UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

MODELO DE AUDITORÍA INFORMÁTICA FORENSE PARA LA MITIGACIÓN DEL RIESGO REPUTACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO "ARTESANOS"

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

AUTOR: Ing. Andrés Ramiro Aldás Portilla

DIRECTOR: Msc. Diego Javier Trejo España

IBARRA - ECUADOR

2025

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	0401792031		
APELLIDOS Y NOMBRES	ALDÁS PORTILLA ANDRÉS RAMIRO		
DIRECCIÓN	AV. ULPIANO PALACIOS Y GARCÍA MORENO		
EMAIL	araldasp@utn.edu.ec		
TELÉFONO FIJO	062280737	**TELÉFONO MÓVIL:**	0999304841

DATOS DE LA OBRA	
TÍTULO:	MODELO DE AUDITORÍA INFORMÁTICA FORENSE PARA LA MITIGACIÓN DEL RIESGO REPUTACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO “ARTESANOS”
AUTOR (ES):	ALDÁS PORTILLA ANDRÉS RAMIRO
FECHA:	17 de marzo del 2025
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA	MAGÍSTER EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA
TUTOR	MSC. DIEGO JAVIER TREJO ESPAÑA

2. **CONSTANCIAS**

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 17 días del mes de octubre del año 2025

EL AUTOR:

ANDRES RAMIRO ALDAS PORTILLA

Firmado digitalmente por ANDRES RAMIRO ALDAS PORTILLA
Fecha: 2025.10.17 11:32:18 -05'00'

Firma_____

Ing. Andrés Aldás Portilla

APROBACIÓN DEL TUTOR

Yo, Diego Javier Trejo España, en calidad de director de la tesis titulada: “MODELO DE AUDITORÍA INFORMÁTICA FORENSE PARA LA MITIGACIÓN DEL RIESGO REPUTACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO ARTESANOS ” de autoría del Ing. Andrés Ramiro Aldás Portilla, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

Ibarra, a los 17 días de octubre del 2025

TREJO ESPANA DIEGO JAVIER

Firmado digitalmente por TREJO ESPANA DIEGO JAVIER
Fecha: 2025.10.17 14:35:50 -05'00'

DIRECTOR DE TESIS

DEDICATORIA

Este pequeño peldaño académico que he decidido marcar en mi carrera profesional, dedico a todas las personas que creyeron, creen y seguirán creyendo en mí, de manera muy particular y especial a mis padres y hermanos, que son mi base que nuca falla, que siempre están ahí apoyándome en las decisiones que tomo, levantándome cada vez que he recaído, brindándome sus consejos sabios y valederos.

Andrés Ramiro Aldas P.

AGRADECIMIENTO

Agradezco a Dios por guiarme en mis decisiones, siempre pidiéndole la bendición y la sabiduría para continuar aprendiendo y alcanzar mis metas profesionales y personales.

Reitero mi agradecimiento a mi madre Yomar, mi padre Andrés y a mis hermanos Gandhy e Ismael, quienes siempre me apoyan y creen en mí y eso es lo más importante y valioso para poder construir sueños, metas y objetivos de vida.

Agradezco infinitamente a mi director Msc. Diego Trejo y asesor PhD. Marco Pusdá quienes fueron quienes guiaron mi trabajo de investigación, y así culminar esta etapa.

De igual forma a toda la planta docente de la Facultad de Maestría de la Universidad Técnica del Norte, quienes impartieron sus conocimientos en esta cohorte, lo cual fue muy productivo y provechoso consolidar nuevo aprendizaje y aplicar en nuestro entorno laboral.

¡Mil Gracias!

Andrés.

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTA DE POSTGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

MODELO DE AUDITORÍA INFORMÁTICA FORENSE PARA LA MITIGACIÓN DEL RIESGO REPUTACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO "ARTESANOS"

Autor: Ing. Andrés Ramiro Aldás Portilla

Tutor: Msc. Diego Javier Trejo España

Año: 2025

RESUMEN

El presente trabajo investigativo tiene como objetivo diseñar un modelo de auditoria informática forense para la mitigación del riesgo reputacional de la Cooperativa de Ahorro y Crédito "Artesanos" al enfrentar fraudes electrónicos financieros, por ello para conseguir dicho objetivo se ha trabajado en tres pilares.

Primero, el presente estudio ha permitido analizar y comparar dos metodologías especializadas en el análisis forense de sistemas informáticos y evidencia digital. Se integró la propuesta técnica de Velarde (2025) con los lineamientos de la norma internacional ISO/IEC 27037, logrando así un marco metodológico completo y estructurado que fortalece todas las etapas del proceso forense: recolección, preservación, manejo y análisis de evidencia digital.

Segundo, como parte del diagnóstico institucional, se realizó un análisis de eventos históricos críticos registrados en la cooperativa, en el que identificó que existe un nivel de riesgo medio-alto de fraude financiero asociado al uso de sistemas informáticos. Siendo incidentes que se relacionan con errores humanos o prácticas no éticas del personal, lo que demuestra la necesidad de mejorar los controles internos.

Tercero, ante esto se desarrolló un modelo de auditoría informática forense diseñado específicamente para la cooperativa. Este modelo incluye todas las fases esenciales del análisis forense digital, desde la detección de incidentes hasta la emisión de un informe probatorio final, el enfoque integral y adaptable permite aplicarlo en diversos escenarios, respondiendo a las exigencias operativas y de seguridad de la institución

Palabras calve: Evidencia digital, auditoria forense, eventos históricos, ISO/IEC 27037.

ABSTRACT

The objective of this research work is to design a forensic IT audit model to mitigate the reputational risk of the "Artesanos" Savings and Credit Cooperative in the face of financial electronic fraud. To achieve this objective, the study is based on three main pillars.

First, this study analyzed and compared two specialized methodologies for forensic analysis of computer systems and digital evidence. The technical proposal by Velarde (2025) was integrated with the guidelines of the international standard ISO/IEC 27037, resulting in a comprehensive and structured methodological framework that strengthens all stages of the forensic process: collection, preservation, handling, and analysis of digital evidence.

Second, as part of the institutional diagnostic, a historical analysis of critical events recorded within the cooperative was conducted. It identified a medium-high level of financial fraud risk associated with the use of IT systems, mainly due to human error or unethical practices by staff, highlighting the need to improve internal controls.

Third, in response to these findings, a forensic IT audit model was developed specifically for the cooperative. This model covers all essential phases of digital forensic análisis, from incident detection to the issuance of a final probative report. Its comprehensive and adaptable approach makes it applicable in various scenarios, aligning with the operational and security demands of the institution.

Keywords: Digital evidence, forensic auditing, historical events, ISO/IEC 27037.

CAPITULO I

1 EL PROBLEMA

1.1 Problema de investigación

En la era tecnológica en el que el humano ha venido adaptándose hasta la actualidad, presta multifuncionalidades necesarias que facilitan la interactividad, la productividad, la optimización de tiempo, la accesibilidad y la comunicación de manera eficiente, abarcando casi la mayoría de sectores sociales, entre ellos, el financiero, que a través de software especializado y aplicaciones facilitan la transaccionalidad y posibilitan de servicios bancarios.

A medida del incremento de la tecnología para el mejoramiento y agilización de las actividades en el sector financiero, se ha incrementado la exposición de riesgos asociados a diferentes amenazas como, ciberataques, fraudes electrónicos, perdida de datos, violación de la privacidad, interrupciones de los servicios, errores operacionales, deficiencia en la usabilidad, riesgo reputacional y otros, como se menciona en (FATF, Interpol y Egmont Group, 2023):

> El fraude y las estafas en línea han dominado el panorama de la delincuencia cibernética. En caso de no ser controlados, crecerían en sofisticación y representarán una mayor amenaza y riesgo a medida que organizaciones criminales con mayor organización se involucren en esa actividad ilícita y aprovechen las oportunidades que presentan las nuevas tecnologías… (p.5)

A pesar de los esfuerzos y estratégicas institucionales al implementar diversos mecanismos de seguridad en el entorno tecnológico, los ciberdelincuentes continúan adaptándose y encontrando nuevos métodos para efectuar sus cometidos como el robo de identidad, clonación de tarjetas de crédito, phishing (obtención de información), accesos no autorizados a canales electrónicos, transferencias sin consentimiento, entre otros, por lo que puede representar pérdidas económicas y una afectación directa con la reputación y la confianza institucional.

A nivel mundial, el crecimiento de los delitos cibernéticos es evidente y su frecuencia cada vez aumenta, por lo que de acuerdo a un informe realizado por la Organización Internacional de Policía Criminal (Interpol) acerca de las tendencias de estafas en línea, basados en datos proporcionados por 195 países, indica que más del 60

% de los participantes en la encuesta consideran que delitos como el blanqueo de capitales, el ransomware, el phishing y las estafas en línea representan una amenaza "alta" o "muy alta". Asimismo, más del 70 % de los encuestados creen que los delitos como el ransomware y los ataques de phishing incrementarán, o incluso lo harán de manera significativa, en los próximos tres a cinco años (Interpol, 2022).

En el sector cooperativo financiero del Ecuador, las necesidades de la digitalización y la cobertura estratégica a socios, usuarios y clientes mediante el apoyo de los recursos tecnológicos han creado debilidades de seguridad que forman parte de los riesgos inherentes de las entidades, según la (Superintendencia de Economía Polpular y Solidaria, 2021) describe que:

> (…) los avances tecnológicos también conllevan vulnerabilidades a las que están expuestos los usuarios de canales digitales. Según datos de la Fiscalía General del Estado, hasta agosto de 2020, se registraron 5.048 denuncias por delitos informáticos, en el Ecuador. El 92% se concentra en los delitos como: suplantación de identidad (43%), falsificación y uso de documento falso (29%) y apropiación fraudulenta por medios electrónicos (20%). Esta alarmante situación incluso se acentuó en el marco de la pandemia ocasionada por el COVID-19.

Al igual que las demás entidades financieras del Ecuador, la Cooperativa de Ahorro y Crédito Artesanos Ltda., de segmento 2, situada su agencia matriz en Ibarra, se encuentra expuesta a riesgos asociados a fraudes financieros que pueden afectar al giro económico de la entidad e incidir con la reputación frente a socios, cliente y usuarios, ya que pueden generarse a nivel operativo sobre el Core Financiero, modificación de la información financiera y en el uso de canales digitales, este último siendo uno de los medios más frecuente que se cometen este tipo de delitos, debido que la agilidad y la innovación digital, propone diversas formas de servicios a través de dispositivos y el uso de internet, por lo que también se presenta como un reto debido a la falta de experiencia de algunos clientes con los sistemas de pago electrónicos. En este contexto, las cooperativas deben intensificar sus esfuerzos para asegurar las transacciones, capacitar a sus usuarios y fomentar la confianza (Maldonado, 2021).

En ese sentido, la cooperativa en los dos últimos años (2023-2024) ha detectado comportamientos inusuales con un perfilamiento de riesgo de fraudes financieros bajo el uso de los canales digitales, en el que usurpadores acceden a las aplicaciones web y móviles y toman el control absoluto de los medios de notificación y autenticación (correo

electrónico) para realizar transacciones no autorizadas, y en otros casos eventos de procedencia interna, en el que el funcionarios directos al giro de negocios violenta la ética profesional y la confidencialidad, haciendo uso indebido de privilegios elevados en los sistemas con la finalidad de realizar movimientos indebidos en beneficio propio.

1.2 Interrogantes de investigación

¿Qué metodología debería aplicarse para inmiscuir un proceso forense a un proceso de auditoria informática respecto a fraudes electrónicos?

¿Mediante que método se puede determinar el nivel de incidencias o eventos de riesgo respecto a fraudes financieros cometidos en sistemas y aplicaciones informáticas de una entidad financiera?

¿De qué manera influye un modelo auditoria informática forense para mitigar el riesgo reputacional en una entidad financiera?

¿Cómo puede influir un modelo de auditoria informática forense para determinar la fuente de un incidente de fraude financiero en un tiempo oportuno para a toma de decisiones?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Diseñar un modelo de auditoria informática forense para la mitigación del riesgo reputacional de la Cooperativa de Ahorro y Crédito “Artesanos” al enfrentar fraudes electrónicos financieros.

1.3.2 Objetivos específicos

- Analizar metodologías de análisis forense, enfocado en los sistemas informáticos financieros.
- Determinar el nivel de indecencias o eventos de riesgo en históricos registrados, provenientes de fraudes financieros cometidos mediante el uso de los sistemas informáticos y aplicaciones financieras de la cooperativa tomada como caso de estudio.
- Desarrollar un modelo de auditoría informática forense para el manejo de la evidencia digital de los sistemas informáticos de la Cooperativa de Ahorro y Crédito “Artesanos”.

1.4 Hipótesis de trabajo

El Diseño de un modelo de auditoria informática forense permitirá la mitigación del riesgo reputacional de la Cooperativa de Ahorro y Crédito “Artesanos” al enfrentar fraudes electrónicos financieros.

1.5 Hipótesis alternativa

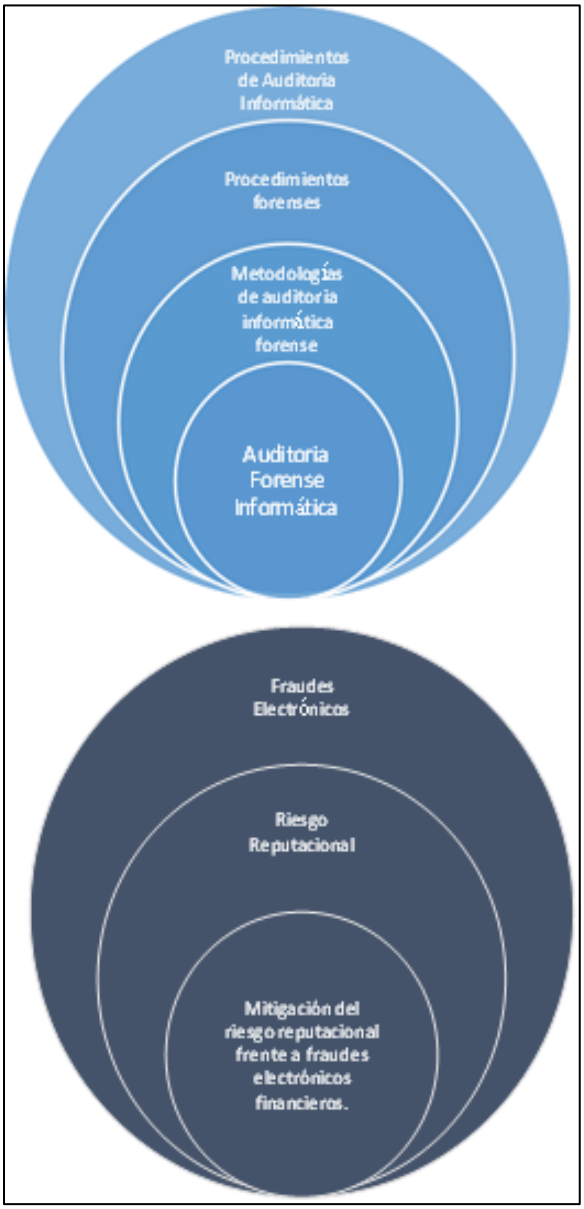
El Diseño de un modelo de auditoria informática forense no contribuye a la mitigación del riesgo reputacional de la Cooperativa de Ahorro y Crédito “Artesanos” al enfrentar fraudes electrónicos financieros.

1.6 Categorización de variables

Variable Independiente: Diseño de un modelo de auditoria informática forense.

Variable Dependiente: Mitigación del riesgo reputacional de la Cooperativa de Ahorro y Crédito "Artesanos" al enfrentar fraudes electrónicos financieros.

Gráfico 1: Categorización de variables



Fuente: Elaboración Propia

1.7 Justificación

Un modelo de auditoria informática forense contribuye a la prevención de delitos informáticos, mediante la aplicación de controles adecuados, y la detección de actividades sospechosas que se presentan en los canales digitales o sistemas financieros de la Cooperativa de Ahorro y Crédito “Artesanos.

Por otra parte, cuando se produce un incidente o delito informático, el cual compromete la operatividad de la cooperativa, es importante contar con evidencia digital adecuada, para procesar a los responsables del incidente o del fraude cometido, es por ello que, un modelo de auditoría informática forense proporciona los procedimientos y las herramientas necesarias para recopilar, preservar y presentar la evidencia digital de manera que sea válida en un proceso legal.

Además, tras ocurrir un incidente de seguridad, un modelo de auditoría informática forense permite realizar un análisis después de la incidencia, de manera sistemática, identificando las causas subyacentes y proporcionando recomendaciones para evitar incidentes similares en el futuro.

La cooperativa está sujeta al control de la Superintendencia de Economía Popular y Solidaria (SEPS), misma que dispone de normativas y reformas para la seguridad de la información, canales electrónicas, gestión de riesgos y entre otras, con la finalidad de garantizar lo protección integral de la entidad; por lo que, un modelo de auditoría informática forense ayuda a cumplir con estas obligaciones, proporcionando un marco estructurado para evaluar, mejorar y garantizar la seguridad de la información.

Se tiene en cuenta que los incidentes relacionados con fraudes electrónicos o incidentes de seguridad de la información, genera un impacto considerable en la reputación y confianza de la organización, siendo resultados desastrosos para el cumplimento de los objetivos corporativos, por ello, implementar un modelo de auditoria informática forense, la cooperativa puede demostrar el compromiso con la seguridad de la información y la protección de los datos de sus socios y clientes, generando la confianza suficiente y proteger la reputación de la misma.

Por lo tanto, es fundamental abordar esta problemática de manera integral, desarrollando estrategias para prevenir, detectar y mitigar los fraudes electrónicos. Esto requiere la colaboración entre diferentes actores, incluyendo la alta gerencia de la entidad financiera, reguladores, áreas de tecnología, entidades judiciales, fiscalía y usuarios

finales. Además, es necesario el desarrollo y la implementación de procedimientos y tecnologías avanzadas para auditoria forense y el análisis de datos, para identificar evidencias y patrones de fraude y mejorar la seguridad de las transacciones en línea.

En resumen, el aumento de los fraudes electrónicos representa un desafío significativo en la sociedad actual, que requiere una respuesta coordinada y multifacética para proteger a los individuos y las organizaciones contra este tipo de delitos.

2 CAPITULO II

MARCO REFERENCIAL

2.1 Antecedentes

Aplicar una auditoria forense informática, se ha convertido una manera recolectar la evidencia necesaria para determinar operaciones y ejecuciones fraudulentas que afecten a una organización; por ello la tesis de pregrado “Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos” del autor (Gioia, 2021), que tiene como objetivo “Elaborar una metodología de análisis forense en base de datos relacionales que sirva de guía para la actuación pericial garantizando la confiabilidad de las actividades de identificación, recolección, adquisición y análisis de evidencia digital admisible como prueba en un proceso judicial.”(p.83), dando como resultado una metodología ForenseDB, con la capacidad de aplicar un proceso que garantiza la confiabilidad, la trazabilidad, la integridad y la suficiencia en el análisis forense de bases de datos relacionales. Esto ayuda a prevenir errores significativos u omisiones críticas en la manipulación de la evidencia digital, en la ejecución de procedimientos o en la aplicación de técnicas, los cuales podrían comprometer una investigación o actuación pericial en su totalidad. Así, se proporcionan garantías a lo largo de todo el proceso y se asegura la adecuada preservación de la cadena de custodia.

Por otra parte, la auditoria forense informática, como acción para la mitigación de riesgos de fraude, el articulo científico “la auditoría forense como fundamento metodológico en la detección de casos de fraudes informáticos” del autor (Díaz, 2021), cuyo objetivo general es “Exponer la importancia de la auditoria forense como fundamento metodológico en la detección de casos de fraude informático” (p, 321), llegando a la conclusión que la base metodológica sobre la cual se sustenta la auditoría forense para detectar casos de fraude informático comprende aspectos relacionados con la seguridad y la protección. Esto asegura que los elementos de prueba presentados sean fiables y no hayan sido alterados, eliminados o manipulados en ninguna etapa de la investigación, con el fin de garantizar la precisión en todas las fases del proceso de investigación.

La informática forense en procesos de auditoría, se define como un método para la identificación de indicios de responsabilidad en delitos informáticos, el articulo científico “aplicación de informática forense en auditorías gubernamentales para la determinación

de indicios de responsabilidad penal con delitos informáticos en ecuador, México y Perú, 2007-2019" del autor (Caraguay, 2020), que tiene como objetivo "...comparar la aplicación de la informática forense en auditorías gubernamentales, herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, en Ecuador, México y Perú"(p. 2), logrando de esa manera explicar de qué forma contribuye los procedimientos de informática frésense dentro de las auditorias gubernamentales de la Contraloría General del Estado, tomando como referencia a Ecuador como base para el caso de estudio.

Como una medida para prevenir riesgos en una institución desde la perspectiva de gestión de talento humano, el articulo "Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional", de los autores (Fernandez y Herrera, 2020), cuyo objetivo es analizar cómo las TIC's desempeñan un papel importante en la gestión del conocimiento, a partir de las competencias adquiridas, lo cual permiten a las organizaciones modernas, mediante la auditoria forense blindarse oportunamente para reaccionar ante cualquier ciberataque que afecte la operación y competitividad dentro de este mundo globalizado (p, 61), y se determina que la ciberseguridad es un instrumento para la prevención, detección de operaciones fraudulentas y sospechosas, la toma de decisiones del capital intelectual al conjugarse bajo un enfoque sistémico, con la auditoría y la gestión del conocimiento.

2.2 Marco Teórico

2.2.1 Auditoria

La auditoría es un proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas objetivamente con el fin de determinar el grado en que se cumplen los criterios de auditoría establecidos. Este proceso permite verificar la conformidad, eficacia y eficiencia de los sistemas, operaciones o controles aplicados en una organización, contribuyendo a la mejora continua y a la toma de decisiones basada en hechos verificables (International Organization for Standardization, 2018).

2.2.2 Auditoría Interna

La Auditoría Interna es una actividad imparcial y autónoma de garantía y asesoramiento, diseñada para añadir valor y perfeccionar las operaciones de una entidad. En la práctica profesional, contribuye a que una entidad alcance sus metas mediante un enfoque ordenado y riguroso para evaluar y mejorar la eficacia de los procedimientos de

gestión de riesgos, control y gobierno. Los trabajos realizados por la Auditoría Interna se llevan a cabo en entornos legales y culturales diversos, dirigidos a entidades que varían en términos de propósito, tamaño y estructura, realizados tanto por personas internas como externas a la organización. (Bhaskar et al., 2019).

2.2.3 Auditoria Informática

La auditoría informática es un proceso sistemático de evaluación que permite examinar y verificar los controles, procesos, sistemas y recursos tecnológicos utilizados en una organización, con el objetivo de asegurar la eficiencia, integridad, seguridad, confidencialidad y disponibilidad de la información. La auditoría informática es la disciplina encargada de evaluar los sistemas de información y los recursos tecnológicos utilizados por una organización, a fin de determinar su correcto funcionamiento, seguridad, cumplimiento normativo y alineación con los objetivos institucionales (Hurtado, 2022).

Procedimientos de auditoria informática

Diversos autores y organismos han propuesto metodologías que estructuran la auditoría informática en fases o etapas que aseguran su desarrollo ordenado, sistemático y con validez técnica. Según Hurtado (2022), una auditoría informática efectiva debe dividirse contener las siguientes fases:

Planificación

En esta etapa se definen los objetivos de la auditoría, su alcance técnico y funcional, los recursos humanos y tecnológicos necesarios, y se elabora el cronograma de trabajo. Se identifican los sistemas, redes, aplicaciones y procesos críticos a auditar. Esta fase permite establecer la metodología y los criterios de evaluación, por lo que una adecuada planificación permite identificar anticipadamente los riesgos tecnológicos y los focos de análisis prioritarios (Hurtado, 2022,).

Ejecución

Consiste en la recolección sistemática de información técnica, entrevistas, observaciones, revisión documental y uso de herramientas forenses. Se evalúa la configuración de sistemas, accesos, registros de eventos (logs), bases de datos y controles

de seguridad, esta fase se apoya en pruebas sustantivas y de cumplimiento que permiten obtener evidencia objetiva" (Sánchez & López, 2020).

Elaboración del Informe

Se redacta el informe técnico con los hallazgos, conclusiones y recomendaciones, por lo que debe ser claro, preciso, respaldado con evidencia, y orientado a la mejora continua, este documento final debe contribuir a la toma de decisiones y a la mitigación de riesgos informáticos" (ISACA, 2019).

Seguimiento

Finalmente, se evalúa la implementación de las recomendaciones emitidas. Esta etapa es clave para cerrar el ciclo de auditoría, asegurando que las debilidades identificadas hayan sido corregidas, este seguimiento da valor al proceso de auditoría al medir su impacto (Sánchez & López, 2020, p. 93).

2.2.4 COSO (Sponsoring Organizations of the Treadway Commission)

Es una organización que promueve la mejora de la gestión empresarial mediante la promoción de marcos y guías sobre control interno, gestión de riesgos y prevención de fraude, es por eso que (Albarrán, Pérez, Salgado, & Valero, 2019) hacen referencia que este modelo está diseñado para proporcionar liderazgo intelectual a través del desarrollo de un marco general y orientación para la gestión de riesgos, controles internos y disuasión del fraude, con el objetivo de mejorar el desempeño organizacional y reducir el alcance del fraude en la organización.

2.2.5 Análisis Forense

El análisis forense, también conocido como investigación forense, es la aplicación de métodos científicos y técnicas especializadas para la recolección, preservación, examen e interpretación de evidencia física o digital, con el propósito de esclarecer hechos, identificar responsables y presentar pruebas sólidas en procesos judiciales. En el contexto digital, se enfoca en recuperar, analizar y documentar datos electrónicos de forma que puedan ser utilizados como evidencia en un tribunal, respetando la cadena de custodia y garantizando su integridad y validez legal. (IBM, 2024)

Según INTERPOL, la evidencia electrónica es un componente de casi todas las actividades delictivas, y el apoyo de la informática forense es crucial para las investigaciones policiales. La evidencia electrónica puede recopilarse de una amplia gama de fuentes, como computadoras, teléfonos inteligentes, almacenamiento remoto, sistemas aéreos no tripulados, equipos a bordo de barcos y más. El objetivo principal de la informática forense es extraer datos de la evidencia electrónica, procesarlos en inteligencia procesable y presentar los hallazgos para su enjuiciamiento. Todos los procesos utilizan técnicas forenses sólidas para garantizar que los hallazgos sean admisibles en los tribunales. (INTERPOL, 2022).

2.2.6 Informática forense

Como se hace referencia en (Iorio, et al., 2017, como se citó en Beltrán, 2020):

> La informática forense es una disciplina que utiliza modelos y técnicas forenses para identificar, obtener, preservar y analizar evidencia a través de la investigación en el campo específico de los casos penales y civiles, permite la resolución de disputas judiciales en los tribunales, por lo que es necesario realizar investigaciones. El personal y los expertos poseen conocimientos en áreas técnicas. La informática forense permite la detección y recuperación de datos e información digital y su uso como evidencia para reconstruir hechos y por tanto se utiliza como valor demostrativo. (p. 18)

2.2.7 Metodología de análisis forense

ISO/IEC 27037

Esta normativa técnica proporciona directrices para el manejo y aseguramiento de las pruebas digitales en los sistemas informáticos, siendo esta, parte de la familia ISO 27000 que se centra en la gestión de seguridad de la información. En el campo forense, esta norma se compone de la identificación, recolección, conservación y presentación de la evidencia electrónica, definiendo los criterios a seguir en cada una de estas actividades (Farfan, 2024) .

A más de presentarse como una normativa técnica para procesos forenses, la ISO/IEC 27037 proporciona elementos calves para el marco legal, importante para especialistas dedicados a la recopilación y mantenimiento de la evidencia digital, por lo que suministra recursos para reforzar y preservar la integridad y autenticidad a lo largo

de los procesos investigativos o auditorias, que a la vez aumenta la fiabilidad y la objetividad en cuando a los hallazgos (Stoykova, 2022, como se citó en Farfán, 2024).

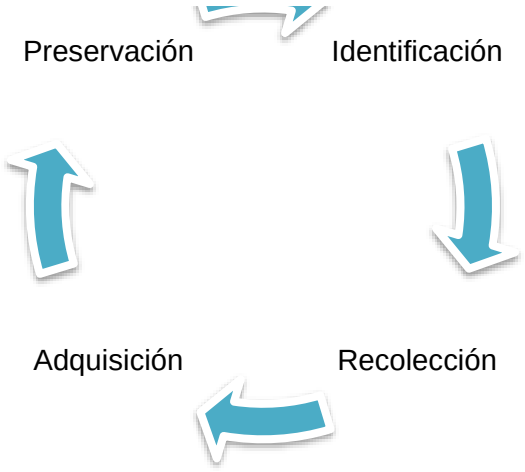
Proceso de recolección de la evidencia digital

La normativa , presenta las directrices enmarcadas por fases o procesos y sus definiciones, es importante mencionar que por contexto de esta metodología se define a dos individuos que intervienen de manera clave en cada una de las fases, que son el DEFR (Digital Evidence First Responder), quien es el primer responsable que asegura la escena del incidente y el DES (Digital Evidence Specialist), quien es el experto en realizar el análisis más profundo de la evidencia digital.

DEFR y DES deben seguir procedimientos escritos para garantizar la integridad y confiabilidad de la posible evidencia digital. Estos procedimientos deben incluir orientación sobre el manejo de posibles fuentes de evidencia digital y los siguientes principios básicos, así lo cataloga la (ISO/IEC, 2012):

- Minimizar la manipulación del dispositivo digital original o de la posible evidencia digital.
- Dar cuenta de todos los cambios y documentar las acciones adoptadas (en la medida en que un experto pueda formarse una opinión sobre la confiabilidad).
- Cumplir con las normas locales de prueba.
- El DEFR y el DES no deberían tomar medidas que excedan su competencia.

Gráfico 2: Proceso del manejo de la evidencia digital- ISO/IEC 27037



Fuente: Elaboración propia.

(Fase 1) Identificación

El proceso de identificación implica buscar, identificar y registrar posibles evidencias digitales. Este proceso debe identificar los medios de almacenamiento digital y los dispositivos de procesamiento que puedan contener evidencia digital relacionada con el incidente. Aquí se debe priorizar la recopilación de evidencia en función de la volatilidad de la recopilación de evidencia. Se debe identificar la volatilidad de los datos para garantizar la secuencia correcta de los procesos de recopilación y adquisición para minimizar el daño a la evidencia digital potencial y obtener la mejor evidencia posible. Además, el proceso debe identificar el potencial de evidencia digital oculta. (ISO/IEC, 2012).

(Fase 2) Recolección

La recopilación es un proceso en la gestión de evidencia digital que implica retirar dispositivos que puedan contener evidencia de su ubicación original y trasladarlos a un laboratorio u otro entorno controlado para su posterior recopilación y análisis. Estos dispositivos pueden estar en dos estados posibles: encendido o apagado, y requieren diferentes métodos y herramientas según su estado. Los procedimientos locales pueden definir los métodos y herramientas utilizados durante la recolección.

El proceso incluye documentación de todo el método, así como el embalaje del equipo antes del envío. DEFR y DES Es importante recopilar cualquier material que pueda estar asociado con posible información digital (por ejemplo, papel con contraseñas escritas, bases y conectores de alimentación para dispositivos de sistemas integrados). Si no se tiene el cuidado adecuado, es posible que se pierdan o dañen posibles pruebas digitales. DEFR y DES deben adoptar el mejor método de recopilación según las circunstancias, el costo y el tiempo, y documentar la decisión de utilizar un método en particular (ISO/IEC, 2012).

(Fase 3) Adquisición

El proceso de adquisición implica crear una copia digital de la evidencia (por ejemplo, disco duro completo, particiones, archivos seleccionados) y documentar los métodos utilizados y las actividades realizadas. El DEFR debe adoptar métodos de adquisición adecuados a las circunstancias, el costo y el tiempo, y documentar las decisiones sobre el uso apropiado de métodos o herramientas específicos.

Los métodos utilizados para obtener posibles pruebas digitales deben documentarse de forma clara y detallada y, cuando sea posible, repetirse o verificarse por el DEFR competente. DEFR o DES deben obtener evidencia digital potencial de la forma menos intrusiva posible para evitar introducir cambios. Al realizar este proceso, DEFR debe considerar el enfoque más adecuado. Si el proceso resulta inevitablemente en cambios en los datos digitales, las actividades realizadas deben documentarse para justificar los cambios (ISO/IEC, 2012).

(Fase 4) Preservación

La evidencia digital potencial debe ser preservada para asegurar su validez en la investigación. Es crucial mantener la integridad de la evidencia. El proceso de preservación consiste en proteger tanto la evidencia digital como los dispositivos que puedan contenerla, evitando su alteración o daño. Esta preservación debe iniciarse y mantenerse durante todo el ciclo de gestión de la evidencia digital, comenzando con la identificación de los dispositivos que la almacenan. Lo ideal es que no se produzcan cambios en los datos ni en sus metadatos asociados, como las marcas de fecha y hora. El DEFR debe ser capaz de demostrar que la evidencia no ha sido modificada desde su recolección o adquisición, o proporcionar la justificación y documentación necesaria si se han realizado cambios inevitables.

Metodología de análisis forense informático de (Velarde, 2025)

Esta es una metodología diseñada para el análisis forense de manera integral, presentándose con una estructura sistemática capaz de contribuir a la ejecución asertiva de diferentes procedimientos que conlleven a la recolección y manejo de evidencias digitales, garantizando la integridad, la formación y concienciación de la seguridad informática, como también culturizar a las personas, de que la ciberseguridad debe ser tratada como una materia cotidiana con los beneficios y cualidades que la misma presenta.

El enfoque de la presente metodología está ligado con el aporte esencial e importante para los procesos judiciales que buscan de alguna forma identificar los involucrados en los incidentes y evitar que no se esclarezca las evidencias de sucesos cometidos a través de los sistemas informáticos, por ello (Velarde, 2025) menciona:

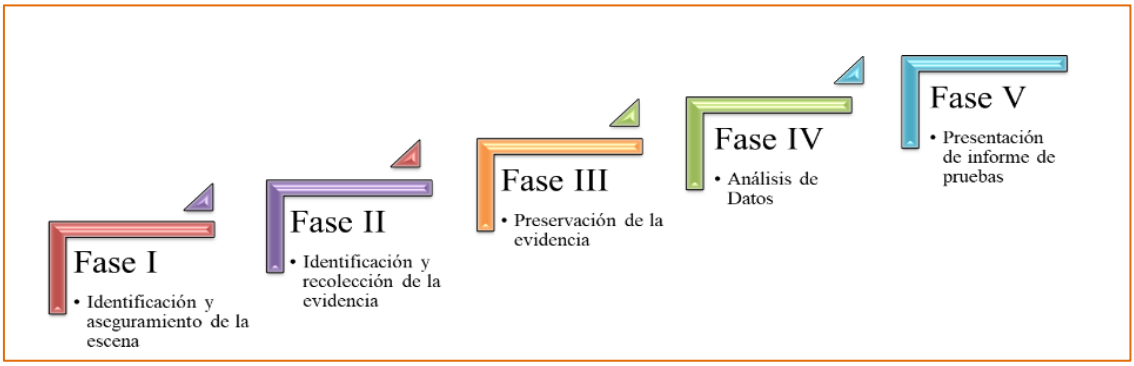
> “Se diseña una metodología, adecuada para la obtención de evidencia digital, que contribuya a su admisibilidad en procesos judiciales y/o en las instancias requeridas; esta norma pretende orientar a especialistas en evidencia digital, en

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" (p, 9).

Proceso de la metodología de (Velarde, 2025)

La metodología tratada, se presenta de 5 fases que inicia desde la identificación y aseguramiento de la escena del incidente hasta la presentación de un informe de las pruebas sustraídas durante el proceso investigativo, planteadas de la siguiente manera:

Gráfico 3: Fases de la metodología de Velarda



Fuente: (Velarda, 2025)

Cada una de las fases que se presentan en esta metodología, presentan las directrices para el manejo correcto de la evidencia digital, y la finalidad de no incurrir a errores que retrasen los procesos y no concluir con la objetividad esperada para la toma de decisiones finales.

(Fase 1) Identificación y aseguramiento de la escena

En esta fase, aunque comúnmente se asocia con casos criminales, es crucial para cualquier análisis forense dentro de una entidad. El investigador realiza un análisis técnico de los equipos implicados y asegura que la escena del incidente permanezca intacta desde su descubrimiento hasta el análisis. Todos los involucrados son conscientes de que cualquier movimiento inapropiado puede comprometer la investigación.

Es fundamental que el investigador tome fotografías del entorno para documentar el estado original de la escena y protegerla de accesos no autorizados. Además, se preservan las huellas dactilares cuando se traten de la manipulación de equipos físicos,

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 se documenta cualquier desfase. Esta atención al detalle es vital para garantizar la integridad de la investigación y obtener resultados precisos.

Además, es importante que los investigadores observen las entradas y salidas de los equipos y graben los procesos en pantalla. Esto permite tener un registro detallado de todas las actividades realizadas durante el análisis. Finalmente, cualquier desconexión de red o eléctrica es cuidadosamente documentada para evitar la pérdida de información valiosa. Una vez que la escena está asegurada, se procede a la identificación y recolección de evidencia en la siguiente fase del proceso.

Es de crucial importancia la documentación exhaustiva para mantener la integridad de la investigación y garantizar que todos los datos relevantes sean capturados y preservados. Los investigadores trabajan diligentemente para asegurar que cada paso del proceso sea meticulosamente registrado, lo cual es esencial para el éxito de la investigación. La atención al detalle en esta fase es fundamental para obtener resultados precisos y completos (Velarde, 2025).

(Fase 2) Identificación y recolección de la evidencia

La segunda fase del análisis forense se divide en dos etapas fundamentales: identificación y recolección de evidencias. En la etapa de identificación, es crucial reconocer la volatilidad de los datos, es decir, el tiempo durante el cual permanecerán accesibles en el equipo. Esta metodología también integra principios y otras directrices como la RFC 3227 (marco para la gestión y preservación de las pruebas digitales), en la que establece un orden de volatilidad y se evalúa la utilidad de cada evidencia para la investigación. Los investigadores documentan y listan 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.

También, se solicita 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. También se crea una segunda

copia como respaldo durante el proceso de investigación para asegurar la disponibilidad de los datos en caso de necesidad.

La documentación detallada y la etiquetación precisa son esenciales para mantener la cadena de custodia y garantizar que las evidencias sean admisibles en procedimientos legales. La recolección de pruebas volátiles es prioritaria para evitar su pérdida y asegurar que toda la información relevante esté disponible para el análisis posterior (Velarde, 2025).

(Fase 3) Preservación de la evidencia

Una preservación inadecuada de las evidencias puede invalidar una investigación fiscal o judicial, destacando la importancia de seguir protocolos rigurosos. En esta etapa, la cadena de custodia es crucial, controlando 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 esencial documentar todos los aspectos en la fase de identificación para fortalecer este proceso. Las evidencias deben ser embaladas y etiquetadas con información básica sobre cada dispositivo, como número de serie y fabricante. Además, se clasifican y almacenan según su naturaleza para protegerlas adecuadamente. Por ejemplo, los discos duros y CD deben guardarse en bolsas antiestáticas para evitar daños por electricidad estática.

El almacenamiento debe ser adecuado, evitando condiciones húmedas o extremas que puedan comprometer la integridad de los dispositivos. Los investigadores trabajan diligentemente para asegurar que todas las evidencias sean tratadas con el cuidado necesario para mantener su integridad y garantizar su validez en procedimientos legales. La atención al detalle en cada paso del proceso es esencial para el éxito de la investigación (Velarde, 2025).

(Fase 4) Análisis de datos

La fase de análisis termina únicamente cuando se identifica la causa del incidente y se evalúa su impacto en el sistema informático estudiado. Es esencial que los investigadores trabajen con copias de los datos y cumplan con las leyes vigentes. Durante este proceso, se consideran varios requisitos importantes como:

- Recopilación de información: Se obtiene documentación sobre el sistema operativo, programas instalados, hardware y configuraciones de red, incluyendo firewalls y conexiones a Internet.
- Preparación del entorno: Antes de comenzar el análisis, se establece un entorno adecuado, eligiendo entre un análisis en caliente, con precauciones en los discos originales, o un análisis en frío, utilizando imágenes de disco en máquinas virtuales.
- Creación de una línea temporal: Se elabora una línea temporal de eventos, registrando fechas de modificaciones y accesos. Es fundamental verificar las fechas del sistema y rastrear instalaciones recientes.
- Determinación del método 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 los responsables: 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 interrupción de operaciones que puede afectar la productividad general de la institución.

  Estos pasos aseguran que el análisis sea completo y se obtengan conclusiones precisas sobre el incidente (Velarde, 2025).

(Fase 5) Presentación de informe de pruebas

En la fase final de un análisis forense, se redactan informes para documentar 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. Aunque ambos abordan los mismos hechos, difieren en enfoque y nivel de detalle a quien será presentado.

Informe Ejecutivo: Se redacta en un lenguaje claro y accesible, evitando tecnicismos, para facilitar la comprensión de directivos como el oficial mayor de la Cámara de Diputados, quienes disponen de poco tiempo para el proceso forense.

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

- **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 (Velarde, 2025).

2.2.8 Auditoria Informática Forense

Proceso en el cual se investiga y analiza la evidencia digital para descubrir y documentar actividades ilícitas, o incidentes de seguridad en sistemas informáticos. Estos procedimientos se llevan a cabo siguiendo métodos y técnicas específicas con el fin de preservar la integridad de la evidencia y garantizar su validez legal en caso de ser utilizada en procesos judiciales, desde una perspectiva similar, (Rozas, 2009, como se citó en Lema, 2019):

> La auditoría forense es aquella labor de auditoría que se enfoca en la prevención y detección del fraude financiero; por ello, generalmente los resultados del trabajo del auditor forense son puestos a consideración de la justicia, que se encargará de analizar, juzgar y sentenciar los delitos cometidos (corrupción financiera, pública o privada) (P, 18)

Características de auditoria forense

Las auditorías forenses se enfocan en delitos contra la propiedad con el fin de requerir la implementación de controles preventivos, investigativos y correctivos necesarios para evitar la recurrencia de dichos delitos en el futuro.

Es por esto que (Mahecha, 2022), menciona que las auditorías forenses deben cumplir con las siguientes características:

- **Propósito:** Prevenir y detectar los delitos patrimoniales
- **Objetivo:** Búsqueda de la verdad histórica de los hechos, basada en la evidencia
- **Metodología:** Se sigue un orden, aplicando técnicas y procedimientos específicos o alternativos de auditoria
- **Normatividad:** Sigue las normas y procedimiento aplicables al caso en concreto
- **Cuantificable:** La evidencia obtenida comprueba contablemente la comisión de un delito patrimonial
- **Auditor y equipo:** profesional con un título profesional que cuente con un equipo multidisciplinario de profesionales en derecho, sistemas, investigación, entre otros (p, 19)

2.2.9 Delitos informáticos

Son actividades ilícitas que se llevan a cabo utilizando computadoras, redes informáticas o dispositivos digitales. Estos delitos pueden variar en gravedad y complejidad, y pueden incluir una amplia gama de actividades, desde el acceso no autorizado a sistemas informáticos hasta el robo de identidad, el fraude en línea, el sabotaje de redes, entre otros.

El ciberdelito, al igual que otros delitos penales, siempre ha sido objeto de análisis por parte de juristas y expertos en seguridad informática alrededor del mundo; esto ha permitido que muchas legislaciones en el continente americano tipifiquen el comportamiento cibercriminal, teniendo en cuenta lo teóricamente analizado y propio de otros continentes (Saltos, Robalino, & Pazmiño, 2021).

2.2.10 Fraudes electrónicos

Se conoce también como ciber fraude, es un tipo de delito que implica el uso de tecnologías de información y comunicación para cometer actividades fraudulentas. Esto puede incluir el robo de información personal o financiera, la suplantación de identidad, el phishing, la manipulación de sistemas informáticos para obtener acceso no autorizado a datos sensibles; también, fraude electrónico para (Rey, 2022) es "…una práctica que puede alterar el normal funcionamiento de una empresa o despojar de los recursos capitales de una persona que realiza una transacción bancaria" (p, 3).

2.2.11 Riesgo Reputacional

Es la amenaza de pérdida de reputación de una organización como resultado de acciones, eventos o circunstancias que dañan su imagen pública, credibilidad o confianza por parte los interesados. Este tipo de riesgo puede surgir de una variedad de situaciones, como escándalos corporativos, fraude financiero, mala conducta de empleados, problemas de calidad del producto, litigios, impacto ambiental negativo, incumplimiento de regulaciones, entre otros.

Como menciona (López et al, 2020):

> La reputación es considerada como un intangible esencial para las diferentes organizaciones y por el cual es un asunto que vienen trabajando sus ejecutivos. Asimismo, es importante mencionar que la reputación se va a ir adaptando y moldeando producto del comportamiento humano y organizacional. (p, 43)

2.3 Marco legal

2.3.1 Código orgánico integral penal

El Código Orgánico Integral Penal entró en vigencia en 2014, reemplazando al antiguo Código Penal ecuatoriano. Este código se diseñó con el objetivo de modernizar y fortalecer el sistema de justicia penal en Ecuador, incorporando principios de garantía de los derechos humanos, enfoques de justicia restaurativa y medidas para combatir la delincuencia organizada, la corrupción y otros delitos graves, en la SECCIÓN TERCERA. - Delitos contra la seguridad de los activos de los sistemas de información y comunicación, la (Asamblea Nacional del Ecuador, 2021) menciona:

> **Art. 230**.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona al ingresar a

una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (p, 88)

Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (p, 89).

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (p, 90)

2.3.2 Superintendencia de Económica Popular y Solidaria SEPS

Según la (SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, 2023) considera que:

Velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente preventiva extra situ y visitas de inspección in situ, que permitan determinar la situación económica y financiera de las entidades, el manejo de sus

negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan. (p, 1)

De acuerdo con la norma de control norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario bajo el control de la superintendencia de economía popular y solidaria. Resolución No. SEPS-IGT-IR-IGJ-2018-0279; la (SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, 2023) en sus artículos menciona:

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

Articulo 4.5.- c) Garantizar una adecuada separación de funciones que evite la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo (p, 15)

Articulo 6.2.- Independencia de funciones: Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias y responsabilidades de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo. (p, 16)

CAPITULO III

3 MARCO METODOLÓGICO

3.1 Descripción del área de estudio

La Cooperativa de Ahorro y Créditos “Artesanos”, es una entidad financiera fundada en 1991 en la ciudad de Ibarra, que actualmente pertenece al segmento 2 de las todas las cooperativas del Ecuador, con un total de 19 agencias en todo el país, que brinda servicios crediticios con productos acorde a las necesidades de sus socios, tales como: créditos de consumo, microcrédito, microcrédito agrícola, crédito verde y otros.

En su estructura organizacional, la cooperativa mantiene áreas estratégicas para el cumplimiento de los objetivos corporativos, tales como, Consejos de Administración y Vigilancia, Gerencia, Jefatura Financiera, Riesgo Operativo, Negocios, Área Legal, Cumplimiento, Tics, Talento Humano, y por último Auditoría Interna, la cual cuenta con un Auditor informática, quien es el especialista para el entorno tecnológico.

Enfoque de investigación

La presente investigación se desarrolla bajo la combinación de un enfoque cualitativo y cuantitativo, siendo un enfoque mixto que mantiene una doble arista, por un lado busca investigar, explorar y entender la aplicación de normativas, metodologías en procedimientos forenses en entornos o ecosistemas informáticos orientados a un ámbito financiero, y por otro lado valorar los riesgos y niveles de las incidencias desde una perspectiva de fraude que también vierte de datos cualitativos a la hora de entender una situación o fenómenos de los incidentes mencionados.

Es por eso, que, desde el enfoque cualitativo, se realiza un análisis profundo y contextual de las metodologías forenses vigentes, particularmente la norma internacional ISO/IEC 27037:2012 y la propuesta metodológica de Velarde (2025). Este enfoque permite comprender los principios, procedimientos y buenas prácticas para la identificación, recolección, preservación y análisis de evidencia digital, así como su aplicabilidad en procesos de revisiones e investigaciones de una entidad financiera.

Asimismo, lo cualitativo posibilita una interpretación sistemática de eventos de fraude reportados en bases históricas de la cooperativa en estudio, bajo un análisis correlacional basado en las experiencias o lecciones aprendidas de los casos registrados. Este enfoque

también se orienta a identificar patrones, fallos de control y vulnerabilidades tanto técnicas como organizacionales.

Por otra parte, el enfoque cuantitativo permite objetivar el estudio mediante el uso de herramientas estadísticas y métricas para la valoración del riesgo, la frecuencia de ocurrencia y el impacto o grado de afectación, Para ello se aplican técnicas de análisis de datos a registros históricos de eventos de riesgo, bajo la parametrización de estimación de riesgos que posee la entidad.

Se estableció una correlación entre probabilidad e impacto, lo que facilita identificar eventos con perfilamiento de fraude digital, ya sea por suplantación de identidad, uso indebido de accesos privilegiados, o manipulación de sistemas críticos como el core financiero o plataformas digitales.

En conjunto, este enfoque mixto permite no solo proponer un modelo de auditoría informática forense técnicamente sólido y normativamente alineado, sino también evaluar su efectividad práctica frente a escenarios reales del sistema financiero.

Tipo de investigación

En el presente trabajo, se enmarca dentro de una investigación de tipo aplicada y descriptiva. Es aplicada porque busca desarrollar un modelo concreto y útil para la práctica profesional en el ámbito del análisis forense digital, y es descriptiva porque identifica y caracteriza los riesgos, metodologías y procesos críticos que intervienen en el análisis forense de sistemas informáticos.

Métodos de recolección de información

Para el análisis documental, se emplearán fuentes secundarias, incluyendo normas internacionales (ISO/IEC 27037), estudios académicos (Velarde-Flores, 2025), bibliografía sobre auditoría forense, regulaciones locales (Superintendencia de Economía Popular y Solidaria - SEPS), y disposiciones legales relevantes (Código Orgánico Integral Penal - COIP).

Adicionalmente, se recopilarán registros de incidencias históricas de eventos de riesgo y posibles fraudes ocurridos en la Cooperativa de Ahorro y Crédito Artesanos Ltda., a partir de reportes internos, matrices de control de eventos y análisis de vulnerabilidades informáticas previamente levantados.

Técnicas de análisis

En cuanto al análisis de metodologías para el análisis forense enfocado a sistemas informáticos, se aplicó un análisis comparativo bajo criterios definidos que permitan evaluar las metodologías estudiadas. Los criterios seleccionados son:

- Estructura y fases de la metodología
- Aplicabilidad en sistemas informáticos financieros
- Alcance en procesos de identificación y análisis de evidencia digital
- Integración con normativas locales
- Soporte en herramientas forenses certificadas
- Capacidad de trazabilidad y legalidad del procedimiento

La comparación se desarrollará mediante una matriz descriptiva que permitirá valorar las fortalezas, oportunidades de mejora y compatibilidad de ambas metodologías.

Asimismo, se realizará un análisis de incidencias de riesgo utilizando estadística descriptiva, con el objetivo de identificar patrones de fraude electrónico, nivel de riesgo, impacto, frecuencia, y posibles perfiles de actores involucrados.

Procedimiento de investigación

Para plasmar un modelo de auditoría forense informática para la mitigación del riesgo reputacional de la Cooperativa de Ahorro y Crédito “Artesanos”, se tomó en cuenta los siguientes procedimientos:

Fase 1: Análisis de metodologías de análisis forense

Se investigó en bases de información y repositorios científicos, metodologías relacionadas con la Auditoria Forense Informática, en donde abarque información requerida para la continuación con este trabajo de investigación.

Se analizó metodologías de auditorías informáticas forense en literatura recopilada, con la finalidad de poder determinar una metodología apropiada, que mantenga criterios de seguridad de la información para aplicarse en el caso de estudio de este trabajo de investigación.

Fase 2: Determinar el nivel de incidencias o eventos de riesgo

Se realizó una evaluación de los incidentes o eventualidades de riesgo que se han materializado en la COAC Artesanos provenientes de fraudes financieros cometidos mediante el uso de los sistemas informáticos y aplicaciones, con la finalidad de medir el impacto que estos incidentes ocasionan.

Fase 3: Desarrollo un modelo de auditoría informática forense

Se diseñó un modelo de auditoría informática forense para el manejo de la evidencia digital de los sistemas informáticos de la Cooperativa, mismo que involucre procedimientos sustanciales para llegar a determinar hallazgos importantes en cuanto a los fraudes electrónicos en sistemas informáticos y las aplicaciones.

Consideraciones bioéticas

En este trabajo de investigación, se tomó en cuenta aspectos bioéticos que involucran el comportamiento y la conducta humana mediante la aplicación de normas éticas y morales para salvaguardar el derecho, la dignidad, el respeto y el bienestar de los implicados en esta investigación, mismos que se describen a continuación:

Normativas, manuales y procedimientos

Bajo las resoluciones y reformas de las normativas de control de la Superintendencia de Economía Popular y Solidaria, se rigen ciertos artículos que deben ser contemplados y alineados para planteamiento del Modelo de Auditoria Forense Informática, con la finalidad de no involucrar procesos y procedimientos que no se aplican dentro de la cooperativa.

Confidencialidad

Bajo los principios de seguridad de la información, es importante poner en conocimiento público información delimitada, separando entre información simple y sensible a la hora de realizar los procesos para realizar de auditoria forense informática y

exponer los resultados, mismo que en su mal manejo podría ocasionar riesgos altos reputacionales e implique incidencias en el giro de negocio de la COAC Artesanos.

Veracidad y Honestidad

Esta investigación pretende mantener la veracidad en toda la información que se maneje para el cumplimiento del objetivo general y generar resultados confiables y honestos para la toma de decisiones acertadas en las acciones que permitan mitigar la ejecución de fraudes financieros cometidos en los canales digitales y sistemas financieros de la cooperativa.

3.2 Análisis de metodologías de análisis forense, enfocado en los sistemas informáticos financieros.

En este apartado se realizó el análisis de metodologías que cumplan con los criterios técnicos, normativos y que brinden las herramientas y recursos para ejecutar un análisis forense enfocado a entornos tecnológicos, con una aplicabilidad del sector financiero.

Mediante la indagación de bases de información, se plantearon las siguientes metodologías, las cuales proponen marcos referenciales respecto al análisis forense informático a fin de abordar investigaciones previas, durante o después de la ocurrencia de eventos de riesgo con un perfilamiento de posibles fraudes financieros, dichas metodologías son:

- **Norma ISO/IEC 27037**
- **Metodología de Velarde (2025)**

En el marco del presente estudio, se analizaron dos metodologías fundamentales para el manejo de evidencia digital en entornos financieros: la norma internacional ISO/IEC 27037:2012 y la propuesta metodológica de Velarde (2025). Ambas metodologías coinciden en la necesidad de contar con procesos estructurados para la identificación, recolección, preservación y análisis de evidencia digital, pero difieren en su grado de normatividad, enfoque práctico y aplicabilidad sectorial.

La ISO/IEC 27037 proporciona un estándar globalmente aceptado que establece lineamientos rigurosos para garantizar la admisibilidad legal de la evidencia digital,

asegurando su integridad, trazabilidad y autenticidad. Su valor se encuentra centralizado en la estandarización de procedimientos técnicos y la incorporación de principios de cadena de custodia digital, lo que resulta clave en entornos donde los hallazgos pueden ser presentados ante organismos judiciales o de control.

Por otro lado, la metodología de Velarde (2025), es un modelo si bien no forma parte de un cuerpo normativo internacional, pero es un modelo que ha sido diseñado específicamente para entornos informáticos locales, en especial entidades con infraestructuras críticas de la región Latinoamericana. Esta metodología incorpora una visión operativa y contextualizada, orientada a la ayuda técnica para la detección de incidentes como fraudes electrónicos, suplantación de identidad, manipulación de privilegios y acceso no autorizado en plataformas críticas como un sistema bancario, bases de datos y canales digitales.

Comparativa de metodologías ISO/IEC 27037 VS Velarde (2025)

En consecución con el análisis de las metodologías para el análisis forense enfocados a los sistemas financieros, es importante realizar una comparativa de estas dos metodologías, a fin de conocer y contrastar características y elementos potenciales dentro del manejo de la evidencia digital en un ecosistema informático direccionado a campo financiero.

Lo que busca esta comparación es determinar la eficiencia, aplicabilidad, flexibilidad y cumplimiento normativo de cada una de las metodologías sobre la ejecución de procesos de auditoría, revisiones de control e investigaciones sobre incidentes de procedencia de entornos tecnológicos.

Estas dos metodologías, se han considerado relevantes para este análisis comparativo, ya que cada una posee características importantes aplicables dentro de un proceso forense con una orientación global bajo las normativas y estandarizaciones internacionales para el análisis forense, mientras que la otra se encuentra adaptada a nivel local, basado a principios latinoamericanos, específicamente en el ámbito financiero y sobre todo el análisis forense.

Criterios de comparativa

Se ha seleccionado un conjunto de criterios de comparación que permiten valorar la idoneidad de las metodologías analizadas para su aplicación en el ámbito forense informático

financiero, dichos criterios han sido definido en función a varios criterios en un contexto apegado a la tangibilidad de la investigación realizada, mismos que son:

Tabla 1: Criterio de comparación de metodologías

Criterio	QUÉ EVALÚA	RELEVANCIA
Estructura y fases de la metodología	Analiza si la metodología tiene fases claras, secuenciales y bien definidas (identificación, recolección, preservación, análisis, documentación).	Permite asegurar procesos consistentes, repetibles y comprensibles, reduciendo errores y fortaleciendo la trazabilidad de la auditoría forense.
Aplicabilidad en sistemas informáticos financieros	Evalúa la factibilidad de aplicar la metodología a plataformas críticas como el core bancario, bases de datos transaccionales y canales digitales.	Garantiza que la metodología sea realista y adecuada para entornos altamente regulados, críticos y de alta disponibilidad como el financiero.
Alcance en identificación y análisis de evidencia digital	Determina si la metodología cubre no solo la recolección inicial de evidencia, sino también su análisis técnico y la interpretación de los hallazgos.	Fundamental para lograr atribuir responsabilidades, identificar causas raíz y fortalecer la respuesta a incidentes.
Integración con normativas locales (seps, coip)	Evalúa la posibilidad de adaptar el modelo a las regulaciones ecuatorianas y su marco jurídico.	Asegura que la evidencia sea válida ante auditores, jueces o entes de control nacionales, evitando su rechazo por incumplimiento normativo.
Soporte en herramientas forenses certificadas	Considera si la metodología impulsa el uso de software forense reconocido, validado y certificado.	Minimiza riesgos de alteración, pérdida o cuestionamiento de la evidencia, fortaleciendo su aceptación en procesos judiciales y de fiscalización.
Capacidad de trazabilidad y legalidad del procedimiento	Revisa si la metodología garantiza el registro cronológico de cada acción, manteniendo cadena de custodia y respetando estándares de legalidad.	Protege la integridad probatoria de la evidencia, esencial para que sea considerada auténtica, confiable y admisible en auditorías o procesos judiciales posteriores.

A continuación, se expresa una matriz comparativa en base a diferentes criterios técnicos y sistemáticos, que serán punto de referencia para lograr hacer una evaluación y

análisis de todos los elementos que hacen de cada una de dichas metodologías de análisis y manejo de la evidencia digital:

Tabla 2: Comparativa ISO 27037 vs Velarde (2025)

Criterio de comparación	ISO/IEC 27037 (2012)	Velarde (2025)
Estructura y fases de la metodología	Presenta una estructura rigurosa y estandarizada, definida en fases claras: identificación, recolección, adquisición y preservación de evidencia, orientada a la cadena de custodia global.	Integra fases: identificación, recolección, preservación, análisis, documentación y retroalimentación, con un enfoque más práctico y flexible, adaptado a procesos internos y sistemas desarrollados a medida.
Aplicabilidad en sistemas informáticos financieros	Alta, pues cubre la evidencia digital en cualquier tipo de infraestructura crítica, incluyendo core bancarios, redes y bases de datos financieras.	Alta, al estar planteada para sistemas a medida, permite adaptarse fácilmente a plataformas financieras personalizadas (core bancario, canales digitales) con procesos complejos y controles internos particulares del sector cooperativo.
Alcance en identificación y análisis de evidencia	Establece parámetros técnicos para la identificación y adquisición de evidencia, sin profundizar en el análisis forense posterior a la adquisición.	Incluye de forma explícita el análisis posterior a la adquisición, incorporando guías y técnicas para procesar la evidencia, investigar incidentes y documentar hallazgos en profundidad dentro del entorno TI de la organización.
Integración con normativas locales (seps, coip)	Puede alinearse con el marco jurídico ecuatoriano (SEPS, COIP), aunque requiere adaptación de formularios y formatos de custodia a la realidad nacional.	Resulta más amigable de adaptar al marco normativo ecuatoriano (SEPS, COIP) porque contempla recursos y formatos más sencillos, lo que facilita incorporarlo en las auditorías forenses internas de entidades financieras cooperativas.
Soporte en herramientas forenses certificadas	Recomienda el uso de herramientas reconocidas internacionalmente, certificadas, y validadas, como FTK, EnCase o X-Ways, siguiendo procesos altamente estandarizados.	Promueve también el uso de herramientas certificadas, pero con la posibilidad de incorporar software libre o de bajo costo para ajustarse a presupuestos de instituciones con

Criterio de comparación	ISO/IEC 27037 (2012)	Velarde (2025)
		recursos limitados o tecnologías no estandarizadas.
Capacidad de trazabilidad y legalidad del procedimiento	Alta, con requisitos estrictos de documentación, sellos de custodia, registro de intervenciones y control de accesos, orientados a cumplir estándares legales internacionales y periciales.	Alta, aunque más flexible, enfatiza el registro cronológico de la evidencia, controles de integridad y seguimiento continuo, garantizando que la cadena de custodia sea válida ante entes judiciales y auditorías regulatorias locales.

3.3 Determinar el nivel de indecencias o eventos de riesgo en históricos registrados, con un perfilamiento de fraudes financieros en el uso de los sistemas informáticos y aplicaciones financieras de la cooperativa tomada como caso de estudio

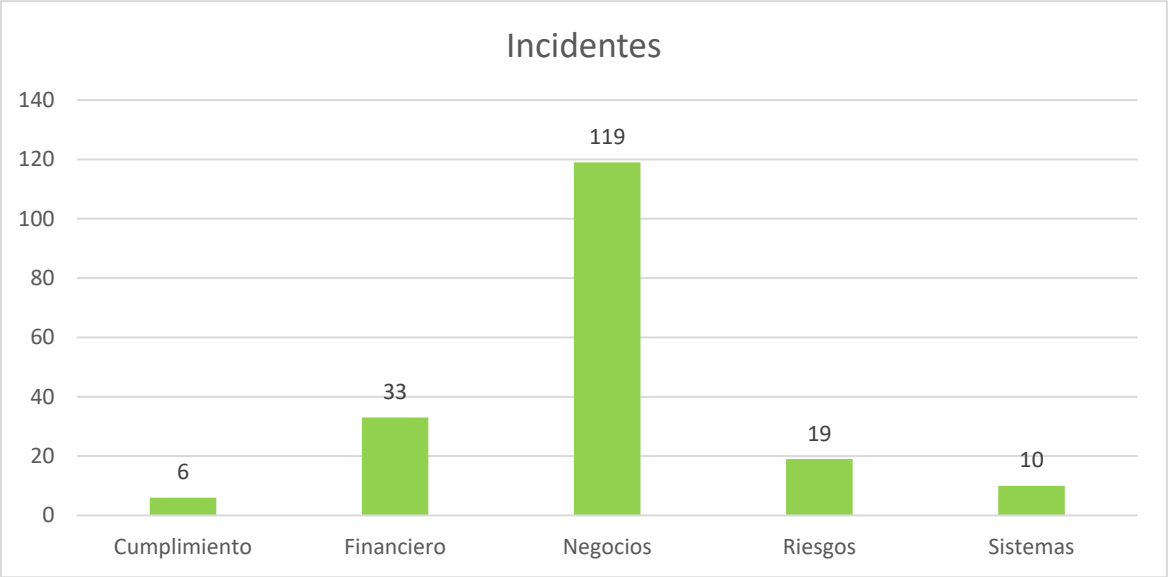
Para lograr determinar el nivel de incidencias o eventos de riesgo de la Cooperativa de Ahorro y Crédito Artesanos, la cual es estudiada en este trabajo de investigación, en primera instancia se revisó datos históricos o bitácoras de incidentes de riesgos, como también catálogos de amenazas en el entorno de TI, a fin de levantar una base de datos de incidentes potenciales que podrían desencadenar un fraude financiero, o a su vez registros de fraudes ya materializados.

Es importante indicar que, debido a los principios de confidencialidad de la entidad en toda su información crítica, los datos serán manejados a niveles generales.

Identificación de incidentes de riesgo

La Cooperativa de Ahorro y Crédito Artesanos, a lo largo de los últimos años (2023-2025) hasta la presente fecha ha registrado diversos eventos de riesgos en diferentes áreas, sin embargo, las áreas de Negocios, Financiera, Cumplimiento (Lavado de Activos), Riesgos y Tecnología son las que más incidentes han mantenido.

Gráfico 5: Incidencias de riesgo por áreas críticas



Fuente: Registro de incidentes COAC Artesanos

Como se aprecia en el gráfico 5, las cinco áreas presentan un promedio de 187 eventos de riesgos, de los cuales 119 se reflejan en el Área de Negocios, siendo el componente con más afectación, esto debido a las condiciones propias del giro de negocio ya que se encuentran expuestas constantemente a la presencia de riesgos inherentes, seguido de eso, se encuentra el Área Financiera que presenta un total 33 eventos y por ultimo las áreas de Riesgo con 19 incidentes y Sistemas con 10.

Bajo este contexto, los datos indican que los incidentes de riesgos no se centran de mayor magnitud en el entorno tecnológico de la cooperativa, pero hay que tener presente que la mayoría de los procesos operativos se apalancan por medio del Core Financiero y otras herramientas complementarias, es decir la mayoría de los procesos operativos recaen en función al Core Financiero.

Este Core Financiero tiene la particularidad de ser desarrollado en la institución de manera propia (In-House), por ello existen diferentes amenazas inherentes, que se las considerará en este marco de estudio como causales posibles de eventos con perfilamiento de riesgo de fraude, es por eso que mediante una matriz de evaluación de riesgos se ha determinado las siguientes amenazas que forma del catálogo en el Sistema de gestión de Seguridad de la Información de la cooperativa (SGSI) bajo los parámetros de la normativa ISO/IEC 27000:

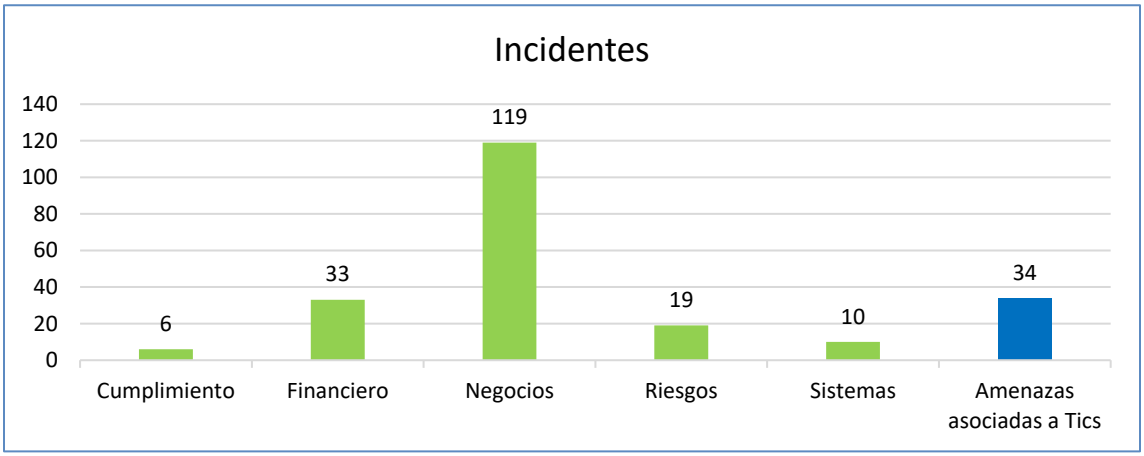
Tabla 3: Amenazas tecnológicas

Nro	Amenazas
1	Acceso no autorizado
2	Accesos de usuarios totales
3	Ausencia de personal capacitado en la operación de la Base de datos
4	Ausencia de programas de protección que detecten y eliminen malware.
5	Avería de origen físico o lógico.
6	Conexiones a redes Wi-Fi públicas o mal configuradas pueden ser vulnerables a intercepciones
7	Configuraciones predeterminadas o incorrectas pueden dejar puertas abiertas para ataques
8	Datos no cifrados pueden ser interceptados y leídos por atacantes.
9	Destrucción de equipo o medios
10	El hardware puede estar sujeto a obsolescencia tecnológica
11	Escucha encubierta
12	Espionaje remoto
13	Explotación de vulnerabilidades conocidas
14	Falsificación de derechos
15	Fuga de información interna
16	Ingreso no autorizado
17	Negación de acciones
18	No existen controles de exfiltración de información
19	No realizar las pruebas necesarios previo lanzamiento a producción
20	Perfiles de usuarios privilegiados, no controlados
21	Proceso de Gestión de identidades, no controlado
22	Robo de datos en la comunicación
23	Sistemas operativos y aplicaciones sin actualizaciones de seguridad pueden ser explotados
24	Uso de contraseñas simples o repetidas facilita el acceso no autorizado.
25	Uso no autorizado del equipo
26	Usuarios con más permisos de los necesarios pueden alterar o acceder a datos sensibles
27	Ataques SQL Injection
28	Ataques Man-in-the-Middle
29	Uso de software desactualizado
30	Configuraciones débiles en servidores web y bases de datos.
31	Uso de credenciales embebidas en código fuente
32	Accesos de intrusos, equipos sin actualización de firmware
33	Suplantación de identidad
34	Verificación de parámetros de seguridad

Al incluir este catálogo de amenazas, se ha obtenido 34 posibles incides asociados al entorno de Tics, por lo que se ha replanteado nuevamente un gráfico descriptivo de los

incidentes de riesgos con un perfilamiento de riesgo de fraudes y las amenazas asociadas al entorno tecnología de la cooperativa de igual manera podrían recaer en incidentes de riesgo que apunten a posibles fraudes financieros.

Gráfico 6: Incidentes de riesgo y amenazas asociadas a Tic's



Fuente: Matriz de riesgos según el SGSI de la COAC Artesanos

Estos tipos de incidentes de riesgos de una u otra forma se encuentran correlacionados con el ecosistema tecnológico, y más aún cuando en los procesos, interviene la manipulación humana, que hoy por hoy se ha convertido en eslabón principal de la seguridad de la información, ya que son instancias en que no solo puede estar involucrado un actor, sino varios, que buscan objetivos en común, y más aún cuando existe un compendio de complicidad entre varias áreas, incluyendo personal del área de tecnologías para ejecutar alguna acción maliciosa.

Valoración del riesgo

De toda la base de incidentes, se realizó un análisis de riesgos en base a la probabilidad de ocurrencia y el impacto tecnológico, reputacional y económico de la cooperativa, por lo que se estableció los criterios de evaluación acordes los parámetros que maneja la cooperativa para la estimación de riesgo, y que en este caso se aplica de la siguiente manera:

Probabilidad

La probabilidad de ocurrencia de dichos incidentes se encuentra categorizados de la siguiente manera.

Tabla 4:Probabilidad de ocurrencia

Factor	Probabilidad	Detalle
1	**Baja**	≤ 2 incidencias al año
2	**Media**	3 a 5 incidencias anuales
3	**Alto**	6 a 10 incidencias anuales
4	**Muy Alto**	6 a 10 incidencias anuales

Fuente: COAC Artesanos

Para el cálculo de la probabilidad, se mantienen las ponderaciones establecidas en 4 niveles que son: Bajo, Medio, Alto y Muy alto, la probabilidad de ocurrencia va en el sentido del número de incidencias que se podrían ocurrir anualmente en la entidad.

Impacto

El impacto es la métrica que se utiliza para medir la repercusión o daño que puede comprometer un incidente, por lo que se encuentra ponderado de la siguiente manera:

Tabla 5: Impacto o nivel de daño generado

Factor	Impacto	Detalle
1	**Insignificante**	No representan amenazas significativas materializarse fraudes y la reputación de la Cooperativa.
2	**Menor**	La organización tiene capacidad de respuesta adecuada, aunque requiere ajustes en controles internos para no degradar las operaciones del negocio, evitar fraudes y cuidar con reputación de la Cooperativa.
3	**Moderado**	Se evidencian debilidades estructurales en controles, y existe una alta probabilidad de pérdida financiera, riesgo reputacional y exposición a fraudes financieros.
4	**Crítico**	La organización está expuesta a consecuencias legales, pérdida financiera clientes, deterioro de su imagen institucional y la materialización de fraudes financieros.

Fuente: COAC Artesanos

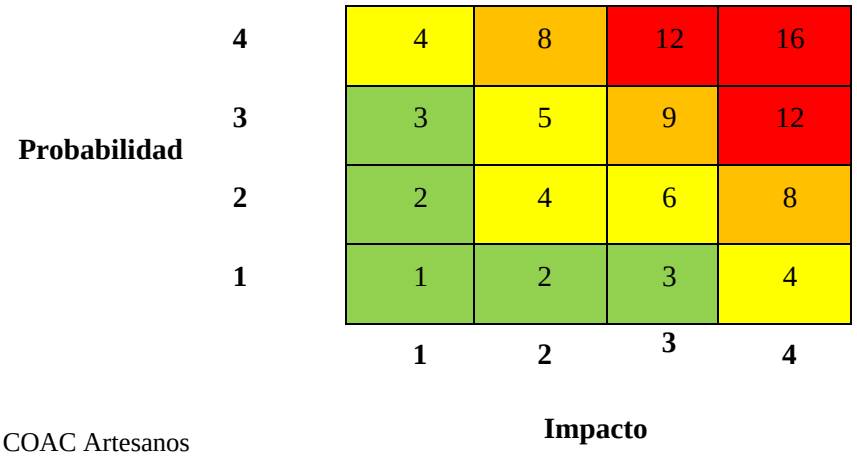
Para medir el impacto o nivel de daño de las incidencias, se ha categorizado en 4 niveles de ponderación, que van desde: Insignificante, Menor, Moderado y Crítico, cada uno de estos niveles se encuentran establecidos bajo parámetros que comprometen a la operatividad del negocio, presencia de fraudes y la imagen reputacional.

Mapa de Calor

Para determinar el nivel de exposición al riesgo, se mantiene un mapa de calor en el que se puede localizar la criticidad de los riesgos de los incidentes evaluando la probabilidad y el impacto, mismo que se encuentra establecido de la siguiente manera:

Nivel de Exposición al Riesgo= Probabilidad * Impacto

Gráfico 7*:* Mapa de Calor



Fuente: COAC Artesanos

Tipo de riesgo

De acuerdo al nivel de exposicion del riesgo ubicado en el mapa de calor, se categoriza el tipo de riesgo, tanto por por su criticidad, la categoria del evento y las medidas o estrategias de mitigacion que deben adoptarse despues de su medicion de exposicion, tal como se describe en el siguiente detalle:

Tabla 6: Tipo de riesgo

Rango	Ponderación	Categoría	Estrategias de mitigación	
1-3	1	**Bajo**	Aceptar	No adoptar ninguna acción para controlar, intentar mitigar en su medida
4-6	2	**Medio**	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
8-10	3	**Medio-Alto**	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
12-16	4	**Alto**	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos

Fuente: COAC Artesanos

Análisis de riesgo

A continuación, se presenta un resumen del análisis de los incidentes, que han sido catalogados como riesgos directos o parciales que poseen características compatibles a fraudes financieros en los sistemas informático de la entidad tomada como caso de estudio (véase el análisis completo en el **anexo 1**)

Tabla 7: Incidentes de riesgos con perfilamiento de posibles fraudes

Incidentes por áreas	Riesgo
Cumplimiento	
Incumplimiento en la entrega de información hacia terceros	
- Deficiencias en controle de cuentas inactivas y pasivos inmovilizados	Medio-Alto
Financiero	
Cortes en los servicios públicos	
- Agencias vulnerables al presentar daño en el sistema de videovigilancia y en el sistema de accesos	Medio
Errores en introducción de datos, mantenimiento o descarga	
- Error de procesamiento de valores de transacciones	Alto
- Incremento sin autorización de tasa pasiva para depósitos a plazo fijo que sobrepasa los límites establecidos.	Medio-Alto
- Que el socio no este con cobertura vigente	Medio
- Sistema de grabación y almacenamiento de imágenes sin respaldos ante incidentes en instalaciones de las agencias	Medio

Incidentes por áreas	Riesgo
Hurto/extorsión/malversación/robo	
- Asalto, robo, extorsión de terceros	Medio-Alto
- Exposición de la oficina a errores operativos y/o actividades ilícitas que no puedan ser verificadas debido a cámaras videovigilancia con tarjeta de video dañada.	Medio-Alto
Hurto/robo (fuente externa)	
- Incidente de posible asalto en el traslado de valores	Alto
Inapropiada utilización de información confidencial	
- Posible pérdida de documentos con información crítica por falencias en seguridad física en lugares de almacenamiento.	Medio-Alto
Operaciones no reveladas/registradas (intencionalmente)	
- Exista diferencias, sea faltante o sobrante.	Medio-Alto
Pérdidas por desastres naturales, terrorismo, vandalismo, etc.	
- Daño en infraestructura de agencia y en equipos tecnológicos.	Medio-Alto
Registros incorrectos de socios y clientes	
- Que tenga una enfermedad preexistente	Medio-Alto
Utilización de cheques sin fondos (Fuente externa)	
- Fraude externo por Confirmación de depósito de cheque sin constatar disponibilidad de fondos.	Medio-Alto
Negocios	
Acceso no autorizado a cuentas	
- Denuncia por movimiento no autorizado de cuentas de ahorros.	Alto
- Denuncias por movimientos de fondos en cuentas de socios sin autorización.	Alto
Actividades no autorizadas	
- Pérdida de confianza por parte de socios de crédito en la cooperativa	Medio
- Sustracción o pérdida de dinero de socios entregado a funcionarios sin el debido respaldo.	Medio-Alto
Documentos jurídicos incompletos/inexistentes	
- Autorizar una inversión sin verificar el origen lícito de los fondos presentados por el socio para el DPF.	Medio-Alto
- Documentos desactualizados	Medio
- Falta de documentación, incompleta, desactualizada	Medio
- Invalidez de pagarés que respalden procesos de cobranza	Medio-Alto

Incidentes por áreas	Riesgo
- No contar con la aprobacion de los representantes de la cuenta de firmas conjuntas	Medio-Alto
- Pérdida de documentos de crédito por inadecuado archivo.	Medio-Alto
- Realizar el cambio de la informacion sin el documento de sustento	Medio-Alto
- Realizar transacciones sin contar con los requisitos necesarios.	Medio-Alto
- Recursos que ingresan mediante SPI a la Cooperativa sin formulario de licitud de fondos regularizada	Medio-Alto
- Requisitos caducados en DPF	Medio-Alto
Errores en introducción de datos, mantenimiento o descarga	
- Acreditar valores de operaciones de socios a cuentas que no le corresponden	Medio-Alto
- Liquidación de créditos novados sin precancelar el crédito anterior, obteniendo dos créditos vigentes.	Medio-Alto
- Al negociar una tasa de inversión y realizar con otra diferente, afecta las ganancias.	Medio
- Control deficiente de comprobantes de recaudación	Medio-Alto
- Crédito en mora por depósito de valores recaudados en cuenta de ahorros incorrecta.	Medio-Alto
- Débito de valores a socios que no corresponden	Medio-Alto
- Doble acreditación en cuenta	Alto
- Documentos de expediente de crédito con detalle de tipo de garantía incongruente a la solicitud de crédito.	Medio-Alto
- Error de digitación de información	Medio-Alto
- Faltante de dinero en bóveda por egresos realizados y no registrados.	Medio-Alto
- Identificar inconsistencias de la información durante la validación	Medio
- Error en ingresos de información de cheque	Medio
- Modificación de información de socios sin realizar el procedimiento correspondiente debido a la accesibilidad del personal operativo.	Medio-Alto
- No actualizar datos conforme establece el proceso de captaciones	Medio-Alto
- No digitalización de firmas en el sistema	Bajo
- Reclamos de beneficiarios de bono de desarrollo humano, por cobros	Medio-Alto
Fallas en la entrega de información	

Incidentes por áreas	Riesgo
- No lograr tener contacto con las personas de referencias mencionadas.	Bajo
- Re proceso de operaciones de crédito tras ser dadas de baja	Medio-Alto
- Reclamo de socios por movimiento de cuentas no autorizados debido a que aduce no ser su firma,	Medio
Falsificación (Fuente externa)	
- Recaudación de valores en campo mediante comprobantes de recaudación haciendo uso fraudulento de la imagen de la Cooperativa	Medio-Alto
- Requisitos falsos en DPF	Alto
- Suplantación de identidad	Alto
Falsificación (Fuente interna)	
- Falsificación de papeleta de retiro para movimientos de cuentas de socios.	Medio-Alto
- Fraude interno en colocación de crédito	Medio-Alto
Falta de difusión y comunicación de políticas	
- Demora en realización de transferencias	Medio-Alto
- No entregar Tarjetas de débito en los tiempos establecidos.	Medio-Alto
- No realizar la confirmación de datos o información del socio	Medio
- Sobrepasar la tasa establecida	Medio-Alto
Fraude	
- Fraude interno en colocación de créditos con baja probabilidad de recuperación	Medio-Alto
Hurto/extorsión/malversación/robo	
- Fraude interno por desvío de fondos de cuentas inactivas de socios	Alto
Hurto/robo (fuente externa)	
- Existencia de objetos extraños en el cajero	Alto
- Fraude externo en área de cajas.	Medio-Alto
Inexistencia de autorizaciones	
- Cierre de cuentas de ahorro o aportación sin la debida autorización formal.	Bajo
- Efectivización de cheques sin autorización	Medio-Alto
- Entregar estados de cuenta a persona que no es el titular sin autorización, o documento no firmado	Medio
- No exista la aprobación correspondiente para el incremento de tasa.	Medio-Alto

Incidentes por áreas	Riesgo
- No tener autorización para el procedimiento de bloqueos y desbloqueos	Medio-Alto
- Que la apertura de cuenta a un menor de edad no sea gestionada por el padre de familia o representante legal	Alto
- Realizar el cierre de cuentas por terceras personas sin autorización	Bajo
- Realizar el pago a una tercera persona sin la debida autorización	Medio-Alto
Operaciones no autorizadas (con pérdidas pecuniarias)	
- Desvío de fondos por confirmación de depósitos.	Alto
Operaciones no reveladas/registradas (intencionalmente)	
- Cargar el dinero en bandejas diferentes a las establecidas para cada denominación	Alto
- No comunicar las diferencias encontradas	Medio-Alto
- No identificar o no registrar diferencias, sea faltante o sobrante.	Medio-Alto
- No reportar sobrantes o faltantes	Alto
Quebrantamiento de la privacidad de información, sobre socios, clientes y usuarios	
- Mal uso de la información de captaciones reservada de la entidad	Medio-Alto
- Movimientos no autorizados o sin conocimiento del titular de la cuenta mediante banca electrónica, debido a el registro de correo electrónico del funcionario de la institución y no del socio.	Medio-Alto
Riesgos	
Documentos jurídicos incompletos/inexistentes	
- Crédito sin garantía	Medio-Alto
Fallas en la entrega de información	
- Al opera con usuarios compartidos no se pude identificar en realidad quien realizó las transacciones de caja y se pueden realizar operaciones no autorizadas.	Alto
Fallos de contrapartes (proveedores)	
- Fuga de información de proveedor de software	Medio-Alto
Inexistencia de autorizaciones	
- Documentos contractuales y de alta confidencialidad inválidos.	Medio-Alto
Operaciones no autorizadas (con pérdidas pecuniarias)	
- Fraude interno/externo en banca electrónica	Alto
Sistemas	
Cortes en los servicios públicos	

Incidentes por áreas	Riesgo
- Duplicidad de transacciones en caja	Medio
Errores en introducción de datos, mantenimiento o descarga	
- Diferencias en cobro de rubros correspondientes a seguro de desgravamen en operaciones de crédito precanceladas	Medio
Fallas en el software	
- Sincronización inestable entre tablas contables de transacciones del core financiero	Medio-Alto
Fallos de contrapartes (proveedores)	
- Pérdida de respaldos de correos electrónicos	Bajo
Total	**84**

De igual forma se hizo el análisis de las amenazas catalogadas como posibles causantes de riesgos de fraude, de la siguiente manera:

Tabla 8: Amenazas de riesgo de TI

Amenazas de Tics	Riesgo
Acceso no autorizado	Medio
Accesos de usuarios totales	Medio
Ausencia de personal capacitado en la operación de la Base de datos	Bajo
Ausencia de programas de protección que detecten y eliminen malware.	Bajo
Avería de origen físico o lógico.	Bajo
Conexiones a redes Wi-Fi públicas o mal configuradas pueden ser vulnerables a intercepciones	Alto
Configuraciones predeterminadas o incorrectas pueden dejar puertas abiertas para ataques	Medio
Datos no cifrados pueden ser interceptados y leídos por atacantes.	Medio
Destrucción de equipo o medios	Alto
El hardware puede estar sujeto a obsolescencia tecnológica	Medio
Escucha encubierta	Alto
Espionaje remoto	Alto
Explotación de vulnerabilidades conocidas	Medio

Amenazas de Tics	Riesgo
Falsificación de derechos	Alto
Fuga de información interna	Medio
Ingreso no autorizado	Alto
Negación de acciones	Medio
No existen controles de exfiltración de información	Medio
No realizar las pruebas necesarias previo lanzamiento a producción	Alto
Perfiles de usuarios privilegiados, no controlados	Medio
Proceso de Gestión de identidades, no controlado	Medio
Robo de datos en la comunicación	Bajo
Sistemas operativos y aplicaciones sin actualizaciones de seguridad pueden ser explotados	Medio
Uso de contraseñas simples o repetidas facilita el acceso no autorizado.	Alto
Uso no autorizado del equipo	Medio
Usuarios con más permisos de los necesarios pueden alterar o acceder a datos sensibles	Alto
Ataques SQL Injection	Medio
Ataques Man-in-the-Middle	Medio
Uso de software desactualizado	Alto
Configuraciones débiles en servidores web y bases de datos.	Medio
Uso de credenciales embebidas en código fuente público	Bajo
Accesos de intrusos, equipos sin actualización de firmware	Bajo
Suplantación de identidad	Medio
Verificación de parámetros de seguridad	Alto
Total	**34**

CAPITULO IV

4 RESULTADOS Y DISCUSIONES

4.1 Resultado del análisis comparativo entre la norma ISO/IEC 27037 (2012) y la metodología propuesta por Velarde (2025).

De acuerdo al ***gráfico 2 (***Comparativa entre norma ISO/IEC 27037 (2012) y Velarde 2025), ha permitido identificar puntos de convergencia y divergencia relevante, de acuerdo a cada uno de los criterios planteados para su contraste, enfocado a las aplicación en auditorías informáticas forenses orientadas al sector financiero, dando los siguientes resultados:

En primer lugar, la estructura y fases de la norma ISO/IEC 27037 destacan por su alineación con estándares internacionales y buenas prácticas consolidadas, definiendo de manera clara procesos de identificación, recolección, preservación y análisis de evidencia digital. Por su parte, la propuesta de Velarde (2025) aporta un modelo más adaptado a realidades institucionales con sistemas desarrollados a medida, añadiendo fases orientadas a fortalecer la auditoría como soporte para investigaciones digitales específicas dentro de entornos complejos. Este enfoque complementa la norma al dotarla de una perspectiva más operativa y contextualizada.

En cuanto a la aplicabilidad en sistemas informáticos financieros, ambas metodologías resultan viables; sin embargo, Velarde prioriza escenarios donde los sistemas pueden presentar debilidades asociadas al desarrollo propio (in-house) y la gestión dentro de un área de TI, mientras que la ISO 27037 resulta más genérica y exige ajustes para cubrir los riesgos particulares del sector financiero cooperativo, donde intervienen plataformas críticas como el core bancario o canales digitales de alto volumen transaccional.

Respecto al alcance en la identificación y análisis de evidencia digital, la ISO 27037 tiene un enfoque exhaustivo en la integridad y confiabilidad probatoria de la evidencia, mientras que Velarde amplía la mirada hacia procesos de auditoría preventiva, permitiendo identificar indicios de irregularidades antes de materializar un incidente de riesgo grave. Esto implica un matiz proactivo que podría resultar valioso para prevenir fraudes recurrentes en instituciones financieras.

En lo concerniente a la integración con normativas locales, la ISO 27037 al ser un estándar internacional requiere una adaptación explícita a la normativa ecuatoriana (SEPS, COIP, JPRF y otras directrices de supervisión financiera), mientras que el modelo de Velarde, si bien desarrollado en otro contexto (Latinoamérica), resulta más flexible para integrarse a marcos regulatorios latinoamericanos similares, lo que facilita su adaptación al entorno ecuatoriano.

En cuanto al soporte en herramientas forenses certificadas, ambas metodologías concuerdan en la necesidad de emplear software y hardware forense reconocido y validado, garantizando así la fiabilidad de los procesos de adquisición y análisis de evidencia. No obstante, la norma ISO 27037 define lineamientos más estrictos para la selección y validación de herramientas, mientras que Velarde abre mayor margen de decisión técnica para los auditores, considerando la disponibilidad de recursos en instituciones de tamaño mediano o pequeño.

Finalmente, sobre la capacidad de trazabilidad y legalidad, la norma ISO 27037 enfatiza de forma rigurosa la preservación de la cadena de custodia y el registro documentado de cada intervención sobre la evidencia, siendo un punto crítico para su aceptación en procesos judiciales internacionales. Velarde-Flores también incorpora la trazabilidad como requisito esencial, pero orienta su registro principalmente a servir de insumo para auditorías internas y peritajes informáticos en el contexto organizacional.

Todo este análisis adyacente, en cual se contrastó entre la norma ISO/IEC 27037 y la metodología propuesta por Velarde (2025) se logró reconocer elementos de intersección o integración que abren la posibilidad de articular un modelo metodológico integral, orientado a fortalecer las auditorías informáticas forenses en sistemas financieros cooperativos.

Por un lado, la norma ISO/IEC 27037 establece un marco sólido, validado a nivel internacional, que prioriza la integridad, autenticidad y preservación de la evidencia digital desde su identificación hasta su conservación. Este marco asegura altos niveles de calidad y confiabilidad probatoria, alineándose con exigencias legales y técnicas que garantizan la admisibilidad de la evidencia en procesos judiciales.

Por otro lado, el modelo de Velarde (2025) aporta un enfoque operativo y contextualizado que complementa la visión estandarizada de la ISO, ampliando el alcance hacia el análisis técnico de la evidencia digital una vez recolectada. Este modelo incorpora

herramientas, técnicas y fases de investigación orientadas a la identificación de actores, patrones de fraude, vulnerabilidades de sistemas desarrollados a medida, y procesos de auditoría que fortalecen las capacidades internas de investigación en las organizaciones.

La intersección de ambas metodologías se observa claramente en aspectos como la trazabilidad de la evidencia, el uso de herramientas forenses certificadas, la cadena de custodia, la protección de la integridad de los datos, y la necesidad de documentar exhaustivamente cada acción durante la investigación. Estos puntos comunes constituyen un eje de integración viable para diseñar un modelo mixto que combine la robustez técnica de la norma internacional con la aplicabilidad especifica que propone Velarde.

Desde la perspectiva de los sistemas financieros, esta integración resulta especialmente relevante. El entorno cooperativo ecuatoriano enfrenta riesgos significativos derivados del uso de tecnologías financieras, exposición a fraudes electrónicos, y manipulación interna de sistemas (core bancarios, base de datos). Por tanto, contar con una metodología que no solo preserve la evidencia conforme a estándares internacionales, sino que también proporcione herramientas para su análisis detallado y adaptado a realidades locales, se convierte en una ventaja estratégica para fortalecer las capacidades de auditoría forense de la institución.

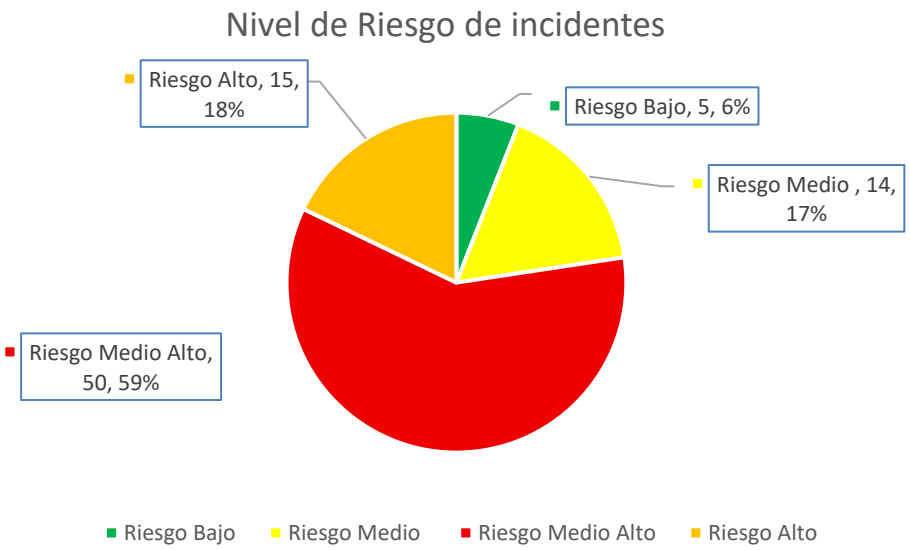
En este sentido, la combinación de ambos enfoques metodológicos potencia la eficacia de la auditoría informática forense, permitiendo anticipar riesgos, mitigar vulnerabilidades, y robustecer la confianza institucional ante eventuales incidentes digitales, todo dentro de un marco legal, técnico y ético sólido.

4.2 Resultados de la determinación nivel de indecencias o eventos de riesgo en históricos registrados, con un perfilamiento de fraudes financieros en el uso de los sistemas informáticos y aplicaciones financieras de la cooperativa tomada como caso de estudio

De la valoración de los riesgos, resumido en las ***tablas 8 y 9***, de los 84 eventos de riesgo registrados en una base histórica de la entidad, y 34 amenazas catalogadas críticas en el entorno de TI de la cooperativa, se logró determinar las incidencias y amenazas de riesgo que poseen un perfilamiento con características compatibles para la materialización de fraudes financieros mediante los sistemas informáticos que posee la cooperativa, obteniendo los siguientes resultados:

Incidentes o eventos de riesgo:

Gráfico 8: Niveles de riesgo en incidentes



Fuente: Elaboración propia

Nivel de Riesgo Bajo (5 eventos – 5.95%)

Estos eventos se han presentado en las áreas de negocios, riesgos, sistemas que exhiben una baja probabilidad de ser explotados para generar un fraude financiero. Son incidentes que, si bien afectan la operación normal o reflejan descuidos que no comprometen directamente los sistemas informáticos ni generan pérdidas.

Se trata de faltas administrativas o de procedimiento sin impacto tecnológico crítico, inexistiendo evidencias de intención fraudulenta ni pérdidas económicas, esto generados tal vez la falta de implementación de mecanismos de control.

El riesgo es residual y puede ser mitigado fácilmente mediante controles básicos y mejora de procedimientos internos.

Nivel de Riesgo Medio (14 eventos – 16.67%)

Son incidentes que exponen fallas operativas o técnicas, en las áreas de Negocios, Financiero, Sistemas, Cumplimiento y Riesgos, con un impacto moderado. Aunque no representan fraudes por sí mismos, dejan brechas que podrían ser aprovechadas si no se controlan.

Estos incidentes contienen características como errores humanos o tecnológicos en procesos críticos (captaciones, créditos, registros), vulnerabilidades en el control documental y en los registros de transacciones y las deficiencias en la validación de datos con socios y clientes.

Estas inflexiones pueden escalar si se combinan con factores como acceso no autorizado o uso inadecuado del sistema, generando pérdida de confianza y afectación reputacional.

Nivel de Riesgo Medio-Alto (50 eventos - 59.52%)

Corresponden a incidentes presentados en las áreas de Negocios (alta concentración), Financiero, Riesgos, Cumplimiento y Sistemas, donde existe una vulnerabilidad evidente que podría facilitar un fraude financiero. En muchos casos, estos incidentes muestran signos de deterioro en los controles internos o exposición constante a riesgos digitales.

Estos incidentes se presentan por el uso indebido de información confidencial, errores críticos en la digitación o procesamiento de datos financieros, documentos legales incompletos o inválidos en procesos de crédito o inversión, incidentes relacionados con sistemas informáticos sin respaldo o sin monitoreo y fallas en la validación de transacciones.

Estos eventos permiten determinar un perfilamiento del riesgo de fraude interno o externo, ya que afectan la integridad, confidencialidad y disponibilidad de la información financiera, que pueden derivar en fraudes complejos si son ejecutados por personal con conocimiento del sistema.

Nivel de Riesgo Alto (15 eventos - 17.86%)

Este grupo incluye incidentes con impacto directo, demostrable y potencialmente recurrente sobre la seguridad financiera y reputacional de la cooperativa. Aquí ya existen señales de fraude o pérdidas verificadas.

Se representan en fraudes confirmados o altamente sospechosos, como accesos no autorizados, falsificaciones o desvíos de fondos, afectación económica directa o potencial, involucran el uso malicioso o manipulación intencionada de sistemas informáticos.

Estas eventualidades requieren respuesta inmediata y aplicación de procesos forenses para identificar responsables, cuantificar daños y fortalecer los mecanismos de auditoría,

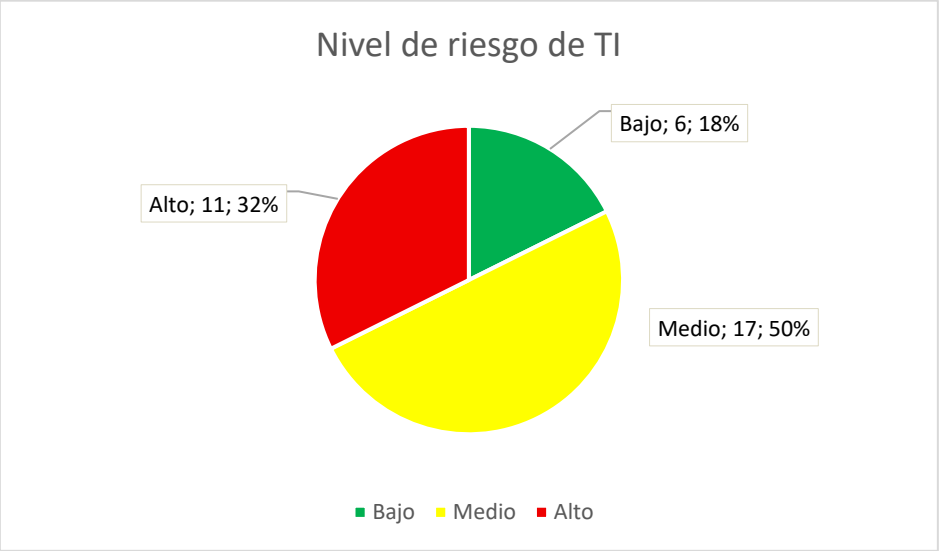
asimismo esto ya representa una amenaza directa a la confianza institucional y la sostenibilidad financiera.

Bajo todo este contexto se revela que más del 73% de las incidencias (62 de 84 eventos) se concentran en los niveles de riesgo medio-alto y alto, los cuales presentan características compatibles con fraudes electrónicos, abuso de accesibilidad en sistemas de información y debilidad en los controles operativos.

Amenazas de riesgo en el entorno de TI:

El análisis de amenazas realizado sobre el entorno tecnológico que soporta el core financiero de la organización permitió identificar un total de 34 amenazas potenciales que pueden materializarse como riesgos, impactando la confidencialidad, integridad y disponibilidad de los activos de información críticos. Estas amenazas se clasificaron en tres niveles de riesgo: alto, medio y bajo.

Gráfico 9: Niveles de riesgo sobre las amenazas en TI



Fuente: Elaboración propia

Riesgo Bajo (6 eventos -17,6%)

Agrupa amenazas de menor probabilidad de ocurrencia o con impacto reducido, tales como averías físicas o lógicas, falta de personal capacitado, uso de firmware desactualizado, o carencia de programas antimalware. Aunque el riesgo es menor en términos relativos, estos eventos podrían ser aprovechados por actores malintencionados en combinación con otras vulnerabilidades, por lo cual resulta necesario mantener

controles operacionales, actividades de mantenimiento preventivo y capacitación constante del personal técnico.

Riesgo Medio (17 eventos - 50%)

Engloba amenazas que podrían derivar en incidentes significativos si no se gestionan adecuadamente. En este grupo destacan vulnerabilidades asociadas a configuraciones por defecto, ausencia de controles de exfiltración, obsolescencia tecnológica, falta de actualizaciones de seguridad, y debilidades en los procesos de gestión de identidades y accesos. La probabilidad de ocurrencia es moderada, pero el impacto puede escalar si no se aplican medidas correctivas en plazos razonables. Se recomienda diseñar un plan de mejora progresivo que contemple fortalecimiento de la infraestructura, gestión de vulnerabilidades continua y auditorías periódicas.

Riesgo Alto (11 eventos - 32,4%)

Incluyen amenazas que, de materializarse, podrían causar impactos críticos, tales como accesos no autorizados, espionaje remoto, destrucción de equipos, suplantación de identidad, uso de contraseñas débiles, presencia de privilegios excesivos en usuarios, configuraciones deficientes en entornos de producción, y la inexistencia de pruebas de seguridad rigurosas. Estas amenazas podrían facilitar el fraude financiero, la pérdida de integridad de los datos o la interrupción total de los servicios. Su mitigación debe considerarse prioritaria e inmediata mediante la implementación de controles técnicos, administrativos y de concienciación.

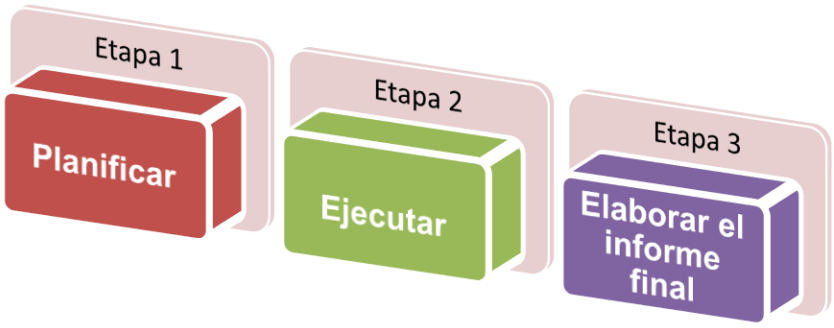
En síntesis, el estudio demostró que un 78% de las amenazas identificadas presentan niveles de riesgo medio y alto, lo cual podría repercutir de forma transversal en la operación del core financiero. Este resultado resalta la urgencia de establecer un programa integral de seguridad de la información, con controles técnicos, procedimientos operativos estandarizados y actividades de concienciación, con el objetivo de salvaguardar los procesos financieros y garantizar la continuidad de los servicios críticos para la organización.

4.3 Modelo de auditoría informática forense para el manejo de la evidencia digital de los sistemas informáticos de la Cooperativa de Ahorro y Crédito "Artesanos

Los procesos críticos para el giro de negocio de la Cooperativa de Ahorro y Crédito Artesanos son los productivos, también conocidos como operativos, mismos que abarcan toda la gestión financiera (Captar, colocar y recuperar), son soportados y ejecutándose mediante el Core Financiero que ha sido desarrollado a medida acorde a las necesidades y requerimientos de la entidad, como también haciendo uso de tecnología complementaria para solidificar las estrategias de negocio, en ese sentido las auditorias informáticas se focalizan en diversos ámbitos, entre ellos, el desarrollo de software, la administración de base de datos, uso de los sistemas de información, seguridad de la información, gestión de vulnerabilidades, infraestructura tecnológica, cumplimiento de normativa interna o externa, canales electrónicos, procesos y controles internos, gestión de TI, servicios de terceros y entre otros.

Las auditorías internas que se ejecutan en la entidad se fundamentan en tres etapas que son: planificar, ejecutar y elaborar el informe final, siendo esta una metodología que se adapta para la ejecución de auditorías informáticas, en tal virtud el modelo que se plantea en este trabajo de investigación, busca unificar directrices de la informática forense en los procesos de auditoria informática a fin de identificar, preservar, analizar y presentar la evidencia digital para apoyar en investigaciones sobre incidentes informáticos, fraudes, accesos no autorizados, o cualquier actividad ilícita que involucre sistemas tecnológicos.

Gráfico 10: Etapas de Auditoria - COAC Artesanos



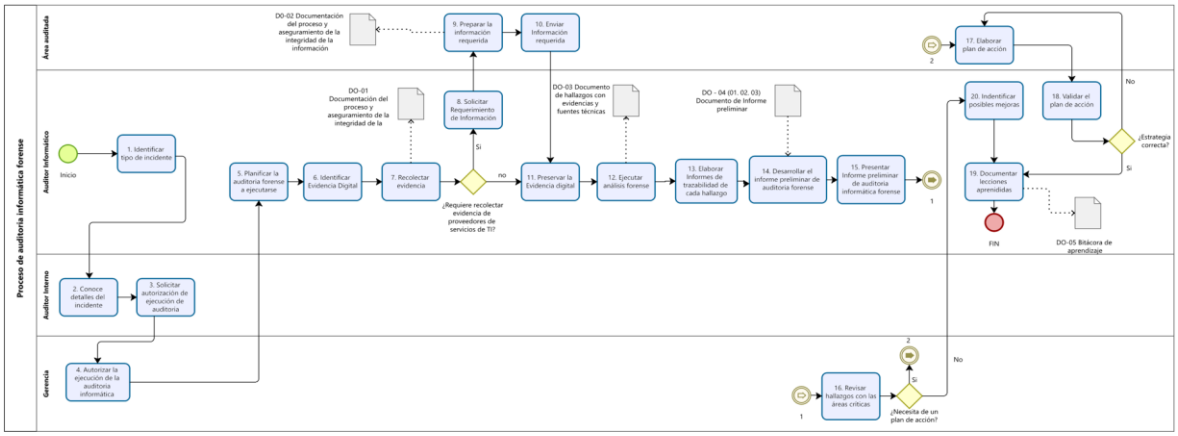
Fuente: Elaboración propia

El modelo de auditoria informática forense para el manejo de la evidencia digital, se plantea en base a una metodología unificada entre los parámetros de la ISO 27037: 2012 y la metodología propuesta por Velarde (2025), las cuales mantienen puntos de intersección

que logran hacer de una metodología integrada que combina estratégicamente elementos, principios y prácticas, logrando adaptarlas a los procesos de auditoria informática de la entidad.

En ese particular, mediante un diagrama de procesos se ha diseñado el modelo de auditoria informática forense, en el que establecen los componentes del proceso de auditoría informática y la metodología integrada para la recolección de la evidencia digital, este modelo se compone de 22 actividades, que inicia desde la identificación de un evento de riesgo con perfilamiento de fraude y finaliza con la realización de un informe de los resultados con las acciones y lecciones aprendidas del evento, tal como se muestra a continuación:

Gráfico 11: Diagrama de proceso de Auditoría Informática forense



Fuente: Elaboración propia

Como se muestra en el ***Gráfico. 11*** que antecede, el proceso mantiene varios involucrados, que son: Gerencia, Auditor Interno, Auditor Informático y el Área auditada. Cada uno de los involucrados cumplen roles importantes para el desarrollo de una auditoria informática forense; particularmente el área auditada se ancla en el proceso al momento de la entrega de requerimientos técnicos o documentales, como también en la aplicación de acciones correctivas tras un dictamen final.

Es importante destacar que este modelo es planteado de acuerdo a los parámetros y ajustes de la cooperativa en estudio, por lo que las actividades que efectúa el DEFR y el DES, serán realizadas por el Auditor Informático, sin embargo, pueden adaptarse a la escalabilidad de la institución en un futuro, en el que pueden intervenir diferentes especialistas en el mismo proceso.

A continuación, se detalla las etapas que componen este modelo de auditoria informática forense para el manejo de la evidencia digital, cada una de ellas mantiene una descripción a detalle de lo que debe ejecutar cada responsable, hay que considerar que existen actividades que como producto final o insumo resulta un documento los cuales aportaran como evidencia y documentación del proceso.

Etapas (Actividades)

4.3.1 Identificar el tipo de incidente

En este apartado, un incidente puede ser proveniente desde distintos orígenes, sea por la detección de actividades irregulares emitidas por otras áreas, por identificación propia del Auditor Informático en revisiones de auditorías del entorno tecnológico o la presencia de incidentes en canales electrónicos informados por socios y clientes.

La identificación del tipo de incidente es muy importante debido que logra poner el primer panorama de la situación o problema, siendo el punto de partida para una correcta planificación y los métodos posibles para el manejo del incidente, sin que altere o salte el proceso adecuado.

Responsable: Auditor Informático.

4.3.2 Conocer detalles del incidente

Se conoce y entiende cada uno de los detalles del incidente reportado, en el que se evalúa la magnitud del problema y el grado de afectación de la entidad, funcionarios, socios o clientes, estableciendo diferentes aristas para abordar el incidente sin que se altere la integridad, manteniendo sigilosamente la investigación sin levantar sospechas o alertas que quebrante con la efectividad de proceso.

Responsable: Auditor Interno y Auditor Informático.

4.3.3 Solicitar autorización a la alta gerencia.

Para inicializar con la auditoria informática forense, es importante contar con una autorización de la alta gerencia, por lo que se deberá solicitar mediante un memorando u oficio la circunstancia de la revisión a ejecutarse y de esa forma cumplir con un protocolo formal, dejando constancia de esta.

Responsable: Auditor Interno.

4.3.4 Autorizar la ejecución de la auditoria informática.

Una vez conocido las circunstancias, el tipo de incidente y su grado de afectación, Gerencia autorizará la ejecución de la auditoria informática, sin embargo, en este punto también se podrá redefinir el alcance de la auditoria, a fin de realizar una investigación integral y profunda, con criterios de la alta gerencia y otras áreas estratégicas que aporten con elementos sustanciales para la búsqueda de resultados.

Responsable: Gerente General.

4.3.5 Planificar la auditoria forense a ejecutarse

Esta etapa, es considerada como fundamental para el proceso de la auditoria en curso, ya que se procede con la planificación de forma detallada y documentada, en la que se deberá estimar los siguientes elementos:

- **Objetivo:** Se define con claridad el propósito de la auditoria, el incidente o hecho que se investiga, y las normativas aplicables (externas o internas).
- **Alcance**: Se establece los elementos que abarcará la auditoria a efectuarse, este puede ser en el ámbito técnico, y funcional.

  Respecto al ámbito técnico se refiere la determinación de los elementos que serán parte de la auditoria, que pueden ser: infraestructura tecnológica (servidores, base de datos, redes, firewalls, IDS/IPS, endpoints, etc), software específico (core financiero, plataforma de administración de canales digitales, etc.), dispositivos (computadores, teléfonos, dispositivos de almacenamiento, etc.) y redes de comunicación (LAN, VPN, wifi, etc.).

En lo funcional, se define las partes del negocio involucradas, considerando que no solo se trata realizar revisiones a la parte tecnológica, sino de entender como interactúa la tecnología y el negocio, por ello se involucran: áreas operativas (Tics, Seguridad de la información, Financiero, Negocios, Riesgos, Talento Humano, entre otras), procesos críticos (gestión de usuarios, manejo de base de datos, transacciones, transferencia de datos, desarrollo de software, parametrizaciones, administración de respaldos, etc.) y la normativa interna (manuales, reglamentos, procesos, procedimientos y políticas).

- **Equipos, sistemas y redes involucrados:** Se describe en forma detallada los elementos tecnólogos que serán objeto de análisis en la auditoria efectuada, la información debe incluir especificaciones como:
    - Software (nombres, versiones)
    - Categoría de equipos (servidores, máquinas virtuales, laptops, dispositivos móviles).
    - Segmentos de red que serán analizados (IPs, VLANs, subredes).
    - Aplicaciones específicas (Canales digitales, software de monitoreo, sistema de centralización de logs, motores de bases de datos, correo electrónico, otras)
- **Roles y responsabilidades:** En este apartado se define el equipo de trabajo que participa en la auditoria, sin embargo, como se expuso en párrafos anteriores, al ser un modelo ajustado a la entidad financiera en estudio, la responsabilidad principal para el manejo de la evidencia digital recae en el auditor informático, como se describe a continuación:

Tabla 9: Roles y responsabilidades

Funcionario	***Rol***	***Responsabilidad***
Auditor Informático	Auditor Forense Líder	Dirige la auditoría, toma decisiones críticas, valida hallazgos.
	Analista Forense o DES (Especialista en evidencia digital)	Recolecta, preserva, analiza la evidencia digital.

	DEFR (Persona en dar primera Respuesta a la Evidencia Digital)	Levanta información del incidente en primera instancia, preserva la integridad.
Jefe de Tics	Encargado de TI	Proporciona acceso e información de los sistemas, asegura la integridad de plataformas.
Oficial de Seguridad de la información	Responsable de Seguridad de la información	
Auditor Interno	Verificador de la ejecución de la auditoria	Acompañar el proceso de auditoría, verifica y socializa hallazgos con las áreas involucradas.

- **Cronogramas:** Se establece un cronograma tentativo de las actividades a realizarse durante el proceso de la auditoria informática forense, en el que se deben incluir todas las fases principales, el tiempo estimado y los recursos a utilizarse (tecnológicos y humanos), siendo este un apartado en el que se define de forma global la estructurada que llevará la auditoria, misma que puede ajustarse durante la ejecución dependiendo las necesidades.

El cronograma se puede definir de la siguiente manera:

Tabla 10:Cronograma tentativo

Fase del Proceso	***Actividades Principales***	***Duración Estimada***
Preparación y planificación	- Revisión de normativa - Reunión inicial con partes interesadas - Elaboración de plan de auditoría	3 días
Identificación y Recolección de Evidencia	- Identificación de fuentes de evidencia - Resguardo inicial (DEFR) - Documentación de la cadena de custodia	5 días
Análisis Técnico	- Procesamiento de evidencia (DES) - Análisis forense - Validación de hallazgos	7 días
4. Elaboración del Informe	- Redacción del informe técnico forense - Respaldo de documentos - Revisión interna del informe	4 días
	- Entrega formal del informe	2 días

5. Presentación de Resultados	- Presentación a las partes interesadas - Revisión de recomendaciones
Total Aproximado	**21 días hábiles**

Nota: El tiempo puede variar según la complejidad del caso, el volumen de datos y la disponibilidad de recursos.

En cuanto los recursos, se pueden categorizar entre herramientas forenses, equipos y materiales y personal especializado, siendo de la siguiente manera:

- **Recursos (Herramientas)*:*** Son herramientas tecnológicas utilizadas para el procedimiento forenses, mismas que permiten obtener evidencias digitales que serán utilizadas para la auditoria, tales como se muestra en el siguiente detalle:

Tabla 11: Recursos - Herramientas forenses

Herramienta	***Uso Principal***
FTK Imager	Creación de imágenes forenses (discos duros, USB).
Autopsy / Sleuth Kit	Análisis forense de sistemas de archivos, búsqueda de artefactos.
Wireshark	Captura y análisis de tráfico de red.
HashCalc / md5sum / sha256sum	Generación de valores hash para integridad de datos.
Write Blocker (Hardware)	Dispositivo para evitar escritura en discos originales.
Cadenas de Custodia Digitales	Formularios para registro y control de evidencia.

Nota: Las herramientas pueden variar según la complejidad del caso, el volumen de datos y la disponibilidad de recursos.

- **Recursos (Equipos y Materiales):** Se debe describir los recursos tecnológicos y materiales que serán de uso durante la auditoria forense, mismos que serán utilizados en dependencia al tipo de auditoría que se vaya a ejecutar, como también se podrá adherir otros recursos que aporten con la auditoria e investigación, tal como se muestra a continuación:

Tabla 12: Recursos – Equipos y materiales

Recurso	*Especificación/Ejemplo*
Discos duros externos de respaldo	Mínimo 2 TB, cifrados preferentemente.
Computadoras de análisis	Con soporte de software forense, mínimo 16 GB RAM, procesador i7 o superior.
Medios de almacenamiento seguros	USB, SSD, CD/DVD, etiquetados y custodiados.
Laboratorio forense (si aplica)	Área segura para análisis, acceso controlado.

Nota: El equipamiento y materiales pueden variar según la complejidad del caso, el volumen de datos y la disponibilidad de recursos.

- **Recursos - Humanos (especializados)**

Se describe el contingente humano que interviene en cada una de las fases, aportando con cada las responsabilidades través de su experticia, es importante indicar que las áreas de tecnologías y seguridad de la información, en dicho proceso se involucra para la entrega de información y los accesos a los sistemas, sin embargo en casos que ameriten dichas áreas podrán aportar en diversas actividades que contemple el auditor líder, interviniendo como un soporte o fuente de información para entender y conocer más a fondo el funcionamiento de los sistemas, el comportamiento de datos, barridos de funcionamiento mediante flujos de trabajo y otras necesidades. Estos recursos se ajustan de acuerdo con la entidad en estudio, no obstante, pueden ser escalados a instancias superiores o referenciales a otras de menor tamaño.

Tabla 13: Recursos - Personal Especializado

Rol	*Funciones principales*	*Formación sugerida*
Auditor Forense (DEFR)	Identificación inicial, resguardo, documentación.	Conocimiento en TI y procedimientos ISO 27037.
Especialista Forense (DES)	Análisis técnico avanzado, herramientas forenses.	Perito forense certificado, experiencia en análisis digital.
Jefe de Auditoría	Validación, revisión de hallazgos, presentación.	Experiencia en auditoría y normas SEPS.

Soporte Técnico TI	Asistencia en infraestructura, redes, seguridad.	Técnico o ingeniero en sistemas.

Nota: El personal especializado, se encuentra limitado al modelo planteado de la cooperativa en estudio, por lo que en un futuro podría inmiscuirse e involucrarse más personal especializado.

Responsable: Auditor Informático

Insumo: Documento preliminar (Opcional), que puede utilizarse para recopilar información útil para empezar a realizar un informe final. (**Anexo 2**)

4.3.6 Identificar evidencia digital

Esta etapa es la fase fundamentar para el manejo total de la evidencia digital, que consiste en reconocer, localizar y documentar con cualquier activo tecnológico o datos que tenga un valor probatorio para un incidente de seguridad, fraude o actividad anormal detectada en una auditoria.

Es muy esencial que en esta fase se enliste todas las posibles fuentes de evidencia del entorno tecnológico, tal como se muestra en el siguiente detalle:

Tabla 14: Fuentes de evidencias

Fuente	*Información que proporciona*
Sistemas gestión de archivos y documental	Archivos de usuario, documentos, imágenes, videos, etc.
Logs de eventos	Registros del sistema, de seguridad, de red, de aplicaciones.
Correos electrónicos	Mensajes enviados/recibidos, adjuntos, cabeceras.
Equipos de almacenamiento	Discos duros, SSDs, USB, CDs, DVDs, tarjetas SD.
Bases de datos	Registros transaccionales, accesos, consultas.
Redes	Capturas de tráfico (pcap), configuraciones, ruteo.
Memoria RAM (volátil)	Procesos activos, sesiones, claves, contraseñas.

Fuente	*Información que proporciona*
Backups	Copias de seguridad almacenadas en medios físicos o nube.
Dispositivos Móviles	Mensajes, contactos, apps, registros de llamadas.
Sistemas de control de acceso	Registros de ingreso, salidas, accesos biométricos.

Nota: Las fuentes de evidencia, pueden variar de acuerdo al tipo de investigación y la necesidad de verificar los incidentes de la investigación, no todas las revisiones tienen un mismo esquema.

Todas las fuentes de recolección de evidencia deberán ser documentadas, detallando la ubicación física y el tipo de dato.

Clasificación de la evidencia

Dentro de la fase de identificación, es importante que la evidencia se clasifique según su naturaleza, que pueden ser volátil y no-volátil.

- ***Evidencia Volátil***

  Se trata de toda la información que desaparece cuando el equipo, dispositivos o unidad de almacenamiento se apaga o cambia de estado, es decir:

  Tabla 15: Evidencia volátil

Tipo de Evidencia Volátil	*Tipo de información*
Memoria RAM	Claves, procesos, contraseñas, llaves de cifrado.
Sesiones activas	Sesiones abiertas en sistemas, VPN, SSH, RDP.
Conexiones de red	Sockets abiertos, puertos en escucha, IPs conectadas.
Datos temporales	Archivos temporales, cachés, páginas web abiertas.

- ***Evidencia no-volátil***

  Es toda aquella información que persiste tras apagar equipos, dispositivos o unidades de almacenamiento, tales como:

Tabla 16: Evidencia Volátil

Tipo de Evidencia No-Volátil	*Tipo de Información*
Archivos de disco	Documentos, hojas de cálculo, imágenes, videos.
Registros de logs	Archivos de sistema, eventos, auditorías, errores.
Correos electrónicos	Mensajes completos, metadatos, adjuntos.
Copias de seguridad	Backups programados, respaldos completos o incrementales.
Bases de datos	Registros históricos, tablas, usuarios, transacciones.
Dispositivos físicos	Discos duros, SSD, USB, CDs, servidores.

Es importante desatacar, que al ser evidencia no volátil, no quiere decir que sea expuesta a cambios o modificaciones por lo que es recomendable realizar un proceso de aseguramiento de la evidencia (imágenes forenses, copias, hash).

Responsable: Auditor Informático.

Insumo o producto: Fuente de evidencias, volátiles y no volátiles (**Anexo 3**)

Recolección y adquisición de evidencia

La recolección y adquisición son etapas claves de una auditoría forense, cuyo objetivo es obtener evidencia digital de manera completa, confiable y repetible sin alterar su contenido ni comprometer la cadena de custodia.

Esta fase implica la extracción de datos de los activos y sistemas tecnológicos involucrados (computadoras, redes, dispositivos móviles, servidores, etc.) utilizando herramientas y técnicas que aseguren la integridad probatoria y la validez legal.

En ese sentido, esta etapa se consolida en los siguientes pasos:

- Uso de herramientas forenses certificadas

- Crear imágenes forenses
- Cálculo de hash
- Mantener cadena de custodia
- Manejo seguro de la evidencia
- Documentar el proceso

Uso de herramientas forense

Se deben usar herramientas que sean reconocidas, confiables y preferentemente auditadas a fin de garantizar la legalidad absoluta en la adquisición de la evidencia que será utilizada en la auditoria forense, a continuación, se enlista algunas herramientas ampliamente aceptadas y utilizadas en el campo de la auditoría forense, y que se pueden acoplar al entorno tecnológico de la cooperativa en estudio.

Tabla 17: Herramientas para la recolección y adquisición de evidencia digital

Categoría	***Herramienta***	***Descripción***
Imágenes Forenses (Bit a Bit)	FTK Imager	Crea imágenes forenses de discos, USB, etc., en formatos E01, AFF, DD. Genera hashes para garantizar integridad (AccessData, 2023).
	EnCase Forensic Imager	Herramienta comercial con alta aceptación legal. Genera imágenes forenses completas, con documentación y hash (OpenText, 2021)
	Guymager	Código abierto. Crea imágenes forenses rápidas en formatos como EWF (DD Guymager, 2023).
	dd / dc3dd	Comando Unix/Linux para copias bit a bit. Usado en entornos forenses (Forensic Focus, 2020).
	X-Ways Forensics	Herramienta avanzada para adquisición, análisis y recuperación (X-Ways Software Technology AG, 2025).
	Magnet Acquire	Permite adquirir imágenes de discos, dispositivos móviles y memoria RAM (Magnet Forensics. 2023).

Captura de Evidencia Digital Volátil (RAM, Sesiones)	DumpIt / Belkasoft RAM Capturer	Captura el estado de la memoria RAM (procesos, sesiones, etc.) (Belkasoft, 2024.
	Magnet RAM Capture	Herramienta gratuita para volcado de memoria RAM. Compatible con análisis en Magnet AXIOM (Magnet Forensics. 2023).
	WinPMEM	Permite capturar memoria RAM para análisis forense (Rekall Team. 2021)
	Volatility Framework	Framework de análisis de memoria RAM para detectar procesos, conexiones de red, etc. (The Volatility Foundation, 2023).
Captura de Tráfico de Red	Wireshark	Captura y analiza tráfico de red en tiempo real. Muy usado en ciberseguridad y análisis forense (Orebaugh, A., et al., 2007).
	tcpdump	Captura paquetes de red en sistemas Linux/Unix. Útil en entornos forenses (Forensic Focus. 2020).
	NetworkMiner	Extrae artefactos como credenciales o archivos a partir de capturas de tráfico (Netresec. 2024)
	Xplico	Analiza tráfico de red y reconstruye sesiones HTTP, correos, etc. (Xplico.org, 2024)
Cálculo y Verificación de Hashes	HashCalc / MD5SUM / SHA256SUM	Generan y verifican hashes MD5/SHA. Permiten comprobar la integridad de archivos (Slay, J., & Koronios, A., 2006).
	Hashdeep	Verifica integridad de múltiples archivos mediante cálculo de hashes (ForensicWiki, 2023).
	FTK Imager / EnCase / X-Ways	Incluyen funciones de hash para verificación.
Dispositivos Móviles	Cellebrite UFED	Herramienta líder para extracción física, lógica y análisis de dispositivos móviles (Cellebrite, 2024).
	Magnet AXIOM	Suite integral para análisis de datos móviles, PCs y la nube (Magnet Forensics. (2023).
	Oxygen Forensics Detective	Extracción avanzada de datos de móviles y nube (Oxygen Forensics. 2024).

Elcomsoft Mobile Forensic Bundle	Extracción de datos cifrados, respaldos y análisis forense de móviles Elcomsoft. (2024).
MOBILedit Forensic Express	Captura de datos móviles con informes listos para tribunales Compelson Labs. (2023).

Es importante que el auditor documente la versión de la herramienta utilizada, y de preferencia mantener evidencias correspondientes (fotografías, grabaciones, capturas u otros), mismas que contribuyan a probar legitimidad a la hora de finalizar la auditoria.

Crear imágenes forenses (adquisición)

La creación de imágenes bit a bit (bitstream) es el método estándar en informática forense para preservar evidencia. Esta técnica garantiza la copia total del dispositivo, incluyendo sectores no utilizados, espacio libre, archivos eliminados, y datos residuales.

Con el listado de herramientas posibles para la creación de imágenes forenses, que se hicieron mención en la ***Tabla 10***, se debe trabajar exclusivamente sobre la copia forense y nunca sobre el original, dichas imágenes deben almacenarse en formatos forenses estándar como: E01, AFF y RAW (DD), también, como establece la norma ISO 27037, como una medida para asegurar la integridad, es el registro de hashes.

Adicionalmente, este proceso también incluye el uso de write blockers para evitar modificaciones accidentales.

Generación de hashes

Se refiere a una huella digital única, generada a partir de una entrada de datos, como un archivo, un disco duro o una imagen forense, aplicando un algoritmo de hash como MD5, SHA-1 o SHA-256 sobre una evidencia digital, y se obtiene una cadena alfanumérica única.

Este cálculo de hash es importante tenerlos en cuenta antes y después de la adquisición de la información, en el que se debe considerar lo siguiente:

- ***Antes (Pre- adquisición)***
    - Se calcula un hash sobre el dispositivo original antes de crear la imagen bit a bit.

- Este valor es el punto de referencia para demostrar el estado inicial de la evidencia.

- Después ***Antes (Post- adquisición)***

  - Se calcula el hash de la imagen forense creada.
  - Si el hash es idéntico al del original, se confirma que la copia es verídica, exacta e íntegra, caso contrario indica que existió algún cambio.

Tipo de hashes

En la actualidad se encuentran diversos métodos y algoritmos para la generación de hashes de imágenes forenses, el auditor informático puede optar por métodos como:

Tabla 18: Tipos de hashes

Algoritmo	Longitud de hash	Uso	Consideraciones
MD5	128 bits	Rápido, común en herramientas básicas.	Vulnerable a colisiones (evitar en casos críticos).
SHA-1	160 bits	Tradicional, mejor que MD5, aún en uso.	Vulnerable a ataques de colisión avanzados.
SHA-256	256 bits	Recomendado en auditoría forense.	Alta seguridad y resistencia a colisiones.
SHA-3	256+ bits	Última generación, resistencia avanzada.	Usado en contextos de alta seguridad.

Mantener la cadena de custodia

De acuerdo a la ISO/IEC 27037:2012, Sección 7.5.3, exige el uso de métodos documentados y verificables que respalden la integridad y autenticidad de la evidencia.

La cadena de custodia, es un proceso metódico y continuo, por lo que se necesita de una ejecución correcta, evitando fallos en el proceso que deriven a la invalidación total de la evidencia, y afecte con la investigación o auditoria.

Para este proceso, los elementos que se deben tomar en son:

Tabla 19: Elementos de la cadena de custodia.

Elemento	Descripción Detallada
Formulario de cadena de custodia	Documento oficial que acompaña la evidencia desde su recolección hasta su análisis. Incluye: • Identificación única de la evidencia • Quién la recolectó • Cuándo y dónde • Bajo qué condiciones • Firma del custodio entrante y saliente
Etiquetas de seguridad inviolables	Etiquetas adhesivas numeradas, con marcas a prueba de manipulación, colocadas en: • Dispositivos • Medios de almacenamiento • Sobres o maletas de transporte
Embalaje seguro	Uso de sobres antiestáticos, cajas con candado, embalaje opaco y sellado. Previene acceso no autorizado, daño físico o contaminación.
Almacenamiento controlado	Debe mantenerse en: • Gabinetes metálicos con llave • Cámaras de videovigilancia • Laboratorios forenses con acceso restringido (en caso de existir)
Control de acceso físico y lógico	Solo personal autorizado debe manipular la evidencia. Se recomienda: • Registro de entrada/salida •Autenticación biométrica o con credenciales • Políticas de acceso y firma electrónica
Trazabilidad digital (hashes)	Uso de funciones hash (SHA-256, SHA-1) antes y después de cada manipulación. Permite comprobar que no hubo alteración.

Manejo seguro de la evidencia digital

El manejo seguro de la evidencia digital garantiza que no se altere, corrompa, pierda o contamine la evidencia desde su recolección hasta su análisis. A diferencia de la evidencia

física, los datos digitales son extremadamente frágiles y pueden cambiar con solo abrir un archivo o conectar un dispositivo sin protección.

Por ello se debe aplicar como buenas prácticas, lo siguiente:

- Uso de medios cifrados para transporte (discos duros cifrados, dispositivos USB de solo lectura).
- Evitar la exposición a contaminantes (polvo, humedad, calor).
- Documentar la ubicación física de cada evidencia (gabinete, rack, locación, edificio, etc), se puede hacer uso de software de gestión de evidencia.
- Minimizar las manipulaciones: solo personal calificado debe acceder a la evidencia.
- Usar contenedores seguros para transporte (maletas con sellos inviolables). Esto preserva la integridad y evita la corrupción o pérdida accidental de datos.

Documentar el proceso

La documentación exhaustiva es un pilar en la recolección forense, en el que se deben considerar especificaciones técnicas que se deben enmarcar de manera cronológica para mantener una continuidad de los hallazgos y el fundamento apropiado para probar lo que se quiere dar a conocer en el dictamen final, por ello es importante considerar lo siguiente:

- Identificar quién realizó la acción (nombre, cargo, firma).
- Registrar la hora de inicio y fin de cada procedimiento.
- Detallar el dispositivo, incluyendo marca, modelo, número de serie, sistema operativo, versión, ubicación física.
- Especificar la herramienta forense utilizada (nombre, versión).
- Describir el tipo de evidencia recolectada (disco duro de servidor, logs, capturas de red).
- Incluir fotografías, si es posible, como respaldo visual.

Esta documentación puede mantener otras consideraciones adicionales acorde al criterio y la experiencia profesional del auditor informático, pero si deberá garantizar que

el proceso de recolección de evidencia digital cumpla con la repetibilidad y el aseguramiento de la cadena de custodia.

En este sentido, la documentación levantada, se convierte automáticamente en un insumo de entrada para alimentar el informe final de la auditoria.

Responsable: Auditor Informático **Insumo**: Formulario de cadena de custodia. **(Anexo 4),** Formulario para recolección y adquisición de evidencia **(Anexo 5).**

Solicitar requerimiento de información (Terceros)

Se debe tomar en cuenta que una auditoria informática forense, la recolección de la evidencia digital debe ser de manera presencial en la escena del incidente, solicitando información de manera formal y directa, sin embargo no todo el entorno de TI es manejado por un área de Tics, sino que también intervienen proveedores de servicios tecnológicos con los cuales la entidad mantiene relaciones comerciales sobre : administración de base de datos, infraestructura de red, canales y servicios, aplicaciones complementarias, entre otros; por ello esta fase es aplicable únicamente en la recolección de evidencias digitales de servicios provistos por terceros, por lo que se debe considerar lo siguiente

- El auditor informático debe realizar el documento del requerimiento a solicitar al área o responsables del servicio provisto, mismo que debe contener (área dirigida, responsable, detalle de la información, plazo de entrega y firmas de legalización, cálculo de hash).
- Especificar los medios seguros por la cual debe ser entregada al auditor informático, asegurándose que mantenga protocolos de seguridad de extremo a extremo (AES, RSA, SSL, etc.).
- En el requerimiento, se puede indicar que información específica sea extraída en presencia del auditor informático bajo los protocolos claros y permisos formales, haciendo uso de software remoto y forense en caso de requerir, además se deberá solicitar el cálculo de hash para no vulnerar la integridad de la evidencia.

- Indicar no hacer uso de canales inseguros o informales para el envío de información (WhatsApp, correos personales, plataformas sin cifrado, o transferencia directa sin autenticación).
- Asegurarse que la entidad cuente con documentos legales como: acuerdo de confidencialidad, uso y tratamiento de datos, y cláusulas que indiquen que el proveedor deberá estar dispuesto a colaborar en procesos investigativos y de auditoría, a fin de que no existan inconformidades a la hora de extraer la evidencia digital y así el proceso se vea interrumpido, perdiendo la eficacia de la auditoria en curso.

Nota: En caso de no ser necesario ni requerirse evidencia digital de terceros, se recomienda saltar al paso ***(11. Preservar la evidencia digital)***

Responsable: Auditor Informático (Solicitante) y Terceros (Remitente) **Insumo**: Documento de requerimiento (**Anexo**).

Enviar información requerida (Terceros)

La información debe prepararse bajo la gestión del Auditor Informático y el proveedor te servicios tecnológicos, directamente, en casos excepcionales, sin que se quebrante la efectividad de la auditoria, el área de Tics, podrá intervenir como un mediador que logre obtener evidencias digitales más claras, debido que por su recurrencia y frecuencia de interacción con los proveedores, se puede entender de mejor manera el trabajo que realizan lo terceros, y en esa forma obtener mejores resultados, por lo que se debe considerar lo siguiente:

- **Dispositivos físicos cifrados**: El proveedor podrá entregar la evidencia en un dispositivo de almacenamiento externo cifrado (discos duros, USB), en caso de tratarse de volúmenes grandes de información, por lo que aumenta la seguridad, sin que se exponga en internet.
- **Correo electrónico cifrado:** Uso de correo electrónico corporativo con cifrado de extremo a extremo (S/MIME, PGP), este se puede utilizar para volúmenes pequeños de información.

- **Plataformas seguras de transferencia de archivos:** Realizar la transferencia de información mediante protocolos seguros o plataformas cifradas (SFTP, FTP) o plataformas de uso corporativo que posea la entidad, ya que permite realizar seguimiento de la ruta de la información hasta el destino final.
- **Entrega física en sobre sellado:** En caso de requerirse, la entrega de dispositivos puede ser directamente o por mensajería con cadena de custodia
- **Acta o protocolo de entrega/recepción:** Generar acta de recepción-entrega, en el que se detalle, descripción de la evidencia, fecha y hora de entrega, medio utilizado, hash del archivo o imagen forense, nombre y firma del proveedor y del auditor.
- **Verificar integridad al recibir:** Comparar los valores hash enviados por el proveedor con los calculados localmente.
- **Registrar todo el proceso en la bitácora de la cadena de custodia**: Se debe incluir capturas, logs y comunicaciones oficiales, en la bitácora de registro.

Responsable: Auditor Informático y Proveedor de TI **Insumo**: Acta Entrega-Recepción (Anexo)

4.3.7 Preservar la evidencia digital

En esta etapa después de realizar la recolección de evidencia, se de forma directa o mediante solicitud a proveedores (en caso de requerir), se deber garantizar que la evidencia recolectada no sea alterada, contaminada, destruida o accedida por personas no autorizadas, asegurando su validez durante todo el proceso de auditoría, análisis, y en caso necesario, ante procesos legales, para efecto se debe utilizar ciertos elementos que podrán contribuir con la preservación de la evidencia, que son:

Almacenamiento en entornos seguros

La evidencia digital debe almacenarse en discos duros externos cifrados, servidores forenses dedicados o almacenamiento en red (NAS) con cifrado activo.

- **Validación de formatos forenses**

Por buenas prácticas forenses, como se mencionó en el ítem ***4.4.7.1 (Crear imágenes forenses)***, se debe estandarizar el uso de los formatos de archivos forenses (E01, AFF, RAW), siendo un esquema que se debe cumplir hasta para su almacenamiento.

- **Copias de seguridad**

Se deben generar copias forenses de respaldo y almacenarlas en ubicaciones seguras diferentes (principio de duplicidad), cada copia debe tener sus hashes verificados y estar registrada.

Protección del acceso (físico y digital)

En cuanto al espacio físico o sala donde se almacena la evidencia debe tener acceso restringido (biometría, cerraduras electrónicas), monitoreado (videovigilancia), así mismo a nivel digital, los accesos en los contenedores deben gestionarse con autenticación de múltiples factores (MFA), o en su medida contar con niveles de acceso solo para personal autorizado, mimos que se encuentran definidos en el ítem ***4.4.5 Planificar la auditoria forense a ejecutar (Roles y Responsabilidades)*** y mantener un control en la trazabilidad total.

Cadena de custodia digital

Cada vez que se utilice, o se acceda a la evidencia digital almacenada, se debe actualizar los registros de la cadena de custodia, quedando en evidencia quién, cuándo, cómo y para qué se ha accedido, transportado o manipulado la evidencia, también se debe considerar lo siguiente:

- Número único de identificación de la evidencia (etiqueta).
- Hash antes y después de cada manipulación (verificación de integridad).
- Formularios firmados física o digitalmente (puede usarse firma electrónica.

Responsable: Auditor informático **Insumo**: Formulario de cadena de custodia.

Ejecutar análisis forense

Esta etapa se considera una de las más importantes donde se interpreta la evidencia digital recolectada para identificar incidentes, vulnerabilidades, actores, métodos utilizados y el posible impacto reputacional en la organización. En otras palabras, transforma los datos técnicos en hallazgos significativos y defendibles en un proceso investigativo o pericial, dependientemente del objetivo de la auditoría.

Cada auditoria mantiene un objetivo que se quiere lograr y un alcance que delimita la investigación, por lo que este modelo, es un proceso que va en función a cada tipo de incidente que se requiere resolver y obtener resultados precisos que dictaminen un resultado o juicio de valor, en ese sentido se plantea carios tipos de análisis de diferentes elementos del ecosistema tecnológico de la entidad, que son:

Tabla 20: Aspectos clave de análisis forense

Componente Tecnológico	Función Principal	Aspectos Clave del Análisis Forense	Herramientas/Técnicas Recomendadas
Servidores	Alojan servicios críticos como autenticación (AD), aplicaciones y bases de datos.	- Revisión de logs del sistema (eventos, acceso, errores). - Servicios activos y tareas programadas sospechosas. - Comparación de integridad de archivos del sistema.	- Event Viewer, journald, FTK Imager, Autopsy, OSSEC.
Bases de Datos	Contienen información sensible: transacciones, usuarios, auditoría.	- Análisis de logs SQL (consultas maliciosas, accesos). - Identificación de cuentas manipuladas. - Integridad de los registros. - Detección de inyecciones SQL.	- ApexSQL Audit, RedGate, pgBadger, MySQL Enterprise Audit, Oracle Audit Vault.
Firewalls e IDS/IPS	Protegen el perímetro, detectan amenazas y actividades anómalas.	- Revisión de reglas de filtrado. - Alertas sobre ataques detectados. - Tráfico no autorizado o fuera de horario. - Exfiltración de datos.	- Snort, Suricata, FortiAnalyzer, pfSense, Cisco Firepower.
Endpoints (PCs, laptops)	Interfaz directa del usuario con los sistemas.	- Análisis de programas - ejecutados. - Dispositivos USB conectados. - Búsqueda de malware o RATs. - Cache de navegador y contraseñas.	- Autopsy, EnCase, FTK Imager, Volatility (RAM), USBDeview.

Componente Tecnológico	Función Principal	Aspectos Clave del Análisis Forense	Herramientas/Técnicas Recomendadas
Dispositivos móviles (teléfonos, USBs, discos)	Pueden contener información sensible o usarse como vector de fuga.	- Revisión de llamadas, chats, apps. - Archivos extraídos/subidos. - Conexiones VPN o remotas no autorizadas.	- Cellebrite UFED, MOBILedit, Oxygen Forensics, XRY.
Red LAN	Conecta internamente la infraestructura y dispositivos.	- Segmentación de redes. - Logs de switches y routers. - Dispositivos sospechosos conectados.	- Nmap, Wireshark, tcpdump, Cisco NetFlow, ARPwatch.
VPN	Canal seguro para conexiones remotas.	- Logs de túneles cifrados. - Autenticaciones sospechosas (horario, IP). - Revisión de configuración.	- FortiClient logs, OpenVPN logs, Elastic Stack.
Wi-Fi	Conexión inalámbrica interna.	- Validación de seguridad (WPA2/WPA3, ocultación SSID). - Control de dispositivos conectados. - Revisión de MAC spoofing.	- Kismet, Aircrack-ng, Fing, WiFi Analyzer.

Responsable: Auditor Informático

4.3.8 Elaborar el informe de trazabilidad de cada hallazgo

Una vez realizado el análisis forense, esta etapa se torna complementaria e importante a la vez, ya que se elabora el informe de los detalles del proceso de auditoría forense de forma clara, detallada y estructurada; así mismo se aplica la trazabilidad para lograr rastrear cada hallazgo o conclusión forense hasta la evidencia específica de donde proviene, asegurando que no haya inferencias sueltas, sino que cada conclusión sea verificable con base técnica rastreable.

En ese contexto, se debe se debe considerar varios elementos para la documentación, tales como:

Tabla 21: Elementos de la documentación del análisis forense

Elemento Documentado	Contenido
Metodología usada	Normas aplicadas (ej. ISO/IEC 27037), procedimientos de adquisición, análisis y preservación.

Elemento Documentado	Contenido
Herramientas utilizadas	Nombre, versión, fabricante y propósito de cada herramienta forense.
Pasos ejecutados	Cronología exacta de las acciones (extracción, análisis, hallazgos, reportes).
Hallazgos técnicos	Logs, capturas de tráfico, hashes, malware detectado, conexiones sospechosas, etc.
Firmas digitales o hashes	Verificación de integridad para imágenes forenses y evidencia digital.
Responsables	Quién ejecutó cada acción, en qué fecha, y con qué autorización.

Aquí se puede evidenciar un ejemplo de la trazabilidad de un hallazgo, por lo que en este sentido se debe hacer para todos los hallazgos resultantes del análisis forense:

Tabla 22: Ejemplo de trazabilidad de un hallazgo (Matriz de trazabilidad)

Hallazgo/ Ejemplo	Evidencia Asociada	Herramienta Usada	Resultado
Usuario accedió fuera de horario desde IP externa	Log de firewall + log de autenticación	Wireshark y Syslog analyzer	Conexión no autorizada detectada
Archivo modificado con malware	Imagen forense del disco	FTK Imager y Autopsy	Archivo invoice.exe alterado

Responsable: Auditor Informático

Insumo: Matriz de trazabilidad de hallazgos (Anexo)

4.3.9 Desarrollar el informe de la auditoria forense

En este apartado, como resultado de la auditoria forense efectuada, el auditor informático elabora un informe puntual y esquematizado con todos los elementos que formaron parte de dicha auditoria, por ello el documento debe mantener la formalidad y capacidad de transmitir resultados concisos, otorgando una validez probatoria en procesos legales, disciplinarios, judiciales, e internos de la institución, para de esa manera emitir un juicio de valor que determine actores, actividades sospechosas, procedimientos ejecutados malintencionados, accesos no autorizados, intentos de/o fraudes financieros y otras actividades que afecten con la reputación de la cooperativa.

Este informe se convierte en un registro formal del proceso de auditoría, lo que garantiza la transparencia, integridad y legalidad del procedimiento.

Para la redacción de este documento, es importante que el auditor recopile y trabaje en base a la información que se encuentra levantándose desde la etapa ***4.4.5 Planificar la auditoria a ejecutarse***, donde se determinan elementos clave (objetivo, alcance, recursos, responsabilidades, cronogramas, etc), por lo que estos parámetros se deben considerar en este informe, no obstante, una estructura correcta de un informe, se establece de la siguiente manera:

- Oficio dirigido a gerencia
- Resumen ejecutivo
- Objetivos y alcance
- Metodología aplicada
- Herramientas utilizadas
- Evidencia recolectada
- Análisis técnico detallado
- Hallazgos forenses
- Conclusiones
- Recomendaciones
- Anexos técnicos (logs, capturas, imágenes, hashes, etc)

Es importante mencionar que esta etapa es la recopilación de los insumos de cada una de las etapas (Procedimientos) anteriores que tienen como resultado un documento o registro de información que es importante para el proceso de auditoria informática forense.

Responsable: Auditor Informático **Insumo**: Informe final

CAPITULO V

5 CONCLUSIONES

Del trabajo realizado se han desprendido las siguientes conclusiones:

- Se ha logrado analizar y contrastar dos metodologías orientadas al análisis forense de sistemas informáticos y elementos tecnológicos, cada una con enfoques complementarios que fortalecen el proceso de recolección, preservación y manejo de la evidencia digital. La integración de la rigurosidad técnica y procedimental propuesta por Velarde (2025) con las directrices internacionales establecidas en la norma ISO/IEC 27037 ha permitido conformar un marco metodológico integral, coherente y estructurado. Este marco no solo asegura la integridad y autenticidad de la evidencia digital recolectada, sino que también garantiza su validez y admisibilidad en contextos investigativos, judiciales y de fiscalización. Asimismo, se establece como una guía robusta y adaptable a las necesidades particulares del proceso de auditoría informática forense dentro de la institución financiera en estudio, ofreciendo un enfoque sistemático, confiable y alineado con las mejores prácticas internacionales.

- Mediante el análisis de una base histórica de eventos considerados riesgosos y críticos en la operatividad de la Cooperativa de Ahorro y Crédito Artesanos, se ha logrado determinar que el nivel de incidentes que poseen un perfilamiento con las características compatibles de fraude financiero mediante el uso de los sistemas informáticos y aplicaciones complementarias, concentrándose en un nivel de riesgo (medio-alto, y alto), ya que son eventos que de acuerdo a la naturaleza del giro de negocio siempre estarán presentes, más aún cuando los procesos operativos interviene la manipulación humana, que debido a errores no intencionados y otras que si han sido producto de faltas éticas y de principios profesionales se ha convertido en eslabones de seguridad de la información, estos eventos de riesgo cada vez reaparecen con diferentes enfoques y grado de afectación, que al estar globalizados en una era tecnológica y accesibilidad a la información y herramientas, hacen uso de estas para ejecutar fraudes electrónicos.

- Se ha planteado un modelo de auditoría informática forense orientado a fortalecer los procesos de investigación digital dentro del contexto organizacional de la Cooperativa de Ahorro y Crédito Artesanos. Este modelo incorpora una

metodología integral que abarca de forma sistemática todas las fases críticas del manejo de la evidencia digital: identificación, recolección, preservación, análisis y documentación, esta propuesta se articula con un enfoque holístico, que no solo cumple con estándares técnicos y normativos, sino que también responde a las particularidades operativas, tecnológicas y de seguridad de la institución financiera en estudio. Cada etapa del modelo ha sido detalladamente estructurada, iniciando desde la detección e identificación de un incidente informático hasta la elaboración de un informe forense final, con carácter probatorio, válido y sustentable que determinar con precisión la existencia de actividades sospechosas, identificar actores y responsables, establecer niveles de complicidad, rastrear accesos no autorizados, evidenciar transacciones fraudulentas, detectar ataques intencionados, documentar errores inducidos y tipificar diversas formas de fraude digital que puedan comprometer la integridad, continuidad operativa y reputación de la entidad.

6 RECOMENDACIONES

De igual forma se han desprendido las siguientes recomendaciones:

- Se recomienda realizar una validación práctica del marco metodológico integrado (Velarde, 2025 y la ISO/IEC 27037) mediante estudios de caso o auditorías piloto dentro de la institución financiera, con el objetivo de identificar posibles brechas entre el diseño teórico y la aplicación operativa, así como ajustar procedimientos en función de los recursos, capacidades y limitaciones del entorno, logrando de esa manera tener una metodología eficiente y optima para considerarse estandarizarla en diferentes escenarios de investigación forense enfocado a entornos tecnológicos.

- En cuanto al análisis de datos históricos de eventos de riesgo, se recomienda implementar un sistema de gestión de riesgos informáticos basado en técnicas de análisis predictivo, que permita anticipar escenarios de fraude digital y fortalecer los controles preventivos, especialmente aquellos relacionados con la intervención humana y la manipulación ética de la información, logrando el control y mitigación del impacto del riesgo reputacional de la entidad, el cual es uno de los riesgos que mayor daño y afectación genera.

- Se recomienda institucionalizar el modelo de auditoría informática forense a través de su incorporación en el marco normativo interno de la cooperativa, respaldado por normativa interna, manuales, y estructuras de gobierno. Esta institucionalización debe estar acompañada por la creación de una unidad especializada en informática forense integrada por profesionales capacitados en investigación digital, derecho informático, ciberseguridad y auditoría.

7 REFERENCIAS BIBLIOGRÁFICAS

AccessData. (2023). FTK Imager in Digital Forensic. Obtenido de: https://sis.binus.ac.id/2023/09/20/ftk-imager-in-digital-forensic/

Albarrán, S., Pérez, J., Salgado, M., & Valero, L. (2019). *Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares.*

Asamblea Bacional del Ecuador. (2021). *CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP*. Obtenido de https://www.defensa.gob.ec/wp- content

Baracaldo, D. F. R.(2022) RESPONSABILIDAD CIVIL EN EL SISTEMA FINANCIERO FRENTE A FRAUDES Y/O TRANSACCIONES ELECTRÓNICAS EN COLOMBIA

Belkasoft. (2024). RAM Capturer. Obtenido de: https://belkasoft.com/ram-capturer

Beltrán, K (2020) MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

Bhaskar, L. S., Schroeder,J. H., & Shepardson, M. L. (2019). Integration of internal control and financial statement audits: Are two audits better than one? The Accounting Review,94(2), 53-81. https://meridian.allenpress.com/accounting-review/article-abstract/94/2/53/11799

Caraguay Ramírez, S. X. (2020). Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019. Estado & *Comunes*,*2*(11),135–153. *Tomado de https://doi.org/10.37228/estado_comunes.v2.n1-1.2020.178.*Cellebrite. (2024). UFED Product Overview. Obtenido de: https://www.cellebrite.com/en/ufed-ultimate/

Díaz, G. (2021). *LA AUDITORÍA FORENSE COMO FUNDAMENTO METODOLÓGICO EN LA DETECCIÓN DE CASOS DE FRAUDES*

Elcomsoft. (2024). Mobile Forensic Bundle. Obtenido de: https://www.mobiledit.com/forensic

Enríquez, P., & Argota, J. (Octubre de 2015). *Descripción interpretativa para la elaboración del perfil de tesis de investigación científica con enfoque cualimétrico (mixto).* Obtenido de https://www.usmp.edu.pe/campus/pdf/revista22/

Farfan, J. (2024). *SO 27037:2012 PARA MEJORAR EL ANÁLISIS INFORMÁTICO FORENSE EN LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA POLICÍA NACIONAL DEL PERÚ.* Obtenido de https://hdl.handle.net/20.500.13084/9138

FATF – Interpol - Egmont Group (2023), Flujos financieros ilícitos procedentes del fraude cibernético, FATF, Paris, France, tomado de: www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html

Fernández, E. E. C., Herrera, R. D. J. G. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional. NOVUM, revista de Ciencias Sociales Aplicadas, 1(10), 61-80.

Forensic Focus. (2020). Linux 'dd' basics. Obtenido de: https://www.forensicfocus.com/articles/linux-dd-basics/

Forensic Focus. (2020). tcpdump for Forensic Use. Obtenido de: https://www.forensicfocus.com/articles/tcpdump-for-forensic-use/

ForensicWiki. (2023). Hashdeep. Obtenido de: https://forensicswiki.xyz/wiki/index.php?title=Hashdeep

Gioia, C. (2021). *Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos*. Obtenido de https://repositoriocyt.unlam.edu.ar/

Guymager. (2023). Guymager homepage. Obtenido de: https://guymager.sourceforge.io/

Habib, A., Ranasinghe, D., Muhammadi, A. H., & Islam, A. (2018). Political connections, financial reporting and auditing: Survey of the empirical literature. Journal of International Accounting, Auditing and Taxation,31, 37-51. https://www.sciencedirect.com/science/article/pii/S1061951818301149

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jesús, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión

sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação,* (E32), 427-440.

INFORMÁTICOS. Obtenido de https://dialnet.unirioja.es

Interpol. (2022). Inerpol. Obtenido de https://www.interpol.int/es/Delitos/Delincuencia-financiera/Papel-de-INTERPOL-en-la-lucha-contra-la-delincuencia-financiera

ISO/IEC. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and identification, collection, acquisition, and* .

Lema, J. (2019). *LA AUDITORÍA FORENSE COMO TÉCNICA PARA DETECTAR HALLAZGOS EN EL SECTOR BANCARIO DEL ECUADOR.*

Lopez Vilcas, C. R. C., & Salazar Caldas, J. B. La auditoría forense como herramienta de prevención de riesgos reputacionales en las principales empresas constructoras de Miraflores y San Isidro, años 2017-2019.

López, V. (2020). La auditoría forense como herramienta de prevención de riesgos reputacionales en las principales empresas constructoras de Miraflores y San Isidro, años 2017-2019. Obtenido de https://repositorioacademico.upc.edu.pe/bitstream-/handle/10757/658316/Lopez_ VC.pdf?sequence=3&isAllowed=y

Magnet Forensics. (2023). Magnet Acquire. Obtenido de: https://www.magnetforensics.com/resources/magnet-acquire/

Magnet Forensics. (2023). Magnet AXIOM Product Page. Obtenido de: https://www.magnetforensics.com/products/magnet-axiom/

Magnet Forensics. (2023). Magnet RAM Capture. Obtenido de: https://www.magnetforensics.com/resources/magnet-ram-capture/

Mahecha, L. H. M. (2022). Auditoría Forense.: Una guía práctica para la excelencia en la ciencia, auditoría e informática forense. Ediciones de la U.

Maldonado, J. (2021). *Estrategias para la prevención de fraudes en el Sector Financiero Popular y Solidario*. Obtenido de https://www.primicias.ec/branded/ciberseguridad-fraude-financiero-prevencion-

80509/.Netresec. (2024). NetworkMiner. Obtenido de: https://www.netresec.com/?page=NetworkMiner

OpenText. (2021). EnCase Forensic Product Overview. Obtenido de: https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-po-encase-forensic-en.pdf

Orebaugh, A., et al. (2007). Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress.

Oxygen Forensics. (2024). Oxygen Forensic Detective. Obtenido de: https://oxygenforensic.com/

Rekall Team. (2021). WinPMEM Documentation. Obtenido de: https://github.com/Velocidex/WinPmem

Rey, D. (2022). *RESPONSABILIDAD CIVIL EN EL SISTEMA FINANCIERO FRENTE A FRAUDES Y/O TRANSACCIONES ELECTRÓNICAS EN COLOMBIA.*

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. Revista Conrado, 17(78), 343-35. Tomado de: *http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343&lng=es&tlng=es.*

Saltos Salgado, Marco Fernando, Robalino Villafuerte, José Luis, & Pazmiño Salazar, Lenin Darío. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343-351. Epub 02 de febrero de 2021.

Saltos, M., Robalino, J., & Pazmiño, L. (2021). ANÁLISIS CONCEPTUAL DEL DELITO INFORMÁTICO EN ECUADOR. Tomado de http://scielo.sld.cu/scielo.php?pid=-s1990-6442021000100343&script=sci_arttext.

Slay, J., & Koronios, A. (2006). Information Systems Forensics.

Superintendencia de Economía Polpular y Solidaria. (Junio de 2021). *SITUACIÓN DE LOS SERVICIOS FINANCIEROS DIGITALES Y SEGURIDAD DE LA INFORMACIÓN EN EL SFPS.* Obtenido de ttps://www.seps.gob.ec/wp-content/uploads/Formato-DNIC-Estudio-de-servicios-financieros-digitales-y-seguridad-informacion

The Volatility Foundation. (2023). Volatility. Obtenido de: https://volatilityfoundation.org/

Trujillo, S. E. A., Merlos, J. C. P., Gallegos, M. S., & Conzuelo, L. L. V. (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.

Velarde, K. (3 de Enero de 2025). *Diseño de una metodología de análisis forense informático para la Cámara de Diputados de Bolivia*. Obtenido de https://revistarebi.org/index.php/rebi/article/view/1561

Xplico.org. (2024). Xplico Open Source Network Forensic Analysis Tool.

X-Ways Software Technology AG. (2025). X-Ways Forensics Manual. Obtenido de: https://www.x-ways.net/winhex/manual.pdf

International Organization for Standardization. (2018). *ISO 19011:2018 – Guidelines for auditing management systems*. ISO.

8 ANEXOS

Anexo 1. Matriz de Riegos de incidentes o eventos de riesgos.

Incidentes por áreas	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Acción	Estrategia
Cumplimiento						
Incumplimiento en la entrega de información hacia terceros						
- Deficiencias en controle de cuentas inactivas y pasivos inmovilizados	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Financiero						
Cortes en los servicios públicos						
- Agencias vulnerables al presentar daño en el sistema de videovigilancia y en el sistema de accesos	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
Errores en introducción de datos, mantenimiento o descarga						
- Error de procesamiento de valores de transacciones	4	4	16	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
- Incremento sin autorización de tasa pasiva para depósitos a plazo fijo que sobrepasa los límites establecidos.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Que el socio no este con cobertura vigente	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Sistema de grabación y almacenamiento de imágenes sin respaldos ante incidentes en instalaciones de las agencias	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
Hurto/extorsión/malversación/robo						
- Asalto, robo, extorsión de terceros	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Exposición de la oficina a errores operativos y/o actividades ilícitas que no puedan ser verificadas debido a cámaras videovigilancia con tarjeta de video dañada.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Hurto/robo (fuente externa)						
- Incidente de posible asalto en el traslado de valores	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Inapropiada utilización de información confidencial						
- Posible pérdida de documentos con información crítica por falencias en seguridad física en lugares de almacenamiento.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo

Operaciones no reveladas/registradas (intencionalmente)						
- Exista diferencias, sea faltante o sobrante.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Pérdidas por desastres naturales, terrorismo, vandalismo, etc.						
- Daño en infraestructura de agencia y en equipos tecnológicos.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Registros incorrectos de socios y clientes						
- Que tenga una enfermedad preexistente	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Utilización de cheques sin fondos (Fuente externa)						
- Fraude externo por Confirmación de depósito de cheque sin constatar disponibilidad de fondos.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Negocios						
Acceso no autorizado a cuentas						
- Denuncia por movimiento no autorizado de cuentas de ahorros.	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
- Denuncias por movimientos de fondos en cuentas de socios sin autorización.	4	4	16	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Actividades no autorizadas						
- Pérdida de confianza por parte de socios de crédito en la cooperativa	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Sustracción o pérdida de dinero de socios entregado a funcionarios sin el debido respaldo.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Documentos jurídicos incompletos/inexistentes						
- Autorizar una inversión sin verificar el origen lícito de los fondos presentados por el socio para el DPF.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Documentos desactualizados	3	2	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Falta de documentación, incompleta, desactualizada	3	2	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.

- Invalidez de pagarés que respalden procesos de cobranza	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No contar con la aprobacion de los representantes de la cuenta de firmas conjuntas	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Pérdida de documentos de crédito por inadecuado archivo.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Realizar el cambio de la informacion sin el documento de sustento	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Realizar transacciones sin contar con los requisitos necesarios.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Recursos que ingresan mediante SPI a la Cooperativa sin formulario de licitud de fondos regularizada	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Requisitos caducados en DPF	4	2	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Errores en introducción de datos, mantenimiento o descarga						
- Acreditar valores de operaciones de socios a cuentas que no le corresponden	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Al liquidar el crédito novado se acredita el monto total a la cuenta del socio, de tal manera que, si el personal operativo no realiza la precancelación del crédito anterior, el socio podría retirar todo el dinero, quedando activos dos créditos.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Al negociar una tasa de inversión y realizar el DPF por otra diferente, afectamos a las ganancias esperadas	3	2	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Control deficiente de comprobantes de recaudación	4	2	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Crédito en mora por depósito de valores recaudados en cuenta de ahorros incorrecta.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Débito de valores a socios que no corresponden	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Doble acreditación en cuenta	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos

- Documentos de expediente de crédito con detalle de tipo de garantía incongruente a la solicitud de crédito.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Error de digitación de información	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Faltante de dinero en bóveda por egresos realizados y no registrados.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Identificar inconsistencias de la información durante la validación	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Error en ingresos de información de cheque	2	3	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Modificación de información de socios sin realizar el procedimiento correspondiente debido a la accesibilidad del personal operativo.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No actualizar datos conforme establece el proceso de captaciones	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No digitalización de firmas en el sistema	2	1	2	Bajo	Aceptar	No adoptar ninguna acción para controlar, intentar mitigar en su medida
- Reclamos de beneficiarios de bono de desarrollo humano, por cobros	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Fallas en la entrega de información						
- No lograr tener contacto con las personas de referencias mencionadas.	1	2	2	Bajo	Aceptar	No adoptar ninguna acción para controlar, intentar mitigar en su medida
- Re proceso de operaciones de crédito tras ser dadas de baja	2	3	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Reclamo de socios por movimiento de cuentas no autorizados debido a que aduce no ser su firma,	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
Falsificación (Fuente externa)						
- Recaudación de valores en campo mediante comprobantes de recaudación haciendo uso fraudulento de la imagen de la Cooperativa	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Requisitos falsos en DPF	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
- Suplantación de identidad	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Falsificación (Fuente interna)						

- Falsificación de papeleta de retiro para movimientos de cuentas de socios.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Fraude interno en colocación de crédito	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Falta de difusión y comunicación de políticas						
- Demora en realización de transferencias	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No entregar TD en los tiempos establecidos.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No realizar la confirmación de datos o información del socio	2	3	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- Sobrepasar la tasa establecida	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Fraude						
- Fraude interno en colocación de créditos con baja probabilidad de recuperación	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Hurto/extorsión/malversación/robo						
- Fraude interno por desvío de fondos de cuentas inactivas de socios	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Hurto/robo (fuente externa)						
- Existencia de objetos extraños en el cajero	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
- Fraude externo en área de cajas.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Inexistencia de autorizaciones						
- Cierre de cuentas de ahorro o aportación sin las debida autorización formal.	2	1	2	Bajo	Aceptar	No adoptar ninguna acción para controlar, intentar mitigar en su medida
- Efectivización de cheques sin autorización	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Entregar estados de cuenta a persona que no es el titular sin autorización, o documento no firmado	2	2	4	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
- No exista la aprobación correspondiente para el incremento de tasa.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia

						al transferir o compartir parte del riesgo
- No tener autorización para el procedimiento de bloqueos y desbloqueos	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Que la apertura de cuenta a un menor de edad no sea gestionada por el padre de familia o representante legal	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
- Realizar el cierre de cuentas por terceras personas sin autorización	2	1	2	Bajo	Aceptar	No adoptar ninguna acción para controlar, intentar mitigar en su medida
- Realizar el pago a una tercera persona sin la debida autorización	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Operaciones no autorizadas (con pérdidas pecuniarias)						
- Desvío de fondos por confirmación de depósitos.	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Operaciones no reveladas/registradas (intencionalmente)						
- Cargar el dinero en bandejas diferentes a las establecidas para cada denominación	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
- No comunicar las diferencias encontradas	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No identificar o no registrar diferencias, sea faltante o sobrante.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- No reportar sobrantes o faltantes	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Quebrantamiento de la privacidad de información, sobre socios, clientes y usuarios						
- Mal uso de la información de captaciones reservada de la entidad	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
- Movimientos no autorizados o sin conocimiento del titular de la cuenta mediante banca electrónica, debido a el registro de correo electrónico del funcionario de la institución y no del socio.	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Riesgos						
Documentos jurídicos incompletos/inexistentes						

- Crédito sin garantía	2	4	8	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Fallas en la entrega de información						
- Al opera con usuarios compartidos no se pude identificar en realidad quien realizó las transacciones de caja y se pueden realizar operaciones no autorizadas.	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Fallos de contrapartes (proveedores)						
- Fuga de información de proveedor de software	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Inexistencia de autorizaciones						
- Documentos contractuales y de alta confidencialidad inválidos.	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Operaciones no autorizadas (con pérdidas pecuniarias)						
- Fraude interno/externo en banca electrónica	3	4	12	Alto	Mitigar/Evitar	Ejecutar acciones para reducir o minimizar probabilidad de ocurrencia y el impacto, o a su vez descontinuar actividades que generen dichos riesgos
Sistemas						
Cortes en los servicios públicos						
- Duplicidad de transacciones por error lógico	3	2	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
Errores en introducción de datos, mantenimiento o descarga						
- Diferencias en cobro de rubros correspondientes a seguro de desgravamen en operaciones de crédito precanceladas	3	2	6	Medio	Monitorear	Monitorear constantemente las acciones que pueden generar el riesgo, hay que adoptar medidas correctivas de manera oportuna.
Fallas en el software						
- Sincronización inestable entre tablas contables de transacciones del core financiero	3	3	9	Medio-Alto	Transferir	Tomar acciones para reducir su impacto o disminuir la probabilidad de ocurrencia al transferir o compartir parte del riesgo
Fallos de contrapartes (proveedores)						
- Pérdida de respaldos de correos electrónicos	2	1	2	Bajo	Aceptar	No adoptar ninguna acción para controlar, intentar mitigar en su medida
Total					**84**	

Anexo 2: Formato de documento preliminar.

COOPERATIVA DE AHORRO Y CRÉDITO artesanos

trabajando tu futuro

Objetivo

Antecedentes

Alcance

- Equipos, sistemas y redes involucrados
- Roles y responsabilidades
- Recursos humanos, materiales
- Cronogramas

Anexo 3. Fuentes de evidencia digital

COOPERATIVA DE AHORRO Y CRÉDITO artesanos

trabajando tu futuro

COOPERATIVA DE AHORRO Y CRÉDITO ARTESANOS

Departamento de Auditoría Interna

Lugar:

Fecha:

Responsable:

Matriz de identificación de fuentes de evidencia digital.

No.	Fuente de Evidencia Digital	Ubicación Física / Lógica	Tipo de Dato (Volátil / No-volátil)	Observaciones / Relevancia
1				
2				
3				
4				
5				
6				
7				
8				
9				

Nota: Esta matriz debe actualizarse cada vez que se identifique una nueva fuente de información o se modifique la infraestructura tecnológica. La información debe ser verificada con el área de TI y documentada bajo cadena de custodia para auditoría.

Firma Responsable

Auditor Informático

Firma - área auditada

Jefe de Tics (Ejemplo)

Anexo 4. Formulario de cadena de custodia

COOPERATIVA DE AHORRO Y CRÉDITO ARTESANOS

FORMULARIO DE CADENA DE CUSTODIA DE EVIDENCIA DIGITAL - AIF-CC-001	
1. DATOS DE IDENTIFICACIÓN DE LA EVIDENCIA	
Código de Evidencia	
Descripción de la Evidencia	
Tipo de Evidencia	
Medio de Almacenamiento	
Hash de Integridad	
Fecha y Hora de Recolección	
Recolectado por (Nombre, Cargo, Firma)	
Herramienta utilizada	

2. REGISTRO DE TRANSFERENCIA DE CUSTODIA

Nº	Fecha y Hora	Responsable (Entrega)	Firma (Entrega)	Responsable (Recepción)	Firma (Recepción)	Motivo / Ubicación Final
1						
2						
3						
4						
5						

3. CONDICIONES DE LA EVIDENCIA	
¿La evidencia fue sellada?	
¿Se utilizó bolsa/sello de seguridad? Código:	
¿Presenta daños visibles?	
¿Hubo apertura o manipulación?	
Observaciones adicionales	

4. OBSERVACIONES FINALES

Describir cualquier incidente, irregularidad, hallazgo o comentario relevante sobre el manejo de la evidencia.

Anexo 5. Formato para documentar la recolección y adquisición de evidencia

COOPERATIVA DE AHORRO Y CRÉDITO ARTESANOS

Departamento de Auditoría Interna

FORMULARIO DE RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL

1. Datos generales:

Ítem	Descripción
Código de procedimiento	Ej. AIF-RAD-001
Fecha de ejecución	dd/mm/aaaa
Hora de inicio	hh:mm
Hora de finalización	hh:mm
Responsable del procedimiento	Nombre completo, cargo, firma
Acompañante/s (si aplica)	Nombre(s), cargo(s), firma(s)
Lugar de ejecución	Dirección física o ubicación lógica

2. Datos de la evidencia:

Ítem	Detalle
Dispositivo o fuente intervenida	Ej. Servidor de archivos, Estación de trabajo, Router
Número de serie / etiqueta	Código identificador único
Sistema operativo / versión	Windows 10, Ubuntu 22.04, etc.
Herramienta utilizada	Ej. FTK Imager, Autopsy, dd, EnCase, etc. (incluir versión)
Método de adquisición	Imagen forense completa / Copia lógica / Exportación controlada
Medio de almacenamiento destino	Disco externo cifrado, USB etiquetado, etc.
Aplicación de Write Blocker	Sí / No – Describir tipo (hardware/software)

3.Registro de integridad de evidencia:

Ítem	Valor
Hash del original	Ej. SHA-256: 1234ABCD5678...
Hash de la copia	Ej. SHA-256: 1234ABCD5678... (debe coincidir)
Algoritmo utilizado	SHA-256 / SHA-1 / MD5 (especificar)
Fecha de cálculo	dd/mm/aaaa

4. Observaciones del Procedimiento

Aquí se debe registrar cualquier novedad, hallazgo preliminar, interrupciones, anomalías observadas, o condiciones especiales del entorno (ej. evidencias fragmentadas, equipos en red, intento de encubrimiento, etc.).

5. Confirmación y custodia

Ítem	Detalle
Medio de almacenamiento custodiado	Ej. HDD externo – Etiquetado con código “EVD-001”
Responsable de la custodia	Nombre completo, cargo
Ubicación segura de almacenamiento	Ej. Laboratorio Forense, Sala de custodia / Bóveda de TI
Fecha y hora de entrega	dd/mm/aaaa – hh:mm
Firma del responsable de entrega	
Firma del responsable de recepción	

6. Anexos

Se debe adjuntar, fotografías del procedimiento (si aplica), capturas de pantalla de la herramienta utilizada, logs del proceso de adquisición y registro de cadena de custodia inicial