ISSN: 2710 - 0901 | ISSN-L: 2710 - 0901

https://revistarebi.org/

REBI. Revista Boliviana de Ingeniería
Volumen 7 | No. 1 | Enero - junio 2025
http://doi.org/10.62319/rebi.v.7i1.22
Páginas 2 - 16

Diseño de una metodología de análisis forense informático para la Cámara de Diputados de Bolivia

Design of a computer forensic analysis methodology for the Chamber of Deputies of Bolivia

Kimberly Luz Velarde-Flores
kimberly2619994@gmail.com
https://orcid.org/0009-0003-5192-7818
Universidad Autónoma del Beni
"José Ballivian" – Bolivia

Recibido 10 de junio 2024 / Arbitrado 18 de agosto 2024 / Aceptado 10 de diciembre 2024 / Publicado 03 de enero 2025

RESUMEN

El análisis forense es crucial en entidades gubernamentales, ya que garantiza la transparencia, previene fraudes y protege la seguridad de los datos. La presente investigación tuvo como objetivo diseñar una metodología de análisis informático forense para la Cámara de Diputados del Estado Plurinacional de Bolivia. Se adoptó un enfoque mixto, descriptivo y propositivo; como técnica se aplicó la encuesta y la entrevista a cinco miembros de la dirección informática de la institución. Los resultados indican una falta de preparación en seguridad informática, el 80% manifiesta que no tiene manuales actualizados, lo que provoca confusiones ante incidentes; el 60% reconoció ataques previos, evidenciando la necesidad urgente de protocolos claros y capacitación. La propuesta de metodología de análisis forense informático, integral y estructurada en cinco fases, contribuye a estandarizar procedimientos, a garantizar la integridad de la evidencia digital, a mejorar la formación continua del personal y a fomentar una cultura proactiva en ciberseguridad.

Palabras Claves: Ataque cibernético; Diseño de metodología; Entidades gubernamentales; Informática forense digital; Integridad de la información.

ABSTRACT

Forensic analysis is crucial in government entities, as it guarantees transparency, prevents fraud and protects data security. The present research aimed to design a methodology for computer forensic analysis for the Chamber of Deputies of the Plurinational State of Bolivia. A mixed, descriptive and propositional approach was adopted; the survey and interview were applied to five members of the institution's IT department as a technique. The results indicate a lack of preparation in computer security, 80% state that they do not have updated manuals, which causes confusion when faced with incidents; 60% recognized previous attacks, evidencing the urgent need for clear protocols and training. The proposed computer forensic analysis methodology, comprehensive and structured in five phases, contributes to standardizing procedures, guaranteeing the integrity of digital evidence, improving the continuous training of staff and fostering a proactive culture in cybersecurity.

Keywords: Cyber attack; Digital forensics; Government entities; Information integrity; Methodology design.

INTRODUCCIÓN

La creciente amenaza de ataques informáticos a entidades gubernamentales ha resaltado la necesidad de adoptar enfoques sistemáticos para la gestión de incidentes cibernéticos. Estos ciberataques son acciones maliciosas dirigidas a sistemas, redes o dispositivos con el objetivo de comprometer su integridad, confidencialidad o disponibilidad (Sema et al., 2024). Pueden definirse como cualquier intento de acceder, modificar o destruir información en un sistema informático sin autorización, lo que resalta la naturaleza intrusiva de tales acciones y su potencial para causar daños significativos a las entidades afectadas (Guaña et al., 2022).

Los ataques pueden variar en su complejidad y motivación, desde simples intentos hasta sofisticadas intrusiones de código malicioso que impide la utilización de los equipos o sistemas que buscan extorsionar a las organizaciones. Los ataques cibernéticos no solo afectan la infraestructura tecnológica, sino que pueden tener repercusiones legales y financieras severas para las organizaciones, especialmente aquellas del sector público (Valencia, 2024). Cada tipo de ataque presenta sus propios métodos y técnicas, lo que requiere que las organizaciones implementen medidas específicas de defensa y respuesta. La diversidad en las tácticas implica que las estrategias deben ser igualmente variadas y adaptativas (Cando y Medina, 2021).

La naturaleza crítica de la información manejada por las entidades gubernamentales hace que sean objetivos atractivos para los atacantes, lo que subraya la urgencia de implementar medidas proactivas y reactivas robustas. Estos ataques no solo comprometen datos sensibles, sino que también pueden afectar la confianza pública en las instituciones (Ponce, 2024b; Ponce, 2024a).

Es por ello que el análisis forense informático se presenta como una herramienta esencial para investigar y mitigar los efectos de estos ciberataques (Guaña et al., 2022). El análisis forense informático se define como el proceso de recolectar, preservar y analizar datos digitales con el fin de investigar incidentes cibernéticos. Este enfoque es fundamental para entender cómo ocurrieron los ataques y qué medidas pueden implementarse para prevenir futuros incidentes. Las medidas preventivas son competencia de la seguridad informática, disciplina que ayuda en la identificación de pistas en casos de delitos cibernéticos, en la detección de robos de información, en el seguimiento de delincuentes a través de chats o correos electrónicos, e incluso, en la recuperación de datos borrados intencionalmente o disponibles en equipos perdidos o dañados (Alemán, 2024; Hermosa et al., 2024).

Para llevar a cabo un análisis forense efectivo es esencial una metodología bien definida, estructurada en fases claras que guíen a los especialistas desde la identificación del incidente hasta la presentación de informes finales, que incluyan la identificación y aseguramiento de la escena, recolección y preservación de evidencia, análisis de datos y presentación del informe final. Cada fase debe seguir protocolos específicos que aseguren la integridad de la evidencia y minimicen el riesgo de contaminación. La adopción de normas y estándares reconocidos es fundamental para garantizar que el análisis forense se realice conforme a las mejores prácticas del sector (Rojas et al., 2023).

La metodología forense permite no solo permite identificar las vulnerabilidades explotadas por los atacantes, sino también evaluar el impacto del ataque en los sistemas afectados. Este proceso se basa en principios científicos y legales, lo cual es crucial en un contexto judicial. La implementación adecuada del análisis forense puede ser determinante para recuperar datos perdidos y restaurar sistemas comprometidos (Rubio y Clemente, 2022).

A pesar de las evidentes ventajas del uso de estas metodologías, existen limitaciones a nivel global, incluidas las instituciones gubernamentales, que están relacionadas con la falta de documentación actualizada, ausencia de protocolos formales para la gestión de incidentes cibernéticos, vulnerabilidades en infraestructura tecnológica, insuficiencias en las auditorías informáticas y deficiente capacitación del personal. Estas condiciones contribuyen a elevar el nivel de vulnerabilidad a los ataques cibernéticos y las dificultades para responder adecuadamente ante incidentes críticos (Hurtado y Casanova, 2022).

En este contexto, se requiere una mayor comprensión y abordaje de los elementos que influyen en este proceso, de ahí que se planteen las siguientes interrogantes ¿cuáles son las principales vulnerabilidades de seguridad informática en las entidades gubernamentales?, ¿cómo una metodología de análisis forense informático contribuye a mejorar la capacidad de respuesta ante incidentes cibernéticos? Teniendo en cuenta lo antes expuesto, el propósito de la presente investigación fue diseñar una metodología de análisis informático forense para la Cámara de Diputados del Estado Plurinacional de Bolivia.

METODOLOGÍA

La investigación tuvo un enfoque mixto, de tipo descriptivo y propositivo. A partir de la caracterización teórica, se realizó un diagnóstico inicial y se realizó la propuesta de diseño.

La variable dependiente la constituyó el análisis forense informático, que incluyó como indicadores a) la identificación de evidencia, b) la adquisición de evidencia, c) la preservación de evidencia, d) el análisis de datos, e) la presentación de informe pericial y f) la muestra de pruebas.

La metodología de análisis forense informático fue la variable independiente, que contribuyó al análisis y sistematización de las evidencias digitales. Se tuvieron en cuenta como indicadores a) el planeamiento del problema, b) la identificación de objeto de estudio, c) la adquisición de evidencia, d) el análisis de datos y e) la presentación de resultados.

La población de estudio estuvo constituida por 70 personas, miembros del personal administrativo de la Cámara de Diputados del Estado Plurinacional de Bolivia, que realizan el uso de las tecnologías de la información y comunicación dentro la institución. Se realizó un muestreo no probabilístico por conveniencia y se seleccionó como muestra a 5 personas que forman la dirección informática de la Cámara de Diputados, entre los que se encontraban el director de informática; el responsable del área de redes, de soporte Informático y de seguridad de sistemas; el responsable del área de desarrollo de sistemas informáticos; el técnico de desarrollo de sistemas informáticos y el de soporte, quienes fungían como encargados de la seguridad informática y el control de las evidencias digitales.

En ese marco, se asumió como criterio de inclusión al personal de informática de la Cámara de Diputados del Estado Plurinacional de Bolivia y se excluyó al personal que desarrolla funciones en otras aéreas administrativas de la entidad.

Procesamiento y análisis de datos

El plan para el procesamiento y análisis de la información se estructura en tres etapas fundamentales. En primer lugar, se llevó a cabo una revisión crítica de la información recogida, lo que permitió evaluar su relevancia y calidad. A continuación, se procedió a la organización de los datos, facilitando su manejo y análisis posterior. Finalmente, se realizó una interpretación de los resultados obtenidos, esenciales para contribuir al desarrollo de la propuesta. Este enfoque sistemático aseguró que la información fuera utilizada de manera efectiva para alcanzar los objetivos planteados. Se realizó, además, una observación de campo para inspeccionar la infraestructura de red y la arquitectura de los sistemas informáticos que se manejan con su respectiva documentación.

REBI. Revista Boliviana de Ingeniería
Volumen 7, Número 1 / Enero - junio 2025 / ISSN: 2710 - 0901 | ISSN-L: 2710 - 0901

Técnicas y procedimientos

Se utilizó la entrevista como técnica para la recolección de información, que permitió obtener datos de manera verbal a través de preguntas cerradas dirigidas al personal del área de informática. Esta técnica incluyó tanto al jefe del departamento como a los empleados, quienes son usuarios actuales del sistema existente y potenciales beneficiarios de la propuesta del presente estudio. Las entrevistas facilitaron la obtención de información directa sobre su experiencia y expectativas respecto a la implementación de nuevas soluciones.

Además, se llevó a cabo una encuesta dirigida a los funcionarios de la Cámara de Diputados en el área de informática. Esta herramienta se diseñó para identificar los procedimientos actuales de recolección de información en respuesta a ciberataques, lo que es crucial para evaluar la efectividad de las medidas de seguridad implementadas en la institución. Ambas técnicas se complementaron para proporcionar una visión integral sobre el estado actual y las necesidades del sistema informático.

Caracterización de la Cámara de Diputados de Bolivia

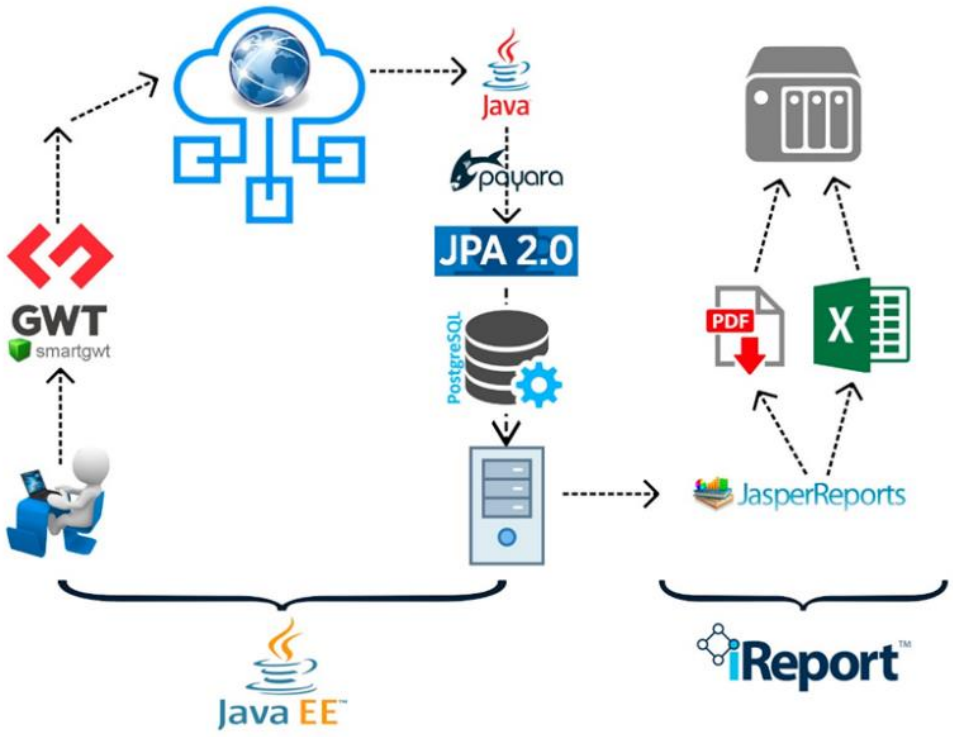
La Cámara de Diputados de Bolivia, es la expresión de la necesidad objetiva del ámbito legislativo del Estado Boliviano, esta institución se encuentra constituida por los representantes electos democráticamente de la sociedad boliviana, denominada el primer Órgano del Estado; es la representación de la multiculturalidad y el pluralismo político de los representantes del país. Siendo una de las instituciones más importantes del Estado, que regula y fiscaliza, mediante las normas y leyes, con la participación de los actores sociales y económicos, la transformación de un estado social e igualitario.

Desde la gestión 2015 hasta el presente, realiza desarrollo de sistemas para la atención y adecuación entre las unidades organizacionales que conforman el ente camaral. Se encuentra organizada por varios departamentos y unidades, para el desarrollo de sus actividades diarias, cuenta con una Dirección de Informática, que es la encargada de crear, implementar y controlar todas las tecnologías de la información dentro de la institución, tanto de las secciones administrativas como la legislativa. Incluye la auditoria informática, la cual, coadyuva en el proceso de monitoreo, seguridad, análisis forense y auditoria informática.

En el año 2017, la Dirección de Informática creó un sistema Enterprise Resource Planning (ERP ARKHE), soporte bajo el que se desarrollan varios sistemas de las unidades que compone este ente camaral, con el fin de contribuir a compartir información entre ellas, a la explotación de datos, la creación del cuadro informativo, entre otras funciones; promoviendo una mejora notable en la agilización de trámites internos, así como la disminución del uso de papel.

Desarrollado bajo el paradigma de software libre, se seleccionó el lenguaje JAVA con el Framework Smartgwt 12, con mapeo de base en JPA II, realizando la conexión a una Base de Datos Postgres, creando empaquetados que contienen cadenas cifradas para la conexión, así como el uso de un Servidor de Aplicaciones Payara, donde se realizan las configuraciones necesarias para la creación de cadenas de conexión JDBC. El manejo del módulo de autenticación está basado en MD5, para incrementar la seguridad del cliente final y para facilitar el despliegue de nuevos sistemas, siempre que tengan características similares con las herramientas de software libre. A nivel físico, en la actualidad se cuenta con una topología tipo estrella (Figura 1) (Cámara de Diputados de Bolivia, 2024).

Figura 1. *Infraestructura y conectividad*



Fuente: Cámara de Diputados de Bolivia (2024).

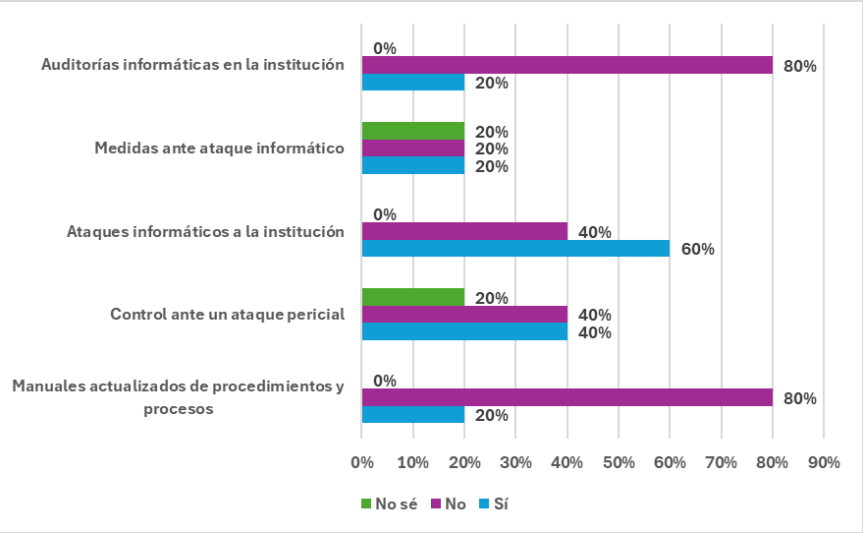
Análisis de resultados de la encuesta

Los resultados de la encuesta reflejan un escenario alarmante respecto al conocimiento y la preparación del personal sobre varios aspectos críticos de la seguridad informática en la institución. En el Gráfico 1 se muestra que, con un 80% de los encuestados indicando que no cuentan con manuales actualizados, se evidencia una falta significativa de documentación que guíe a los empleados en la ejecución de procedimientos y procesos. Esta carencia puede derivar en confusiones operativas y en una respuesta inadecuada ante incidentes, lo que pone en riesgo la eficiencia y seguridad de las operaciones.

La división equitativa entre respuestas afirmativas y negativas, 40% cada una, sugiere que existe una percepción dividida sobre la capacidad de la institución para gestionar ataques periciales. Sin embargo, el 20% declara no conocer sobre el tema, lo que indica una falta de claridad o conocimiento sobre los protocolos existentes, lo cual es alarmante, ya que podría llevar a una subestimación de los riesgos asociados.

El 60% de los encuestados reconocen haber experimentado ataques informáticos, mientras que el 40% restante no lo sabe o no está seguro. Este dato resalta una realidad inquietante, la institución ha sido objeto de amenazas cibernéticas, lo que subraya la necesidad urgente de implementar medidas proactivas y reactivos más robustos para protegerse contra futuras intrusiones.

Gráfico 1. *Percepción y conocimiento sobre seguridad informática en la Institución*



La distribución equitativa entre las respuestas, 20% para cada una, indica una falta de consenso sobre las medidas adoptadas para enfrentar ataques informáticos. Esto sugiere que el personal puede no estar completamente informado sobre las políticas o estrategias implementadas, lo que podría comprometer su efectividad en caso de un incidente real.

Con un alarmante 80% de los encuestados afirmando que no se realizan auditorías informáticas, se pone de manifiesto una grave deficiencia en el monitoreo y evaluación de los sistemas de seguridad existentes. Las auditorías son esenciales para identificar vulnerabilidades y garantizar el cumplimiento de las normativas; su ausencia podría dejar a la institución expuesta a riesgos significativos.

En conjunto, estos resultados subrayan la necesidad urgente de mejorar la capacitación del personal, actualizar los manuales y procedimientos, y establecer protocolos claros para la gestión de incidentes cibernéticos. La falta de conocimiento y preparación en estos aspectos puede tener consecuencias graves para la seguridad institucional y su operatividad general.

Análisis de resultados de la entrevista

Las entrevistas realizadas a los jefes de distintas áreas de la Dirección de Informática de la Cámara de Diputados de Bolivia permitieron obtener información valiosa sobre la situación actual en relación con los delitos informáticos y la preparación institucional para enfrentarlos. Los entrevistados, que incluyen al jefe de informática, al jefe del área de redes y soporte, y al jefe del área de desarrollo de sistemas, han proporcionado perspectivas cruciales para el diseño e implementación de una metodología de análisis forense informático.

En respuesta a la primera pregunta sobre si la institución ha sufrido ataques informáticos, todos los entrevistados confirmaron la ocurrencia de múltiples incidentes, lo que indica una vulnerabilidad significativa en la infraestructura tecnológica. Este hallazgo resalta la necesidad urgente de fortalecer las defensas cibernéticas y mejorar la conciencia sobre las amenazas existentes. Se identificaron diversas modalidades de ataques informáticos sufridos, incluyendo *malware*, *phishing*, *ransomware* e inyección SQL. La variedad y gravedad de estos ataques sugieren que la institución maneja información altamente sensible, lo que aumenta su atractivo para los atacantes.

Esto implica que se deben adoptar medidas más robustas para proteger los datos críticos y mitigar los riesgos asociados.

Cuando se cuestiona sobre la seguridad de las tecnologías utilizadas, las respuestas reflejaron una falta de confianza en la protección actual. Aunque se mencionaron protocolos y herramientas como *firewalls* y la implementación de *proxy*, los entrevistados coincidieron en que no existe una protección total contra las amenazas. Esto indica una necesidad clara de revisar y actualizar las medidas de seguridad implementadas. Por otra parte, los daños causados por incidentes previos incluyen pérdidas de información y daños a equipos, lo que subraya el impacto tangible que tienen estos ataques en la operatividad institucional. Las respuestas sobre las medidas adoptadas para enfrentar estos problemas revelan un enfoque empírico hacia la formación y concientización del personal en temas de ciberseguridad, lo cual es un paso positivo, pero insuficiente sin un marco formalizado.

En cuanto a las medidas adecuadas a tomar ante un ataque informático, los entrevistados señalaron que su conocimiento es también empírico. Esto pone en evidencia una falta generalizada de capacitación formal en procedimientos críticos para manejar incidentes cibernéticos. Asimismo, se identifica la ausencia de lineamientos formales para obtener informes periciales y para aplicar procedimientos tecnológicos, lo que refuerza la idea de que no hay una estructura clara en torno a la gestión de incidentes. Además, el hecho de que no exista un plan formal de contingencia ante violaciones a la seguridad pone en riesgo la capacidad institucional para responder eficazmente a situaciones adversas.

El control efectivo ante un ataque recae en el jefe del área de redes y soporte; sin embargo, esto podría no ser suficiente si no hay protocolos claros o un equipo preparado para manejar tales crisis. Aunque se mencionó que existen lineamientos para el análisis y recolección de evidencias, estos no son formales, lo que limita su efectividad. La falta de manuales actualizados sobre procedimientos y procesos es otra deficiencia crítica identificada. Sin documentación clara y accesible, el personal carece del soporte necesario para actuar adecuadamente durante incidentes cibernéticos.

Finalmente, aunque se reconoció la necesidad urgente de diseñar una metodología para el análisis forense informático, actualmente no se han implementado prácticas formales al respecto. Este consenso entre los entrevistados destaca una oportunidad clara para desarrollar protocolos estandarizados que mejoren la capacidad institucional para llevar a cabo investigaciones forenses efectivas. Estos resultados indican una situación preocupante en términos de preparación y respuesta ante delitos informáticos dentro de la Cámara de Diputados. La falta de procedimientos formales, manuales actualizados y planes de contingencia pone en riesgo tanto la integridad de la información manejada como la operatividad general del sistema.

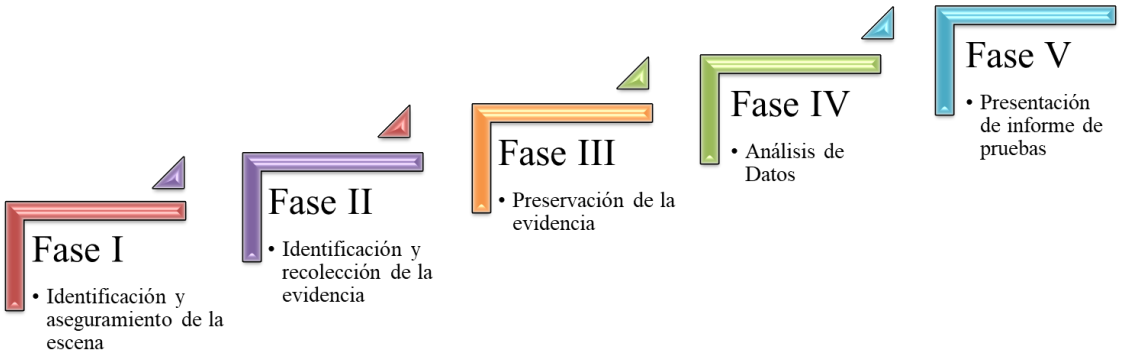
A partir de lo expuesto, se evidencia la ausencia de una metodología unificada que permita a los profesionales del sector llevar a cabo sus tareas dentro de un marco común. Aunque algunas directrices, como la RFC 3227 y las normas UNE 71505 y UNE 71506, ofrecen orientaciones valiosas, no constituyen un enfoque integral. Por lo tanto, se reconoce la necesidad de diseñar una metodología que proporcione al sector una guía práctica para realizar análisis forenses con garantías de éxito en la institución, que considere todas las premisas de seguridad, así como las recomendaciones y estándares existentes, asegurando su efectividad y aplicabilidad en el contexto actual.

Desarrollo de la propuesta de metodología de análisis forense informático

Se diseña una metodología, adecuada para la obtención de evidencia digital, que contribuya a su admisibilidad en procesos judiciales y/o en las instancias requeridas; esta norma pretende orientar a especialistas en evidencia digital, en respuesta a incidentes y gerentes de laboratorios forenses. Se definen y diseñan las fases de la propuesta, que incluirán los procedimientos de análisis de datos forenses, para obtener evidencia válida y suficiente de la operación y preservar la integridad de la información y las pruebas sustantivas.

En la Figura 2 se muestra la secuencia de la metodología, cuyo orden debe ser respetado, en cuanto a las fases, ya que el proceso de investigación logra provisionalidad, consistencia, precisión y objetividad en la búsqueda de análisis y recolección de análisis de datos y evidencia digital.

Figura 2. *Esquema de las fases de la propuesta*



En cada una de las fases, se ofrecieron las mejores recomendaciones y los pasos más comunes para evitar errores.

Fase I - Identificación y aseguramiento de la escena

En esta fase, aunque comúnmente asociada a casos criminales, es crucial para cualquier análisis forense dentro de la institución. El investigador no solo debe realizar un análisis técnico de los equipos implicados, sino también asegurar que la escena del incidente permanezca intacta desde su descubrimiento hasta el análisis. Todos los involucrados deben ser conscientes de que cualquier movimiento inapropiado puede comprometer la investigación. Es fundamental tomar fotografías del entorno para documentar el estado original de la escena y protegerla de accesos no autorizados. También se deben preservar las huellas dactilares, utilizando guantes de látex. El registro de la hora y fecha de los equipos es esencial, incluso si no coincide con la hora real, y debe documentarse cualquier desfase.

Además, es importante observar las entradas y salidas de los equipos y grabar procesos en pantalla. Finalmente, cualquier desconexión de red o eléctrica debe ser cuidadosamente documentada para evitar la pérdida de información valiosa. Una vez asegurada la escena, se procederá a la identificación y recolección de evidencia en la siguiente fase.

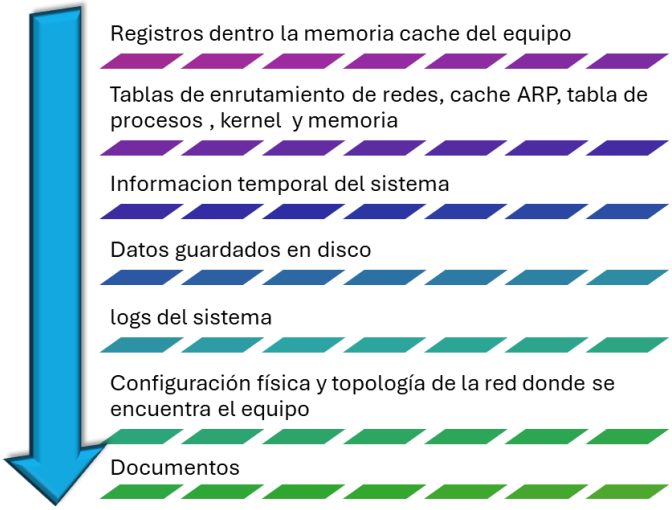
Fase II - Identificación y recolección de la evidencia

La segunda fase del análisis forense se subdivide en dos etapas: identificación y recolección de evidencias. La identificación es crucial para reconocer la volatilidad de los datos, es decir, el tiempo durante el cual permanecerán accesibles en el equipo. Se deben recolectar primero las pruebas

más volátiles. Según la RFC 3227, se debe establecer un orden de volatilidad y evaluar la utilidad de cada evidencia para la investigación. Es necesario documentar y listar los dispositivos observados en la escena, así como el personal involucrado, incluyendo nombres, identificaciones y acciones realizadas desde el incidente. Todos los equipos deben etiquetarse correctamente, anotando marca, modelo y número de serie. Además, se debe solicitar autorización por escrito para la recolección de evidencias, especialmente si se manejan datos confidenciales.

En la etapa de recolección, una vez identificadas las evidencias, se procede a su recolección. Esto incluye realizar copias exactas del contenido de los discos incautados, asegurando que se obtengan todos los archivos relevantes. La integridad de las copias se verifica calculando el hash o CRC, garantizando que no se haya manipulado la información. Se debe crear una segunda copia como respaldo durante el proceso de investigación.

Figura 3. *Proceso de Identificación*



Fase III - Preservación de la evidencia:

Una preservación inadecuada de las evidencias puede invalidar toda la investigación ante un tribunal, lo que resalta la importancia de seguir protocolos rigurosos. Esta etapa incluye la cadena de custodia, procedimiento controla las evidencias desde su descubrimiento hasta su análisis en el laboratorio, evitando manipulaciones y asegurando un registro detallado de quién, cómo, por qué y cuándo se manejaron los elementos incautados. Es fundamental documentar todos los aspectos en la fase de identificación para fortalecer esta etapa. Las evidencias deben ser embaladas y etiquetadas con información básica sobre cada dispositivo, incluyendo número de serie y fabricante.

Se realiza, además, la clasificación y almacenamiento de las evidencias según su naturaleza para protegerlas adecuadamente. Por ejemplo, discos duros y CD deben almacenarse en bolsas antiestáticas para evitar daños por electricidad estática. Además, es crucial que el lugar de almacenamiento sea adecuado, evitando condiciones húmedas o extremas que puedan comprometer la integridad de los dispositivos.

Fase IV - Análisis de Datos:

La fase de análisis concluye solo cuando se determina la causa del incidente y su impacto en el sistema. Es fundamental trabajar con copias de datos, respetando las leyes vigentes. Se tienen en cuenta los siguientes requisitos:

Información necesaria: Se debe recopilar documentación sobre el sistema operativo, programas instalados, hardware y configuraciones de red, incluyendo firewalls y conexiones a Internet.

Preparación del entorno: Antes de analizar, se debe establecer un entorno adecuado, optando entre análisis caliente, en discos originales con precauciones o análisis frío, usando imágenes de disco en máquinas virtuales.

Línea temporal: Se crea una línea temporal de eventos, registrando fechas de modificaciones y accesos. Es crucial verificar las fechas del sistema y rastrear instalaciones recientes.

Determinación del procedimiento de ataque: Se realiza un volcado de memoria para identificar procesos en ejecución y posibles *malware*. Esto incluye el análisis de cadenas de ejecutables para detectar comportamientos sospechosos.

Identificación de autores: Se verifican conexiones de red abiertas y datos del volcado para rastrear el origen del ataque.

Evaluación del impacto: El impacto se mide no solo en términos económicos, como la necesidad de reemplazar dispositivos o reinstalar sistemas, sino también en la paralización de operaciones que puede afectar la productividad general de la institución.

Fase V - Presentación de informe de pruebas

La fase final de un análisis forense consiste en redactar informes que documenten el evento, el trabajo realizado, el método seguido y las conclusiones sobre el incidente. Se elaboran dos tipos de informes: el técnico y el ejecutivo. Ambos abordan los mismos hechos, pero difieren en enfoque y nivel de detalle.

Informe Ejecutivo: Utiliza un lenguaje claro y accesible, evitando tecnicismos para facilitar la comprensión de directivos, como el oficial mayor de la Cámara de Diputados, quienes tienen poco tiempo para dedicar al proceso forense.

Informe Técnico: Destinado a un público técnico, como los empleados de la Dirección de Informática, este documento detalla todos los procesos, programas y técnicas utilizados. Debe incluir:

- Motivos de la intrusión: Propósito del ataque.
- Desarrollo de la intrusión: Cómo se llevó a cabo.
- Resultados del análisis: Daños causados y posibles autores.
- Recomendaciones: Medidas para prevenir futuros incidentes.

El informe técnico es más extenso y abarca antecedentes del incidente, recolección de datos, descripción de evidencias, entorno de trabajo, análisis detallado y una línea temporal completa. Además, incluye conclusiones y recomendaciones sobre protección y acciones legales.

Procedimientos para que la evidencia digital sea admitida en Bolivia

Para que la evidencia digital sea admitida en Bolivia, es crucial que se obtenga de manera lícita, respetando las garantías constitucionales. Según el Nuevo Código de Procedimiento Penal, las pruebas obtenidas mediante tortura o violaciones de derechos fundamentales son inadmisibles. Es necesario contar con una orden judicial para identificar y preservar la evidencia digital, ya que su manipulación puede vulnerar derechos. La cadena de custodia debe mantenerse para asegurar la autenticidad de las pruebas, documentando cada transferencia de custodia. Además, se deben seguir procedimientos específicos para el secuestro y almacenamiento de evidencias digitales, garantizando su integridad y evitando alteraciones. La preservación adecuada es vital, dado que la evidencia digital es frágil y susceptible a modificaciones irreversibles (Ministerio de Justicia, 2010).

Estos resultados confirman que, en un entorno digital cada vez más complejo, contar con un enfoque estructurado en el análisis forense es esencial para mitigar riesgos y responder adecuadamente a incidentes de seguridad. La implementación de una metodología de análisis forense informático en la Cámara de Diputados de Bolivia será crucial para fortalecer la seguridad cibernética y proteger la integridad de la información.

DISCUSIÓN

Los resultados de la encuesta sobre la seguridad informática en la Cámara de Diputados de Bolivia revelan un panorama preocupante que refleja limitaciones en la preparación y conocimiento del personal en aspectos críticos de la ciberseguridad. Este hallazgo es respaldado por el World Economic Forum (2024), donde se exponen los riesgos para las entidades gubernamentales que no cuentan con manuales actualizados, lo que pone de manifiesto una carencia significativa de documentación que guíe a los empleados en la ejecución de procedimientos y procesos. Esta ausencia puede resultar en confusiones operativas y en respuestas inadecuadas ante incidentes, lo que pone en riesgo tanto la eficiencia como la seguridad de las operaciones. El estudio enfatiza la importancia de contar con protocolos claros y actualizados para enfrentar las amenazas cibernéticas.

En el presente estudio se evidencia la a percepción dividida entre los encuestados sobre la capacidad institucional para gestionar ataques periciales. Esta falta de claridad puede llevar a una subestimación de los riesgos asociados, lo que es respaldado por los resultados obtenidos por Fernández (2022), quien subraya que el aumento de la digitalización y las tensiones geopolíticas han incrementado el riesgo de ciberataques con consecuencias sistémicas, lo que resalta aún más la necesidad urgente de mejorar la preparación del personal y establecer protocolos claros para la gestión de incidentes.

Los participantes en esta investigación reconocieron, en su mayoría, haber experimentado ataques informáticos, lo que indica que la institución ha sido objeto de amenazas cibernéticas. Este dato resalta la necesidad imperiosa de implementar medidas proactivas y reactivas más robustas para protegerse contra futuras intrusiones. Resultado que coincide con Izaguirre y León (2018), quienes en su análisis sobre los ciberataques reportados en América Latina, determinan las deficiencias que existen en los países de la zona con respecto a mecanismos de defensa contra ataques cibernéticos, entre los que se encuentra el desconocimiento sobre las medidas adoptadas para enfrentarlos y las políticas o estrategias a implementar, lo cual compromete su efectividad en caso de un incidente real.

En este sentido, Ávila (2024), revelan desafíos significativos en la implementación efectiva de políticas de seguridad, destacando la brecha entre la formulación de marcos normativos y su aplicación práctica, junto con las limitaciones en recursos y capacitación. Además, resaltan la importancia de fomentar una cultura organizacional de ciberseguridad y la necesidad de avanzar en la digitalización como elementos clave para mejorar la resiliencia institucional. La investigación sugiere que la efectividad de los programas de formación en esta área depende de su personalización y la inclusión de elementos prácticos, considerando esencial la mejora de la claridad y efectividad de la legislación en seguridad de la información para fortalecer la confianza en las instituciones públicas y garantizar una protección de datos robusta.

La presente investigación demuestra la importancia de las auditorías para identificar vulnerabilidades y garantizar el cumplimiento normativo; su ausencia podría dejar a la institución expuesta a riesgos significativos. Este hecho es respaldada por Garzón (2002), que subraya la importancia de las auditorías tecnológicas como herramientas diagnósticas esenciales para detectar debilidades en la infraestructura informática, lo que permite a las organizaciones mitigar amenazas antes de que se conviertan en incidentes graves. Por su parte, Bailon (2019) y Salcán (2022), indican que las auditorías no solo ayudan a identificar vulnerabilidades, sino que también optimizan las inversiones tecnológicas al asegurar que los recursos se utilicen de manera efectiva y alineada con los objetivos estratégicos de la organización.

Las entrevistas realizadas revelan que todos los jefes confirmaron haber sufrido múltiples incidentes cibernéticos, lo que indica una vulnerabilidad significativa en la infraestructura tecnológica. La variedad y gravedad de estos ataques sugieren que se maneja información altamente sensible, aumentando su atractivo para los atacantes. Se coincide con Vaca y Dulce (2024), quienes plantean que la necesidad de garantizar la cadena de custodia en investigaciones forenses es esencial para preservar el registro y procedencia de la evidencia digital. En su investigación revelaron diversos marcos, pruebas de concepto, prototipos y protocolos de *blockchain* en el registro, intercambio y trazabilidad de evidencia digital en diferentes contextos, así como los beneficios, limitaciones y desafíos asociados con su implementación.

La propuesta metodológica diseñada para el análisis forense informático incluye fases críticas como identificación y aseguramiento de la escena, recolección y preservación de evidencia, análisis de datos y presentación del informe; atendiendo a las vulnerabilidades detectadas en el diagnóstico inicial. Este diseño coincide con la propuesta de Echeverría (2024), quien considera que este enfoque estructurado es esencial para mitigar riesgos y responder adecuadamente a incidentes de seguridad. De acuerdo con Albarrán et al. (2020), las auditorías informáticas que se realizan en las organizaciones deben utilizar metodologías de apoyo, y su uso depende de la experiencia del auditor, del conocimiento de esta y de complementarlas con buenas prácticas y estándares mundialmente aceptados, con el fin de robustecerlas y minimizar la parte subjetiva que tienen de manera general las auditorías, al ser ejecutadas.

En este mismo contexto Angamarca (2022), considera que, un marco metodológico bien definido es fundamental para garantizar la validez y suficiencia de la evidencia digital en diversos sectores, propone estrategias de auditoría informática en la era de la transformación digital, basándose en normas recomendadas como ISO/IEC 27000, ITIL, COBIT y PCI DSS

para garantizar la seguridad y protección de la información. Estas estrategias concuerdan con la metodología del presente estudio, ya que incluyen la adaptación a la transformación digital, la evaluación oportuna de riesgos, la realización de auditorías periódicas, el cumplimiento normativo y la búsqueda de la mejora continua, lo que permite a las organizaciones enfrentar los desafíos y aprovechar las oportunidades que brinda la tecnología actual en un medio en constante evolución.

Los resultados obtenidos concuerdan con los de estudios previos, lo que reafirma que la falta de procedimientos formales, manuales actualizados y planes de contingencia pone en riesgo tanto la integridad como la operatividad general del sistema. Es imperativo desarrollar e implementar una metodología única y definitiva que proporcione al sector una guía práctica para realizar análisis forenses con garantías de éxito, considerando todas las premisas de seguridad necesarias en este entorno digital cada vez más complejo.

CONCLUSIONES

Los resultados de la encuesta y las entrevistas realizadas a los directivos del área de informática de la Cámara de Diputados de Bolivia revelan limitaciones en la preparación y conocimiento en materia de seguridad informática. El 80% de los participantes manifiesta que se carece de manuales actualizados, lo que puede llevar a confusiones operativas y respuestas inadecuadas ante incidentes. La percepción dividida sobre la capacidad para gestionar ataques cibernéticos, junto con un 60% de reconocimiento de ataques previos, subraya la necesidad urgente de implementar protocolos claros y mejorar la capacitación del personal para mitigar riesgos y fortalecer la seguridad institucional.

La metodología diseñada propone estandarizar los procedimientos, garantizar la integridad de la evidencia digital, lo cual es crucial para cualquier acción legal o investigativa. Al establecer un enfoque sistemático que contemple todas las fases del análisis forense, se asegura una respuesta más efectiva ante ataques, se mejorará la seguridad informática, se contribuirá a crear una cultura organizacional más consciente y preparada frente a las amenazas digitales y la protección de la integridad de la información manejada.

Para la implementación efectiva de la metodología propuesta y la capacitación de especialistas y funcionarios, es crucial establecer un programa integral de formación continua, que incluya talleres prácticos y teóricos que aborden cada fase del análisis forense, asegurando que todos los participantes comprendan no solo los procedimientos técnicos, sino también la importancia de seguir protocolos rigurosos. Además, se sugiere realizar simulacros regulares de incidentes cibernéticos para evaluar la preparación del personal y ajustar las estrategias de respuesta según los resultados obtenidos.

REFERENCIAS

Albarrán, S. E., Pérez, J. C., Salgado, M. y Valero, L. L. (2020). Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares. *Ideas en Ciencias de la Ingeniería*, *1*(1), 49-70. https://ideasencienciasingenieria.uaemex.mx/article/view/14591/10992

Alemán, A. (2024). Análisis forense digital en dispositivos móviles. *Revista Cathedra*(21), 45-64. https://doi.org/10.37594/cathedra.n21.1419

Angamarca, L. (2022). Estrategias de auditoría informática en la era de la transformación digital. *Technology Rain Journal*, *1*(1), e1-e1. https://doi.org/10.55204/trj.v1i1.e1

Ávila, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic Social Science Research*, *4*(2), 140-156. https://doi.org/10.55813/gaea/jessr/v4/n2/96

Bailon, W. A. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. *CIENCIAMATRIA*, *5*(1), 73-87. https://doi.org/10.35381/cm.v5i1.248

Cámara de Diputados de Bolivia. (2024). *Sistema CaDi, Enterprise Resource Planning (ERP)*. Cámara de Diputados de Bolivia. https://cadi.diputados.bo/

Cando, M. R. y Medina, R. P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. *3 c TIC: cuadernos de desarrollo aplicados a las TIC*, *10*(1), 17-41. https://dialnet.unirioja.es/servlet/articulo?codigo=7888164

Echeverría, E. A. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. Una revisión sistemática. *593 Digital Publisher CEIT*, *9*(6), 644-652. https://doi.org/10.33386/593dp.2024.6.2775

Fernández, E. (2022). Derecho de la ciberseguridad de las infraestructuras críticas: Más allá de la perspectiva penalista. *Revista Jurídica de Castilla y León*(56), 109-141. https://dialnet.unirioja.es/servlet/articulo?codigo=8231537

Garzón, C. A. (2002). Auditorías tecnológicas. *Ingeniería e investigación*(50), 30-35. https://dialnet.unirioja.es/servlet/articulo?codigo=4902831

Guaña, J., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P. y Pillajo, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. *Revista Ibérica de Sistemas e Tecnologias de Informação*(E54), 87-100. https://www.proquest.com/docview/2812112763?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals

Hermosa, I. H., Arcos, L. A., Murillo, H. X. y Recalde, P. E. (2024). Evaluación del peritaje informático forense en Quito: Desafíos, estándares y recomendaciones para mejorar su eficacia. *Revista Científica Ciencia y Tecnología*, *24*(44). https://doi.org/10.47189/rcct.v24i44.723

Hurtado, R. F. y Casanova, C. I. (2022). La Auditoría Forense como Herramienta para la Detección de Fraudes Financieros en Ecuador. *Revista Científica Zambos*, *1*(1), 33-50. https://revistaczambos.utelvtsd.edu.ec/index.php/home/article/view/52

Izaguirre, J. y León, F. (2018). Análisis de los ciberataques realizados en América Latina. *Innova research journal*, *3*(9), 172-181. https://doi.org/10.33890/innova.v3.n9.2018.837

Ministerio de Justicia. (2010). Código Penal y Código de Procedimiento Penal. En Bolivia: Dirección General de Asuntos Jurídicos.

Ponce, M. A. (2024a). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119-123. https://doi.org/10.36097/rsan.v1i58.2667

Ponce, M. A. (2024b). Desafíos y respuestas legales ante los delitos informáticos en Ecuador. Revista San Gregorio, 1(58), 111-118. https://doi.org/10.36097/rsan.v1i58.2667

Rojas, J., Patiño, S. y Sacón, H. (2023). Implementación de la metodología para el análisis forense de imágenes de unidades de almacenamiento. IPSA Scientia, revista científica multidisciplinaria, 8(4), 37-52. https://doi.org/10.62580/ipsc.2023.8.6

Rubio, J. y Clemente, C. M. (2022). Peritaje informático, análisis forense digital y respuesta a incidentes. RUIDERAe: Revista de Unidades de Información (19), 9. https://dialnet.unirioja.es/servlet/articulo?codigo=8442626

Salcán, C. (2022). Comparativa de herramientas TICS aplicadas en el proceso de auditoria informática. Technology Rain Journal, 1(1), e3-e3. https://doi.org/10.55204/trj.v1i1.e3

Sema, W., Yayeh, Y. y Abeshu, A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031

Vaca, P. A. y Dulce, E. (2024). Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático. TecnoLógicas, 27(60). https://doi.org/10.22430/22565337.3049

Valencia, E. H. (2024). Implicaciones y desafíos del ciberespacio para la aplicación del Derecho Internacional. Revista Política Internacional, 6(1), 219-233. https://doi.org/10.5281/zenodo.10396392

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. Insight report. World Economic Forum, Davos-Klosters, Suiza