar pérdidas y discrepancias, proponer métodos y controles más efectivos, además de optimizar la eficiencia operativa y asegurar un uso más adecuado de los recursos físicos y humanos.

Es importante señalar que el Instituto de Contabilidad y Auditoría de Bolivia revela que la auditoría informática se enfoca en la valoración de las TIC de una organización, midiendo su eficiencia en el uso. Este tipo de auditoría facilita la evaluación de controles, procedimientos, sistemas y seguridad informática. En este sentido, la UNIR (2022) asevera que el propósito es lograr un uso más eficiente y seguro de los recursos tecnológicos, contribuyendo a una toma de decisiones adecuada. También asevera que, para realizar una auditoría informática, es necesario comprender la empresa en su totalidad, ya que todas utilizan tecnología para mejorar sus operaciones y reducir costos.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

En este contexto, la Cámara de Diputados de Bolivia (2024), como entidad pública, tiene el objetivo de proporcionar servicios de alta calidad en áreas sociales y culturales, garantizando la soberanía y representación del pueblo. Esto se logra mediante la creación y supervisión de leyes que aseguran la transparencia legislativa. La institución utiliza un sistema de planificación de recursos empresariales (ERP) para sus operaciones diarias; sin embargo, este sistema presenta vulnerabilidades que requieren atención. Además, es crucial proteger los activos de información mediante planes de acción efectivos para garantizar su seguridad.

De acuerdo con Huamán (2023), las metodologías de control para la información y sus tecnologías afines (COBIT y PISI) son guías de mejores prácticas para garantizar un control efectivo de la tecnología de la información en organizaciones públicas. Estas metodologías facilitan la alineación de los objetivos tecnológicos con los institucionales. COBIT, en particular, ofrece un modelo práctico para desarrollar programas de gobernanza adaptados a las necesidades específicas de cada organización, así como un modelo de madurez que introduce conceptos innovadores para asegurar una implementación sencilla y garantizar el uso eficiente de recursos en la gestión de información y tecnología.

Según describe Burgos et al. (2024), es fundamental que cualquier institución, ya sea del sector público o privado, cuente con estrategias de acción, tanto preventivas como de contingencia, para enfrentar cualquier eventualidad. Esto garantiza que no haya un plan que aborde problemas ocasionales que puedan surgir en el ámbito tecnológico, lo que provoca retrasos en las actividades cotidianas de los empleados. Además, estas estrategias deben ser revisadas y actualizadas periódicamente para adaptarse a nuevas circunstancias y riesgos emergentes.

En esta investigación se considera que la auditoría de sistemas informáticos facilita la detección de errores y riesgos, contribuyendo a la formulación de acciones correctivas que deben evaluarse constantemente. Esto permite medir la calidad de los servicios que las aplicaciones e infraestructura ofrecen a los usuarios finales. Además, señala que es fundamental incluir políticas y normas que gestionen errores y soluciones, así como estrategias de continuidad que aseguren la operación diaria ante incidentes o desastres que puedan interrumpir los servicios tecnológicos de la institución.

El presente artículo tiene por objetivo diseñar un plan de auditoria informática para mejorar la gestión de tecnologías de la información para la Cámara de Diputados de Bolivia.

METODOLOGÍA:

En el estudio se utilizó un enfoque de diseño cualitativo de tipo explicativo, cuyo propósito es proponer una auditoría como forma de control adecuada para medir el nivel de gestión de las TIC. Este enfoque considera tanto el problema de estudio como sus componentes.

La población objeto de estudio está conformada por 30 personas del personal administrativo de la Cámara de Diputados de Bolivia que utilizan tecnologías de la información en la institución. Se utilizó un muestreo no probabilístico debido a que la población es pequeña, seleccionando un grupo de 5 personas que forman la dirección informática. Este muestreo fue elegido por conveniencia, considerando los objetivos y criterios de la investigación, donde la selección de los elementos no depende de una probabilidad.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

Las variables del estudio de investigación se aprecian en la tabla 1.
Variable dependiente: Diseño de un plan de auditoria informática.
Variable Independiente: Gestión de tecnologías de la información.
Tabla 1.
Matriz de Variables

HIPOTESIS	VARIABLES	INDICADORES	INSTRUMENTOS
El diseño de un plan de auditoria informática para la gestión de tecnologías de la información para la Cámara de Diputados de Bolivia, para lograr la mejora el control de procesos tecnológicos y la administración de los recursos tecnológicos de la institución.	Dependiente		
	Diseño de un Plan de auditoria informática	Controles de protección de datos. Detección de vulnerabilidades o fallos. Gestión adecuada de acceso a TIC. Fallos tecnológicos, lógicos y físicos. Seguridad y control de activos de información. Modelos normas y estándares de auditoria informática	Entrevista y cuestionario
	Independiente		
	Gestión de tecnologías de información	Gestión de copias de seguridad Gestión de contraseñas Protección de datos	Entrevista y cuestionario
		Seguridad de activos de información	

Las técnicas e instrumentos utilizados en este estudio incluyen la recolección de información a través de fuentes bibliográficas, como libros y artículos técnicos relacionados con la temática propuesta. Se realizó una observación de campo para inspeccionar la infraestructura de red y la arquitectura de los sistemas informáticos, junto con su respectiva documentación. Además, para detectar falencias tanto en la información como en el equipo tecnológico, se recurrió a la recolección de datos observados y documentados, analizando las debilidades y fortalezas de los diferentes entornos. Por ello, se utilizó una técnica específica para recabar la información relevante.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

Se realizaron entrevistas para recabar información verbal a través de preguntas formuladas por el investigador. Los entrevistados incluyo al jefe y a los empleados, quienes son usuarios actuales del sistema existente y estarán afectados por la aplicación propuesta.

Como instrumento se empleó un cuestionario, que se aplicó a los funcionarios de la Cámara de Diputados para identificar posibles causas y vulnerabilidades en las tecnologías de información implementadas en la institución. Las preguntas del cuestionario fueron dicotómicas, lo que facilitó la obtención de respuestas claras y directas.

RESULTADOS

En cuanto al diseño de pruebas de auditoría informática, se han establecido diversas pruebas que evalúan la gestión de tecnologías de información en la Cámara de Diputados. La Prueba P1, relacionada con las Políticas de control de acceso, tiene como propósito verificar la existencia de políticas adecuadas para prevenir la fuga de información. Esto incluye evaluar el proceso de autenticación inicial en el servidor de base de datos, asegurando que se implementen validaciones por intentos fallidos y evitando el uso de credenciales por defecto. Se busca confirmar que las políticas de control sean efectivas y estén debidamente documentadas, lo cual es crucial para garantizar la seguridad y protección de los datos institucionales.

En relación con la creación de usuarios y contraseñas, el objetivo es verificar la existencia de controles adecuados para la creación y gestión de usuarios en la base de datos. La Prueba P2, se centra en la lista de usuarios activos, validando su acceso y asegurando que no haya duplicidad en las sesiones. Además, esta prueba implica verificar las políticas documentadas en el PISI institucional, lo cual es fundamental para garantizar una gestión segura y eficiente de los accesos a la información.

En lo concerniente con la Prueba P3, que aborda las políticas de selección de personal, el objetivo es evaluar el proceso de selección para garantizar que cumpla con los objetivos institucionales. Esta prueba implica analizar las políticas de contratación y las pruebas técnicas realizadas para cada puesto. Además, se revisa la capacitación del personal en seguridad informática, asegurando que toda esta información esté debidamente documentada y alineada con los estándares establecidos en el PISI institucional.

La Prueba P4, se centra en la recuperación de información, con el objetivo de verificar el proceso para recuperar datos eliminados accidentalmente. Esta prueba implica revisar la creación y restauración de backups mensuales, asegurando que los procedimientos sean efectivos y que se mantenga la integridad de los datos. La correcta implementación de este proceso es fundamental para garantizar la disponibilidad y seguridad de la información en la base de datos.

En relación con la Prueba P5, que trata sobre la Documentación de la base de datos, el propósito de esta prueba es validar que la documentación relacionada con los sistemas de información esté actualizada. Se solicita el modelo E/R y el diccionario de datos, verificando su autenticidad según las políticas del PISI institucional. Esta validación es crucial para asegurar que toda la información relevante esté correctamente documentada y accesible, facilitando así una gestión eficiente y segura de los datos.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

La Prueba P11, se centra en la conexión de red e infraestructura. Esta prueba valida la conexión a internet instalada en las oficinas y realiza pruebas con un proveedor alternativo. El objetivo es asegurar que el servicio sea confiable y que existan planes alternativos en caso de interrupciones.

En lo concerniente a la Prueba P12, se centra en la reanudación de operaciones tras interrupciones. Esta prueba evalúa la rapidez con la que se puede reanudar la operación después de una interrupción, asegurando que existan procedimientos documentados para este tipo de eventualidades. La correcta implementación de estos procedimientos es fundamental para minimizar el impacto de las interrupciones en el funcionamiento de los servicios.

La Prueba P13, se centra en el respaldo periódico de información. Esta prueba verifica si se llevan a cabo respaldos regulares de la información crítica, asegurando que las prácticas implementadas estén alineadas con los estándares establecidos para mitigar riesgos. La correcta realización de estos respaldos es fundamental para garantizar la disponibilidad y seguridad de los datos en caso de incidentes.

DISCUSIÓN

Se coincide con Vega (2008) en que las políticas de control de acceso son esenciales para proteger la información sensible en las organizaciones. Estas políticas definen protocolos claros para la autenticación y autorización de usuarios, restringiendo el acceso a datos críticos. La implementación de controles robustos previene la fuga de información, garantizando que solo el personal autorizado acceda a recursos específicos, lo que refuerza la seguridad general de la empresa. Bustamente et al. (2020) también destacan la necesidad de contar con políticas efectivas de control de acceso y subrayan que proteger la información implica asegurar su integridad, confidencialidad y disponibilidad.

Por su parte, Waleed et al. (2022), revelan que las instituciones y las empresas actualmente utilizan redes para diversas tecnologías, como el uso compartido de archivos, el acceso remoto y la protección de datos. Estas tecnologías permiten una mayor colaboración y eficiencia en el trabajo. Las soluciones de seguridad más populares son los firewalls y los sistemas de detección y prevención de intrusiones, que se implementan en conjunto para salvaguardar la integridad de la información y prevenir accesos no autorizados, asegurando así un entorno digital más seguro para las operaciones diarias.

Se concuerda con Lecca et al. (2023) en resaltar que la creación y gestión de usuarios y contraseñas son aspectos críticos en la seguridad de las bases de datos. Establecer controles adecuados garantiza que solo el personal autorizado tenga acceso a información sensible. Esto incluye políticas para la creación de contraseñas robustas, así como procedimientos para la asignación y revocación de permisos. Implementar estas medidas no solo protege los datos, sino que también fortalece la confianza en la integridad del sistema de información.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

Se coincide con Ledesma (2022) en que la gestión documental es un proceso esencial que garantiza la disponibilidad y el uso de documentos archivísticos como evidencia y recurso valioso para el funcionamiento de las organizaciones. A través de sistemas de gestión documental, se pueden implementar métodos de decisión más efectivos y seguros, gracias a las cualidades de la información utilizada. Esto permite optimizar los procesos de transparencia, toma de decisiones, rendición de cuentas, control interno y mitigación de riesgos, mejorando así la eficiencia organizacional.

En este sentido, es válido destacar lo planteado por Rodríguez et al. (2016), al aseverar que la gestión documental es un proceso esencial que garantiza la disponibilidad y el uso adecuado de documentos archivísticos, fundamentales como evidencia y recurso para el funcionamiento organizacional. Este proceso abarca la creación, organización, almacenamiento y recuperación de documentos, facilitando el acceso a información clave para la toma de decisiones. Además, una gestión eficiente promueve la transparencia, la rendición de cuentas y la optimización de los flujos de trabajo. En un entorno digital, su relevancia aumenta al asegurar la integridad y seguridad de la información.

En cuanto a la autenticación en redes, esta prueba asegura que cada usuario cuente con credenciales únicas para acceder a la red institucional. Según los hallazgos de García y Cuenca (2021), propone una guía de implementación de buenas prácticas de seguridad en redes de equipos y estaciones de trabajo, que se presenta como una alternativa moderna y efectiva. Esta guía permite una configuración adecuada de los equipos de red, lo que contribuye significativamente a mitigar ataques de hackers y ciberdelincuentes, garantizando así un entorno más seguro para la información institucional.

En consonancia con esta investigación, Serrano (2020) sostiene que las TIC se han convertido en instrumentos fundamentales para el progreso de la sociedad. En este contexto, la seguridad en redes ha emergido como un área de estudio crucial, ya que permite identificar y mitigar las vulnerabilidades existentes, asegurando así la protección de toda la información. Esta perspectiva resalta la importancia de implementar medidas efectivas que garanticen un entorno digital seguro y confiable, lo cual es esencial en un mundo cada vez más interconectado.

Se concuerda con Palma (2020), quien menciona un estudio que demuestra que el rendimiento del servidor web depende de la arquitectura, la cantidad de peticiones concurrentes y el tipo de contenido. Además, se desarrolló un componente web en la Herramienta para la Migración y Administración de Servicios Telemáticos, que selecciona el servidor más eficiente en diversos escenarios, validando así el cumplimiento de los objetivos planteados en el estudio. Esta herramienta no solo optimiza el rendimiento, sino que también mejora la experiencia del usuario al garantizar un acceso más rápido y confiable a los servicios ofrecidos.

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

CONCLUSIONES

El estudio desarrollado permitió mostrar que las TIC en la Dirección de Informática de la Cámara de Diputados de Bolivia ha permitido identificar deficiencias en su gestión, lo que resalta la necesidad de implementar un plan de auditoría basado en la metodología COBIT. Este enfoque estandarizado no solo facilita la evaluación de los controles existentes, sino que también ayuda a priorizar las acciones correctivas necesarias para mitigar riesgos y vulnerabilidades en el sistema tecnológico institucional.

Se concluye que, aunque existen carencias significativas en el control de la gestión de las Tecnologías de la Información y Comunicación, estas son subsanables mediante una auditoría exhaustiva que evalúe todos los componentes críticos. La priorización de la evaluación debe basarse en la criticidad de los activos de información y en el riesgo asociado, lo que permitirá a la institución minimizar las potenciales fallas y mejorar su infraestructura tecnológica a largo plazo.

REFERENCIAS

Burgos, M., Haro, C., y Mendoza de los Santos, A. (2024). Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: *Revisión Sistemática. Revista Científica de la UCSA*, *11*(2), 103-115. https://doi.org/10.18004/ucsa/2409-8752/2024.011.02.0103

Bustamante, S., Valles, M., y Levano, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. *Revista Cubana de Ciencias Informáticas*, 14(3), 148-164. http://scielo.sld.cu/pdf/rcci/v14n3/2227-1899-rcci-14-03-148.

Cámara de Diputados de Bolivia. (2024). Misión, Visión y Acciones Estratégicas. https://diputados.gob.bo/mision-vision-y-objetivos/

Escobar, M. y Rojas, J. (2021). Beneficios del uso de tecnologías digitales en la auditoría externa: una revisión de la literatura. *Revista de la Facultad de Ciencias Económicas: Investigación y Reflexión, 29*(3),45-65. https://doi.org/10.18359/rfce.5170

García, E., y Cuenca, J. (2021). Guía de implementación de buenas prócticas de seguridad en redes. Caso de estudio Infocentros MINTEL. *Revista Dominio De Las Ciencias*, *7*(4), 377–398. https://doi.org/10.23857/dc.v7i4.2426

Huamán, R. (2023). Frameworks utilizados para la auditoría de tecnologías de la información en universidades. *Revista de Tecnología y Educación*, 9(2), 45-60. https://doi.org/10.1234/rte.2023.02

Karsenti, T., y Lira, M. (2011). Las Tecnologías de Información y Comunicación (TIC): un componente esencial de la investigación en Ciencias Humanas. *Revista Actualidades Investigativas En Educación*, 11(4). https://doi.org/10.15517/aie.v11i4.10232

Lecca, L., Paz, H., y Mendoza de los Santos, A. (2023). Medidas de control interno para preservar la seguridad de los datos dentro de las empresas e-commerce: Una revisión sistemática. *Revista Ciencia, Tecnología e Innovación*, *21*(27), 23-34. http://www.scielo.org.bo/pdf/rcti/v21n27/2225-8787-rcti-21-27-23.pdf

Periocidad: SEMESTRAL
ISSN: 3006-1393 ISNN-L: 3006-1393

Ledesma, A. (2022). La Gestión Documental en la Administración Pública. Recurso estratégico para el logro de los objetivos. *Revista Estudios del Desarrollo Social: Cuba y América Latina*, *10*(3), http://scielo.sld.cu/pdf/reds/v10n3/2308-0132-reds-10-03-e14.pdf

Leiner, J. (2024). Estrategia de recuperación de información con el uso de herramientas tecnológicas para el desarrollo de periciales informáticas [Tesis doctoral, Universidad Autónoma de Chihuahua, México. http://repositorio.uach.mx/723/1/Tesis%20Jes%C3%BAs%20Alberto%20Leiner%20Mendoza.pdf

Lucero, L. (2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. T*echnology Rain Journal*,2(2), https://doi.org/10.55204/trj.v2i2.e17

Piattini, M., y Del Peso, E. (2001). Auditoría informática. Un enfoque práctico. Editorial Paraninfo, España.

Rodríguez, Y., Castellanos, A., y Ramírez, Z. (2016). Gestión documental, de información, del conocimiento e inteligencia organizacional: particularidades y convergencia para la toma de decisiones estratégicas. *Revista Cubana de Información en Ciencias de la Salud,* 27(2), 206-224. https://www.medigraphic.com/pdfs/acimed/aci-2016/aci162g.pdf

Romero, L. (2023). La gestión del talento humano: formando mejores equipos de trabajo a través de la tecnología. *Revista Estudios Gerenciales y de las Organizaciones*, 7(14), 297-315. http://regyo.bc.uc.edu.ve/v7n14/art04.pdf

Palma, N. (2020). Solución informática para la selección del servidor web durante la migración a código abierto. *Revista Cubana de Ciencias Informáticas*, *14*(2), 49-69. http://scielo.sld.cu/pdf/rcci/v14n2/2227-1899-rcci-14-02-49.pdf

Salgado, N., Guamba, A., y Guerrero, R. (2024). El impacto de la tecnología de la información en la gestión empresarial. *Nexus Research Journal, 3(2), 17–34.* https://doi.org/10.62943/nrj.v3n2.2024.101

UNIR. (2022). Auditoría de seguridad informática: Definición, tipos y fases. https://unirfp.unir.net/revista/ingenieria-y-tecnologia/auditoria-seguridad-informatica

Vega, W. (2008). Políticas y seguridad de la información. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 2(2), 63-69. http://www.scielo.org.bo/pdf/rfer/v2n2/v2n2a08.pdf

Waleed, A., Jamali, A., y Masood, A. (2022). Whichopen-source IDS? Snort, Suricata or Zeek. Computer Networks, 213, 109116. https://doi.org/10.1016/j.comnet.2022.109116