ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESQUEMA DE SEGURIDAD EN LA GESTIÓN Y CONTROL EN LA CUSTODIA DE EVIDENCIAS DIGITALES DEL ÁREA DE CONTROL DE TRÁNSITO DE LA EMOV-EP"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

Verónica Alexandra Guamán Reibán

Eduardo Roberto Williams Cascante

GUAYAQUIL – ECUADOR

2017

AGRADECIMIENTO

A Dios por conducir siempre nuestro camino profesional, a nuestras familias por ser un apoyo incondicional, a nuestras amistades por el intercambio de ideas y a nuestra tutora por su colaboración y guía aportada para el desarrollo de esta tesis.

DEDICATORIA

A Dios, a nuestras familias, a nuestros maestros y compañeros de maestría, y a todas aquellas personas que de alguna u otra manera han contribuido al crecimiento de nuestra vida profesional.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire

DIRECTOR MSIA

MSIG. Laura Ureta Arreaga

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MGS. Karina Astudillo

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

Verónica Alexandra Guamán Reibán
AUTOR DE TESIS

Eduardo Roberto Williams Cascante
AUTOR DE TESIS

RESUMEN

Con el progreso significativo de las Tecnologías de la Información y la Comunicación, simultáneamente se ha presentado incidentes de seguridad de la información, delitos informáticos, criminalidad informática; así, se maximiza la importancia que tienen las evidencias digitales que sirven de medios de prueba en un proceso judicial, por lo que es procedente garantizar su autenticidad e integridad cumpliendo una cadena de custodia que respalde su valor probatorio.

A nivel internacional existen estándares y guías para el tratamiento de las evidencias digitales. En el Ecuador, entidades del estado han propuesto instructivos generales para su manejo y se han creado leyes y reglamentos relacionados con las tecnologías de la información y comunicación, que rigen ciertos elementos informáticos, en base a los cuales, se ha realizado un compendio, y en conjunto con las normas ISO adoptadas por la INEN (Servicio Ecuatoriano de Normalización) orientadas a la seguridad de la información, se implementó un esquema de seguridad en la gestión y control en la cadena de custodia de evidencias digitales de la Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP, encargada de controlar el tránsito del cantón Cuenca, ya que por la naturaleza de su actividad genera evidencias digitales que son indispensables como argumento de contravenciones y delitos de tránsito.

En primer lugar se realizó un inventario de los activos relacionados con las evidencias digitales y posteriormente se analizaron todas sus posibles amenazas y vulnerabilidades, para de esta forma poder valorar el impacto que tuvieran estas al materializarse.

Una vez realizado este análisis de riesgo, se procedió a elaborar los controles internos, además de realizar recomendaciones técnicas para cada caso. Asimismo, se diseñó un formulario para el protocolo de la cadena de custodia de estas evidencias, desde su fase de identificación y recolección, hasta su eliminación.

Adicionalmente, se instaló y capacitó al personal de la EMOV-EP en herramientas de software para el tratamiento de las evidencias digitales, que garanticen la autenticidad e integridad de las mismas.

Como resultado de esta implementación, el nivel de riesgo disminuyó notablemente, por lo que se sugiere replicar esta metodología en otros procesos críticos de la empresa.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ACT	Agente Civil de Tránsito
ALPR	Automatic License Plate Recognition
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
ART.	Artículo
CD	Compact Disc
COIP	Código Orgánico Integral Penal
CONATEL	Consejo Nacional de Telecomunicaciones
CORDICOM	Consejo de Regulación y Desarrollo de la Información y Comunicación
CRC	Cyclic Redundancy Check
DEFR	Digital Evidence First Response
DES	Digital Evidence Specialist
DVD	Digital Versatile Disc
DVR	Digital Video Recorder
EMOV EP	Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca
GLPI	Gestionnaire Libre de Parc Informático
IDE	Integrated Drive Electronics
IEC	International Electrotechnical Commission
IEPI	Instituto Ecuatoriano de Propiedad Intelectual
INEN	Servicio Ecuatoriano de Normalización
ISO	International Organization for Standardization
LOTAIP	Ley Orgánica de Transparencia y Acceso a la Información Pública

MD5	Message Digest Algorithm 5
NAS	Network Attached Storage
NTE	Norma Técnica Ecuatoriana
OIAT	Oficina de Investigación de Accidentes de Tránsito
ONG	Organización no gubernamental
PDA	Personal Digital Assistant
PHVA	Planear-Hacer-Verificar-Actuar
RACI	Responsible - Accountable - Consulted - Informed
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFC	Request For Comments
SCSI	Small Computer System Interface
SENATEL	Secretaría Nacional de Telecomunicaciones
SERT	Sistema de Estacionamiento Rotativo Tarifado
SGSI	Sistema de Gestión de Seguridad de la Información
SHA	Secure Hash Algorithm
SUPERCOM	Superintendencia de la Información y Comunicación
SUPERTEL	Superintendencia de Telecomunicaciones
TCP/IP	Transmission Control Protocol / Internet Protocol
TICS	Tecnologías de la Información y Comunicación
UPS	Uninterrupted Power System
USB	Universal Serial Bus
UTP	Unshielded twisted pair

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La Empresa Pública Municipal de Movilidad, Tránsito y Transporte EMOV EP, es la responsable de gestionar, administrar, regular y controlar el sistema de movilidad del cantón Cuenca, por lo que en sus operaciones diarias se generan evidencias digitales, debido a contravenciones y delitos de tránsito. Estas evidencias deben cumplir el debido procedimiento de cadena de custodia para que tengan valor probatorio dentro de un proceso judicial, por lo que se propone la implementación de un esquema de seguridad, que respalde la autenticidad e integridad de las mismas a lo largo de todo el proceso.

Con la finalidad de tener un sustento legal, el marco teórico describe las leyes ecuatorianas vigentes a la fecha, que rigen los temas relacionados a las tecnologías de la información y comunicación, como por ejemplo: la Ley Orgánica de Transparencia y Acceso a la Información Pública, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Código Orgánico Integral Penal, las Normas de Control Interno para el Sector Público del Ecuador; así como también las Normas ISO internacionales y las adoptadas por el Servicio Ecuatoriano de Normalización: Norma NTE INEN-ISO/IEC 27001:2011, Norma NTE INEN-ISO/IEC 27002:2009, Norma NTE INEN-ISO/IEC 27005:2012, Norma ISO/IEC 27037:2012.

Adicionalmente se detallan los conceptos generales del procedimiento de cadena de custodia.

Posteriormente se efectúa el levantamiento de información mediante entrevistas al personal involucrado en las áreas que manejan las evidencias digitales, aplicando un enfoque de gestión de riesgo, en donde se realiza la identificación y clasificación de los activos de información, la identificación y evaluación del riesgo: amenazas, vulnerabilidades, controles existentes y consecuencias, y la valoración y mapeo de riesgos con su correspondiente tratamiento.

A continuación, se diseña el esquema de seguridad de gestión de cadena de custodia de la evidencia digital, apoyados en el desarrollo de los controles internos que mitiguen los riesgos identificados anteriormente, además de la instalación de herramientas de software y el protocolo de cadena de custodia que se debe seguir.

Por último, se realiza la implementación del diseño propuesto, la capacitación en las herramientas de software, la ejecución de los casos de pruebas y el análisis de resultados.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

Con el auge de las Tecnologías de la Información y Comunicación (TICs), a la par ha ido evolucionando una serie de incidentes de seguridad, criminalidad informática, delitos informáticos; por lo que es necesario proporcionar guías, métodos, procedimientos herramientas que ayuden a proteger la información. En consecuencia surge la importancia de resguardar las evidencias digitales que garantice su autenticidad e integridad para que puedan servir como medios de prueba en un proceso judicial. Existen guías, estándares internacionales para el tratamiento de las evidencias digitales, la Legislación Nacional del Ecuador actualmente ha puesto interés en éste ámbito, la Fiscalía General del Estado, la Policía Judicial son entidades que han propuesto instructivos para el manejo de indicios y/o evidencia digital.

La EMOV al ser una institución que maneja elementos digitales que ha servido como pruebas en los tribunales, es de vital importancia implementar controles para la correcta gestión de la cadena de custodia de las evidencias digitales y garantizar la autenticidad e integridad de las mismas.

1.2 Descripción del problema

La Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP, responsable de gestionar, administrar, regular y controlar el sistema de movilidad del cantón de Cuenca, cuenta con un departamento de tecnología y control, en donde se gestiona toda la tecnología implementada para los procedimientos de los Agentes Civiles de Tránsito.

El departamento tiene entre sus responsabilidades resguardar fotos y videos de los diferentes equipos tecnológicos que son utilizados por los agentes civiles de tránsito en los patrulleros, como: equipos móviles para alcohotectores y radares, DVR’s (Digital Video Recorder) de las patrullas, cámaras de video, micrófonos, tabletas y computadoras.

El sistema de cámaras internas que lleva el vehículo registra todas las acciones y procedimientos que ejecutan los agentes civiles de tránsito.

El objetivo de la adecuación del vehículo con todos los dispositivos electrónicos es que los agentes cumplan con un trabajo eficiente y transparente al momento de la detención de un infractor de tránsito. Pero a pesar de toda la tecnología implementada, existen falencias en este proceso debido a la falta de

procedimientos para la extracción de las evidencias, la preservación, el transporte y la custodia de las mismas.

Los DVR's incorporados en las patrullas graban las 24 horas del día y aproximadamente a los 20 días se hacen las descarga de estas grabaciones. En el momento que los videos son descargados los agentes civiles deben solicitar la evidencia, porque debido a la falta de un servidor o un medio de almacenamiento masivo los videos son borrados al instante. Esto ha generado que cuando se realizan impugnaciones por parte de los contraventores, esta prueba se ha perdido debido a que no existen procedimientos para precautelarla.

De los PDA's de alcohotectores y de los radares se obtienen las fotografías de las pruebas de alcoholemia y de los operativos de velocidad respectivamente, fotografías que son descargadas pero que tampoco pueden ser almacenadas tanto por falta de los procedimientos y de los equipos correspondientes, las fotografías son entregadas en cualquier medio de almacenamiento portable pudiendo ser alterada antes de que la presentación de la evidencia sirva como prueba para defensa o aclaración.

Las evidencias que se obtienen de las operaciones realizadas por los Agentes Civiles de Tránsito, han servido para aclarar los incidentes de tránsito, y son pruebas válidas para que basado en ellas el juez pueda dictar su sentencia, por lo que se resalta la importancia de la seguridad que se debe implementar, tanto como políticas, procedimientos, la cadena de custodia que se debe seguir, herramientas que ayuden a la detección de la veracidad de las mismas,

herramientas para la gestión de casos, y sobretodo sensibilizar al personal que tiene acceso a las evidencias.

1.3 Solución propuesta

La solución consiste en proporcionar a la Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP, un mecanismo óptimo y confiable de seguimiento y control de todas las evidencias digitales que los agentes recaben durante sus operaciones, para que estas evidencias puedan servir de apoyo en procesos tanto judiciales como de auditorías internas y externas. En otras palabras, la solución al problema planteado es la **implementación de un esquema de seguridad para la gestión y control en la custodia de evidencias digitales**, que garantice la integridad de estas evidencias durante todo su ciclo de validez.

El desarrollo de esta solución contempla la definición del control interno para la adecuada extracción, preservación, transportación y custodia de las evidencias digitales, mediante el uso de instrumentos idóneos que aseguren que estas evidencias no sean alteradas por factores naturales o artificiales, ni por el movimiento en el transporte o cambios de ambiente, así como también permitir su manipulación por personal que tenga capacidad técnica y la debida autorización, es decir, el objetivo común de cada una de estas etapas es evitar la alteración, suplantación, destrucción, contaminación, o cualquier acción que varíe el estado original de las evidencias durante toda la cadena de custodia.

Este control interno será establecido en base a la legislación ecuatoriana vigente (COIP, LOTAIP, Ley de comercio electrónico, etc.), a estándares internacionales y a las políticas internas de la Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP.

En cuanto al software que será aplicado, se capacitará sobre el uso de herramientas que ayuden a la gestión de cadena de custodia de las evidencias digitales, las cuales briden los mecanismos de comprobación necesarios para verificar la integridad y autenticidad de las mismas, a lo largo de todo el proceso. Adicionalmente, se recomendarán herramientas tecnológicas que ayuden a la automatización de la preservación de las evidencias capturadas por los Agentes Civiles de Tránsito, de manera que disminuya la manipulación de las mismas y aumente su grado de fiabilidad dentro de un proceso judicial.

Las actividades a realizar en esta implementación serían las siguientes:

- Desarrollar los controles internos necesarios para la gestión de la cadena de custodia de las evidencias digitales, en cuanto a su extracción, preservación, transporte y cambio de custodios; determinados con enfoque al análisis de riesgo.
- Difundir el detalle de los controles internos establecidos al personal involucrado, luego de su revisión y aprobación por parte del directorio de la Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP.
- Capacitar al personal responsable del registro de las evidencias digitales, sobre el uso de las herramientas de software.

- Verificar los resultados obtenidos sobre distintos escenarios y recomendar acciones a tomar para la optimización de los procedimientos basados en la Norma NTE INEN-ISO/IEC 27001.

Entre los beneficios que se obtendrán después de la implementación, se pueden mencionar los siguientes:

- Dar garantía técnica de la integridad de la evidencia digital, que al momento de ser presentada en un juicio o auditoría, no haya sido contaminada y sea la misma que se recabó o decomisó en el escenario del delito u otro lugar relacionado con el hecho.
- Mitigar las brechas de seguridad existentes en la gestión de la cadena de custodia de la evidencia digital.
- Cambio de cultura organizacional sobre la seguridad de la información y el tratamiento de la evidencia digital.
- Facilitar la integración de otros sistemas de gestión.
- Control y monitoreo constante, lo que se traduce en mejora continua de las operaciones.
- Se alinea con la visión de la institución, la cual menciona la ejecución de procesos racionalizados y efectivos orientados a la excelencia, soportados en tecnologías de comunicación e información de última generación.

1.4 Objetivo general

Implementar un esquema de seguridad nivel 1, en la gestión y control en la custodia de evidencias digitales del área de control de tránsito de la Empresa

Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP, garantizando de esta manera la autenticidad e integridad de las mismas, para que puedan ser utilizadas como medio probatorio en un tribunal penal.

1.5 Objetivos específicos

- Describir la situación actual del manejo de las evidencias digitales en el área de tecnología y control de la EMOV EP, mediante los activos de información involucrados, roles y sus responsables.
- Realizar el análisis de levantamiento de información y requerimientos del área de tecnología y control de la EMOV EP.
- Diseñar e implementar el esquema de seguridad de gestión y control de la evidencia digital.
- Ejecutar pruebas con distintos escenarios y analizar los resultados.

1.6 Metodología

El enfoque metodológico del esquema de seguridad propuesto se realizará en base a la Norma ISO 27001, que nos permitirá identificar y calificar los activos de información relacionados con el proceso a tratar; así como para la Gestión de Riesgos de Tecnologías de la Información se tomará como base la norma NTE INEN-ISO/IEC 27005:2012, la cual nos permitirá realizar un análisis de riesgos de confidencialidad, integridad y disponibilidad de la información concerniente al proceso que maneja las evidencias digitales.

Posteriormente, los estándares y guías que serán la base para desarrollar los controles internos para la gestión de la cadena de custodia de las evidencias

digitales es la Norma para la Recopilación de Evidencias ISO/IEC 27037:2012; y con la Norma NTE INEN-ISO/IEC 27002:2009 se especificarán controles adicionales que requiera el proceso.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Conceptos básicos

Desde el punto de vista jurídico, la información tiene tres pilares fundamentales que son: el derecho de la información, el derecho a la información y el derecho sobre la información.

El derecho de la información trata a la misma como un objeto al cual puede regir y regular, mediante un conjunto de reglas y principios.

Por otra parte, el derecho a la información comprende el derecho a informar y a ser informado, además del derecho a elegir el tipo de información que se desea consumir.

La libertad de información se considera una de las formas en que se representa la libertad de expresión; el artículo 19 de la Declaración Universal de Derechos Humanos dicta que “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.” [1]

Por último, el derecho sobre la información se refiere a que si bien es intangible, la información no deja de ser un bien y por lo tanto es susceptible de apropiación.

El valor de la información en muchos de los casos es incuantificable, sobre todo para las empresas, hasta el punto de considerarse parte del patrimonio de las mismas, y por eso está expuesta a ser objetivo de delitos que atenten contra su integridad, confidencialidad y disponibilidad.

Estos delitos pueden consistir en: acceso a información privada o a sistemas informáticos sin autorización, robo, alteración, destrucción o eliminación de información, fraudes y falsificaciones cometidos por medios electrónicos, entre otros. Asimismo, la motivación para cometerlos puede ir desde la diversión hasta fines económicos. Por este motivo surgió la necesidad de crear organismos y leyes que protejan este bien y regulen su utilización, difusión, propiedad y privacidad. En nuestro país existen los siguientes:

- Superintendencia de la Información y Comunicación – SUPERCOM

Es un organismo técnico que tiene capacidad constitucional y legal de velar por la vigilancia, auditoría, intervención y control de las actividades comunicacionales de producción y difusión de contenidos, a través de la radio, televisión, prensa y de las páginas web, registradas en Ecuador.

- Agencia de Regulación y Control de las Telecomunicaciones – ARCOTEL

  Es la entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes. Esta agencia se originó con la Ley Orgánica de Telecomunicaciones y absorbió las siguientes entidades:

  - Superintendencia de Telecomunicaciones – SUPERTEL
  - Consejo Nacional de Telecomunicaciones – CONATEL
  - Secretaría Nacional de Telecomunicaciones – SENATEL

- Superintendencia de Telecomunicaciones – SUPERTEL

  Es un organismo técnico de control, creado según la Ley Especial de Telecomunicaciones publicada el 10 de Agosto de 1992. Actualmente se encarga del monitoreo y control de las entidades certificadoras de firma electrónica y servicios relacionados, en Ecuador.

- Consejo de Regulación y Desarrollo de la Información y Comunicación – CORDICOM

  Es la institución articuladora del sistema nacional de comunicación social, la cual tiene como misión diseñar e implementar normativa y mecanismos

para desarrollar, proteger y regular los derechos de la comunicación e información.

- Instituto Ecuatoriano de Propiedad Intelectual - IEPI

  Es una entidad estatal que tiene como función principal regular y controlar la aplicación de las leyes de la propiedad intelectual y velar por sus derechos, reconocidos en la Ley y la Constitución, así como también en tratados convenios internacionales.

2.2 Legislación nacional

La legislación nacional vigente comprende un conjunto de normas jurídicas cuyo objetivo en general es regir la vida en sociedad dentro del territorio ecuatoriano. Este sistema orgánico está compuesto de leyes, normas, ordenanzas y reglamentos de diversas índoles y alcances, por ejemplo, se podría distinguir entre las leyes civiles, laborales, del consumidor, etc. Debido a esta diversidad, es importante tener clara cuál es la prioridad que se le debe dar a cada uno de estos reglamentos.

Figura 2.1 Pirámide de Kelsen

La pirámide de Kelsen (Figura 2.1) detalla el orden jerárquico normativo, en el que se establece que la norma jerárquicamente superior prevalece sobre la norma jerárquicamente inferior, y bajo esta regla se resuelven todos los posibles conflictos entre normas de diversas jerarquías.

2.2.1 Constitución del Ecuador

La constitución del Ecuador es la norma jurídica jerárquicamente superior a todas las demás, y que se distingue por la fuente de donde se obtiene su validez: la voluntad popular, soberana y organizada, manifestada por medio de una votación.

En temas de información, la Constitución del Ecuador ampara el acceso a la información pública, así como también el derecho que tienen las personas sobre la información que cada uno considere como privada.

El Art. 18 indica que “Todas las personas, en forma individual o colectiva, tienen derecho a acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas.” [2]

Así mismo, el Art. 91 referente a la acción de acceso a la información pública, dicta que “La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de

la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley.” [2]

Por otra parte, el Art. 92 referente a la acción de hábeas data, expresa que toda persona tendrá derecho a acceder a los documentos, archivos de datos personales e informes sobre sí misma o sus bienes, que consten en entidades públicas o privadas, en soporte físico o electrónico; así como también el derecho a conocer el uso que se haga de ellos, su actualización, rectificación e incluso su eliminación. [2]

2.2.2 Ley Orgánica de Transparencia y Acceso a la Información Pública

La LOTAIP, Ley Orgánica de Transparencia y Acceso a la Información Pública, garantiza y norma el ejercicio del derecho fundamental de las personas a la información, y entre sus objetivos principales se encuentran:

- Cumplir lo dispuesto en la Constitución del Ecuador, referente a la transparencia y rendición de cuentas de todas las instituciones del Estado del sector público y sus funcionarios.
- Cumplir las convenciones internacionales de las cuales Ecuador es signatario, como por ejemplo: el Pacto Internacional de Derechos Civiles y Políticos, Convención Interamericana sobre Derechos Humanos, etc.

- Garantizar la protección de la información personal en poder del sector público.
- Facilitar la participación ciudadana en decisiones de interés general.

De acuerdo esta ley “Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.” [3]

Además de las instituciones del sector público, existen otros entes que deben someterse al principio de publicidad de la información pública, la que dicta que el acceso a esta es un derecho de las personas garantizado por el Estado. Estas entidades son las siguientes:

- Las personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste.
- Las personas jurídicas cuyas acciones pertenezcan total o parcialmente al Estado.
- Las organizaciones de trabajadores y servidores de las instituciones del Estado.
- Las instituciones de educación superior que perciban rentas del Estado.
- Las organizaciones no gubernamentales (ONG).

Las personas interesadas en acceder a información pública deberán hacerlo por medio de una solicitud escrita ante el titular de la institución, en la misma deberá constar la identificación del solicitante y el motivo de la solicitud. La denegación o falta de respuesta a la solicitud dentro del plazo señalado por esta Ley, dará lugar a las sanciones pertinentes.

Siempre y cuando no se trate de información considerada como reservada o confidencial por el Consejo de Seguridad Nacional o alguna otra Ley, el solicitante a quien le haya sido negada, podrá interponer un recurso de acceso a la información ante cualquier juez de lo civil o tribunal de instancia del domicilio del poseedor de la información requerida.

Corresponderá a la Defensoría del Pueblo, la promoción, vigilancia y garantías establecidas en esta Ley, como órgano promotor del cumplimiento del derecho de acceso a la información pública.

2.2.3 Código Orgánico Integral Penal

El Código Orgánico Integral Penal o COIP, que entró en vigencia en Febrero del 2014, es un conjunto organizado de normas jurídicas que establece infracciones penales y sus correspondientes penas conforme al sistema penal ecuatoriano, dividiendo estas infracciones penales en delitos y contravenciones. Mientras que un delito es una infracción sancionada con detención mayor a treinta días, una contravención es una infracción penal menor sancionada con detención hasta de treinta días o sin reclusión.

Esta relación entre delitos o contravenciones y penas también se traslada al campo de las infracciones cometidas en contra de la información, y la utilización de medios electrónicos para cometerlas.

Retomando un poco el tema de la información personal privada, el Art. 178, del COIP, justamente hace referencia a la violación a la intimidad, donde indica que la persona que, sin contar con autorización legal, acceda, intercepte, grabe, difunda o publique datos personales, mensajes de datos, voz, video y audio, información contenida en medios informáticos, comunicaciones privadas o reservadas de otra persona, será sancionada con pena privativa de libertad de uno a tres años. [4]

Por otra parte el Art. 190, tipifica la apropiación fraudulenta por medios electrónicos, expresando que la persona que utilice fraudulentamente un sistema informático o redes de telecomunicaciones para la apropiación de un bien ajeno o para la transferencia no consentida de bienes, valores o derechos en perjuicio de esta, en beneficio suyo o de otra persona, manipulando o modificando el funcionamiento de redes, sistemas informáticos, telemáticos y equipos de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años, al igual que si la infracción se comete con inutilización de sistemas de alarma, descifrado de claves encriptadas, utilización de tarjetas magnéticas, controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. [4]

De igual manera, en los artículos siguientes se tipifican las siguientes infracciones en las que se involucran equipos móviles, así como también el poseer la infraestructura (equipos y programas) necesaria para cometerlas:

- Reprogramación de equipos móviles (Art. 191)
- Intercambio, comercialización o compra de información de equipos móviles (Art. 192)
- Reemplazo de identificación de equipos móviles (Art. 193)
- Comercialización ilícita de equipos móviles (Art. 194)

En la sección tercera del COIP se profundiza sobre las infracciones que afectan la seguridad de los activos de los sistemas de información y comunicación.

El Art. 229 pena la revelación ilegal de bases de datos, es decir, será sancionada la persona que saque provecho revelando información registrada en archivos o bases de datos de un sistema informático, violando su condición de secreta, además de la intimidad y privacidad de las personas. [4]

El Art. 230 en cambio, contempla las penas a las infracciones referentes a la intercepción ilegal de datos:

- Será sancionada la persona que saque provecho de la intercepción, escucha, desvío, grabación u observación de un dato informático, ya sea en su origen, destino o durante la transmisión del mismo. Según

el Art. 476, la intercepción de las comunicaciones o datos informáticos solamente está permitido bajo solicitud de un fiscal, cuando existan indicios que resulten relevantes para fines de la investigación y dadas ciertas condiciones.

- Será sancionada la persona que envíe páginas electrónicas, enlaces o ventanas emergentes alteradas, de forma que induzca a una persona a ingresar a un sitio de internet diferente al que realmente quiere acceder, con el objetivo de obtener su información privada, como claves, números de tarjetas de crédito, etc. Esta técnica es conocida como phishing.
- Será sancionada la persona que clone y distribuya información contenida en bandas magnéticas u otro dispositivo electrónico, de las tarjetas de crédito, débito o similares. [4]

En el Art. 232 se pena el ataque a la integridad de los sistemas informáticos, con tres a cinco años de privación de la libertad, en los siguientes casos:

- Será sancionada la persona que destruya, elimine, altere, cause mal funcionamiento o comportamientos no deseados, de forma parcial o total, en un sistema informático, telemático o de telecomunicaciones.
- Será sancionada la persona que desarrolle, envíe, distribuya o ejecute programas maliciosos (virus) destinados a causar los efectos citados en el punto anterior.

- Será sancionada la persona que destruya los componentes tecnológicos utilizados para la transmisión, recepción o procesamiento de la información. [4]

En el Art. 233 se pena la destrucción, revelación o apropiación de información pública reservada que pueda comprometer la seguridad del Estado. [4]

El acceso no permitido a un sistema informático, con la finalidad de explotar ilegítimamente el acceso logrado, está contemplado y penado en el Art. 234. [4]

Por lo general, las penas a todas estas infracciones se agudizan si son cometidas por servidores públicos o si los bienes afectados están destinados a brindar servicios públicos o de seguridad ciudadana.

2.2.4 Ley de comercio electrónico, firmas electrónicas y mensajes de datos

En el año 2002 se expidió la Ley de comercio electrónico, firmas electrónicas y mensajes de datos, que tiene como objetivo regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

De acuerdo a esta ley, un mensaje de datos “Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.” [5]

Desde los primeros artículos de esta ley se otorga el reconocimiento jurídico que tienen los mensajes de datos, indicando que estos tendrán igual valor que los documentos escritos. De igual manera la firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Es necesario hacer hincapié en que un certificado de firma electrónica no es lo mismo que la firma electrónica en sí. Un certificado es un mensaje de datos que certifica la vinculación de una firma electrónica con una persona, a través de un proceso de comprobación de su identidad, por parte de una entidad certificadora. Para que un certificado tenga validez debe contener entre otros, lo siguiente:

- Identificación de la entidad de certificación, su domicilio legal y su firma electrónica

- Información del titular del certificado que permita su identificación y ubicación
- Fechas de emisión y caducidad del certificado
- Limitaciones y restricciones de uso del certificado

Las entidades de certificación de información son empresas que emiten certificados de firma electrónica y brindan otros servicios relacionados a esta. Estas entidades deben ser autorizadas por el Consejo Nacional de Telecomunicaciones – CONATEL, que es el organismo encargado de la autorización, registro y regulación de estas empresas, por otra parte, la Superintendencia de Telecomunicaciones – SUPERTEL será el organismo encargado del control de las mismas.

Para estar debidamente acreditadas, las entidades de certificación deben cumplir ciertas condiciones entre las que se puede mencionar las siguientes:

- Deben estar legalmente constituidas y demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios.
- Mantener respaldos de la información de los certificados.
- Estar en condiciones de acatar de manera inmediata las disposiciones de la Superintendencia de Telecomunicaciones, en cuanto a la suspensión de certificados.
- Alertar a los titulares de certificados, situaciones de riesgo de uso indebido de los mismos.

- Contar con una garantía para cubrir daños y perjuicios ocasionados por el incumplimiento de las leyes.

2.2.5 (400) Normas de Control Interno para el Sector Público, para el Área de Sistemas de Información Computarizados

La Contraloría General del Estado ha emitido Normas de Control Interno para el Sector Público del Ecuador las cuales constituyen guías para promover una adecuada administración de los recursos públicos, así como el correcto funcionamiento de las entidades. En su clasificación constan las normas para el área de sistemas de información computarizados, en donde especifican pautas para la organización y funciones del área informática; para el desarrollo de un plan integral informático, el procedimiento para la adquisición o actualización de sistemas, tanto a nivel de software como de hardware; la operación y mantenimiento de los sistemas; el acceso a los sistemas y modificación de la información; el diseño de controles y procedimientos que protejan la entrada y salida de datos; procedimientos para transacciones rechazadas a causa del procesamiento de la información; controles que aseguren el procesamiento y entrega de datos; la segregación de funciones en el área de informática, determinada en la estructura orgánica, constando las responsabilidades y la estructura jerárquica; la seguridad general en los centros de procesamiento de datos; procedimientos para la correcta utilización de los equipos, programas e información institucional; aprovechamiento de los recursos computarizados del sector público

mediante el intercambio de información institucional, aplicaciones desarrolladas internamente; administración del software en relación a la parte legal.

2.3 Normas Internacionales y Ecuatorianas

ISO es la Organización Internacional para la Estandarización, establece normas que ayudan a garantizar la calidad tanto en productos como servicios ofrecidos por las organizaciones. Las normas brindan guías, herramientas, métodos de implementación para diferentes ramas o familias como se les llama, abarcan una variedad de aspectos tales como de seguridad, medio ambiente, riesgos, medidas, magnitudes, entre otros.

IEC es la Comisión Electrónica Internacional, la cual establece normas en las áreas eléctrica, electrónica y tecnologías similares.

La ISO y la IEC componen el sistema especializado para la normalización a nivel internacional.

INEN, encargado de la reglamentación, normalización y metrología del Ecuador en base a las leyes constitucionales, tratados, acuerdos y convenios internacionales.

Las Normas Técnicas Ecuatorianas (NTE) abarcan reglas, instrucciones, guías para la seguridad y calidad de sus actividades y productos. El Ecuador trabaja con normas internacionales y ha adoptado algunas de las mismas como normas

nacionales, con el fin de fortalecer la cultura de calidad y alcanzar los beneficios de la normalización en un enfoque global.

2.3.1 Norma NTE INEN-ISO/IEC 27001:2011

La ISO 27001 es el estándar que norma la adopción de un SGSI (Sistema de Gestión de Seguridad de la Información) en todas sus fases: creación, implementación, operación, supervisión, revisión, mantenimiento y mejora.

El objetivo principal de un SGSI es preservar la confidencialidad, integridad y disponibilidad de la información, y proteger todos los activos relacionados a esta; es posible que un SGSI no sea aplicado a todos los procesos de la empresa en primera instancia, sino de forma parcial, a los procesos más críticos, todo dependerá de las necesidades y objetivos de cada organización, así como de sus requisitos de seguridad. [6]

Se considera que el SGSI es parte del sistema de gestión general de una empresa, por lo que para su implementación es necesario el compromiso de todos sus colaboradores, cumpliendo con las responsabilidades definidas para cada rol.

2.3.2 Norma NTE INEN-ISO/IEC 27002:2009

La ISO 27002 es una norma complementaria a la 27001. En esta se describe cómo seleccionar, implementar y gestionar los controles de seguridad de la información necesarios para la adopción de un SGSI,

aunque se puede tomar como referencia si se quieren implementar de forma independiente a un sistema de gestión.

La seguridad de la información se logra mediante la integración de un conjunto adecuado de controles, que incluyen políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software, por lo que estos controles necesitan ser no solo establecidos e implementados, sino también seguidos, revisados y mejorados, para asegurar que se cumplan los objetivos específicos de seguridad y del negocio.

Existen tres fuentes principales de requisitos de seguridad que deben considerarse al momento de seleccionar los controles:

- La evaluación de riesgos, mediante la cual se identifican las amenazas a los activos de la información, ya que se evalúa la vulnerabilidad de estos y la probabilidad de ocurrencia, y como resultado se obtendrá el impacto que tendría para el negocio si estas amenazas llegan a materializarse.
- Los requisitos legales, reglamentarios y contractuales que tienen que cumplir
  la organización.
- Las políticas y procedimientos ya existentes en la organización en cuanto al manejo, procesamiento, almacenamiento, comunicación y archivo de la información, mediante las cuales apoya sus operaciones diarias. [7]

Esta norma incluye varias secciones o grupos de controles, entre los que se encuentran:

- Políticas internas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad relacionada a recursos humanos
- Gestión de activos de la información
- Controles de acceso a los sistemas de información
- Criptografía
- Seguridad física y ambiente
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con los proveedores
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad del negocio
- Cumplimiento de requisitos legales y contractuales

2.3.3 Norma NTE INEN-ISO/IEC 27005:2012

La Norma ISO 27005 es una guía para la gestión del riesgo de seguridad de la información, tiene como objetivo proporcionar directrices y soporte para la implementación de la seguridad de la información a partir de la gestión del riesgo, esta norma es aplicable para todo tipo de organización.

Tiene como referencias normativas la ISO 27001 y la ISO 27002 y aplica los términos y definiciones de las mismas normas y adicional los propios de la norma; está estructurada con los procesos y sus actividades para la gestión del riesgo.

Comprende el alcance y los objetivos de la gestión de riesgos dentro de la organización, así como a los criterios de valoración del riesgo sobre los activos de información, determinando las amenazas que pueden explotar vulnerabilidades sobre los mismos; el análisis del tipo de tratamiento que se debe dar a los riesgos identificados, de tal manera que se pueda gestionar oportunamente comunicando el plan de mitigación al directorio de la organización; y el monitoreo que se debe ejecutar una vez gestionados los riesgos.

La norma 27005 asocia la gestión de riesgos de la seguridad de la información con las cuatro fases, planificar, hacer, verificar y actuar (PHVA) del SGSI. Planificar, alcance y objetivos de la gestión de riesgos, valoración y aceptación del riesgo; hacer, plan de mitigación del riesgo; verificar, monitoreo del riesgo; y actuar, mantener y mejorar continuamente las actividades de la gestión de los riesgos identificados en la gestión de riesgos. [8]

2.3.4 Norma ISO/IEC 27037:2012

La norma ISO/IEC 27037:2012, establece directrices que son reconocidas internacionalmente para la identificación, recolección, adquisición y

preservación de la evidencia digital; actualmente es la norma que se toma como base para los procedimientos de prácticas forenses informáticas, ya que está dirigida a dispositivos y técnicas actuales, renovando así la guía RFC 3227 (Request For Comments). La aplicación de esta norma requiere el cumplimiento con la legislación nacional.

La estructura de la norma está basada en los procesos de identificación, en donde se localiza las evidencias concernientes al hecho; de recolección y/o adquisición, tanto de la documentación y de los dispositivos, o la copia bit a bit de la información contenida; y de conservación y/o preservación para mantener la integridad de la evidencia en todo el proceso y pueda tener valor probatorio.

La norma prevalece en los principios de la Evidencia Digital de la relevancia, confiabilidad y suficiencia.

El alcance de la norma es para los siguientes dispositivos: medios de almacenamiento, dispositivos móviles, sistemas móviles de navegación, cámaras digitales, redes (TCP/IP y otros protocolos), ordenadores estándar, entre otros.

La norma define los roles para quienes tratan con evidencia digital:

- DEFR (Digital Evidence First Response), es la persona preparada, con las habilidades y formación requerida para actuar en la escena de un incidente, que además con la autorización respectiva podrá recoger las evidencias digitales, brindando garantía a las mismas.

- DES (Digital Evidence Specialist), es la persona que también pudiera actuar como DEFR, lo que le caracteriza son sus conocimientos especializados en el área tecnológica, tanto científicos y prácticos, generalmente llamados peritos informáticos. [9]

2.4 Cadena de custodia

La cadena de custodia es un conjunto de procedimientos aplicados a la protección, aseguramiento y preservación de elementos probatorios o también llamados evidencias, sean estas físicas o digitales, dentro de la escena de un delito.

El objetivo principal de la cadena de custodia es garantizar la autenticidad e integridad de las evidencias, desde su recolección en el lugar de los hechos, hasta su presentación en el juicio y disposiciones finales, evitando su alteración, pérdida, sustitución, contaminación o destrucción parcial o total.

La Fiscalía General del Estado elaboró manuales, protocolos, instructivos y formatos del Sistema Especializado Integral de Investigaciones, de Medicina Legal y Ciencias Forenses, los cuales fueron publicados el 08 de agosto de 2014, en cumplimiento de la Disposición Transitoria Octava del Código Orgánico Integral Penal (COIP), publicado en Registro Oficial Suplemento 180 de 10 de febrero de 2014, en vigencia desde el 10 de agosto del 2014. Estos manuales y protocolos están distribuidos en tres áreas: ciencias forenses, medicina legal, y cadena de custodia, en éste último grupo se encuentra los instructivos de procedimientos para el manejo de indicios y/o evidencia digital.

En el Manual de Cadena de Custodia se encuentra la definición de la misma como: "…Es el conjunto de actividades y procedimientos secuenciales que se aplican en la protección y aseguramiento de los indicios y/o evidencias físicas y digitales, desde la localización en la escena del delito o lugar de los hechos, hasta su presentación ante el Juzgador y/o disposición final." [10]

La Cadena de Custodia, según el Código Integral Penal, art. 456 "…se aplicará a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio." [4]

2.4.1 Principios de la Cadena de Custodia

Principio de garantía: Mediante este principio se garantiza la autenticidad e integridad de las evidencias.

Principio de responsabilidad: En el COIP, art. 458 hace referencia a que toda persona que entre en contacto con las evidencias será responsable directo de su preservación hasta la llegada del personal especializado. [4]

Principio de registro: Se debe dejar constancia del lugar donde se encontraron las evidencias, la persona responsable y las condiciones en que se encontraron.

Principio de preservación: Las evidencias deben ser preservadas de manera adecuada, durante todo el proceso mediante embalaje, sellado y etiquetado.

Principio de verificación: Cada custodio o responsable debe verificar que los principios anteriores hayan sido cumplidos, caso contrario deberá elaborar un informe detallado de las anomalías encontradas, ante una autoridad competente.

2.4.2 Tipos de Evidencia

Como se mencionó, las evidencias principalmente pueden ser físicas o digitales. Las **evidencias físicas** son elementos tangibles que pueden ser detectados y recolectados con mayor facilidad en la escena de un crimen: armas, ropa, incluso personas. Por otra parte, existen elementos intangibles, como por ejemplo los datos dentro un sistema informático, los cuales se transforman en **evidencia digital** cuando son usados para la aclaración de un caso penal. Este tipo de evidencia debe ser recolectada y analizada con herramientas técnicas especiales debido a las características de volatilidad, duplicidad, alteración, eliminable, modificable; y asimismo necesita un marco legal y científico apropiado.

En la mayoría de casos, cuando se encuentran involucradas evidencias de tipo digital, es porque se intenta descubrir casos de manipulación fraudulenta de computadores o de un sistema informático para desvío de recursos económicos, acceso y uso indebido de información privada,

pornografía infantil, robo de bases de datos, etc. Todos estos casos (entre otros) son conocidos como delitos informáticos y por su naturaleza son difíciles de detectar, ya que por lo general el criminal es una persona de muchos conocimientos técnicos y lo más seguro es que elimine todo registro de su accionar.

La información que servirá como evidencia digital puede encontrarse en dos instancias o estados: volátil y no volátil.

La información volátil es aquella que se encuentra almacenada en las tarjetas de memoria del computador (memoria RAM), mientras este esté encendido, y la cual se podrá visualizar e incluso interactuar con ella, pero que desaparecerá en el momento en que el computador se apague, ya que aún no ha sido guardada o registrada en los dispositivos de almacenamiento. Este tipo de información debe recolectarse de manera prioritaria, en medida de lo posible, y debe incluir: fecha y hora del sistema, información de los procesos activos del computador al momento de la recolección, conexiones de red, puertos de red abiertos y el detalle de las aplicaciones activas en cada uno de ellos, usuarios conectados (locales y remotos), aplicaciones abiertas y capturas de pantallas.

Por otra parte, la información no volátil o fija, es la que ya ha sido grabada o registrada en los dispositivos de almacenamiento del equipo: discos duros, discos duros externos, pen drives, tarjetas de memoria, etc. De este tipo de información se puede extraer todos los datos relacionados o relevantes para el caso a partir de los archivos contenidos en estos

dispositivos, pero es importante también analizar otros elementos como: la tabla de asignación de archivos, logs de programas y del sistema operativo, fecha, hora y usuario de modificación de los ficheros, información contenida en las carpetas temporales o recientes, y elementos eliminados.

2.4.3 Elementos para Recolección de Evidencia Digital

De manera general, estos son los implementos necesarios para realizar una correcta recolección de evidencias: guantes de látex, gorros, tapabocas, gafas, cámaras fotográficas, filmadoras, grabadoras, lápices, plumas, marcadores, cuaderno o bloc para notas, formularios o formatos para registro de evidencias, adhesivos, sobres de papel, fundas plásticas antiestáticas, pulseras antiestáticas, rollos de cinta adhesiva, destornilladores de todo tipo y medida, y cajas para transporte de las evidencias en caso de ser necesario.

En cuanto a hardware hay muchos elementos en los cuales apoyarse al momento de la recolección de evidencias, siendo estos los más importantes: computador portátil que cuente con una unidad lectora/grabadora de CD y DVD, tarjeta de red, modem, antenas Wireless y bluetooth, interfaces firewire y usb, lector de tarjetas de diferentes tipos; dispositivos de almacenamiento para realizar copias, estos deben tener suficiente capacidad y preferentemente estar vacíos, convertidores o adaptadores para diferentes tipos de discos duros; pen drives, CD y DVD en blanco, tarjetas de memoria; switches y cables IDE, SCSI, USB, UTP

(punto a punto y cruzados), coaxiales, seriales, paralelos, cables de poder; UPS y reguladores de voltaje. Y en cuanto a software: CD de arranque o live CD, software para realizar copias bit a bit, software forense como por ejemplo Encase o Forensic explorer, software para análisis de información de particiones, como Partinfo o Norton ghost.

2.4.4 Responsabilidad de la Evidencia Digital y de aplicar la Cadena de Custodia

El custodio, es la persona encargada de resguardar la evidencia bajo los protocolos, manuales, procedimientos, procesos establecidos; cumpliendo con el recibo, llenado de registros, verificación de sellos, embalajes, firmas y autorizaciones correspondientes.

El Registro de Cadena de Custodia es una de las mayores responsabilidades del custodio, ya que en este se detalla todo el recorrido de la evidencia; ofreciendo crédito de la autenticidad, estado original de la misma; la documentación de la cadena de custodia debe responder preguntas del lugar, fecha, nombres de quién descubrió y recogió la evidencia; nombres de quién ha examinado la evidencia; nombres de los custodios así como el período de tiempo que las mantienen, tipo de almacenamiento, entre otros.

Es responsabilidad de toda persona que por su función intervenga en un hecho presuntamente delictivo preservar los elementos probatorios; el COIP sanciona la falta de cumplimiento en su art. 292 “…La persona o

servidor público, que altere o destruya evidencias materiales u otros elementos de prueba para la investigación de una infracción, será sancionado con la pena privativa de libertad de uno a tres años.” [4]

2.4.5 Etapas de la Gestión de Evidencias Digitales y Cadena de Custodia

El manejo de evidencias y la cadena de custodia comprende varias fases que van desde el instante en que se alerta sobre el cometimiento de un posible delito hasta la presentación de los elementos probatorios en juicio. Antes de iniciar con el proceso de recolección y análisis de las evidencias es muy importante que se cuente con el debido permiso judicial, orden de allanamiento e incautación, de ser necesario, ya que de lo contrario estos elementos podrían ser excluidos por falta de garantías constitucionales.

Otro aspecto a considerar es que desde la llegada al lugar de los hechos se debe documentar cronológicamente cada actividad que se realice. Sería importante contar con la presencia de un notario de ser posible, que certifique las acciones realizadas, para al finalizar el proceso generar un acta de recolección de evidencias detallando las acciones tomadas con sus respectivos tiempos, además de la información del caso como el número, el nombre del juez o juzgado asignado.

2.4.5.1 Diseño

Esta es una etapa previa al inicio de recolección de evidencias en sí. En esta etapa ya se tiene un conocimiento y confirmación del delito, y se obtiene información sobre la empresa o persona afectada, su actividad económica, tipo de negocio, detalle de la denuncia realizada, etc., y conforme a esto se tiene una idea sobre el tipo de evidencia que se podría y desearía encontrar y cuál tendrá mayor relevancia. Adicionalmente, en esta etapa se preparan los elementos necesarios para su recolección y se diseñan los formatos donde se va a registrar la información obtenida.

2.4.5.2 Manejo del lugar de los hechos

Una vez que se tiene acceso al lugar de los hechos, es importante dar prioridad a los peritos en dactiloscópica, si es que ellos aún no han realizado sus actividades, para que puedan verificar la existencia de huellas dactilares sobre los equipos y otros elementos. A continuación, diligenciar el formato de entrega de la escena, para dejar constancia de las condiciones en que se recibe el lugar (fotografiar), y a partir de ese momento tomar las medidas de seguridad necesarias, como por ejemplo bloquear el acceso a personas o animales, prohibir la manipulación de las evidencias a testigos presentes o terceros,

en otras palabras asegurar el lugar de los hechos para evitar la pérdida o alteración de las evidencias.

2.4.5.3 Observación

Una vez que se tiene el control sobre el lugar de los hechos hay que realizar una inspección ocular tomando en cuenta todos los detalles, tomar notas sobre sus condiciones físicas, fotografiar, filmar, verificar la existencia y ubicación de cámaras de seguridad, ya que lo captado por ellas puede servir también como evidencia o constancia del procedimiento realizado.

Dependiendo de las características del lugar y las circunstancias del hecho, se pueden aplicar los siguientes métodos de búsqueda de evidencias: punto a punto, por sector cuadrante, por franjas o líneas, por cuadrícula o rejilla, siendo por círculo o espiral uno de los métodos más utilizados, y que consiste en caminar por el lugar de los hechos en forma circular hasta llegar al centro.

Una vez que se ha realizado la inspección ocular del sitio de manera general, es necesario centrarse en el territorio digital, es decir, en todos los elementos de los que se podrá extraer evidencias electrónicas, tomando en cuenta el estado de los equipos, del cableado, ubicaciones, tipología de red, dispositivos periféricos conectados, operadores (si los hay), etc.

De este proceso puede resultar un documento o acta de inspección técnica, soportado por fotografías, videos, planos, etc., y adicionalmente una lista de los equipos encontrados, codificados de tal forma que se pueda relacionar fácilmente a estos con sus periféricos, como lo muestra el siguiente ejemplo:

1 Servidor, 1.1 Monitor 17'', 1.2 Teclado, 1.3 Mouse

2 Computador, 2.1 Monitor 17'', 2.2 Teclado, 2.3 Mouse, 2.4 Impresora

2.4.5.4 Recolección de evidencias

Para iniciar con la recolección de evidencias digitales es importante tener en cuenta estas precauciones:

- No tomar ningún objeto sin guantes
- Evitar el uso de agentes químicos o biológicos
- Tener precaución con pisar o tropezar con el cableado
- Manipular un equipo a la vez

A continuación:

- Fotografiar y documentar el estado del equipo antes de manipularlo, es decir verificar si se encuentra encendido o apagado, si tiene algún daño físico, dispositivos conectados a él, etc.

- Registrar marca, modelo y número de serie del equipo, y de cada uno de sus componentes: teclados, mouse, impresoras u otros dispositivos conectados.
- Si el equipo se encuentra apagado evitar encenderlo, y si por el contrario el equipo se encuentra encendido no apagarlo y realizar las siguientes acciones, con el fin de extraer la información volátil:
    - Recuperar la fecha y hora del sistema
    - Recuperar la lista de los usuarios conectados (locales y remotos)
    - Enumerar los puertos de red abiertos y las aplicaciones asociadas a ellos
    - Deshabilitar las interfaces de red, para evitar que algún usuario (o el criminal informático) conectado al equipo pueda alterar o eliminar las evidencias o registros del sistema
    - Capturar las pantallas de las aplicaciones abiertas
    - Enumerar los procesos activos del sistema
    - Visualizar las configuraciones del sistema
- Para el caso de la información no volátil, realizar los siguientes pasos:
    - Realizar una copia bit a bit (copia exacta) de los discos duros encontrados, a fin de analizarlos posteriormente en el laboratorio forense. Esta copia es preferible realizarla

con un dispositivo bloqueador de escritura, para evitar la modificación de los archivos del disco origen.

- Generar los respectivos códigos Hash de las copias realizadas con el objetivo de garantizar la integridad de los datos que se encuentran en los dispositivos.

- En el lugar de los hechos donde se ha cometido el delito podría existir información escrita, que si bien no es digital, pudiera estar relacionada con transacciones generadas desde el sistema, por lo tanto se debe considerar como evidencia: facturas, estados de cuenta, vouchers, comprobantes de transacciones por cajeros automáticos, anotaciones en post-it como usuarios, passwords, direcciones de correo, números de teléfono o códigos.
- Plásticos que contengan bandas magnéticas o chips electrónicos, como por ejemplo tarjetas de crédito o débito, tarjetas de acceso, también deben recolectarse como evidencia.
- Por último, otra forma de recolectar evidencia es mediante entrevistas a los usuarios o testigos que se encuentren presentes en la escena del delito.

En cuanto a los documentos que deben diligenciarse en esta etapa se encuentran:

- Inventario de evidencias

- Formato de cadena de custodia para cada evidencia recolectada (detalle de la evidencia: fecha, hora, custodios, identificaciones, cargos de quien entrega y recibe).
- En caso de necesitar acceder a otros equipos que se encuentren fuera del lugar de los hechos, pero que se sospeche que de los cuales se puede extraer más evidencia, será necesario tramitar la autorización judicial correspondiente.

Posteriormente a la identificación y recolección de la evidencia el fin es mantener la integridad del origen de la evidencia, ya que para que sea aceptada en un proceso judicial tiene que ser autenticada, para esto se usa los códigos de integridad o las llamadas funciones hash, mencionadas anteriormente. Una función hash es un algoritmo matemático que al aplicarlo se obtiene un valor numérico único de tamaño fijo, también llamado número resumen, el cual depende del tipo de función que se utilice. El cálculo de hashes nos ayuda a comprobar que los archivos no hayan sido alterados; es decir los valores hash obtenidos originalmente en los equipos tecnológicos en el lugar del hecho se debe comparar con los obtenidos en la etapa del juicio, al ser idénticos se demostrará la integridad de la evidencia.

Los estándares para las funciones hash son las siguientes:

- MD4-MD5 (Algoritmo de Resumen del Mensaje) se basa en RFC 1321. Realiza la comprobación de la integridad mediante una función hash de 128 bits.

- SHA-1 (Algoritmo de Hash Seguro 1) se basa en el MD5. Genera una función hash de 160 bits.

- SHA-2 (Algoritmo de Hash Seguro 2) Conjunto de 4 funciones hash, SHA-224, SHA-256, SHA-384, SHA-512. Es similar a SHA-1.

- SHA-3 (Algoritmo de Hash Seguro 3), SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256, no es derivado del SHA-2, es considerado como herramienta de última generación para asegurar la integridad de la información.

2.4.5.5 Embalaje y rotulado de las evidencias

Esta etapa corresponderá en los casos en que se identifique que existe evidencia que debe ser movilizada para analizarla en un laboratorio de criminalística o forense, distinto al lugar de los hechos, o a los almacenes de evidencias.

Al desmontar los equipos es importante que se tomen en cuenta las siguientes recomendaciones:

- Primero se deben apagar los equipos que se van trasladar. Una vez apagados se procederá a desconectar todos los cables, empezando por el cable de poder.
- El levantamiento de cada equipo y sus periféricos se debe registrar en una ficha donde conste el estado en que se encontró antes del desmontaje (encendido, apagado), la marca, modelo y número de serie. Si se encuentra documentación relacionada como manuales del fabricante, garantías, etc., adjuntar a cada ficha de ser posible.
- Colocar sellos en cada una de las entradas (puertos) del mainboard de los equipos, asimismo en los tornillos.

Para embalar y rotular:

- Colocar cada elemento en una funda plástica o recipiente antiestático, o cartón, de forma individual. Estos contenedores deben ser capaces de prevenir rayones, golpes o movimientos bruscos.
- Para embalar no utilizar nunca papel pre-impreso, como por ejemplo periódicos o revistas.
- Para rotular se debe utilizar: tinta indeleble, letra clara, legible, sin enmiendes ni tachones.
- La fecha de los rótulos se debe expresar en formato dd/mm/aaaa y la hora en formato de 24 horas.

- Cada rótulo debe ir pegado al contenedor del elemento o evidencia, ya sean estas fundas plásticas o de papel, frascos o cajas de cartón.

En esta etapa se diligencian los siguientes formatos:

- Rótulos
- Formato de cadena de custodia
- Documento de acta de entrega de la escena, y detalle de los equipos (ficha técnica) allanados, o llevados al laboratorio forense o centros de acopio

2.4.5.6 Traslado y preservación o almacenamiento de la evidencia

Ya sea que la evidencia sea trasladada a un laboratorio forense o a una bodega de evidencias, se deben seguir las siguientes normas:

- El lugar a donde sea trasladada la evidencia debe cumplir las condiciones de preservación y seguridad, que garanticen la integridad, continuidad, autenticidad, identidad y registro de acuerdo a su clase y naturaleza.
- Se debe evitar el contacto de los equipos con otros de mayor campo electromagnético, agentes químicos, u otros agentes que puedan destruir la información contenida, o producir cualquier daño interno o externo de los equipos.

- Cuando se trate de interceptación de comunicaciones, la evidencia debe ser mantenida en una sección especial dentro del centro de acopio, hasta que sea requerida por una autoridad competente.
- En el caso de los centros de acopio o bodegas de evidencias, estos pueden ser temporales o permanentes, sin embargo, en ambos casos las evidencias deben ser operadas por personal especializado en archivo, que esté en capacidad de clasificar las evidencias según su naturaleza, tipo de volatibilidad y grado de importancia.
- Por lo general, una evidencia puede permanecer máximo 48 horas en un almacén temporal y estos son usados en los siguientes casos:
    - El almacén o bodega permanente no está disponible, o no dispone de espacio
    - Por motivos de fuerza mayor no se puede trasladar la evidencia a la bodega permanente de manera inmediata
    - Cuando no se tiene definido aún si antes debe pasar por un laboratorio forense

Los documentos gestionados en esta etapa son:

- Formato de cadena de custodia
- Acta de diligencia con el debido oficio, resolución u orden de traslado por parte del juez competente

- Bitácoras de entrada y salida de los almacenes temporales y definitivos, de los laboratorios forenses y de los despachos de los investigadores

2.4.5.7 Requerimiento judicial de las evidencias

En esta etapa el juez o juzgado designado solicita el traslado de las evidencias desde los laboratorios forenses o centros de acopio, para cumplir con una diligencia judicial o presentación de estas evidencias en audiencia.

La admisibilidad de la evidencia por parte de un juez en un proceso judicial está basada en el cumplimiento de un procedimiento estándar establecido por la institución competente; de los principios básicos reconocidos en el manejo de evidencias digitales y de la legislación nacional vigente.

De los criterios de valoración el COIP en su art.457 establece que "…La valoración de la prueba se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales. La demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente". [4]

Los documentos que se diligencian en esta fase son:

- Oficio de solicitud de traslado de las evidencias por parte de la autoridad judicial.
- Formato de cadena de custodia

2.4.5.8 Disposición final de las evidencias

La disposición final de las evidencias será dispuesta por el juez competente o fiscal mediante resolución, una vez se haya finalizado el proceso judicial, pudiendo ser esta la devolución, destrucción, remate, etc., dependiendo de su naturaleza.

Los documentos que se gestionan en esta fase son:

- Oficio o resolución donde se detalla la disposición del destino final de la evidencia
- Formato de cadena de custodia

Bitácoras de entrada y salida de los almacenes temporales y definitivos, y de los laboratorios forenses.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1 Situación Actual

En la actualidad, todo el flujo de información que conforma la base de evidencias digitales de la Empresa Pública Municipal de Movilidad, Tránsito y Transporte de Cuenca EMOV EP, está soportada principalmente en el subproceso de Subgerencia de Control de Tránsito y Transporte Terrestre perteneciente al proceso agregador de valor de Control de Tránsito y Transporte. Este subproceso en conjunto con uno de los procesos habilitantes de apoyo, Tecnología de Información y Comunicación, gestionan todos los equipos y recursos tecnológicos necesarios para que los agentes civiles de tránsito puedan detectar, evaluar y recolectar la mayor cantidad de información

posible, para poder sustentar las citaciones y detenciones realizadas a causa de infracciones de tránsito.

Figura 3.1 Organigrama por áreas de la EMOV

Entre el equipamiento con el que cuenta la EMOV para cumplir sus funciones y responsabilidades y que son fuente para que se pueda obtener una evidencia digital son:

- Radares móviles: equipo que sirve para medir la velocidad de un vehículo, utilizados en los operativos de control con presencia de agentes civiles de tránsito en las vías en donde se puede producir la detención al infractor.
- Alcohotectores: aparato dosificador de medición de alcohol en el aliento, que se apoya en las impresoras portables y PDA para obtener las fotos.
- Patrullas equipadas con sistema ALPR (Automatic License Plate Recognition), que incluye computadora, software para reconocimiento automático de placas, sistema de comunicaciones, sistemas de foto radar móviles, sistemas de cámaras de gestión con DVR.

La Subgerencia de Control de Tránsito y Transporte Terrestre tiene a su cargo:

- Especialista 1 Control Zona A
- Jefe de Grupo Control de Tránsito
- Supervisor Control de Tránsito
- Agentes Civiles de Tránsito (Directamente involucrados con las evidencias digitales)

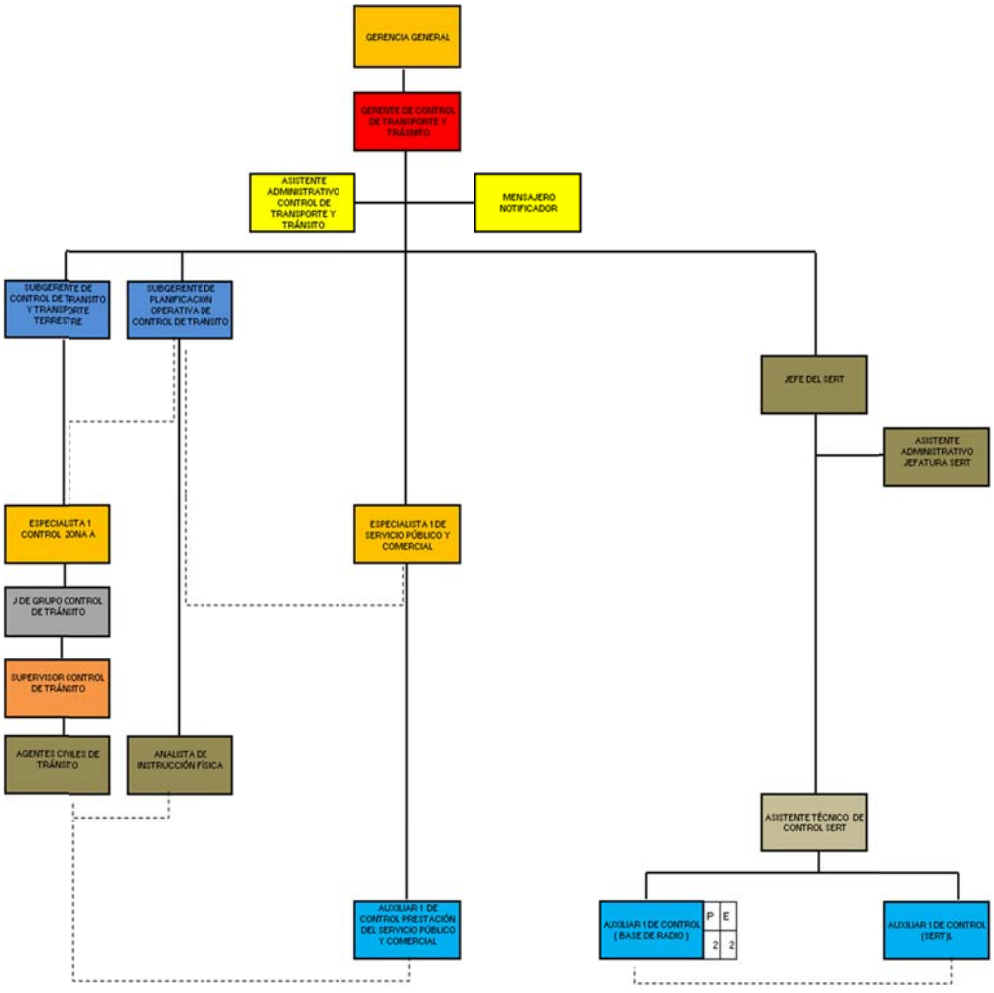


Figura 3.2 Organigrama específico del área por cargos de la EMOV

3.2 Roles y Responsabilidades (internos y externos)

La misión de la Subgerencia de Control de Tránsito y Transporte Terrestre es planificar, coordinar, ejecutar y controlar los procesos operativos internos y externos que realizan los Agentes Civiles de Tránsito, como parte del sistema de movilidad en base a las normativas y reglamentos vigentes, con el fin de mejorar la movilidad, contribuyendo a la reducción de accidentabilidad y mejorar la seguridad de peatones y conductores del cantón Cuenca. [11]

A su vez, los Agentes Civiles de Tránsito tienen la misión de cumplir y hacer cumplir la constitución, leyes, ordenanzas, reglamentos y la normativa de los gobiernos autónomos descentralizados Municipales con el fin de velar por la integridad física de los usuarios de la vía desarrollando funciones de asistencia, vigilancia y control de las normas de tránsito y transporte terrestre.

Dentro de las funciones de los Agentes Civiles de Tránsito están:

- Sustentar por cualquier medio físico o digital y custodiarlas, las infracciones y delitos en materia de Tránsito, Transporte Terrestre y Seguridad Vial a fin de que evidencien el lugar del suceso y los resultados de la infracción.
- Informar por escrito todas las violaciones a las leyes, ordenanzas y reglamentos en materia de Tránsito, Transporte Terrestre y Seguridad Vial, que tenga conocimiento, mediante el diligenciamiento de partes informativos y demás informes pertinentes.

- Administrar las cámaras de video vigilancia de las vías públicas con autorización del jefe inmediato a fin de apoyar en el control, dirección y vigilancia dentro de su jurisdicción.
- Registrar la entrega recepción de libretas de comparendos, equipos, dispositivos e insumos, verificando su numeración y estado a fin de ejercer las funciones asignadas.
- Entregar al área de digitación las órdenes de comparendo diligenciadas.
- Detener y trasladar a los presuntos autores de un delito de tránsito, siempre que cuenten con los elementos o indicios probatorios en concordancia al marco regulatorio a fin de seguir el proceso legal pertinente. [11]

El manual de normas básicas sobre infracciones de tránsito y su procedimiento en el Código Orgánico Integral Penal – COIP indica:

- La intervención de los ACT, Agentes OIAT (Oficina de Investigación de Accidentes de Tránsito), Fiscal, Juez de turno en los delitos de tránsito:

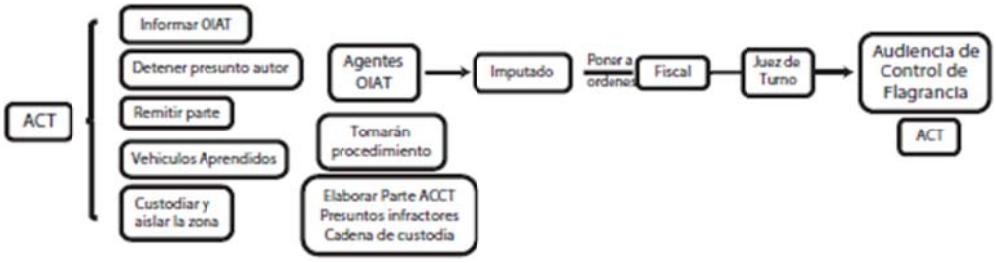


Figura 3.3 Procedimiento en delitos de tránsito

- En las contravenciones de tránsito el ACT deberá elaborar el parte, en forma personal, remitirlo inmediatamente / infractor a órdenes del Juez,

quien tiene 24 horas desde el cometimiento de la infracción para el juzgamiento. Si la pena es privativa de libertad, la sentencia podrá ser apelada ante la Corte Provincial.

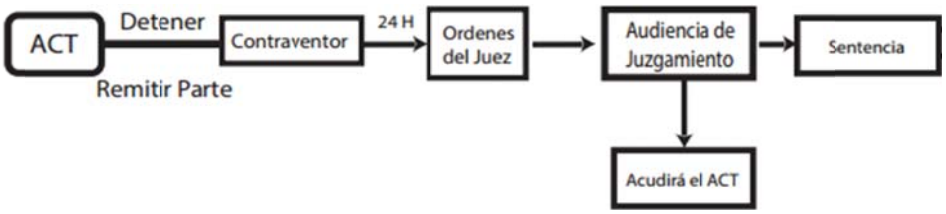


Figura 3.4 Procedimiento en contravenciones de tránsito

- A la persona que conduzca el vehículo en estado de embriaguez, el ACT deberá:
  1. Informarle de los derechos al infractor
  2. Informar que se le va a realizar la prueba de alcoholemia
  3. Realizarle el examen de alcohotest
  4. Que su negativa será considerada como presunción de estar en el máximo grado de intoxicación y que se procederá a su detención.
  5. Que se le va a grabar y se remitirá al Juez.
  6. Hacerle el examen sicosomático (pupilas, equilibrio, ambulatorios, dedo índice nariz: derecho, izquierdo, conversación, lectura)

  El ACT deberá remitir las pruebas al Juez. [12]

- Contravenciones de tránsito, primera clase:

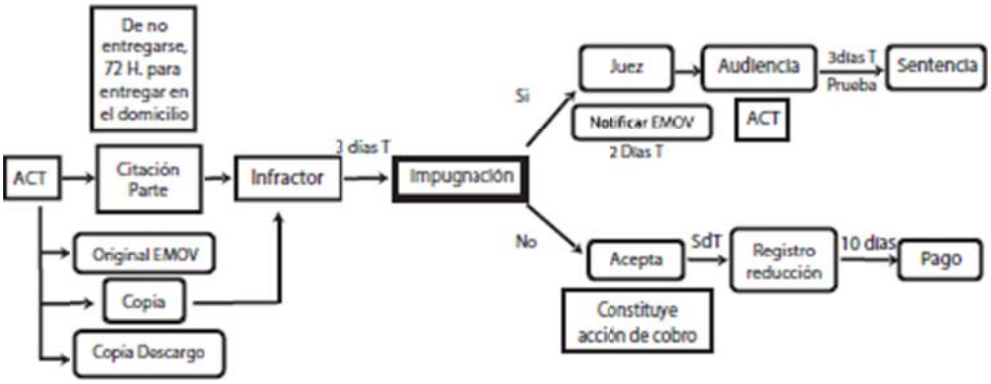


Figura 3.5 Procedimiento en contravenciones de primera clase

Para el cumplimiento de las funciones administrativas de los ACT internamente se han distribuido de la siguiente manera:

Tabla 1 Funciones internas de los ACT del área de Control de Tránsito

Dominio	Responsabilidades
Estadística	Generación de estadísticas de incidentes de tránsito e índice de evaluación de procedimientos de los ACT Elaborar y actualizar semanalmente la base de datos de los incidentes de tránsito Entregar oportunamente la información para su difusión a través de los canales y medios establecidos por la empresa
Planificación	Mantenimiento de dispositivos de control, alcoholímetros y equipos de fotoradar Coordindar y elaborar las órdenes de cuerpo Gestión de las fotos de los dispositivos (alcoholímetros y radar)
Registro	Control, registro, asignación y verificación de Citaciones Manejo y custodia de los archivos de la subgerencia de planificación y control de tránsito terrestre, CRV, CDIT, unidad operativa logística. Recepción y entrega de libretas de comparendos al personal operativo Asignación de series de libretas en el sistema AXIS de la ANT a cada agente
Monitoreo	Elaboración de reporte bitácora de recursos asignados según orden de cuerpo Elaboración semanal de informes de monitoreo de los recursos asignados a los distritos rurales y detalle de novedades no justificadas sobre las funciones de los ACT Verificar denuncias a través de la ubicación de los recursos
Función Judicial	Mantener el control, registro y seguimiento de los procedimientos de flagrancia de tránsito
Central de Radio	Elaboraración de los partes informativos (contravenciones de tránsito) y los partes por delitos de tránsito, cargar los partes de accidentes de tránsito en el Sistema David. Remitir los partes
CDIT - Centro de Detención de Infractores de Tránsito	Gestión de los formularios de ingreso y autorizaciones de salida de los detenidos. Administración del ingreso, salida y consulta de los detenidos Monitoreo y vigilancia de los detenidos
CRV - Centro de Retención Vehicular	Gestión de la documentación para el ingreso o salida de vehículos. Registro fotográfico del estado del vehículo, pertenencias, etc.

Dominio	Responsabilidades
TICS	Soporte técnico de los dispositivos tecnológicos de las patrullas y de las aplicaciones instaladas en los departamentos de PLL Descarga de videos de los DVR de las patrullas
Secretaría Planificación	Elaboración de documentación de coordinación de las funciones operativas de los ACT, informes, solicitudes, memorandos Gestión de denuncias a los ACT Revisiones y control de los procedimientos realizados en CDIT y CRV Manejo del archivo

3.3 Identificación y Gestión del Riesgo

La Norma ISO/NTE 27005 proporciona directrices para el análisis del riesgo, aplicado para describir los requisitos de seguridad de la información para la gestión de la cadena de custodia de las evidencias digitales que maneja el sub proceso Subgerencia de Control de Tránsito y Transporte Terrestre.

La metodología planteada conforma la identificación y clasificación de los activos de información, identificación y evaluación de los riesgos, y el tratamiento de los riesgos.

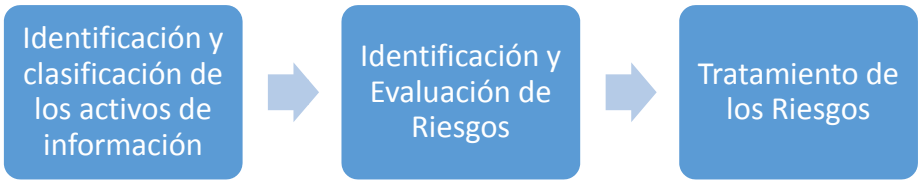


Figura 3.6 Metodología de gestión del riesgo aplicada

3.3.1 Identificación de Activos de Información

Para la implementación de los controles internos y los procedimientos necesarios para la gestión en la cadena de custodia de las evidencias

digitales, se requiere partir de un inventario y clasificación de los activos de información.

Se identifican los activos de información mediante entrevistas al personal propietario de cada activo; el inventario persigue obtener información que relacione el proceso de la empresa, las actividades que componen el proceso, activo de la información, tipo de activo, propietario, el nivel de impacto por pérdida de confidencialidad, integridad y disponibilidad.

El cuestionario aplicado en las entrevistas al personal propietario de los activos de información está dividido en las siguientes secciones:

a) Identificación del activo de información

Conoce la información que se genera en cada subproceso y qué información necesita para generar la misma. El nombre del activo así como el tipo de activo los cuales según la Norma ISO/NTE 27005 puede ser:

- Procesos, subprocesos, actividades del negocio
- Información estratégica
- Hardware
- Software
- Redes
- Personal
- Ubicación
- Estructura de la organización [8]

b) Ubicación del activo de información

Identifica al propietario (s), custodio (s) y usuario (s); el medio de soporte que puede ser físico, digital o físico/digital; los permisos de acceso de lectura, escritura, modificación y eliminación; el formato (en caso de ser digital), la ubicación física o electrónica; la frecuencia de actualización y si el activo de información cuenta con respaldo o copia.

c) Seguridad del activo de información

Busca conocer el nivel de la seguridad existente en la información, plantea atributos para calificar la confidencialidad, integridad y disponibilidad de los activos de información:

Confidencialidad

(A1) El activo de información debe ser restringido a un número limitado de personas.

(A2) La divulgación del activo de información causaría un daño irreparable, grave o de difícil reparación.

(A3) El activo de información debe ser protegido de personas externas.

Integridad

(A4) La alteración del activo de información causaría un incumplimiento legal o normativo para la institución.

(A5) La alteración del activo de información no es de fácil identificación, su corrección es complicada y causa daños en las operaciones de la institución.

(A6) El activo de información puede ser alterado o comprometido para fraudes o corrupción.

Disponibilidad

(A7) La falta de acceso oportunamente al activo de información por personal autorizado podría afectar la seguridad de las operaciones institucionales.

(A8) La falta de acceso al activo de información por personal autorizado ocasiona la interrupción parcial de las operaciones, poniendo en riesgo el cumplimiento de algún compromiso institucional.

(A9) La inactividad del activo inesperadamente puede causar daños graves a la institución.

Y el atributo (A10) complementa la valoración de impacto.

(A10) ¿Cuál es el tiempo de tolerancia de inactividad para el acceso al activo de información? (Horas/minutos)

d) Clasificación del activo de información

Cada nivel de clasificación posee características propias de protección, manejo y tratamiento del activo de información.

Uso público: Información que ha sido declarada de conocimiento público de acuerdo con alguna norma jurídica o por parte de las autoridades de la institución. Información que puede ser conocida y utilizada sin autorización por cualquier persona. Se encuentra en registros públicos o en fuentes de acceso al público según el art. 7 de la LOTAIP. [3]

Uso interno: Información que puede ser conocida y utilizada por todos los funcionarios de la entidad, cuya divulgación y uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad o a terceros.

Uso restringido: Información que solo puede ser conocida y utilizada por un grupo muy reducido de empleados debidamente autorizados por el propietario de la información, generalmente de la alta dirección, su divulgación o uso no autorizados podría ocasionar pérdidas graves a la institución como impactos financieros, daño a la seguridad pública, problemas judiciales o penales.

3.3.1.1 Valoración de los Activos de Información

Según las propiedades de confidencialidad, integridad y disponibilidad los activos de información pueden estar expuestos a daños que comprometen la misión de la entidad. Se asigna un valor cualitativo, que permita posteriormente realizar el análisis de riesgos de cada activo, de acuerdo a los siguientes criterios: A - Alto, M - Medio, B – Bajo.

Alto: Afecta a los procesos estratégicos de la institución.

Medio: Afecta a los procesos de apoyo de la institución.

Bajo: Afecta a los procesos de manera leve sin causar ningún daño considerable a la institución.

Tabla 2 Criterio de valoración de activos

Nivel de impacto	Clasificación
4 - 5	Alto
3	Medio
1 -2	Bajo

Se califica a cada activo de información en base a la escala, se promedian y se obtiene una calificación de impacto única por activo, se considera los siguientes criterios para la calificación:

- Por la pérdida de confidencialidad, integridad y disponibilidad de los activos de información.
- Las pérdidas financieras que puede generar a la institución.
- Las consecuencias negativas que puede ocasionar a la reputación de la empresa al darse la comprobación de una evidencia digital falsa.
- Incumplimiento de los requisitos legales, contractuales.

3.3.1.2 Criterios de Valoración para los requerimientos de Confidencialidad, Integridad y Disponibilidad

Confidencialidad:

Alto

a. La divulgación de la información ocasiona pérdidas financieras significativas a la institución.

b. La información se restringe a un número limitado de personas

Medio

a. El conocimiento de la información es solo de uso interno, depende de la función, requerimientos institucionales o bajo autorizaciones correspondientes.

b. La divulgación de la información afecta de manera moderada a la institución, se pueden solucionar a tiempo los daños.

Bajo

a. La información es conocida por personal interno o externo a la institución.

b. No hay ningún efecto negativo al poner de conocimiento público la información.

Integridad:

Alto

a. La alteración de la información compete incumplimientos legales y normativos.

b. La alteración de la información es fuente de actos corruptos o utilizado para fraudes.

Medio

a. La alteración de la información causa daños moderados, los cuales pueden ser recuperados y disminuir el impacto negativo a los procesos de negocio.

Bajo

a. La alteración de la información es identificada fácilmente y su corrección es instantánea

b. La alteración de la información no tiene consecuencias en las operaciones de negocio.

Disponibilidad:

Alto

a. La falta de acceso oportuna a la información por personal autorizado ocasiona implicaciones legales y económicas para la institución.

Medio

a. El no tener acceso adecuado a la información puede ocasionar un impacto considerable a las actividades operativas de la institución.

Bajo

a. El no disponer de la información de manera inmediata implica un perjuicio leve para la institución.

Se obtiene una matriz de inventario y clasificación de la información en donde se detalla los activos de información que son declarados por sus propietarios en las entrevistas realizadas.

La clasificación de activos se ha realizado en base a la criticidad que mantienen en la intervención de la cadena de custodia de las evidencias digitales:

Tabla 3 Tipo de activo: Hardware

No.	Activo de información	Valor
1	Portátiles	Alto – Medio
2	PC escritorio	Alto – Medio
3	PDA	Alto
4	Alcoholímetros	Alto
5	Radares	Alto
6	Impresoras radar	Medio
7	DVR	Alto
8	Cámaras	Medio

Tabla 4 Tipo de activo: Software

No.	Activo de información	Valor
1	Sistema David 20.i2	Alto
2	Sistema CDIT	Alto
3	Sistema CRV	Alto
4	Aplicación Dasc Móvil	Alto
5	Aplicación Easy Street Draw	Medio
6	Aplicación Safety Vision	Medio

Tabla 5 Tipo de activo: Información

No.	Activo de información	Valor
1	Fotos radar	Alto
2	Fotos alcoholímetros	Alto
3	Fotos partes de tránsito	Alto
4	Videos partes de tránsito	Alto
5	Videos patrullas	Alto
6	Partes informativos	Alto
7	Partes incidentes de tránsito	Alto
8	Órdenes de cuerpo	Medio
9	Citaciones ANT	Medio

3.3.2 Identificación y Evaluación del Riesgo

Los criterios de evaluación de riesgo están planteados en base a:

- La criticidad de los activos de información involucrados en la cadena de custodia de las evidencias digitales.
- Los requisitos legales y reglamentarios de los que debe cumplir las evidencias digitales de la EMOV.
- La valoración de la confidencialidad, integridad y disponibilidad de la información para el proceso agregador de valor Control de Tránsito y Transporte.

3.3.2.1 Identificación de las amenazas

La amenaza es una posible acción que se produzca para explotar una vulnerabilidad de un activo de información comprometiendo su confidencialidad, integridad o disponibilidad; esta acción

puede ser producida de manera accidental o intencional, con origen humano ya sea dentro o fuera de la institución; y también hay amenazas que se producen por origen natural como los fenómenos climáticos, sísmicos, volcánicos y meteorológicos. [8]

Las amenazas se identifican en una clase general y si es necesario se abarca amenazas individuales. Hay amenazas que no solo afectan a un activo y dependiendo de los activos afectados el impacto variará.

A partir de las entrevistas realizadas a los propietarios, custodios y usuarios de los activos, de los incidentes ocurridos se obtiene información de las amenazas que tienen los activos involucrados con las evidencias digitales, así también como del catálogo de amenazas se selecciona las amenazas que afectan a los activos del proceso, se evalúa la probabilidad de ocurrencia y se realiza su valoración.

Se obtiene el listado de amenazas con su identificación y origen:

Tabla 6 Amenazas: Portátiles

Tipo	Amenaza	Origen
Daño físico	Destrucción del equipo o los medios	Accidentales Ambientales Deliberadas
Compromiso de la información	Hurto de equipo	Deliberadas
	Manipulación con hardware	Deliberadas
	Manipulación con software	Deliberadas
Fallas técnicas	Falla del equipo / Mal funcionamiento del equipo	Accidentales
	Mal funcionamiento del software	Accidentales
Acciones no autorizadas	Uso no autorizado del equipo	Deliberadas
	Uso de software falso o copiado	Accidentales Deliberadas
	Procesamiento ilegal de los datos	Deliberadas
Compromiso de las Funciones	Error en el uso	Accidentales
	Abuso de derechos	Accidentales Deliberadas
Pirata informático, intruso ilegal	Intrusión, accesos forzados, acceso no autorizado	Deliberadas

Tabla 7 Amenazas: Pc escritorio

Tipo	Amenaza	Origen
Daño Físico	Daño por agua	Ambientales
	Destrucción del equipo o los medios	Accidentales Ambientales Deliberadas
Compromiso de la información	Hurto de equipo	Deliberadas
	Manipulación con hardware	Deliberadas
	Manipulación con software	Deliberadas
Fallas técnicas	Falla del equipo / Mal funcionamiento del equipo	Accidentales
	Mal funcionamiento del software	Accidentales
Acciones no autorizadas	Uso no autorizado del equipo	Deliberadas
	Uso de software falso o copiado	Accidentales Deliberadas
	Procesamiento ilegal de los datos	Deliberadas
Compromiso de las Funciones	Error en el uso	Accidentales
	Abuso de derechos	Accidentales Deliberadas
Pirata informático, intruso ilegal	Intrusión, accesos forzados, acceso no autorizado	Deliberadas

Tabla 8 Amenazas: PDA

Tipo	Amenaza	Origen
Daño Físico	Destrucción	Deliberadas
Compromiso de la Información	Hurto de equipo	Deliberadas
	Manipulación con Software/Código malicioso	Deliberadas
Fallas técnicas	Falla del equipo / Mal funcionamiento del equipo	Accidentales
Acciones no autorizadas	Uso no autorizado del equipo	Deliberadas
Intrusos	Observar información reservada	Deliberadas

Tabla 9 Amenazas: Alcoholímetro

Tipo	Amenaza	Origen
Daño físico	Destrucción del equipo o los medios	Accidentales Ambientales Deliberadas
Compromiso de la información	Hurto de equipo	Deliberadas
Fallas técnicas	Falla del equipo / Mal funcionamiento del equipo	Accidentales
Acciones no autorizadas	Uso no autorizado del equipo	Deliberadas
Compromiso de las funciones	Error en el uso	Accidentales

Tabla 10 Amenazas: Radares

Tipo	Amenaza	Origen
Daño Físico	Destrucción del equipo o los medios	Accidentales Ambientales Deliberadas
Fallas técnicas	Falla del equipo / Mal funcionamiento del equipo	Accidentales
Acciones no autorizadas	Uso no autorizado del equipo	Deliberadas
Compromiso de las Funciones	Error en el uso	Accidentales

Tabla 11 Amenazas: DVR

Tipo	Amenaza	Origen
Daño Físico	Destrucción del equipo o los medios	Accidentales Ambientales Deliberadas
Compromiso de la información	Hurto de equipo	Deliberadas
Fallas técnicas	Falla del equipo / Mal funcionamiento del equipo	Accidentales
Acciones no autorizadas	Uso no autorizado del equipo	Deliberadas
Compromiso de las Funciones	Error en el uso	Accidentales

Tabla 12 Amenazas: Sistemas

Tipo	Amenaza	Origen
Fallas técnicas	Mal funcionamiento del software	Accidentales
Acciones no autorizadas	Uso de software falso o copiado	Accidentales Deliberadas
Compromiso de las funciones	Error en el uso	Accidentales
	Abuso de derechos/Falsficación de derechos	Accidentales Deliberadas
	Negación de acciones	Deliberadas
Pirata informático, intruso ilegal	Intrusión, accesos forzados al sistema, accesos no autorizados al sistema, sabotaje del sistema	Deliberadas
Intrusos	Ingreso de datos falsos o corruptos	Deliberadas
	Errores en el sistema (bugs)	Deliberadas

Tabla 13 Amenazas: Fotos

Tipo	Amenaza	Origen
Compromiso de la información	Hurto de medios o documentos	Deliberadas
	Divulgación	Accidentales Deliberadas
	Manipulación con software	Accidentales Deliberadas
Acciones no autorizadas	Corrupción de los datos	Deliberadas
Compromiso de las funciones	Error en el uso	Deliberadas
	Abuso de derechos / Falsificación de derechos	Deliberadas
	Negación de acciones	Deliberadas
Pirata informático, intruso ilegal, criminal de la computación	Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	Deliberadas

Tabla 14 Amenazas: Videos

Tipo	Amenaza	Origen
Compromiso de la información	Hurto de medios o documentos	Deliberadas
	Divulgación	Accidentales Deliberadas
	Manipulación con software	Accidentales Deliberadas
Acciones no autorizadas	Corrupción de los datos	Deliberadas
Compromiso de las funciones	Error en el uso	Deliberadas
	Abuso de derechos / Falsificación de derechos	Deliberadas
	Negación de acciones	Deliberadas
Pirata informático, intruso ilegal, criminal de la computación	Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	Deliberadas

Tabla 15 Amenazas: Partes contravenciones – Delitos de tránsito

Tipo	Amenaza	Origen
Compromiso de la información	Hurto de medios o documentos	Deliberadas
	Divulgación	Accidentales Deliberadas
Compromiso de las funciones	Error en el uso	Deliberadas
	Abuso de derechos	Deliberadas
	Negación de acciones	Deliberadas
Pirata informático, intruso ilegal	Intrusión, accesos forzados al sistema, acceso no autorizado al sistema	Deliberadas
Criminal de la Computación	Soborno de la información (Interno)	Deliberadas

3.3.2.2 Identificación de Controles Existentes

Es necesario identificar los controles que posee actualmente la empresa para no duplicar controles o realizar gastos innecesarios en los controles que posteriormente se implementen para dar soporte a la cadena de custodia de las evidencias digitales.

En base a las Normas para el Uso de los Recursos Informáticos de la Empresa Pública Municipal de Movilidad de Tránsito y Transportes de Cuenca – EMOV EP y a los reportes de las auditorías se identifica los controles internos. Con los propietarios y usuarios de los activos se verifica la funcionalidad de los mismos: si el control es efectivo y opera correctamente, es efectivo y necesita controles complementarios o es inefectivo es decir no funciona adecuadamente o el control no existe.

Tabla 16 Controles existentes: Portátiles

Amenaza	Controles existentes	Funcionalidad
Destrucción del equipo o los medios	4 Restricciones emanadas de la constitución y operación de la red (4.2) 5.2 Controles para hardware y software (5.2.2)	Efectivo con oportunidad de mejora
Hurto de equipo	5.2 Controles para hardware y software (5.2.3, 5.2.11, 5.2.12)	Insuficiente
Manipulación con hardware	4 Restricciones emanadas de la constitución y operación de la red (4.23, 4.24) 5.2 Controles para hardware y software (5.2.4)	Insuficiente
Manipulación con software	4 Restricciones emanadas de la constitución y operación de la red (4.4, 4.5, 4.8, 4.18) 5.2 Controles para hardware y software (5.2.4, 5.2.5)	Insuficiente
Falla del equipo / Mal funcionamiento del equipo	5.2 Controles para hardware y software (5.2.10) 5.15 Responsabilidades de la Subgerencia de Tecnología (5.15.5)	Efectivo con oportunidad de mejora
Mal funcionamiento del software	5.2 Controles para hardware y software (5.2.14)	Insuficiente
Uso no autorizado del equipo	4 Restricciones emanadas de la constitución y operación de la red (4.10) 5.4 Conexión de equipos informáticos a la red de la EMOV-EP (5.4.3)	Insuficiente
Uso de software falso o copiado	4 Restricciones emanadas de la constitución y operación de la red (4.7) 5.2 Controles para hardware y software (5.2.4, 5.2.5, 5.2.8, 5.2.13)	Insuficiente
Procesamiento ilegal de los datos	5.2 Controles para hardware y software (5.2.5)	Insuficiente
Error en el uso	5.2 Controles para hardware y software (5.2.14)	Efectivo con oportunidad de mejora
Abuso de derechos	5.1 Disposiciones generales en el uso de la red (5.1.7)	Insuficiente
Intrusión, accesos forzados, acceso no autorizado	5.2 Controles para hardware y software (5.2.3) 5.8 Controles de seguridad (5.8.5, 5.8.9) Seguridad de la información - Implementación de Firewall	Insuficiente

Tabla 17 Controles existentes: Pc escritorio

Amenaza	Controles existentes	Funcionalidad
Daño por agua	No existe	Inefectivo
Destrucción del equipo o los medios	4 Restricciones emanadas de la constitución y operación de la red (4.2) 5.2 Controles para hardware y software (5.2.2)	Efectivo con oportunidad de mejora
Hurto de equipo	5.2 Controles para hardware y software (5.2.11, 5.2.12)	Efectivo con oportunidad de mejora
Manipulación con hardware	4 Restricciones emanadas de la constitución y operación de la red (4.23, 4.24) 5.2 Controles para hardware y software (5.2.4)	Efectivo con oportunidad de mejora
Manipulación con software	4 Restricciones emanadas de la constitución y operación de la red (4.4, 4.5, 4.8, 4.18) 5.2 Controles para hardware y software (5.2.4, 5.2.5)	Insuficiente
Falla del equipo / Mal funcionamiento del equipo	5.2 Controles para hardware y software (5.2.10) 5.15 Responsabilidades de la Subgerencia de Tecnología (5.15.5)	Efectivo con oportunidad de mejora
Mal funcionamiento del software	5.2 Controles para hardware y software (5.2.14)	Efectivo con oportunidad de mejora
Uso no autorizado del equipo	4 Restricciones emanadas de la constitución y operación de la red (4.10) 5.4 Conexión de equipos informáticos a la red de la EMOV-EP (5.4.3)	Efectivo con oportunidad de mejora
Uso de software falso o copiado	4 Restricciones emanadas de la constitución y operación de la red (4.7) 5.2 Controles para hardware y software (5.2.4, 5.2.5, 5.2.8, 5.2.13)	Efectivo con oportunidad de mejora
Procesamiento ilegal de los datos	5.2 Controles para hardware y software (5.2.5)	Efectivo con oportunidad de mejora
Error en el uso	5.2 Controles para hardware y software (5.2.14)	Efectivo con oportunidad de mejora
Abuso de derechos	5.1 Disposiciones generales en el uso de la red (5.1.7)	Efectivo con oportunidad de mejora
Intrusión, accesos forzados, acceso no autorizado	5.8 Controles de seguridad (5.8.5, 5.8.9) Seguridad de la información - Implementación de Firewall	Efectivo con oportunidad de mejora

Tabla 18 Controles existentes: PDA

Amenaza	Controles existentes	Funcionalidad
Destrucción	4 Restricciones emanadas de la constitución y operación de la red (4.2) 5.12 Responsabilidades de los usuarios (5.12.3, 5.12.5)	Insuficiente
Hurto de equipo	5.2 Contrcles para hardware y software (5.2.1, 5.2.12)	Insuficiente
Manipulación con Software/Código malicioso	4 Restricciones emanadas de la constitución y operación de la red (4.5, 4.26)	Insuficiente
Falla del equipo / Mal funcionamiento del equipo	5.15 Responsabilidades de la Subgerencia de Tecnología (5.15.5)	Efectivo con oportunidad de mejora
Uso no autorizado del equipo	5.4 Conexión de equipos informáticos a la red de la EMOV-EP (5.4.3)	Insuficiente
Observar información reservada	5.2 Contrcles para hardware y software (5.2.15, 5.2.17, 5.2.18, 5.2.20) 5.3 Identificaciones o usernames (5.3.1)	Efectivo con oportunidad de mejora

Tabla 19 Controles existentes: Alcoholímetro

Amenaza	Controles existentes	Funcionalidad
Destrucción del equipo o los medios	4 Restricciones emanadas de la constitución y operación de la red (4.2)	Insuficiente
Hurto de equipo	No existe	Inefectivo
Falla del equipo / Mal funcionamiento del equipo	No existe	Inefectivo
Uso no autorizado del equipo	5.4 Conexión de equipos informáticos a la red de la EMOV-EP (5.4.3)	Insuficiente
Error en el uso	No existe	Inefectivo

Tabla 20 Controles existentes: Radares

Amenaza	Controles existentes	Funcionalidad
Destrucción del equipo o los medios	4 Restricciones emanadas de la constitución y operación de la red (4.2)	Insuficiente
Falla del equipo / Mal funcionamiento del equipo	5.15 Responsabilidades de la Subgerencia de Tecnología (5.15.5)	Insuficiente
Uso no autorizado del equipo	5.4 Conexión de equipos informáticos a la red de la EMOV-EP (5.4.3)	Efectivo con oportunidad de mejora
Error en el uso	5.12 Responsabilidades de los usuarios (5.12.3)	Insuficiente

Tabla 21 Controles existentes: DVR

Amenaza	Controles existentes	Funcionalidad
Destrucción del equipo o los medios	4 Restricciones emanadas de la constitución y operación de la red (4.2) 5.2 Controles para hardware y software (5.2.2)	Insuficiente
Hurto de equipo	5.2 Controles para hardware y software (5.2.3)	Insuficiente
Falla del equipo / Mal funcionamiento del equipo	5.15 Responsabilidades de la Subgerencia de Tecnología (5.15.5)	Insuficiente
Uso no autorizado del equipo	5.4 Conexión de equipos informáticos a la red de la EMOV-EP (5.4.3)	Efectivo con oportunidad de mejora
Error en el uso	No existe	Inefectivo

Tabla 22 Controles existentes: Sistemas

Amenaza	Controles existentes	Funcionalidad
Mal funcionamiento del software	No existe	Inefectivo
Uso de software falso o copiado	4 Restricciones emanadas de la constitución y operación de la red (4.5, 4.8) 5.2 Controles para hardware y software (5.2.5) 5.13 Legalidad (5.13.1)	Insuficiente
Error en el uso	5.2 Controles para hardware y software (5.2.7)	Insuficiente
Abuso de derechos/Falsficación de derechos	5.12 Responsabilidades de los usuarios (5.12.4)	Insuficiente
Negación de acciones	5.2 Controles para hardware y software (5.2.6)	Insuficiente
Intrusión, accesos forzados al sistema, accesos no autorizados al sistema, sabotaje del sistema	Seguridad de la información - Implementación de Firewall	Insuficiente
Ingreso de datos falsos o corruptos	No existe	Inefectivo
Errores en el sistema (bugs)	4 Restricciones emanadas de la constitución y operación de la red (4.18, 4.19)	Insuficiente

Tabla 23 Controles existentes: Fotos

Amenaza	Controles existentes	Funcionalidad
Hurto de medios o documentos	4 Restricciones emanadas de la constitución y operación de la red(4.1) 5.1 Disposiciones generales en el uso de la red (5.1.6, 5.1.7) 5.2 Controles para hardware y software (5.2.2, 5.2.15, 5.2.16, 5.2.17, 5.2.18) 5.3 Identificaciones o Usernames (5.3.1, 5.3.3) 5.8 Seguridad (5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8)	Insuficiente
Divulgación	4 Restricciones emanadas de la constitución y operación de la red(4.27) 5.11 Confidencialidad (5.11.1, 5.11.2, 5.11.3, 5.11.4) 2.1 Política general de la seguridad de la información (2.1.8)	Insuficiente
Manipulación con software	4 Restricciones emanadas de la constitución y operación de la red(4.5) 5.2 Controles para hardware y software (5.2.5)	Insuficiente
Corrupción de los datos	No existe	Inefectivo
Error en el uso	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.2 Controles para hardware y software (5.2.7)	Insuficiente
Abuso de derechos / Falsificación de derechos	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.12 Responsabilidades de los usuarios (5.12.1, 5.12.5) 5.16 Sanciones (5.16.3)	Efectivo con oportunidad de mejora
Negación de acciones	5.8 Seguridad (5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8)	Efectivo con oportunidad de mejora
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	5.8 Seguridad (5.8.5, 5.8.9) Seguridad de la información - Implementación de Firewall	Insuficiente

Tabla 24 Controles existentes: Videos

Amenaza	Controles existentes	Funcionalidad
Hurto de medios o documentos	4 Restricciones emanadas de la constitución y operación de la red(4.1) 5.1 Disposiciones generales en el uso de la red (5.1.6, 5.1.7) 5.2 Controles para hardware y software (5.2.2, 5.2.15, 5.2.16, 5.2.17, 5.2.18) 5.3 Identificaciones o Usernames (5.3.1, 5.3.3) 5.8 Seguridad (5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8)	Insuficiente
Divulgación	4 Restricciones emanadas de la constitución y operación de la red (4.27) 5.11 Confidencialidad (5.11.1, 5.11.2, 5.11.3, 5.11.4) 2.1 Política general de la seguridad de la información (2.1.8)	Insuficiente
Manipulación con software	4 Restricciones emanadas de la constitución y operación de la red (4.5) 5.2 Controles para hardware y software (5.2.5)	Insuficiente
Corrupción de los datos	No existe	Inefectivo
Error en el uso	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.2 Controles para hardware y software (5.2.7)	Insuficiente
Abuso de derechos / Falsificación de derechos	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.12 Responsabilidades de los usuarios (5.12.1, 5.12.5) 5.16 Sanciones (5.16.3)	Efectivo con oportunidad de mejora
Negación de acciones	5.8 Seguridad (5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8)	Insuficiente
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	5.8 Seguridad (5.8.5, 5.8.9) Seguridad de la información - Implementación de Firewall	Insuficiente

Tabla 25 Controles existentes: Partes contravenciones – Delitos de tránsito

Amenaza	Controles existentes	Funcionalidad
Hurto de medios o documentos	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.2 Controles para hardware y software (5.2.15, 5.2.16, 5.2.17, 5.2.18) 5.8 Seguridad (5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8)	Efectivo con oportunidad de mejora
Divulgación	4 Restricciones emanadas de la constitución y operación de la red (4.27) 5.11 Confidencialidad (5.11.1, 5.11.2, 5.11.3, 5.11.4) 2.1 Política general de la seguridad de la información (2.1.8)	Insuficiente
Error en el uso	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.2 Controles para hardware y software (5.2.7)	Efectivo con oportunidad de mejora
Abuso de derechos	5.1 Disposiciones generales en el uso de la red (5.1.7) 5.12 Responsabilidades de los usuarios (5.12.5)	Insuficiente
Negación de acciones	5.8 Seguridad (5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8)	Insuficiente
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema	Seguridad de la información - Implementación de Firewall	Efectivo con oportunidad de mejora
Soborno de la información (Interno)	5.8 Seguridad (5.8.7)	Insuficiente

3.3.2.3 Identificación de las vulnerabilidades

La vulnerabilidad es la condición que facilita que una amenaza se materialice sobre el activo de información.

Se detecta las vulnerabilidades en conjunto con los propietarios de los activos, las cuales están relacionadas con las amenazas identificadas, si solo existe la vulnerabilidad no causa efecto en el activo si no es explotada por una amenaza y la implementación

de controles podría no ser necesaria en este momento, sí se reconocen debido a que con el tiempo puede variar y es recomendable monitorear los cambios. Así, una amenaza sin vulnerabilidad no ocasiona un impacto al activo de información.

Se obtiene el listado de vulnerabilidades relacionadas con las amenazas que afectan a los activos de información:

Tabla 26 Vulnerabilidades: Portátiles

Amenaza	Vulnerabilidad
Destrucción del equipo o los medios	Uso inadecuado o descuido de parte de los usuarios
Hurto de equipo	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información Ausencia de política formal sobre la utilización de computadores portátiles Ausencia de control de los activos que se encuentran fuera de las instalaciones
Manipulación con hardware	Uso inadecuado o descuido del cotrol de acceso físico a las edificaciones y los recintos
Manipulación con software	Descarga y uso no controlado de software Ausencia de copias de respaldo
Falla del equipo / Mal funcionamiento del equipo	Ausencia de planes de continuidad Mantenimiento insuficiente de los equipos
Mal funcionamiento del software	Software nuevo o inmaduro Especificaciones incompletas o no claras para los desarrolladores Ausencia de control de cambios eficaz
Uso no autorizado del equipo	Ausencia de revisiones regulares por parte del personal competente
Uso de software falso o copiado	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
Procesamiento ilegal de los datos	Habilitación de servicios innecesarios Ausencia de mecanismos de monitoreo Ausencia o insuficiencia en las disposiciones con respecto a la seguridad de la información en los contratos con los empleados
Error en el uso	Ausencia de un eficiente control de cambios en la configuración
Abuso de derechos	Ausencia de pistas de auditoría Asignación errada de los derechos de acceso Ausencia de procedimiento formal para el registro y retiro de usuarios Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso Ausencia de procedimientos de monitoreo de los recursos de procesamiento de información Ausencia de auditorías (supervisiones) regulares Ausencia de procedimientos de identificación y valoración de riesgos
Intrusión, accesos forzados, acceso no autorizado	Ausencia de procedimientos para la detección de vulnerabilidades de seguridad Ausencia de registro y monitoreo de eventos de seguridad

Tabla 27 Vulnerabilidades: Pc escritorio

Amenaza	Vulnerabilidad
Daño por agua	Instalaciones con afectaciones por lluvias
Destrucción del equipo o los medios	Uso inadecuado o descuido de parte de los usuarios
Hurto de equipo	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información Ausencia de política formal sobre la utilización de computadores portátiles Ausencia de control de los activos que se encuntran fuera de las instalaciones
Manipulación con hardware	Uso inadecuado o descuido del cotrol de acceso físico a las edificaciones y los recintos
Manipulación con software	Descarga y uso no controlado de software Ausencia de copias de respaldo
Falla del equipo / Mal funcionamiento del equipo	Ausencia de planes de continuidad Mantenimiento insuficiente de los equipos
Mal funcionamiento del software	Software nuevo o inmaduro Especificaciones incompletas o no claras para los desarrolladores Ausencia de control de cambios eficaz
Uso no autorizado del equipo	Ausencia de revisiones regulares por parte del personal competente
Uso de software falso o copiado	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
Procesamiento ilegal de los datos	Habilitación de servicios innecesarios Ausencia de mecanismos de monitoreo
Error en el uso	Ausencia de un eficiente control de cambios en la configuración
Abuso de derechos	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo Ausencia de pistas de auditoría Asignación errada de los derechos de acceso Ausencia de procedimiento formal para el registro y retiro de usuarios Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso Ausencia de procedimientos de monitoreo de los recursos de procesamiento de información Ausencia de auditorías (supervisiones) regulares Ausencia de procedimientos de identificación y valoración de riesgos
Intrusión, accesos forzados, acceso no autorizado	Ausencia de procedimientos para la detección de vulnerabilidades de seguridad Ausencia de registro y monitoreo de eventos de seguridad

Tabla 28 Vulnerabilidades: PDA

Amenaza	Vulnerabilidad
Destrucción	Uso inadecuado o descuido de parte de los usuarios Ausencia de esquemas de reemplaza periódico
Hurto de equipo	Ausencia de control de los activos que se encuentran fuera de las instalaciones
Manipulación con Software/Código malicioso	Descarga y uso no controlado de software
Falla del equipo / Mal funcionamiento del equipo	Mantenimiento insuficiente de los equipos
Uso no autorizado del equipo	Ausencia de revisiones regulares por parte de los supervisores
Observar información reservada	Ausencia de mecanismos de control de accesos a este tipo de dispositivos

Tabla 29 Vulnerabilidades: Alcoholímetros

Amenaza	Vulnerabilidad
Destrucción del equipo o los medios	Uso inadecuado o descuido de parte de los usuarios
Hurto de equipo	Ausencia de control de los activos que se encuentran fuera de las instalaciones
Falla del equipo / Mal funcionamiento del equipo	Mantenimiento insuficiente de los equipos
Uso no autorizado del equipo	Ausencia de procedimientos formales para la asignación y responsabilidad de los equipos Ausencia de revisiones regulares por parte de los supervisores
Error en el uso	Ausencia de procedimienos formales en la configuración y calibración de equipos

Tabla 30 Vulnerabilidades: Radares

Amenaza	Vulnerabilidad
Destrucción del equipo o los medios	Uso inadecuado o descuido de parte de los usuarios
Falla del equipo / Mal funcionamiento del equipo	Mantenimiento insuficiente de los equipos
Uso no autorizado del equipo	Ausencia de procedimientos formales para la asignación y responsabilidad de los equipos Ausencia de revisiones regulares por parte de los supervisores
Error en el uso	Ausencia de procedimienos formales en la configuración y calibración de equipos

Tabla 31 Vulnerabilidades: DVR

Amenaza	Vulnerabilidad
Destrucción del equipo o los medios	Uso inadecuado o descuido de parte de los usuarios
Hurto de equipo	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información Ausencia de política formal sobre la utilización de computadores portátiles Ausencia de control de los activos que se encuntran fuera de las instalaciones
Falla del equipo / Mal funcionamiento del equipo	Ausencia de planes de continuidad Mantenimiento insuficiente de los equipos
Uso no autorizado del equipo	Ausencia de revisiones regulares por parte del personal competente
Error en el uso	Ausencia de procedimientos formales para el manejo del equipo

Tabla 32 Vulnerabilidades: Sistemas

Amenaza	Vulnerabilidad
Mal funcionamiento del software	Software nuevo o inmaduro Especificaciones incompletas o no claras para los desarrolladores Ausencia de control de cambios eficaz
Uso de software falso o copiado	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
Error en el uso	Interfaz de usuario compleja Ausencia de documentación Configuración incorrecta de parámetros Ausencia de procedimientos para la introducción del software en los sistemas operativos
Abuso de derechos/Falsficación de derechos	Defectos bien conocidos en el software Ausencia de pistas de auditoria Asignación errada de los derechos de acceso
Negación de acciones	Ausencia de procedimientos de gestión de control de cambios
Intrusión, accesos forzados al sistema, accesos no autorizados al sistema, sabotaje del sistema	Ausencia de escaneo de vulnerabilidades en la seguridad de aplicaciones Ausencia de registro y monitoreo de eventos de seguridad
Ingreso de datos falsos o corruptos	Ausencia de filtrados de entrada o procesos de inspección de datos Ausencia de procedimientos de rastreo del recorrido de los datos, entrada y salida
Errores en el sistema (bugs)	Especificaciones incompletas o no claras para los desarrolladores Ausencia o insuficienia de procesos de depuración y pruebas de software

Tabla 33 Vulnerabilidades: Fotos

Amenaza	Vulnerabilidad
Hurto de medios o documentos	Almacenamiento sin protección Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
Divulgación	Ausencia de procedimientos documentados de gestión de seguridad de la información Ausencia de procedimientos para seguir la cadena de custodia Falta de conciencia acerca de la seguridad Ausencia de una definición de clasificación de la información
Manipulación con software	Falta de comprobación y garantía de la integridad de las fotos Ausencia de copias de respaldo
Corrupción de los datos	Ausencia de procedimiento formal de sistema de almacenamiento, respaldo y recuperación
Error en el uso	Ausencia de documentación Entrenamiento insuficiente en seguridad Uso incorrecto de software y hardware Falta de conciencia acerca de la seguridad Ausencia de responsabilidad en la seguridad de la información en la descripción de los cargos
Abuso de derechos / Falsificación de derechos	Ausencia de supervisiones regulares
Negación de acciones	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	Ausencia de procedimientos para la detección de vulnerabilidades de seguridad Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad

Tabla 34 Vulnerabilidades: Videos

Amenaza	Vulnerabilidad
Hurto de medios o documentos	Almacenamiento sin protección
Divulgación	Ausencia de procedimientos documentados de gestión de seguridad de la información Ausencia de procedimientos para seguir la cadena de custodia Falta de conciencia acerca de la seguridad Ausencia de una definición de clasificación de la información
Manipulación con software	Falta de comprobación y garantía de la integridad de los videos Ausencia de copias de respaldo
Corrupción de los datos	Ausencia de procedimiento formal de sistema de almacenamiento, respaldo y recuperación
Error en el uso	Ausencia de documentación Entrenamiento insuficiente en seguridad Uso incorrecto de software y hardware Falta de conciencia acerca de la seguridad Ausencia de responsabilidad en la seguridad de la información en la descripción de los cargos
Abuso de derechos / Falsificación de derechos	Ausencia de supervisiones regulares
Negación de acciones	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	Ausencia de procedimientos para la detección de vulnerabilidades de seguridad Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad

Tabla 35 Vulnerabilidades: Partes contravenciones – Delitos de tránsito

Amenaza	Vulnerabilidad
Hurto de medios o documentos	Almacenamiento sin protección Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
Divulgación	Ausencia de procedimientos para el manejo de información clasificada
Error en el uso	Ausencia de procedimientos para el manejo de información clasificada
Abuso de derechos	Ausencia de terminación de la sesión, cuando se abandona la estación de trabajo Disposición o reutilización de los medios del almacenamiento sin borrado adecuado Ausencia de pistas de auditoria
Negación de acciones	Ausencia de registros de auditoría (responsable, fecha, hora)
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema	Ausencia de procedimientos para la detección de vulnerabilidades de seguridad Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
Soborno de la información (Interno)	Ausencia o insuficiencia de disposiciones con respecto a la seguridad de la información en los contratos con los empleados

3.3.2.4 Identificación de las consecuencias

A partir de las amenazas y vulnerabilidades identificadas se describen los escenarios de incidentes y las consecuencias que se pudiera ocasionar si la amenaza explotara una o varias vulnerabilidades. En base a los criterios de impacto descritos en la valoración de los activos de información, se determina el

impacto de los escenarios de incidente que aportan para la posterior medición del riesgo.

Tabla 36 Consecuencias: Portátiles

Escenario	Consecuencia
Uso inadecuado de las baterías u obstrucción del sistema de ventilación	Deterioro y reducción de su vida útil
Robo del equipo y que se haga mal uso de la información contenida	Pérdida de información
Robo del equipo y que se haga mal uso de la información contenida	Pérdida de evidencias digitales
Acceso no autorizado a la red	Mal uso de la información alojada en los servidores
Acceso no autorizado a la red o a la información de loca de la máquina	Mal uso de la información
Falla del equipo provocando la falta de acceso total al mismo	Retraso de las operaciones por falta de acceso al equipo
Sentencias del sistema no debidamente probados como por ejemplo: delete	Puede causar daños a la información
Equipo utilizado por personas ajenas a la institución	Acceso a información confidencial
Instalación de programas craks, keygen	Intalación de programas ocultos como software espía, backdoors
Manipulación de información reservada	Mal uso de la información, consecuencias legales
Manipulación errónea de la configuración y programas del equipo	Inutilización del hardware y software
Los usuarios pueden cambiar las configuraciones de la máquinas, por ejemplo cambios en la red para acceso a páginas no autorizadas de internet	Provoca que las portátiles se llenen de virus
Acceso de usuarios no permitidos con el fin de obtener información confidencial	Mal uso de información confidencial

Tabla 37 Consecuencias: Pc escritorio

Escenario	Consecuencia
Daño de pantallas por goteras en la oficina	Pérdida económica para la institución
Mal funcionamiento del equipo por apagar incorrectamente	Pérdida económica para la institución
Robo del equipo y que se haga mal uso de la información contenida	Pérdida de información
Robo del equipo y que se haga mal uso de la información contenida	Pérdida de evidencias digitales
Acceso no autorizado a la red	Mal uso de la información alojada en los servidores
Acceso no autorizado a la red o a la información local de la máquina	Mal uso de la información
Falla del equipo provocando la falta de acceso toal al mismo	Retraso de las operaciones por falta de acceso al equipo
Sentencias del sistema no debidamente probado como por ejemplo un delete	Puede causar daños a la información
Equipo utilizado por personas ajenas a la institución	Acceso a información confidencial
Instalación de programas cracks, keygen	Intalación de programas ocultos como software espía, backdoors
Manipulación de información reservada	Mal uso de la información, consecuencias legales
Manipulación errónea de la configuración y programas del equipo	Inutilización del hardware y software
Los usuarios pueden cambiar las configuraciones de la máquinas, por ejemplo cambios en la red para acceso a páginas no autorizadas de internet	Provoca que las portátiles se llenen de virus
Acceso de usuarios no permitidos con el fin de obtener información confidencial	Mal uso de información confidencial

Tabla 38 Consecuencias: PDA

Escenario	Consecuencia
Por mal uso, golpes, por una manipulación incorrecta del equipo	Se genera un gasto para reponer el equipo dañado
Por mal uso, golpes, por una manipulación incorrecta del equipo	Pérdida de información
Robo del equipo con información del operativo realizado	Afecta a la privacidad de la información contenida en el dispositivo
Se contagia con código malicioso	Se daña la información y el dispositivo
En operativo el equipo no funcione adecuadamente y no se pueda utilizar	Pérdida de información
Acceder al equipo para acciones personales	Desconfigurar, descargar virus, etc.
Empleados que no sean del área accedan al equipo	Obtener información reservada

Tabla 39 Consecuencias: Alcoholímetros

Escenario	Consecuencia
Deterioro del equipo por el uso	Falta de disponibildiad para los operativos, sin poder recopilar evidencias
Pérdida del equipo por descuido del personal	Perjuicio económico y limitación de recursos para los operativos
Presenta fallas el equipo por falta de mantenimiento	Arroja datos incorrectos
Uso del equipo en operativos no autorizados	Implicaciones legales
Desconocimiento en la configuración del instrumento	Toma de datos inválidos

Tabla 40 Consecuencias: Radares

Escenario	Consecuencia
Falta de cuidado en la manipulación del equipo	Mal funcionamiento del equipo
Presenta fallas el equipo por falta de mantenimiento	No se pueden llevar a cabo los operativos programados
Uso del equipo en operativos no autorizados	Implicaciones legales
Desconocimiento en la configuración del equipo (configuración, calibración)	Recopilación de datos erróneos

Tabla 41 Consecuencias: DVR

Escenario	Consecuencia
Equipo estropeado sin la posibilidad de almacenar los videos	Incapaciad de obtener evidencias digitales
Robo del equipo y que se haga mal uso de la información contenida	Pérdida de información
Robo del equipo y que se haga mal uso de la información contenida	Pérdida de evidencias digitales
Falla del equipo provocando la falta de acceso total al mismo	Retraso de las operaciones por falta de acceso al equipo
Cables del DVR desconectados intencionalmente	Pérdida de evidencias digitales
Negligencia en el manejo del equipo	Pérdida de evidencias digitales

Tabla 42 Consecuencias: Sistemas

Escenario	Consecuencia
Aplicaciones mal programadas que realizan diferentes funciones a las requeridas	Obtención de datos erróneos e información no confiable
Uso de software comercial sin licenciamiento	Generación de multas por el uso no permitido
Ingreso de información incorrecta o incompleta	Información no confiable
Explotación de las debilidades del software	Acciones ilegales
Requerimientos de cambios realizados sin autorización	Contravención de requisitos normativos y legales
Modificación, eliminacion de los datos del sistema	Pérdidas económicas para la institución
Alteración de archivos de entrada de procesos por lotes	Adulteración de los datos de salida
Uso de exploits para un ataque dirigido	Infección de todos los equipos de la red

Tabla 43 Consecuencias: Fotos

Escenario	Consecuencia
Acceso a información reservada	Mal uso de la información obtenida
Divulgación de la información a los implicados	Pérdida de eficacia de la evidencia digital
Divulgación de la información a los implicados	Incumplimiento de los requisitos legales
Alteración de la fotos y videos	Prueba no aceptada en la Función Judicial
Falla de la tarjeta de almacenamiento y se corrompa los datos	No se puede obtener una evidencia digital válida
Pérdida de información por desconocimiento en el tratamiento de la misma	Pérdida de la evidencia digital
Fotos utilizadas para otros fines	Mala reputación de la institución y dudas de la confidencialidad de la información
Usuarios mal intencionados	Pérdida de información
Usurpación de usuarios para realizar acciones no autorizadas	Pérdida de información
Accesos de usuarios no permitidos con el fin de eliminar evidencias	Pérdida de evidendias digitales

Tabla 44 Consecuencias: Videos

Escenario	Consecuencia
Mediante accesos no autorizados se da el robo de la información	Pérdida de evidencia digital
Videos capturados por celulares personales pueden ser transferidos a terceros	Violación a la intimidad personal
Videos cortados o con montajes	Pérdida de la validez de la evidencia
Videos mal descargados	Pérdida de evidencia
Pérdida de información por desconocimiento en el tratamiento de la misma	Pérdida de la evidencia digital
Videos utilizados para otros fines	Mala reputación de la institución y dudas de la confidencialidad de la información
Usurpación de usuarios para realizar acciones no autorizadas	Pérdida de información
Accesos de usuarios no permitidos con el fin de eliminar evidencias	Pérdida de evidendias digitales

Tabla 45 Consecuencias: Partes contravenciones – Delitos de tránsito

Escenario	Consecuencia
Sustracción de información sensible	Falta de soporte para justificar los incidentes de tránsito
Violación a información personal y privada	Denuncias y sanciones por divulgar información no correspondiente
Mal registro de la información	Pérdida de información relevante
Usuario podría eliminar o modificar información de los partes ingresados	Pérdida de evidencia sobre la infracción
Manipulación de la información mediante el uso de otros usuarios	Encubrimiento de los usuarios responsables
Eliminación de la información relevante	Pérdida de evidencia sobre la infracción
Chantaje a los implicados a cambio de beneficios económicos	Mala reputación de los ACT

3.4 Valoración y Mapeo de Riesgos

La metodología aplicada para la estimación del riesgo es cualitativa, para de esta manera obtener una indicación general del nivel de riesgo y reflejar los riesgos más importantes que afecten a la cadena de custodia de las evidencias digitales.

La valoración del impacto se establece por el daño que puede ocasionar la materialización de las amenazas sobre los activos de información, de acuerdo a la siguiente clasificación:

Tabla 46 Criterios para la valoración del impacto

Valor	Nivel	Descripción
1	Menor	Leves consecuencias en los procesos de la institución
2	Moderado	Medianas consecuencias en los procesos, se puede corregir en corto tiempo sin afectar los objetivos estratégicos
3	Mayor	Daño significativo en la operatividad de los procesos, con un tiempo prolongado de recuperación
4	Crítico	Graves consecuencias en los procesos estratégicos de la institución, pérdidas económicas, incumplimientos legales, normativos

Los criterios para la clasificación de la probabilidad están expresados en la posibilidad de ocurrencia del suceso:

Tabla 47 Criterios para la valoración de la probabilidad

Valor	Ocurrencia	Descripción
1	Baja	Improbable
2	Media	Posible
3	Alta	Probable
4	Muy Alta	Muy probable

En base al histórico de la empresa y la definición de los propietarios, usuarios de los activos se estima la frecuencia de ocurrencia.

La clasificación del nivel de riesgo se realiza en base a la siguiente matriz:

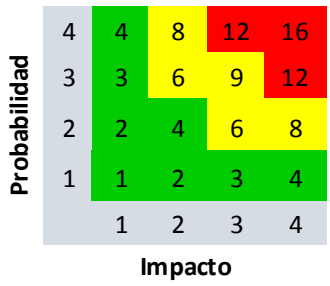


Figura 3.7 Matriz de Nivel de Riesgo

En donde:

Probabilidad (P)

Impacto (I)

Nivel de Riesgo (NR)

$$P * I = NR$$

El nivel de riesgo tiene las siguientes calificaciones y las acciones que se requieren ejecutar según el nivel:

Tabla 48 Determinación del Riesgo

Nivel de riesgo	Escala	Acciones
1 Aceptable	1 - 4	Se acepta el riesgo
2 Tolerable	6 - 9	Requiere de tratamiento, plan de acción a mediano plazo
3 No tolerable	12 -16	Requiere de tratamiento prioritario, plan de acción a corto plazo

3.4.1 Tratamiento de los Riesgos

Para el tratamiento de los riesgos se selecciona controles adecuados con el fin de mitigar o reducir los riesgos identificados, se consideran los activos con nivel de riesgo alto y medio, debido a su relevancia los altos son tratados a corto plazo y los de nivel medio en un plazo más largo.

Las opciones consideradas para el tratamiento del riesgo son las siguientes:

Tabla 49 Opciones de tratamiento del riesgo

Medida	Descripción
Evitar	Eliminar las actividades que generen el riesgo
Aceptar	Reconocer el riesgo y monitorear por su posible cambio de estado
Transferir	Compartir el riesgo con terceros
Mitigar	Implementar controles para mitigar, reducir el riesgo

Los controles están definidos en base a la norma NTE-ISO-IEC 27001 y en consideración con la norma ISO 27037:2012 en particular con los requerimientos de controles concernientes con la adquisición de evidencia digital. Para la selección de los controles se ha considerado algunos factores como el costo beneficio, legislación y regulaciones, política organizacional, impacto operacional, seguridad y confiabilidad.

Los resultados de los riesgos con nivel alto y nivel medio, con los controles recomendados son los siguientes:

Tabla 50 Riesgo inherente: Portátiles

Amenaza	Riesgo inherente	Controles recomendados
Hurto de equipo	Tolerable	A.9.1.5 Trabajo en áreas seguras A.9.2.5 Seguridad de los equipos fuera de las instalaciones A.11.7.1 Equipos portátiles y comunicaciones móviles A.12.3.1 Política de uso de los controles criptográficos A.12.3.2 Gestión de claves A.15.1.3 Protección de los documentales de la organización A.15.1.6 Regulación de los controles criptográficos
Manipulación con hardware	Tolerable	A.9.1.3 Seguridad de oficinas, despachos e instalaciones A.9.2.5 Seguridad de los equipos fuera de las instalaciones
Manipulación con software	Tolerable	A.10.4.1 Controles contra el código malicioso A.10.4.2 Controles contra el código descargable en el cliente
Mal funcionamiento del software	Tolerable	A.12.4.1 Control de software en explotación A.12.5.1 Procedimientos de control de cambios A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo A.12.5.3 Restricciones a los cambios en los paquetes de software
Uso de software falso o copiado	Tolerable	A.15.1.2 Derechos de propiedad intelectual
Procesamiento ilegal de los datos	Tolerable	A.11.2.2 Gestión de privilegios A.11.2.4 Revisión de los derechos de acceso de usuario A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
Abuso de derechos	Tolerable	A.11.2.4 Revisión de los derechos de acceso de usuario
Intrusión, accesos forzados, acceso no autorizado	Tolerable	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.11.5.4 Usos de los recursos del sistema A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad A.13.2.1 Responsabilidades y procedimientos A.13.2.2 Aprendizaje de los incidentes de seguridad de la información A.13.2.3 Recopilación de evidencias A.15.2.1 Cumplimiento de las políticas y normas de seguridad A.15.2.2 Comprobación del cumplimiento técnico

Tabla 51 Riesgo inherente: Pc escritorio

Amenaza	Riesgo inherente	Controles recomendados
Manipulación con software	Tolerable	A.10.4.1 Controles contra el código malicioso A.10.4.2 Controles contra el código descargable en el cliente

Tabla 52 Riesgo inherente: PDA

Amenaza	Riesgo inherente	Controles recomendados
Destrucción	Tolerable	A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.9.2.4 Mantenimiento de los equipos A.10.1.1 Documentación de los procedimientos de operación
Hurto de equipo	Tolerable	A.7.1.1 Inventario de Activos A.7.1.2 Propiedad de los activos A.9.2.5 Seguridad de los equipos fuera de las instalaciones
Manipulación con Software/Código malicioso	Tolerable	A.10.4.1 Controles contra el código malicioso A.10.4.2 Controles contra el código descargable en el cliente
Uso no autorizado del equipo	Tolerable	A.9.2.1 Emplazamiento y protección de equipos

Tabla 53 Riesgo inherente: Alcoholímetros

Amenaza	Riesgo inherente	Controles recomendados
Destrucción del equipo o los medios	No tolerable	A.9.2.4 Mantenimiento de los equipos A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.10.1.1 Documentación de los procedimientos de operación
Hurto de equipo	Tolerable	A.7.1.1 Inventario de Activos A.7.1.2 Propiedad de los activos A.9.2.5 Seguridad de los equipos fuera de las instalaciones
Falla del equipo / Mal funcionamiento del equipo	No tolerable	A.9.2.4 Mantenimiento de los equipos A.10.10.5 Registro de fallos
Uso no autorizado del equipo	Tolerable	A.9.2.1 Emplazamiento y protección de equipos
Error en el uso	Tolerable	A.10.1.1 Documentación de los procedimientos de operación

Tabla 54 Riesgo inherente: Radares

Amenaza	Riesgo inherente	Controles recomendados
Destrucción del equipo o los medios	No tolerable	A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.10.1.1 Documentación de los procedimientos de operación
Falla del equipo / Mal funcionamiento del equipo	Tolerable	A.9.2.4 Mantenimiento de los equipos A.10.10.5 Registro de fallos
Error en el uso	Tolerable	A.10.1.1 Documentación de los procedimientos de operación

Tabla 55 Riesgo inherente: DVR

Amenaza	Riesgo inherente	Controles recomendados
Destrucción del equipo o los medios	No tolerable	A.7.1.2 Propiedad de los activos A.8.2.3 Proceso disciplinario A.9.2 Seguridad de los equipos A.9.2.4 Mantenimiento de los equipos A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.10.1.1 Documentación de los procedimientos de operación A.10.10.2 Supervisión del uso del sistema
Hurto de equipo	Tolerable	A.9.1.5 Trabajo en áreas seguras A.9.2.5 Seguridad de los equipos fuera de las instalaciones A.11.7.1 Equipos portátiles y comunicaciones móviles A.12.3.1 Política de uso de los controles criptográficos A.12.3.2 Gestión de claves A.15.1.3 Protección de los documentales de la organización A.15.1.6 Regulación de los controles criptográficos
Falla del equipo / Mal funcionamiento del equipo	Tolerable	A.9.2.4 Mantenimiento de los equipos A.10.10.5 Registro de fallos
Error en el uso	Tolerable	A.10.1.1 Documentación de los procedimientos de operación A.10.10.2 Supervisión del uso del sistema

Tabla 56 Riesgo inherente: Sistemas

Amenaza	Riesgo inherente	Controles recomendados
Mal funcionamiento del software	No tolerable	A.12.4.1 Control del software en explotación A.12.5.1 Procedimiento de control de cambios A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad
Uso de software falso o copiado	Tolerable	A.15.1.2 Derechos de propiedad intelectual
Error en el uso	Tolerable	A.12.2.1 Validación de los datos de entrada Capacitacion en el uso de los sistemas de información y actualización de los manuales de usuario cuando amerite
Abuso de derechos/Falsficación de derechos	Tolerable	A.12.4.3 Control de acceso al código fuente de los programas A.12.5.4 Fugas de información A.12.6.1 Control de vulnerabilidades técnicas A.13.1.2 Notificación de los puntos débiles de seguridad
Negación de acciones	Tolerable	A.12.5.1 Procedimientos de control de cambios
Intrusión, accesos forzados al sistema, accesos no autorizados al sistema, sabotaje del sistema	Tolerable	A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad A.10.10.1 Registro de auditorías
Ingreso de datos falsos o corruptos	Tolerable	A.12.2.1 Validación de los datos de entrada A.12.2.2 Control del procesamiento interno A.12.2.3 Integridad de los mensajes A.12.2.4 Validación de los datos de salida A.10.10.1 Registro de auditorías
Errores en el sistema (bugs)	No tolerable	A.12.1.1 Análisis y especificación de los requisitos de seguridad A.12.4.1 Control del software en explotación A.12.5.1 Procedimiento de control de cambios A.12.5.2 Revisión técnica A.12.5.4 Fugas de información A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad

Tabla 57 Riesgo inherente: Fotos

Amenaza	Riesgo inherente	Controles recomendados
Hurto de medios o documentos	Tolerable	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.10.5.1 Copias de seguridad de la información
Divulgación	No tolerable	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.8.2.2 Concienciación, formación y capacitación en seguridad de la información
Manipulación con software	No tolerable	A.10.5.1 Copias de seguridad de la información - Verificar la información de la metadata para confirmar su integridad mediante herramientas de software - Planes corporativos de los celulares que utilicen los ACT para capturar las fotos que servirán como evidencia
Corrupción de los datos	No tolerable	A.10.5.1 Copias de seguridad de la información ISO TR 15801 / Suma de comprobación calculada después de captura de información - Herramientas de almacenamiento sincronizado en linea Mantenimiento periódico de las tarjetas - Herramientas de recuperación de archivos - Planes corporativos de los celulares que utilicen los ACT para capturar las fotos que servirán como evidencia
Error en el uso	Tolerable	A.5.1.1 Publicar y distibuir a todos los empleados de la EMOV y terceros afectados el Documento de Política de Seguridad. A.5.1.2 Revisión de la política de seguridad de la información A.8.1.1 Funciones y Responsabilidades A.8.2.1 Respondabilidad de la Dirección A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.10.1.1 Documentación de los procedimientos de operación
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	Tolerable	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad

Tabla 58 Riesgo inherente: Videos

Amenaza	Riesgo inherente	Controles recomendados
Hurto de medios o documentos	Tolerable	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.10.5.1 Copias de seguridad de la información
Divulgación	No tolerable	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.8.2.2 Concienciación, formación y capacitación en seguridad de la información
Manipulación con software	No tolerable	A.10.5.1 Copias de seguridad de la información - Verificar la información de la metadata para confirmar su integridad mediante herramientas de software - Planes corporativos de los celulares que utilicen los ACT para capturar los videos que servirán como evidencia
Corrupción de los datos	No tolerable	A.10.5.1 Copias de seguridad de la información ISO TR 15801 / Suma de comprobación calculada después de captura de información - Herramientas de almacenamiento sincronizado en linea - Mantenimiento periódico de las tarjetas - Herramientas de recuperación de archivos - Planes corporativos de los celulares que utilicen los ACT para capturar los videos que servirán como evidencia
Error en el uso	Tolerable	A.5.1.1 Publicar y distibuir a todos los empleados de la EMOV y terceros afectados el Documento de Política de Seguridad. A.5.1.2 Revisión de la política de seguridad de la información A.8.1.1 Funciones y Responsabilidades A.8.2.1 Respondabilidad de la Dirección A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.10.1.1 Documentación de los procedimientos de operación
Negación de acciones	Tolerable	A.10.10.1 Registro de auditorías A.10.10.2 Supervisión del uso del sistema
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	Tolerable	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.11.6 Control de Acceso a las aplicaciones y a la información A.11.6.2 Aislamiento de sistemas sensibles A.12.6.1 Control de las vulnerabilidades técnicas A.13.1 Notificación de eventos de seguridad de la información A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad

Tabla 59 Riesgo inherente: Partes contravenciones – Delitos de tránsito

Amenaza	Riesgo inherente	Controles recomendados
Divulgación	Tolerable	A.7.2.2. Etiquetado y manejo de la información
Abuso de derechos	Tolerable	A.10.1.3 Segregación de Tareas A.10.10.1 Registro de auditorías A.10.10.2 Supervisión del uso del sistema A.11.2.4 Revisión de los derechos de acceso de usuario
Negación de acciones	Tolerable	A.10.10.1 Registro de auditorías A.10.10.2 Supervisión del uso del sistema
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema	Tolerable	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.11.6 Control de Acceso a las aplicaciones y a la información A.11.6.2 Aislamiento de sistemas sensibles A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad
Soborno de la información (Interno)	Tolerable	A.8.1.2 Investigación de antecedentes A.8.1.3 Términos y condiciones de contratación A.8.2.1 Responsabilidades de la Dirección A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.8.2.3 Proceso disciplinario

Las soluciones de los activos que están involucrados en la generación de las evidencias digitales son la base para la gestión de la cadena de custodia de las mismas y el desarrollo efectivo de los procedimientos correspondientes.

CAPÍTULO 4

DISEÑO DEL ESQUEMA DE GESTIÓN DE CADENA DE CUSTODIA DE LA EVIDENCIA DIGITAL

4.1 Alcance del Esquema de Gestión de Cadena de Custodia de la Evidencia Digital

Según el análisis y valoración de riesgos, realizados en el capítulo anterior, y a pesar de la existencia de ciertos controles, encontramos varios activos con un riesgo inherente no tolerable, que afecta a la gestión de la cadena de custodia de la evidencia digital, por lo que requieren de un tratamiento prioritario mediante un plan de acción a corto plazo.

Entre los activos relacionados directamente con las evidencias digitales se puede enumerar los siguientes: DVR, sistemas, portátiles, radares, y entre los activos propios como evidencia digital son las fotos y videos, por lo que se desarrolla los controles para la gestión de la cadena de custodia, que permita

garantizar su integridad desde el momento de la recolección hasta la presentación ante un juez.

El detalle de los controles internos se basa en las Norma NTE-ISO-IEC 27001:2011, y se aplica tanto para las amenazas con riesgo no tolerable, como para las de riesgo tolerable, de estos activos. Además, se considera la Norma ISO-IEC-27307:2012 para la gestión de la evidencia digital en sus diversas fases y los criterios de valoración en los que el juez se basa para la aceptación de las pruebas:

Principio de legalidad, es decir, que la prueba sea legalmente obtenida, si es que estas pruebas son obtenidas de manera ilegal, por mandato constitucional carecen de eficacia probatoria.

Principio de autenticidad, que no sea alterado y no exista un mecanismo a través del cual no se pueda confiar en las evidencias.

Principio de idoneidad, la prueba debe ser auténtica, relevante y exclusiva del motivo de investigación, suficiente para el caso. [13]

Las videograbaciones que pueden ser aceptadas como pruebas son:

- Videos de seguridad, captados en lugares públicos y de libre circulación, con fundamento legal, en el Decreto Ejecutivo 988 publicado en el Registro Oficial Nro. 618 el 13 de enero del 2012, que regula el servicio integrado de la Seguridad ECU 911, que se establece como una herramienta tecnológica e integradora de los servicios de emergencia: salud, seguridad ciudadana,

incendios, rescate, riesgos de origen natural y otros que pongan en riesgo la seguridad de las personas; no existe vulneración a la intimidad porque los dispositivos están ubicados en espacios públicos. [14]

- Videos capturados por los ACT, con fundamento legal, artículo 393 de la Constitución de la República *"El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno".* [2]
- Videos e información emitida por los dispositivos de control de transporte de tránsito y transporte terrestre que está basado en el artículo 149 de la Ley Orgánica de Transporte Terrestre y Seguridad Vial: *"Para el juzgamiento de las infracciones de tránsito constituyen medios de prueba la información emitida por los dispositivos de control de tránsito, sean electrónicos, magnéticos, digitales o analógicos, fotografías, videos y similares. Son aplicables para las infracciones de tránsito las normas que, respecto de la prueba y su valoración contiene el Código de Procedimiento Penal".* [15]

Existen dispositivos detector de infracciones de transporte terrestre que pueden ser fijos o instalados en lugares definidos, móviles instalados en un vehículo en movimiento o estacionado en la vía. Los detectores de infracciones son los radares que permiten detectar la velocidad, si está dentro o fuera del rango permitido; los alcohotectores que permitan efectuar las pruebas de alcohotest sobre los conductores que se presuma se encuentren en estado de embriaguez,

estos dispositivos deben estar homologados por la Agencia Nacional de Tránsito, conforme con las disposiciones constantes en la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial y en el respectivo reglamento.

- Videos captados por las cámaras instaladas en las patrullas de la EMOV, se aceptan solo los grabados en la vía pública y si el video es cortado pierde toda validez.
- Videos realizados por los medios de comunicación o capturados de forma espontánea por cámaras privadas.

Las videograbaciones, las imágenes realizadas desde la vía pública sobre hechos que se desarrollan las vía pública, tienen límites y deben ser respetados, como la dignidad del ser humano, es decir no puede afectar a la intimidad personal, no se puede captar grabaciones para tomar imágenes, sonidos en el interior de un vehículo salvo el consentimiento de su titular, el eje al derecho a la intimidad está el consentimiento.

Cabe señalar que las infracciones de tránsito se dividen en delitos y contravenciones, de lo cual depende para el tratamiento de los videos como pruebas:

- **Delitos de tránsito,** en donde la Fiscalía necesariamente nombra un perito a fin de que establezca un informe, de acuerdo al art. 467 del COIP del reconocimiento de objetos, en donde reconocerá las grabaciones, nombra dos peritos que juren guardar reserva en una audiencia privada, procede a la exhibición del video, escucha, examina su contenido y los registros digitales. [4]

- **Contravenciones,** por la poca monta de la infracción, de la pena no es posible nombrar un perito para que establezca si el video es íntegro, si es fidedigno, esto se hace dentro de una sala de audiencia en la que están las partes procesales y este video se somete a la contradicción en donde el impugnante puede verificar el video tomado y en base a la verificación puede hacer las alegaciones que él se crea asistido.

Para el activo Videos, se consideran controles que contribuirán a mejorar los siguientes aspectos:

- Obtener la evidencia en los repositorios de la EMOV-EP, en el momento en que se suscita la contravención (videos captados desde teléfonos celulares)
- Mantener copias de seguridad de los videos captados por los DVR, por lo menos 90 días por el tipo de procedimientos gestionados
- Comprobar la integridad entre los videos en su ubicación original y las copias de seguridad realizadas en los repositorios de la EMOV-EP
- Restringir el acceso a estas evidencias a personal no autorizado
- Obtener un log de las acciones (creación, modificación, eliminación) realizadas sobre estos archivos

Las fotografías, son elementos representativos que sirve para probar el estado del hecho que existía al momento de ser tomada, es una prueba demostrativa. En la EMOV se utilizan foto radar, fotos de los alcohotectores y las de las propias cámaras para adjuntar a los partes que remiten, en el art. 163 de la Ley Orgánica de Transporte Terrestre y Seguridad Vial especifica que *"El parte policial por delitos y contravenciones de tránsito, debe contener una relación detallada y minuciosa del hecho y sus circunstancias, incluyendo croquis y de*

ser posible, fotografías que evidencien el lugar del suceso y los resultados de la infracción…" [15]

En el caso del activo Fotos se propone la implementación de herramientas que ayudan principalmente a:

- Obtener la evidencia en los repositorios de la EMOV-EP, en el momento en que se suscita la contravención, siempre y cuando esta sea captada desde un teléfono celular
- Mantener copias de seguridad de estas evidencias
- Comprobar la integridad entre las imágenes captadas y las almacenadas en los repositorios de la EMOV-EP, esto es por ejemplo, a través de la obtención de un código único que garantice la integridad de las imágenes
- Comprobar la veracidad de las imágenes
- Restringir el acceso a estas evidencias a personal no autorizado
- Obtener un log de las acciones (creación, modificación, eliminación) realizadas sobre estos archivos

Se define también el protocolo de cadena de custodia que avale la veracidad e integridad de ambos activos, cuando estos constituyan una evidencia digital y sean requeridos dentro de un proceso judicial.

4.2 Definición de los controles internos

A.5 Política de seguridad

Tabla 60 Control A.5.1.1

A.5.1.1	Documento de política de seguridad de la información	*Control* La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.

Si bien existe la Política de Seguridad de la Información, esta debe ser socializada a todo el personal de la EMOV y a terceros involucrados, por las diferentes vías de comunicación utilizadas por la empresa (correos electrónicos, carteleras informativas, sesiones grupales).

Tabla 61 Control A.5.1.2

A.5.1.2	Revisión de la política de seguridad de la información	*Control* La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Es recomendable que la Política de Seguridad de la Información sea revisada y actualizada anualmente. En la actualidad la política vigente tiene fecha de aprobación del año 2015 por lo que es necesaria su revisión inmediata.

A.7 Gestión de activos

Tabla 62 Control A.7.2.1

A.7.2.1	Directrices de clasificación	*Control* La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.

Según el inventario de activos realizado se identifica que existe información que es dirigida a uso público, uso interno y uso restringido, por lo que se clasifica con los propietarios de los activos de información bajo estos criterios:

- Uso Público: Información que ha sido declarada de conocimiento público es decir que puede ser conocida y utilizada sin autorización por cualquier persona. LOTAIP Art. 7 Difusión de la Información Pública. Como por ejemplo las Estadísticas de Incidentes de tránsito.
- Uso Interno: Información que puede ser conocida y utilizada solo por los funcionarios de la EMOV. Ejemplo las Órdenes de Cuerpo.
- Uso Restringido: Información que solo puede ser conocida y utilizada por un departamento o grupo de empleados específicos. Ejemplo: Fotos, Videos.

Esta clasificación se recomienda que sea validada en conjunto con los propietarios de los activos de información, el administrador de seguridad de la información (personal de TICS y el responsable de gestión documental.

Tabla 63 Control A.7.2.2

A.7.2.2	Etiquetado y manejo de la información	*Control* Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

En base a la clasificación anterior se debe etiquetar la información de la siguiente manera: en caso de información de uso restringido y de uso interno se debe identificar la clasificación, ya sea en el encabezado del documento, en el nombre del archivo, en la etiqueta del medio de almacenamiento o en una nota

anexa. La información que no esté etiquetada se asume que es de uso público, tomando como opcional su etiquetado.

A.8 Seguridad ligada a los recursos humanos

Tabla 64 Control A.8.1.1

A.8.1.1	Funciones y responsabilidades	*Control* Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.

La Política de Seguridad de la Información, tiene que ser de lectura obligatoria al momento de incorporar personal nuevo a la empresa, así mismo con los proveedores externos o terceras personas que accedan a la información de le EMOV. Cada una de estas personas debe conocer los activos de información con los que va a interactuar, cuál es su clasificación y quién es el propietario del mismo.

Tabla 65 Control A.8.2.1

A.8.2.1	Responsabilidades de la Dirección	*Control* La Dirección debe exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.

Establecer por parte de la Dirección mecanismos de monitoreo y control como encuestas, entrevistas dirigidos a los empleados, auditorías, pruebas de incidentes controlados. Según los resultados obtenidos se puede optar por brindar mayores capacitaciones o aplicar sanciones dependiendo del caso.

Tabla 66 Control A.8.2.2

A.8.2.2	Concienciación, formación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.

Definir un plan de capacitación periódico sobre las nuevas herramientas tecnológicas de las que dispone la EMOV y la seguridad de la información relacionada a estas con el objetivo de generar un cambio de cultura y sensibilizar a los empleados para dar la importancia debida como por ejemplo en temas de ingeniería social, gestión de usuarios, uso de recursos, etc.

A.10 Gestión de comunicaciones y operaciones

Tabla 67 Control A.10.1.1

A.10.1.1	Documentación de los procedimientos de operación	*Control* Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

Elaborar y actualizar manuales de usuarios y procedimientos de todas las herramientas de software con los que cuenta la EMOV, los mismos tendrían que tener facilidad de acceso, alojados en la intranet de la empresa, sección Manuales o Biblioteca Digital.

Tabla 68 Control A.10.1.3

A.10.1.3	Segregación de tareas	*Control* Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

Elaborar el documento correspondiente y aprobarlo sobre las tareas y responsabilidades de la parte administrativa que cumplen los ACT en la actualidad.

Tabla 69 Control A.10.5.1

A.10.5.1	Copias de seguridad de la información	*Control* Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente conforme a la política de copias de seguridad acordada.

Almacenar el repositorio de la estructura de carpetas de documentos digitales, en un servidor de archivos en lugar de tener en computadoras independientes, de esta forma se pueden obtener las siguientes ventajas:

- Los permisos a las carpetas son centralizados, el administrador gestionará los respectivos permisos a los usuarios de red.
- De esta forma se pueden habilitar las auditorias de los archivos para saber cuándo un archivo es modificado.

Adicionalmente, se recomienda que la estructura de carpetas en el tercer nivel el formato de fechas sea yyyyMMdd (Ej.: 20170618).

Es necesario que una vez centralizada la información (fotos), sea incluida en el respaldo general que mantiene la EMOV.

Para el caso de los videos la solución recomendable es la implementación de un NAS (Network Attached Storage), que consiste en un disco duro de gran capacidad que cuenta con conexión directa a la red, entre las ventajas que se obtienen con esta solución:

- El NAS puede incluir dos o más discos lo que permite configurar discos espejos o sistema RAID (Redundant Array of Independent Disks), de esta forma siempre se contará con un respaldo implícito en caso de que uno de los discos falle.
- Al ser un disco de red, este podrá ser accedido por varios usuarios y máquinas concurrentes
- Obtener soluciones de este tipo a bajo costo
- Permite habilitar el acceso al NAS desde redes externas, lo que permite que información capturada desde dispositivos móviles pueda ser almacenada directamente al disco en tiempo real como por ejemplo los videos capturados por los celulares de los ACT.

Tabla 70 Control A.10.10.1

A.10.10.1	Registro de auditorias	*Control* Se deben generar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deberían mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.

A nivel de servidor se debe activar las directivas de seguridad correspondientes para auditar los eventos de aplicaciones y del sistema. Asimismo se debe habilitar la auditoría de acceso a objetos para las carpetas que contengan evidencias digitales, con el fin de conocer cuándo estas son creadas, modificadas o eliminadas, incluyendo el usuario que ejecuto alguna de estas acciones.

Tabla 71 Control A.10.10.2

A.10.10.2	Supervisión del uso del sistema	*Control* Se deben establecer procedimientos para supervisar el uso de los recursos de tratamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión.

Realizar supervisiones periódicas tanto de hardware como de software para verificar el estado de los equipos, software instalado no autorizado, configuraciones generales, uso correcto de recursos asignados.

A.11 Control de acceso

Tabla 72 Control A.11.2.4

A.11.2.4	Revisión de los derechos de acceso de usuario	*Control* La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.

Realizar una revisión periódica por muestreo utilizando el “formulario para creación y modificación de usuarios de los sistemas informáticos de la EMOV” que son aplicados para dar los respectivos permisos a los usuarios.

Tabla 73 Control A.11.4.4

A.11.4.4	Diagnóstico remoto y protección de los puertos de configuración	*Control* Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.

En medida de lo posible es recomendable no tener puertos de configuración abiertos que puedan ser accedidos remotamente, si es que estos no son estrictamente necesarios. Caso contrario estos puertos deben ser correctamente habilitados, solo a los usuarios que lo necesiten y bajo la autorización de la Subgerencia de TICS, se debe evitar habilitar este puerto al usuario administrador por default del sistema. Y realizar un monitoreo continuo de las conexiones realizadas por acceso remoto. Puede incluirse la asignación y uso de dispositivos removibles matriculados.

Tabla 74 Control A.11.6.2

A.11.6.2	Aislamiento de sistemas sensibles	*Control* Los sistemas sensibles deben tener un entorno dedicado (aislado) de computadores.

Como se recomendó en el apartado A.10.5.1 la implementación de un NAS, permitiría la creación de una red aislada ya que el disco cuenta con un puerto de red, de esta forma se puede crear la subred entre el disco y los equipos designados para la gestión de los videos.

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

Tabla 75 Control A.12.6.1

A.12.6.1	Control de las vulnerabilidades técnicas	*Control* Se debe obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

Detallar todas las novedades encontradas en la experiencia de la utilización del programa de descargar de videos, mantener el registro y reportar a los responsables de TICS.

A.13 Gestión de incidentes de seguridad de la información

Tabla 76 Control A.13.1.1

A.13.1.1	Notificación de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible.

Elaborar un procedimiento de gestión de incidentes en donde se describa los roles, acciones a tomar cuando se presenten los eventos y qué medios utilizar para la notificación como por ejemplo tickets, correo electrónico, llamadas, mesa de usuario, para esto se pueden apoyar en herramientas de gestión de incidentes, mesas de ayuda, en la actualidad hay varias herramientas gratuitas orientadas a este fin como GLPI (Gestionnaire Libre de Parc Informático), osTicket, REDMINE, entre otras.

Tabla 77 Control A.13.1.2

A.13.1.2	Notificación de los puntos débiles de seguridad	*Control* Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios.

Partiendo de la concienciación y de la cultura de seguridad de la información que deben tener los empleados y terceros, tienen la responsabilidad de notificar cualquier vulnerabilidad detectada, la misma que debe estar debidamente documentada para su justificación.

4.3 Prototipo de implementación de componentes tecnológicos para la gestión de cadena de custodia de la evidencia digital

Los componentes tecnológicos para la gestión de la cadena de custodia están basados en mantener la autenticidad e integridad de la evidencia digital desde la identificación en la escena de los hechos, recolección/adquisición, análisis, preservación, presentación, hasta su eliminación y de esta manera garantizar su valor probatorio.

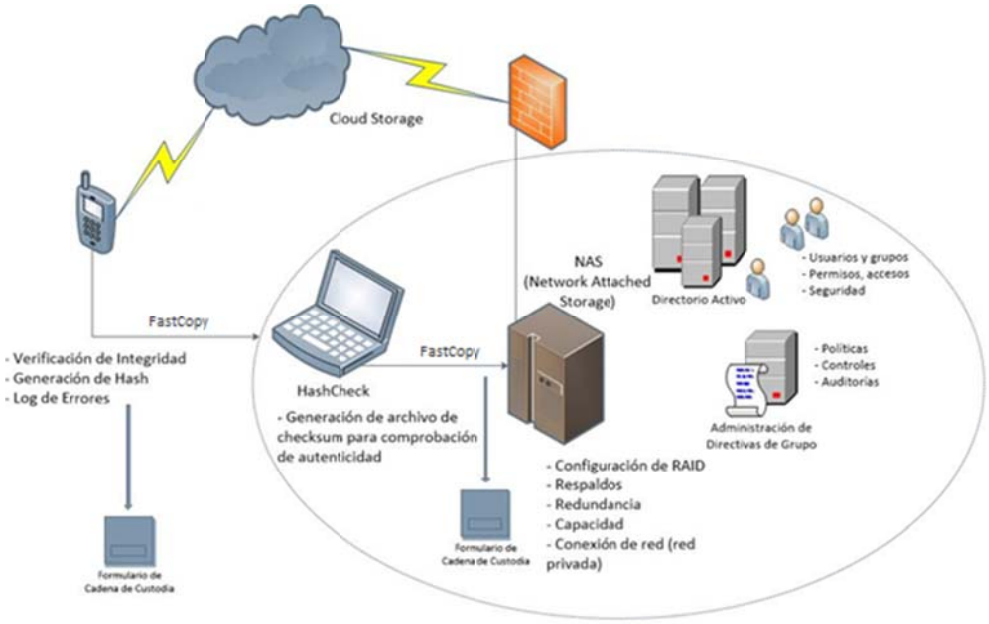


Figura 4.1 Prototipo de esquema de seguridad nivel 1

El modelo contempla herramientas y procedimientos básicos para establecer un esquema de seguridad de nivel 1, para el cumplimiento de la cadena de custodia de las evidencias captadas por los ACT con sus dispositivos móviles. En este diseño se encuentran herramientas de software que verifican la integridad y autenticidad de las mismas, mediante sumas de comprobación, mecanismos para almacenamiento en la nube, y respaldos, además del diligenciamiento del respectivo formulario de cadena de custodia en las diferentes etapas de las evidencias.

4.3.1 Protocolo de Cadena de Custodia de la Evidencia digital

Se define el procedimiento y las personas que intervienen como responsables en las diferentes etapas de la cadena de custodia de las evidencias digitales, desde su captura hasta su disposición final:

1. Identificación de las evidencias

Figura 4.2 Procedimiento etapa identificación de las evidencias

Desde que se capta el video entra en el proceso de cadena de custodia, es así en el lugar de los hechos, el ACT debe tratar de que todos los procedimientos aplicados sean captados en su totalidad, la ubicación de la patrulla tiene que ser dirigida a que las cámaras capten los sucesos y mediante la observación directa identificará las evidencias que pueden ser captadas por un dispositivo móvil de su propiedad; además que se debe cumplir con el reglamento para la elaboración de los partes por accidentes de tránsito y personas aprehendidas en donde se especifica el requerimiento de una fotografía panorámica y de las diferentes partes de los vehículos involucrados (parte frontal-lateral derecha-posterior-lateral izquierda).

Actores:

- ACT, responsable del procedimiento

2. Recolección / Adquisición

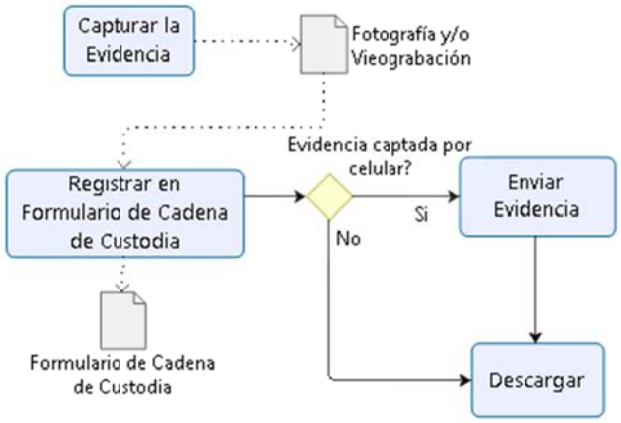


Figura 4.3 Procedimiento etapa recolección / adquisición

El ACT que toma procedimiento realizará la fijación de la evidencia mediante la fotografía y/o la videograbación; las que son capturadas por el celular son enviadas a la Central de Radio, mediante la aplicación de mensajería instantánea WhatsApp. El ACT de la Central de Radio recibe las evidencias y se encarga de la descarga de las mismas.

Las videograbaciones capturadas por las cámaras de las patrullas, son descargadas únicamente cuando se solicita, por la Gerencia de Control, Subgerencia de Control, o los Agentes Civiles de Tránsito, siendo responsable de la descarga el ACT de TICs.

En esta etapa se debe diligenciar la sección 1 del Formulario de la Cadena de Custodia.

Actores:

- ACT, responsable del procedimiento
- ACT en turno, responsable de la Central de Radio

- ACT, responsable de las descargas de DVRs

Documentos:

- Formulario de Cadena de Custodia

3. Análisis

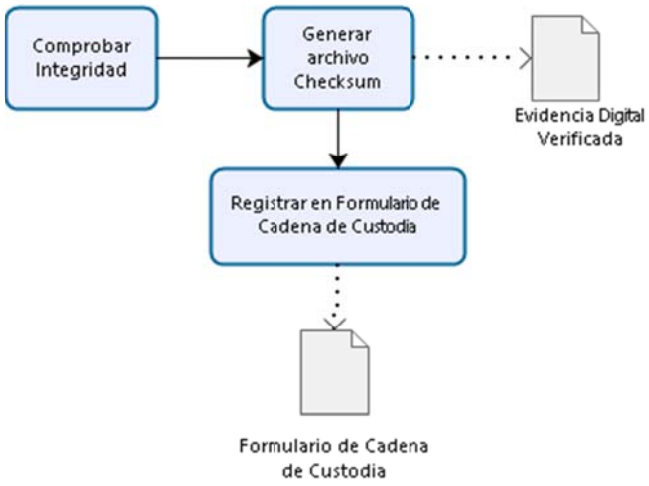


Figura 4.4 Procedimiento etapa análisis

Para la descarga y la verificación de las evidencias enviadas, el ACT de la Central de Radio, se apoyará en una herramienta de software para el tratamiento de evidencias digitales. Esta herramienta a más de presentar información como la cantidad de archivos copiados, el tiempo de duración, genera logs de las copias realizadas, en donde contiene información de la carpeta origen, la carpeta destino, el nombre del archivo con su tamaño y el hash tipo SHA-1 e indica si es que se dieron errores o no al momento de la transferencia. El ACT debe verificar que todos los archivos fueron copiados exitosamente.

A continuación, el ACT se apoyará en otra herramienta para la generación del archivo de checksum (SHA), lo cual ayudará posteriormente a la comprobación de la autenticidad de la evidencia.

En esta etapa se debe registrar la sección 2 del formulario de la cadena de custodia, en el que se debe incluir el nombre del archivo de checksum generado y el hash del mismo.

Actores:

- ACT en turno, responsable de la Central de Radio
- ACT, responsable de las descargas de los DVRS

Documentos:

- Formulario de Cadena de Custodia

Herramientas:

- Herramienta 1 (Comprobación de Integridad): FastCopy
- Herramienta 2 (Comprobación de Autenticidad): Hashcheck

4. Preservación

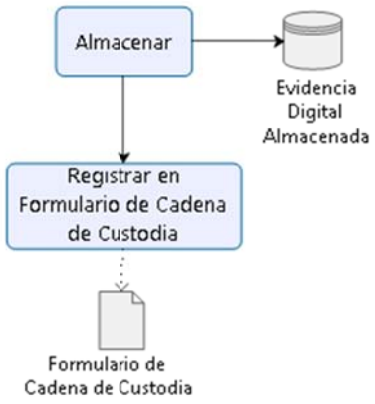


Figura 4.5 Procedimiento etapa preservación

Si la evidencia no ha sido descargada directamente en el repositorio designado para la preservación de evidencias digitales, estas deberán ser movidas a dicho repositorio, para esto se deberá utilizar la primera herramienta de software descrita en la etapa anterior (FastCopy).

El tiempo que se ha definido para la preservación de las evidencias, antes de que estas puedan ser eliminadas es de 90 días por el tipo de procedimientos que se gestiona.

En esta etapa se debe registrar la sección 3 del formulario de la cadena de custodia.

Actores:

- ACT en turno, responsable de la Central de Radio
- ACT TICS, responsable de los DVRS

Documentos:

- Formulario de Cadena de Custodia

5. Presentación

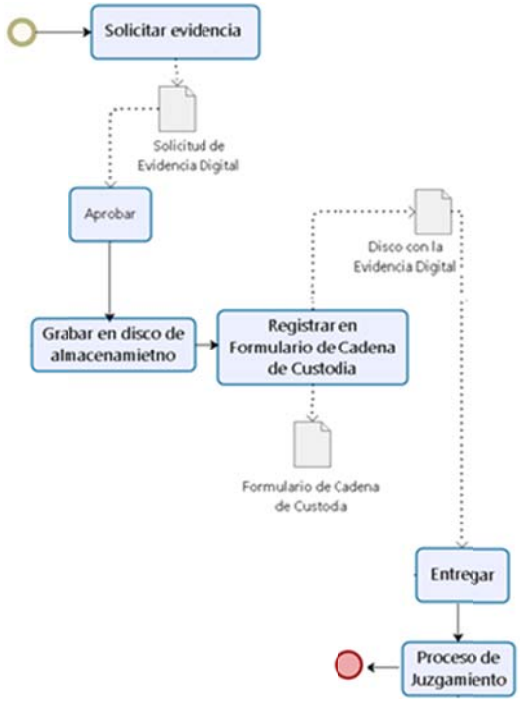


Figura 4.6 Procedimiento etapa presentación

La evidencia digital verificada en la etapa de análisis será grabada en un disco de almacenamiento por parte del ACT en turno de la Central de Radio y será entregado al ACT responsable del procedimiento, quién presentará al juez designado para el caso.

Las videograbaciones de las patrullas son solicitados generalmente para impugnaciones, requerimientos del Gerente y/o Subgerente de Control; en las impugnaciones las videograbaciones serán solicitadas mediante oficio por parte del ACT responsable del procedimiento impugnado, luego de la aprobación de la solicitud por el Subgerente de Planificación, el ACT

de TICS procederá a grabar en el disco las evidencias correspondientes y entregará al ACT solicitante, quién presentará al juez.

Esta etapa será diligenciada en la sección 4 del formulario de la cadena de custodia, en el que se registrará el tipo de medio en el que se graba la evidencia, fecha y hora de entrega del medio, el nombre y firma del ACT quien recibe el medio de almacenamiento e información del fiscal y/o juez según corresponda.

Actores:

- ACT, responsable del procedimiento
- Subgerente de Planificación de Control de Tránsito
- Juez de Tránsito

Documentos:

- Formulario de Cadena de Custodia
- Parte de Tránsito

6. Eliminación

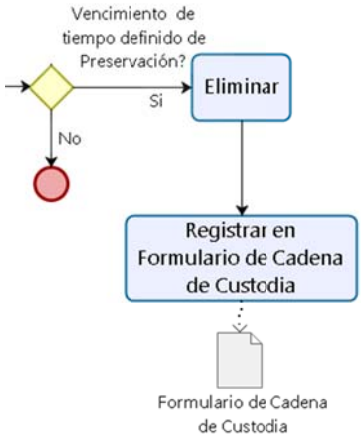


Figura 4.7 Procedimiento etapa eliminación

Considerado el tiempo de preservación de los 90 días, se realizará la eliminación de las evidencias digitales alojadas en el repositorio que se encuentra en línea, a cargo de un responsable designado de TICS. La fecha, hora y responsable de la acción será registrada en el Formulario de Cadena de Custodia, en la sección 5.

Actores:

- ACT, designado para la acción por parte de la Central de Radio
- ACT, designado para la acción por parte de Planificación para los videos de los DVRS

Documentos:

- Formulario de Cadena de Custodia

CAPÍTULO 5

IMPLEMENTACIÓN DEL ESQUEMA DE GESTIÓN DE CADENA DE CUSTODIA DE LA EVIDENCIA DIGITAL

5.1 Instalación y configuración de software a ser utilizado

5.1.1 Instalación de FastCopy

Esta herramienta no tiene un instalador, sino que sus archivos vienen comprimidos en un .zip, por lo que lo primero que se debe hacer es crear una carpeta llamada ***FastCopy*** en el disco ***C***.

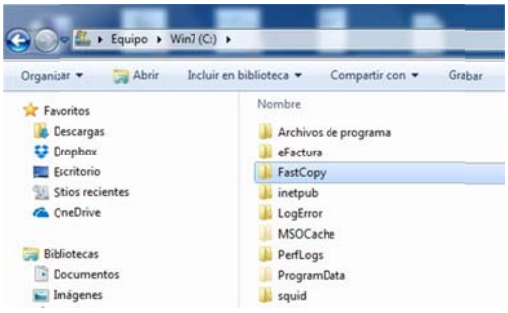


Figura 5.1 Carpeta FastCopy

A continuación se debe copiar el archivo ***FastCopy330.zip*** dentro de ella

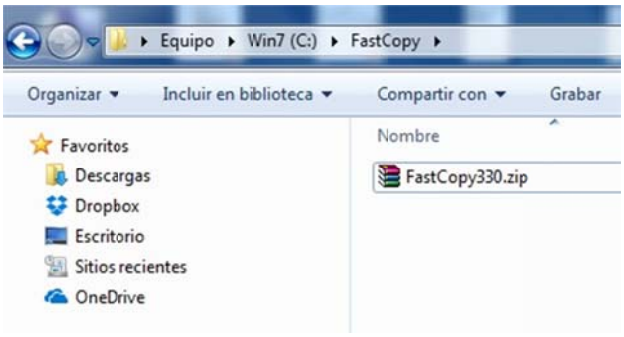


Figura 5.2 Archivos de FastCopy

Una vez copiado el archivo en la carpeta se debe descomprimir su contenido. Hay varias formas de hacerlo y se puede realizar por medio de varios programas, incluso las versiones actuales de Windows permiten hacerlo sin necesidad de usar un programa adicional, pero para este caso se utilizará el ***Winrar***. Se debe dar click derecho sobre el archivo .zip y seleccionar la opción ***Extraer aquí***.

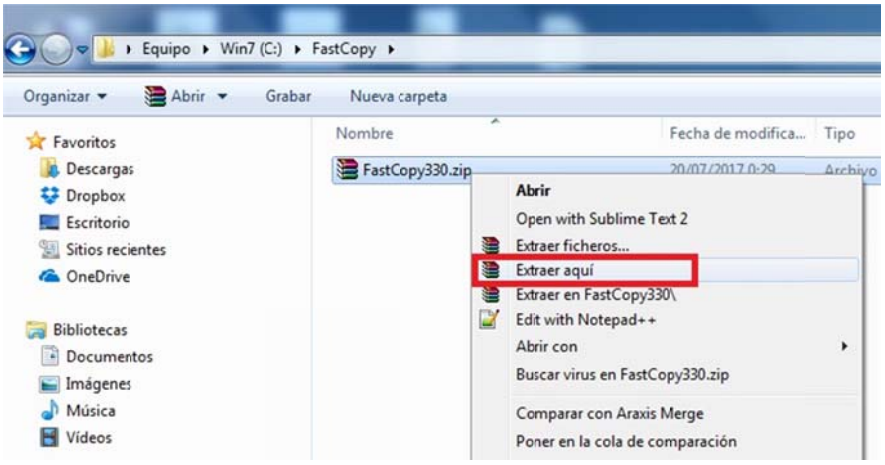


Figura 5.3 Extracción de archivos de FastCopy

Como se puede ver en la figura 5.4, los archivos se han descomprimido en la carpeta.

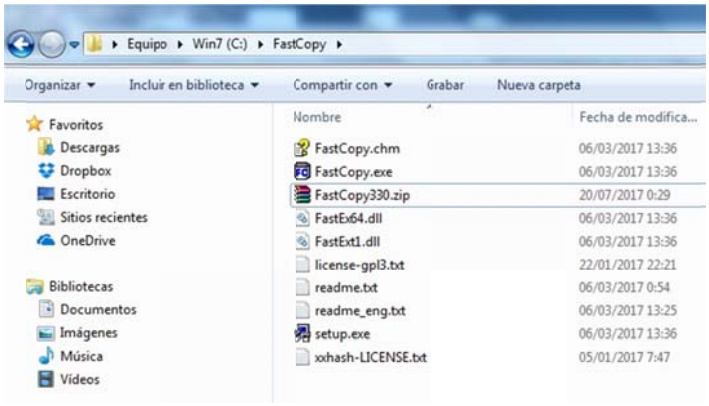


Figura 5.4 Archivos extraídos de FastCopy

Por último se crea un acceso directo al programa. Dar click derecho sobre el archivo ***FastCopy.exe***, seleccionar la opción ***Enviar a*** y luego dar click en ***Escritorio (crear acceso directo)***.

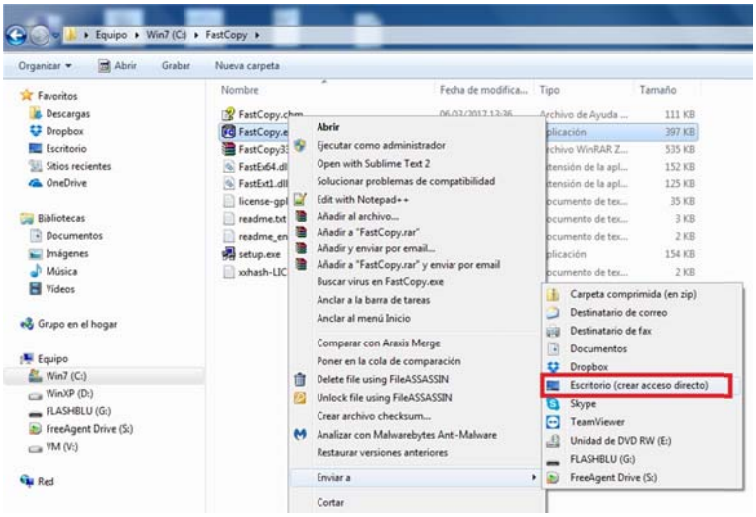


Figura 5.5 Creación de acceso directo de FastCopy

5.1.2 Configuración de FastCopy

Para abrir el programa, ubicar el acceso directo creado en el escritorio y dar doble click sobre él.

Figura 5.6 Acceso directo a FastCopy

A continuación se abre la pantalla principal del programa.

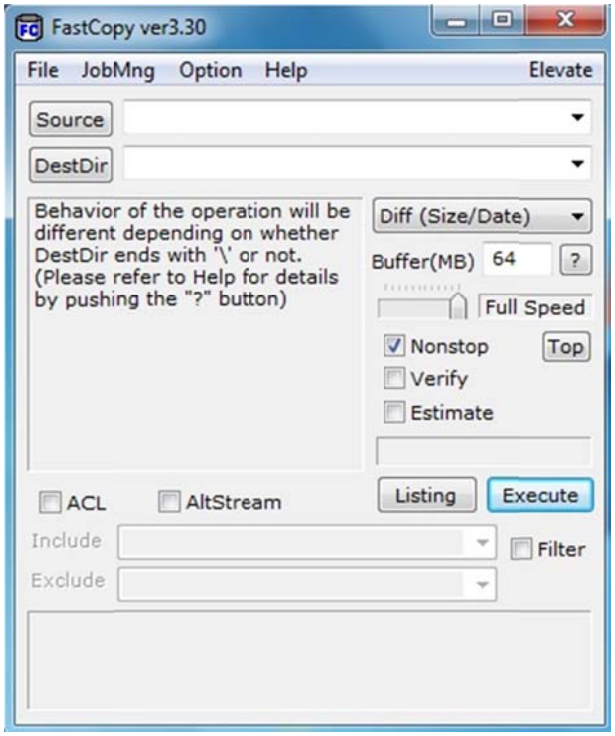


Figura 5.7 Ventana principal de FastCopy

Para configurarlo se debe seleccionar ***Main Settings*** en el menú ***Option.***

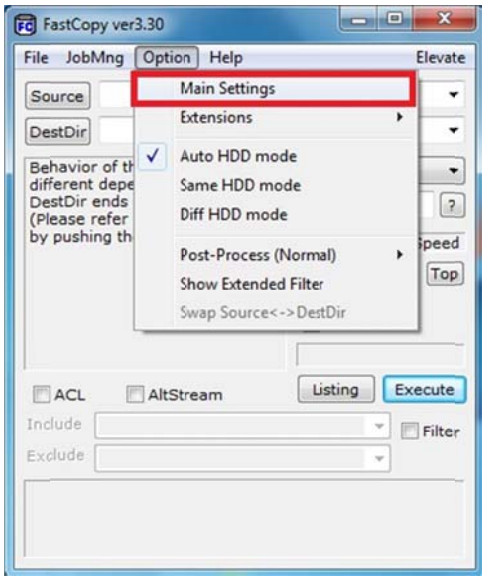


Figura 5.8 Configuración de FastCopy

Se abre una nueva pantalla, donde del lado izquierdo hay varias categorías para configurar. Primero se debe seleccionar ***Defaults*** y checkear la casilla ***Verify***. Esto le indicará al programa que debe verificar la copia de los archivos al finalizar la misma.

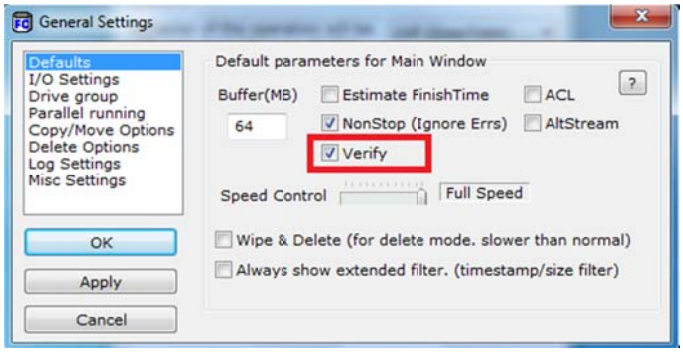


Figura 5.9 Configuración de FastCopy – Defaults

El programa puede hacer uso de varios mecanismos para realizar la verificación de integridad de la copia, uno de esos mecanismos es el SHA-1, por lo que en la categoría ***Copy/Move Options***, en el campo ***Hash mode*** seleccionar ***SHA-1***.

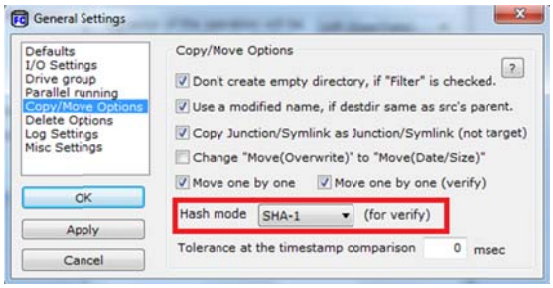


Figura 5.10 Configuración de FastCopy – Copy/Move options

Por último, se le debe indicar al programa que genere un log con el resultado de la copia, para esto se debe habilitar, dentro de la categoría ***Log Settings***, las siguientes casillas:

- Write to File Log (Log\DATE.log)
- FileDate
- FileSize

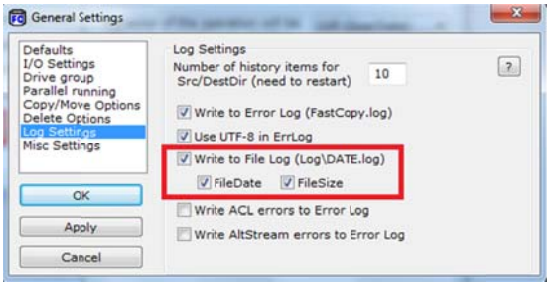


Figura 5.11 Configuración de FastCopy – Log settings

Para guardar los cambios realizados en la configuración, presionar el botón ***OK.***

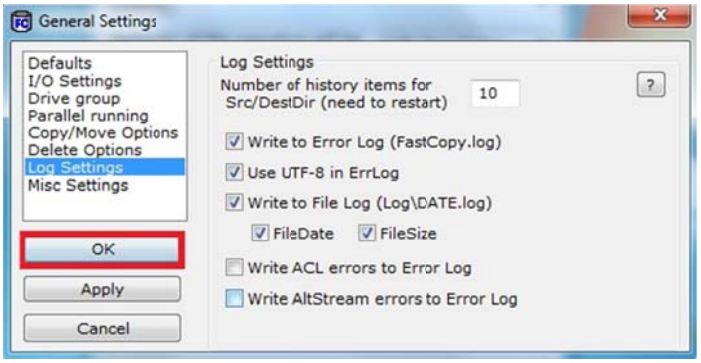


Figura 5.12 Guardar configuración de FastCopy

5.1.3 Instalación HashCheck

Ubicar el instalador del programa (Versión 2.1.11), llamado ***HashCheckInstall-2.1.11.exe.***

Figura 5.13 Instalador de HashCheck

Para ejecutar la instalación, dar click derecho sobre el archivo y seleccionar la opción ***Ejecutar como administrador*** en el menú desplegable que se presenta.

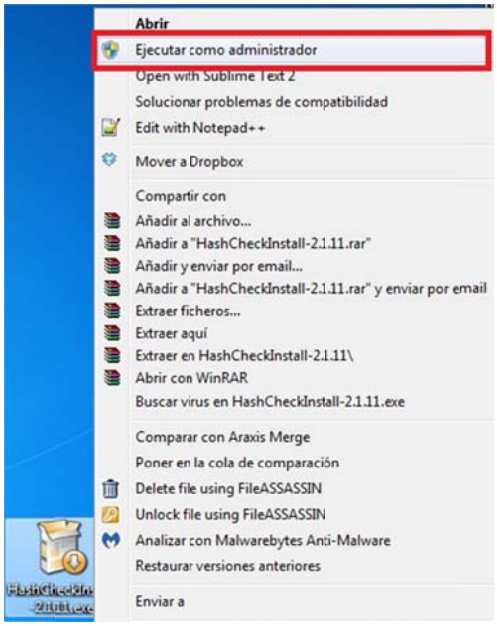


Figura 5.14 Ejecución del instalador de HashCheck

A continuación se presenta una pantalla que contiene el acuerdo de licencia. Presionar el botón ***Yes*** para continuar.

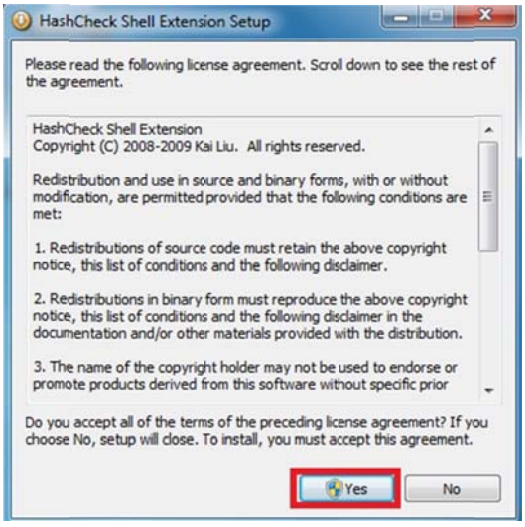


Figura 5.15 Acuerdo de licencia de HashCheck

Después de aceptar los términos de licencia se realiza la instalación automáticamente, y al finalizar se presenta un mensaje que indica que la misma se completó. Presionar el botón ***Aceptar*** para salir.

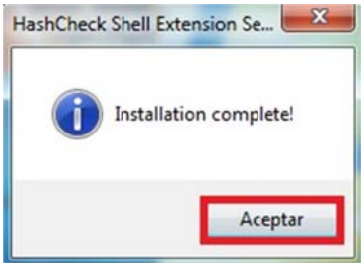


Figura 5.16 Fin de la instalación de HashCheck

5.2 Planes de pruebas

El objetivo del plan de pruebas es validar y verificar el flujo de gestión de la cadena de custodia de las evidencias digitales que maneja la EMOV para determinar el cumplimiento de los requerimientos y garantizar su ejecución.

5.2.1 Alcance de las pruebas

Los elementos considerados para el plan de pruebas son las evidencias digitales (fotografías, videograbaciones) de casos habituales contemplados en la EMOV, herramientas de software para el tratamiento de evidencias digitales, archivos generados por las herramientas y el diligenciamiento del formulario de cadena de custodia, enfocados para cada fase de la cadena de custodia:

Tabla 78 Plan de pruebas por fases de la cadena de custodia

Fase	Elementos de prueba
Identificación de evidencia en el lugar de los hechos	o Fotografías y videograbaciones que cumplan con evidencia relacionada al caso o Fotografías que cumplan las consideraciones descritas en el reglamento de la elaboración de los partes por accidentes de tránsito y personas aprehendidas (fotografía panorámica y fotografías de las diferentes partes de los vehículos involucrados parte frontal-lateral derecha-posterior-lateral izquierda)
Recolección y/o adquisición	o Fotografías y videograbaciones descargadas del dispositivo móvil o Herramienta para descarga: FastCopy o Registro en el Formulario de Cadena de Custodia (Sección 1)
Análisis	o Herramienta de comprobación de integridad: FastCopy o Log con el detalle de archivos transferidos correctamente, fecha y hora de transferencia y el número de checksum o Log con el detalle de archivos que no pudieron ser copiados o presentaron errores en la transferencia o Herramienta de comprobación de autenticidad Hashcheck o Nombre del archivo checksum y el hash de las evidencias o Registro en el Formulario de Cadena de Custodia (Sección 2)
Preservación	o Herramienta para transferencia de archivos FastCopy o Registro en el formulario de Cadena de Custodia (Sección 3)
Presentación	o Solicitud aprobada o Grabación en el medio de presentación (cd, dvd) o Registro en el formulario de Cadena de Custodia (Sección 4)
Eliminación	o Eliminación de evidencias digitales o Registro en el formulario de Cadena de Custodia (Sección 5)

5.2.2 Recursos

Se especifica los requerimientos de equipos, software, red y personal necesarios para ejecutar las actividades del plan de pruebas.

5.2.2.1 Requerimientos de entornos

Hardware:

- Computadora de Escritorio (Central de Radio), marca HP, Intel (R) Core (TM) i7 2.7GHz, Windows 10 Pro, 16 GB RAM, x64.
- Laptop (TICS ACT) marca HP, Intel (R) Core (TM) i7 2.7 GHz, Windows 10, 16 GB RAM, x64.

Software:

- Herramienta FastCopy
- Herramienta Hashcheck

Red:

- Conexión de área local

5.2.2.2 Personal

Se designa el personal que participa en el plan de pruebas con los roles correspondientes. Mediante una matriz RACI (responsable, aprobador, consultado, informado) se designa las

responsabilidades de los integrantes del equipo del plan de pruebas.

Tabla 79 Matriz RACI

Actividades	Tesistas	ACT Central de radio	ACT TICS	Subgerente de TICS	Subgerente de Planificación
1. Instalar herramientas para el tratamiento de evidencias digitales	C	I	R	A	C
2. Descargar fotografías y videos del celular		R		C	A
3. Descargar videos de las patrullas		I	R	C	A
4. Diligenciar Formulario de Cadena de Custodia		R	R	C	A
5. Grabar en medio para presentación		R	R	C	A
6. Eliminar evidencias digitales		I	R	C	A

Responsable (R): personas que ejecutan la actividad.

Aprobador (A): persona que responde por la actividad y aprueba la tarea realizada por el responsable.

Consultado (C): personas con las que se debe consultar las decisiones respecto a la actividad.

Informado (I): personas que se les informa de las decisiones y resultados ya que se pueden ver afectadas por la actividad.

5.2.3 Casos de pruebas

Los casos de pruebas seleccionados son partes por accidentes de tránsito y por personas aprehendidas:

Caso 1: Atropello

El primer caso se refiere a un accidente de tránsito que se suscitó vía a Gullanzhapa, parroquia Tarqui del cantón Cuenca. En el que el conductor se encontraba en estado de embriaguez y atropelló a dos peatones con su motocicleta, la misma que también sufrió daños y cuyas fotografías fueron captadas con el teléfono celular del Agente Civil de Tránsito que intervino en el accidente, por lo que se procede a su respaldo y registro del formulario de cadena de custodia.

En primer lugar, el Agente Civil de Tránsito descarga las fotos desde su celular a la computadora, con ayuda de la herramienta FastCopy. Luego de verificar que no hubo errores en la copia realizada diligencia la sección 1 del formulario, como se muestra en la figura 5.17:

FORMULARIO DE CADENA DE CUSTODIA

EMOV-EP

Número de formulario : 20170625-001

1. RECOLECCIÓN / ADQUISICIÓN

1.1 Información del Agente Civil de Tránsito que captura la evidencia

Liliana Bernardita Orellana Chacha	0105674006	
Nombres y Apellidos	Número de cédula	Firma

1.2 Información del incidente

ATROPELLO	Vía a Gullanzhapa (Tarqui)	25/Jun/2017 03:23
Tipo	Lugar	Fecha y hora

1.3 Tipo de evidencia : [X] FOTOS [ ] VIDEOS

1.4 Información del equipo o dispositivo

CELULAR	SAMSUNG	
Medio (DVR, celular, etc.)	Marca	Modelo

1.5 Información del Agente Civil de Tránsito que recibe y descarga la evidencia

Liliana Bernardita Orellana Chacha	0105674006	
Nombres y Apellidos	Número de cédula	Firma

1.6 Fecha y hora de la descarga : 25/Jun/2017 06:15

Figura 5.17 Caso 1 – Formulario de cadena de custodia, sección 1

A continuación se genera el archivo de checksum (.sha1), con el programa HashCheck, a partir de los archivos descargados como evidencia del accidente, como se muestra en las figuras 5.18 y 5.19:

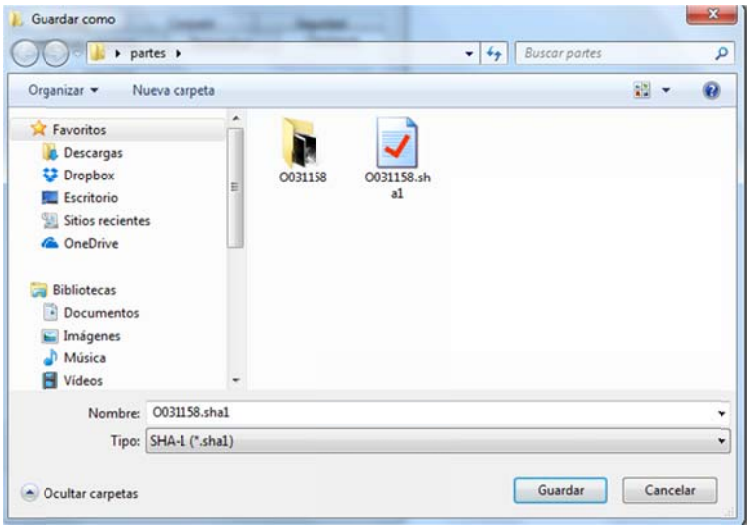


Figura 5.18 Caso 1 – Generación de archivo de checksum

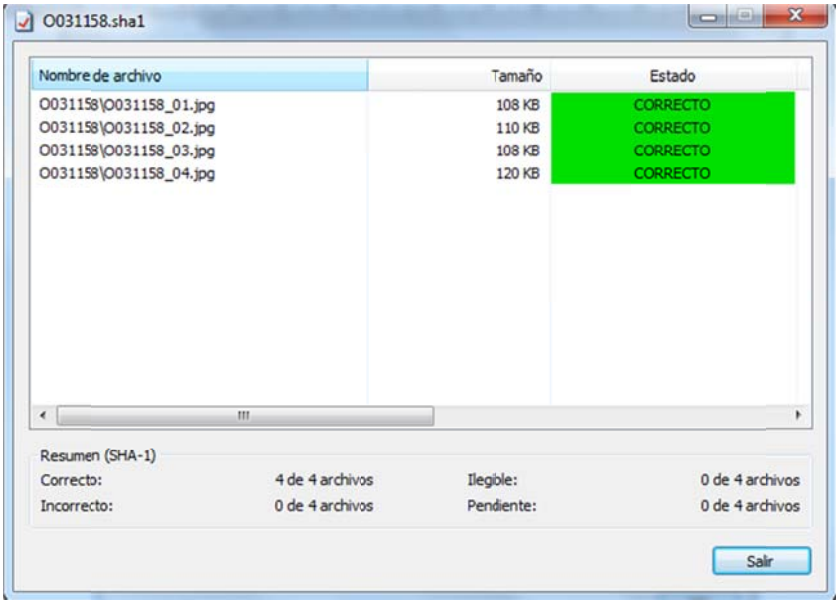


Figura 5.19 Caso 1 – Contenido del archivo de checksum

Con esta información se gestiona la sección 2 del formulario de cadena de custodia:

2. ANÁLISIS				
2.1 Información del archivo de checksum				
O031158.sha1		3a1a93aa4871ee8a8692e505209fec7125b43d1e		
Nombre del archivo		Hash		
2.2 Detalle de las evidencias				
Número	Nombre del archivo	Tipo (Foto / Video)	Hash	Información adicional
1	0031158_01.jpg	FOTO	85a9daf922d963547d38ce0fe883	
2	0031158_02.jpg	FOTO	2c36647564c1b51a14a76e90017	
3	0031158_03.jpg	FOTO	c77f4aac91ce7c93ff0f23d5bb21	
4	0031158_04.jpg	FOTO	379dacc0e69f08d660b6c1ff8fda	

Figura 5.20 Caso 1 – Formulario de cadena de custodia, sección 2

Los archivos de evidencia se guardan en el disco de respaldo general, donde se conservarán las fotografías y videos. Esta copia también se

realiza mediante FastCopy. Luego de finalizar correctamente la copia, se registra la información correspondiente en la sección 3 del formulario.

3. PRESERVACIÓN		
3.1 Información del repositorio		
Disco Backup	E:\FOTOGRAFIAS\LORELLANA\20170625\O031158	90 días
Nombre del equipo	Ruta de almacenamiento	Tiempo mínimo

Figura 5.21 Caso 1 – Formulario de cadena de custodia, sección 3

Con el fin de realizar la diligencia de avalúo de daños materiales del vehículo, el Subt. John Ariel Brito Mendoza, en calidad de Perito-Investigador, requiere una copia de las evidencias, por lo que se genera una copia de los archivos en un CD y posteriormente se registra esta acción en la sección 4 del formulario de cadena de custodia.

4. PRESENTACIÓN		
4.1 Información general		
21368	E10000027	Dr. Emilio Izquierdo
Número de parte	Número de citación	Fiscal / Juez
4.2 Información del Agente Civil de Tránsito que recibe la evidencia		
John Ariel Brito Mendoza		
Nombres y Apellidos	Número de cédula	Firma
4.3 Fecha y hora de entrega : 25/Jun/2017 08:50	4.4 Tipo de medio (CD, DVD, etc.) : CD	

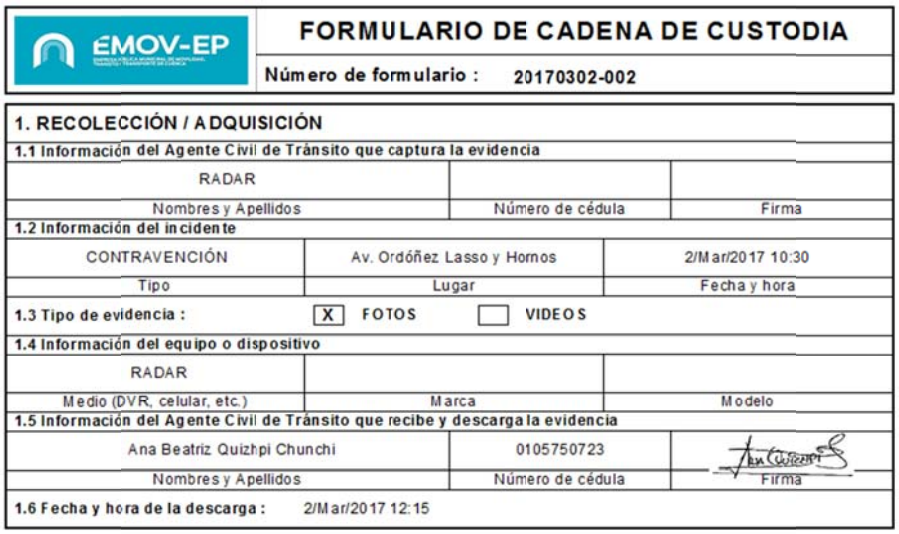
Figura 5.22 Caso 1 – Formulario de cadena de custodia, sección 4

La sección 5 del formulario no será diligenciada, hasta que se cumpla el tiempo mínimo de preservación de las evidencias.

Caso 2: Exceso de velocidad

Este caso hace referencia a la detención de un conductor por rebasar los límites de velocidad permitidos dentro de una zona urbana. En este caso, la evidencia es tomada por un radar de la Av. Ordóñez Lasso, en la parroquia San Sebastián del cantón Cuenca.

El Agente Civil de Tránsito que interviene en el incidente descarga la imagen del radar, para tener el respaldo de la evidencia y posteriormente diligencia la sección 1 del formulario de cadena de custodia.



EMOV-EP

FORMULARIO DE CADENA DE CUSTODIA

Número de formulario : 20170302-002

1. RECOLECCIÓN / ADQUISICIÓN

1.1 Información del Agente Civil de Tránsito que captura la evidencia

RADAR		
Nombres y Apellidos	Número de cédula	Firma

1.2 Información del incidente

CONTRAVENCIÓN	Av. Ordóñez Lasso y Hornos	2/Mar/2017 10:30
Tipo	Lugar	Fecha y hora

1.3 Tipo de evidencia : [X] FOTOS [ ] VIDEOS

1.4 Información del equipo o dispositivo

RADAR		
Medio (DVR, celular, etc.)	Marca	Modelo

1.5 Información del Agente Civil de Tránsito que recibe y descarga la evidencia

Ana Beatriz Quizhpi Chunchi	0105750723	
Nombres y Apellidos	Número de cédula	Firma

1.6 Fecha y hora de la descarga : 2/Mar/2017 12:15

Figura 5.23 Caso 2 – Formulario de cadena de custodia, sección 1

A continuación, por medio del programa HashCheck, genera el archivo checksum (.sha1) y a partir de la información obtenida registra la sección 2 del formulario.

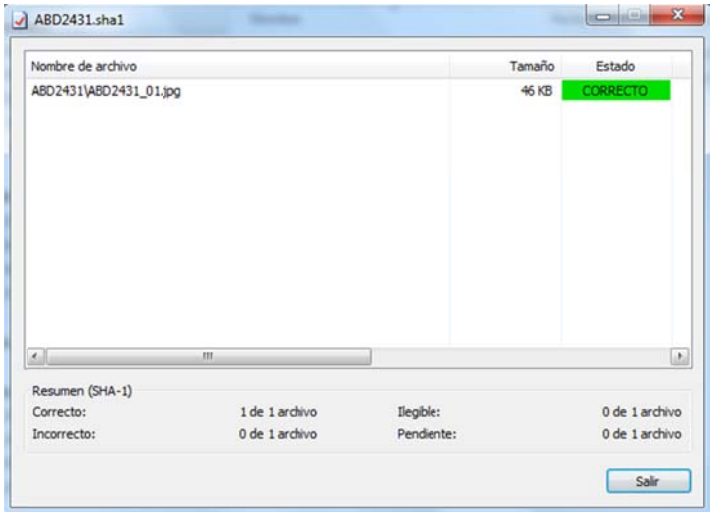


Figura 5.24 Caso 2 – Archivo de checksum

2. ANÁLISIS				
2.1 Información del archivo de checksum				
ABD2431.sha1		00ab8c4016db36bdea8d4651c794c220d3dcae2b		
Nombre del archivo		Hash		
2.2 Detalle de las evidencias				
Número	Nombre del archivo	Tipo (Foto / Video)	Hash	Información adicional
1	ABD2431_01.jpg	FOTORADAR	e0ac12e3f79b5a953c1ceb2d1f35	

Figura 5.25 Caso 2 – Formulario de cadena de custodia, sección 2

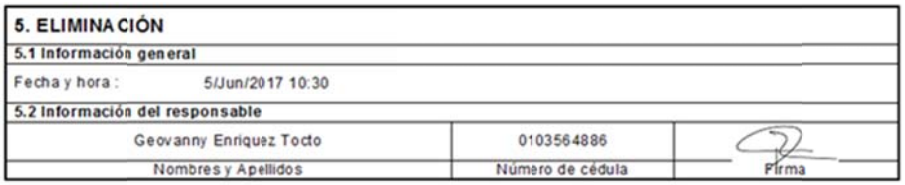
Se respalda la evidencia en el disco de respaldo general, en una ubicación según la estructura de directorios establecida para el respaldo de las evidencias. Para esta copia se utiliza el FastCopy, para asegurar la integridad de la copia.

3. PRESERVACIÓN		
3.1 Información del repositorio		
Disco Backup	E:\FOTORADAR\AQUIZHPI\20170302\ABD2431	90 días
Nombre del equipo	Ruta de almacenamiento	Tiempo mínimo

Figura 5.26 Caso 2 – Formulario de cadena de custodia, sección 3

En este caso no se requiere la presentación de evidencias, por lo que la sección 4 del formulario quedará en blanco.

Debido a que se ha cumplido el tiempo mínimo de preservación de evidencias, se procede a la eliminación de la misma, por parte del Agente Civil de Tránsito de TIC's, acción que se registra en la sección 5 del formulario.



5. ELIMINACIÓN		
5.1 Información general		
Fecha y hora: 5/Jun/2017 10:30		
5.2 Información del responsable		
Geovanny Enriquez Tocto	0103564886	
Nombres y Apellidos	Número de cédula	Firma

Figura 5.27 Caso 2 – Formulario de cadena de custodia, sección 5

5.2.4 Verificación de las pruebas

Tabla 80 Verificación de las pruebas

Caso	Actividad	Recolección Adquisición	Análisis	Preservación	Presentación	Eliminación
#1	FastCopy	X		X		
	HashCheck		X			
	Registro de Cadena de custodia	X	X	X	X	X
#2	FastCopy	X		X		
	HashCheck		X			
	Registro de Cadena de custodia	X	X	X	X	X

5.3 Revisión, aprobación y difusión de los controles internos

Para la implementación de los controles determinados en el análisis de riesgo se requiere la participación del directorio con los responsables de todas las áreas involucradas:

- Área de TICS
- Área de Control de Tránsito y Transporte Terrestre
- Área Operativa de Transporte Terrestre
- Área de Talento Humano
- Área de Planificación
- Área de Comunicación Social
- Área de Auditoría Interna
- Área Jurídica
- Área Financiera
- Área Administrativa

Una vez efectuada la revisión y aprobación de la implementación de los controles es necesario realizar la difusión a los empleados de la empresa y a terceros implicados; todos son responsables de dar cumplimiento de los controles de seguridad de la información. La revisión y aprobación debe estar documentada, con la fecha de aprobación y designación de los responsables para los respectivos controles.

Es recomendable conformar un Comité de Seguridad de la Información en donde se designe un Oficial de Seguridad de la Información, quien lidere,

coordine, planifique y gestione las políticas, normas, procesos, procedimientos, tecnologías y estrategias para conservar la seguridad de la información y se puede replicar la metodología aplicada para todos los procesos de la empresa progresivamente.

5.4 Capacitación de las herramientas aplicadas

La capacitación de las herramientas aplicadas está dirigida a los responsables de las áreas que gestionan las evidencias digitales:

Central de Radio: cuatro personas distribuidos en grupos (A-B-C-D) que laboran por turnos rotativos (6h00-14h00, 14h00-22h00, 22h00-6h00 y franco).

TICS: una persona que labora en el horario de 8h00 a 13h00 y 15h00 a 18h00.

Para el diligenciamiento del formulario de cadena de custodia se realizará la demostración con los supervisores de grupo de los ACT y a su vez será quienes impartan las indicaciones a su equipo.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 Monitoreo y control de los Resultados obtenidos en las pruebas

Para el seguimiento, mantenimiento y mejora continua de los controles internos es necesario realizar el proceso de monitoreo, que permite valorar la calidad de desempeño de los controles implementados.

Se realiza el monitoreo de la gestión de cadena de custodia de las evidencias digitales mediante los informes de monitoreo de actividades, entrevistas con los responsables de ejecutar las actividades, revisión de los archivos logs de las herramientas y de los registros de los formularios de cadena de custodia.

Tabla 81 Listado de verificación del monitoreo

Listado de Verificación del Monitoreo							
Caso N°: 1		**Área: Central de Radio / TICs ACT**			**Fecha:**		
Fase	**Actividad**	**Pregunta**	**Método**	**Medio de Comprobación**	**Cumplido**	**No cumplido**	**Observación**
Identificación de evidencia en el lugar de los hechos	Fotografías y videograbaciones relacionadas al caso	Las fotografías y videograbaciones están relacionadas al caso?	Observación	Fotos - Videos	X		
		Las fotografías cumplen con las consideraciones descritas en el reglamento de la elaboración de los partes por accidentes de tránsito y personas aprehendidas?	Observación	Fotos - Videos	X		
		El formulario de Cadena de Custodia es llenado en la sección qué corresponde a esta etapa (Sección 1: 1.1-1.2-1.3-1.4)?	Observación	Formulario de Cadena de Custodia	X		
		El formulario de Cadena de Custodia tiene la firma de responsabilidad del ACT que toma procedimiento?	Observación	Formulario de Cadena de Custodia	X		
Recolección y/o Adquisición	FastCopy, Formulario de Cadena de Custodia	El ACT de la Central de Radio descarga las fotografías y las videograbaciones con la herramienta FastCopy?	Observación	Archivo log de texto	X		
		El ACT de TICS descarga las videograbaciones solicitados de los DVRS de las patrullas?	Observación	Archivo log de texto		X	
		El formulario de Cadena de Custodia es llenado en la sección qué corresponde a esta etapa (Sección 1: 1.5, 1.6)?	Observación	Formulario de Cadena de Custodia	X		
		El formulario de Cadena de Custodia tiene la firma de responsabilidad del ACT que descarga las evidencias?	Observación	Formulario de Cadena de Custodia	X		
Análisis	HashCheck, Formulario de Cadena de Custodia	El ACT de la Central de Radio genera el archivo checksum (.sha1) con el programa HashCheck?	Observación	Archivo .sha1	X		
		El formulario de Cadena de Custodia es llenado en la sección qué corresponde a esta etapa (Sección 2: 2.1, 2.2)?	Observación	Formulario de Cadena de Custodia	X		
Preservación	FastCopy, Formulario de Cadena de Custodia	Están almacenadas las evidencias digiltales en un disco de respaldo externo?	Observación	Disco de respaldo externo		X	
		La copia de las evidencias digitales es realizada con la Herramienta FastCopy?	Observación	Archivos log de texto	X		
		El formulario de Cadena de Custodia es llenado en la sección qué corresponde a esta etapa (Sección 3: 3.1)?	Observación	Formulario de Cadena de Custodia	X		
Presentación	Formulario de Cadena de Custodia	Son grabadas las evidencias en un dispositivo de almacenamiento (cd-dvd) para su presentación?	Observación	Medio de almacenamiento	X		
		El formulario de Cadena de Custodia es llenado en la sección qué corresponde a esta etapa (Sección 4: 4.1, 4.2, 4.3, 4.4)?	Observación	Formulario de Cadena de Custodia	X		
Eliminación	Formulario de Cadena de Custodia	Se ha cumplido el tiempo mínimo de preservación de las evidencias digitales?	Observación	Parte de Tránsito Formulario de Cadena de Custodia		X	No ha transcurrido el tiempo mínimo de preservación de la evidencia

Se debe aplicar auditorías internas para medir el nivel de eficacia de los controles, comprobar el estado e identificar la necesidad de cambio para que cumplan los requisitos de seguridad de la información y cumplan con el resultado previsto.

Regularmente realizar supervisiones por parte de la Subgerencia de TICs, verificar información, mantener reuniones habituales.

La Dirección es responsable de hacer revisiones periódicas con el objetivo de comprobar el cumplimiento de la eficacia de los controles y con la oportunidad de mejora en base al control realizado de los resultados obtenidos en las auditorías, revisiones, mediciones, cambios en la empresa, registros de eventos de seguridad, las recomendaciones por parte de los propietarios de la información y en sí de todas las partes interesadas.

6.2 Valoración y Mapeo de Riesgos (Riesgos Residuales)

La empresa es consciente del riesgo que permanece después de que se hayan tomado las medidas necesarias para el tratamiento del riesgo, a lo que se le denomina **Riesgo Residual.**

Tabla 82 Riesgo residual: Portátiles

Amenaza	Controles implementados	Riesgo residual
Hurto de equipo	A.9.1.5 Trabajo en áreas seguras A.9.2.5 Seguridad de los equipos fuera de las instalaciones A.11.7.1 Equipos portátiles y comunicaciones móviles A.12.3.1 Política de uso de los controles criptográficos A.12.3.2 Gestión de claves A.15.1.3 Protección de los documentales de la organización A.15.1.6 Regulación de los controles criptográficos	Aceptable
Manipulación con hardware	A.9.1.3 Seguridad de oficinas, despachos e instalaciones A.9.2.5 Seguridad de los equipos fuera de las instalaciones	Aceptable
Manipulación con software	A.10.4.1 Controles contra el código malicioso A.10.4.2 Controles contra el código descargable en el cliente	Aceptable
Mal funcionamiento del software	A.12.4.1 Control de software en explotación A.12.5.1 Procedimientos de control de cambios A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo A.12.5.3 Restricciones a los cambios en los paquetes de software	Aceptable
Uso de software falso o copiado	A.15.1.2 Derechos de propiedad intelectual	Aceptable
Procesamiento ilegal de los datos	A.11.2.2 Gestión de privilegios A.11.2.4 Revisión de los derechos de acceso de usuario A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Aceptable
Abuso de derechos	A.11.2.4 Revisión de los derechos de acceso de usuario	Aceptable
Intrusión, accesos forzados, acceso no autorizado	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.11.5.4 Usos de los recursos del sistema A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad A.13.2.1 Responsabilidades y procedimientos A.13.2.2 Aprendizaje de los incidentes de seguridad de la información A.13.2.3 Recopilación de evidencias A.15.2.1 Cumplimiento de las políticas y normas de seguridad A.15.2.2 Comprobación del cumplimiento técnico	Aceptable

Tabla 83 Riesgo residual: PC escritorio

Amenaza	Controles implementados	Riesgo residual
Manipulación con software	A.10.4.1 Controles contra el código malicioso A.10.4.2 Controles contra el código descargable en el cliente	Aceptable

Tabla 84 Riesgo residual: PDA

Amenaza	Controles implementados	Riesgo residual
Destrucción	A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.9.2.4 Mantenimiento de los equipos A.10.1.1 Documentación de los procedimientos de operación	Aceptable
Hurto de equipo	A.7.1.1 Inventario de Activos A.7.1.2 Propiedad de los activos A.9.2.5 Seguridad de los equipos fuera de las instalaciones	Aceptable
Manipulación con Software/Código malicioso	A.10.4.1 Controles contra el código malicioso A.10.4.2 Controles contra el código descargable en el cliente	Aceptable
Uso no autorizado del equipo	A.9.2.1 Emplazamiento y protección de equipos	Aceptable

Tabla 85 Riesgo residual: Alcoholímetros

Amenaza	Controles implementados	Riesgo residual
Destrucción del equipo o los medios	A.9.2.4 Mantenimiento de los equipos A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.10.1.1 Documentación de los procedimientos de operación	Tolerable
Hurto de equipo	A.7.1.1 Inventario de Activos A.7.1.2 Propiedad de los activos A.9.2.5 Seguridad de los equipos fuera de las instalaciones	Aceptable
Falla del equipo / Mal funcionamiento del equipo	A.9.2.4 Mantenimiento de los equipos A.10.10.5 Registro de fallos	Tolerable
Uso no autorizado del equipo	A.9.2.1 Emplazamiento y protección de equipos	Aceptable
Error en el uso	A.10.1.1 Documentación de los procedimientos de operación	Aceptable

Tabla 86 Riesgo residual: Radares

Amenaza	Controles implementados	Riesgo residual
Destrucción del equipo o los medios	A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.10.1.1 Documentación de los procedimientos de operación	Tolerable
Falla del equipo / Mal funcionamiento del equipo	A.9.2.4 Mantenimiento de los equipos A.10.10.5 Registro de fallos	Aceptable
Error en el uso	A.10.1.1 Documentación de los procedimientos de operación	Aceptable

Tabla 87 Riesgo residual: DVR

Amenaza	Controles implementados	Riesgo residual
Destrucción del equipo o los medios	A.7.1.2 Propiedad de los activos A.8.2.3 Proceso disciplinario A.9.2 Seguridad de los equipos A.9.2.4 Mantenimiento de los equipos A.9.2.5 Seguridad de los equipos fuera de las instalaciones. A.10.1.1 Documentación de los procedimientos de operación A.10.10.2 Supervisión del uso del sistema	Tolerable
Hurto de equipo	A.9.1.5 Trabajo en áreas seguras A.9.2.5 Seguridad de los equipos fuera de las instalaciones A.11.7.1 Equipos portátiles y comunicaciones móviles A.12.3.1 Política de uso de los controles criptográficos A.12.3.2 Gestión de claves A.15.1.3 Protección de los documentales de la organización A.15.1.6 Regulación de los controles criptográficos	Aceptable
Falla del equipo / Mal funcionamiento del equipo	A.9.2.4 Mantenimiento de los equipos A.10.10.5 Registro de fallos	Aceptable
Error en el uso	A.10.1.1 Documentación de los procedimientos de operación A.10.10.2 Supervisión del uso del sistema	Aceptable

Tabla 88 Riesgo residual: Sistemas

Amenaza	Controles implementados	Riesgo residual
Mal funcionamiento del software	A.12.4.1 Control del software en explotación A.12.5.1 Procedimiento de control de cambios A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad	Aceptable
Uso de software falso o copiado	A.15.1.2 Derechos de propiedad intelectual	Aceptable
Error en el uso	A.12.2.1 Validación de los datos de entrada Capacitacion en el uso de los sistemas de información y actualización de los manuales de usuario cuando amerite	Aceptable
Abuso de derechos/Falsificación de derechos	A.12.4.3 Control de acceso al código fuente de los programas A.12.5.4 Fugas de información A.12.6.1 Control de vulnerabilidades técnicas A.13.1.2 Notificación de los puntos débiles de seguridad	Aceptable
Negación de acciones	A.12.5.1 Procedimientos de control de cambios	Aceptable
Intrusión, accesos forzados al sistema, accesos no autorizados al sistema, sabotaje del sistema	A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad A.10.10.1 Registro de auditorías	Aceptable
Ingreso de datos falsos o corruptos	A.12.2.1 Validación de los datos de entrada A.12.2.2 Control del procesamiento interno A.12.2.3 Integridad de los mensajes A.12.2.4 Validación de los datos de salida A.10.10.1 Registro de auditorías	Aceptable
Errores en el sistema (bugs)	A.12.1.1 Análisis y especificación de los requisitos de seguridad A.12.4.1 Control del software en explotación A.12.5.1 Procedimiento de control de cambios A.12.5.2 Revisión técnica A.12.5.4 Fugas de información A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad	Aceptable

Tabla 89 Riesgo residual: Fotos

Amenaza	Controles implementados	Riesgo residual
Hurto de medios o documentos	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.10.5.1 Copias de seguridad de la información	Aceptable
Divulgación	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.8.2.2 Concienciación, formación y capacitación en seguridad de la información	Tolerable
Manipulación con software	A.10.5.1 Copias de seguridad de la información - Verificar la información de la metadata para confirmar su integridad mediante herramientas de software - Planes corporativos de los celulares que utilicen los ACT para capturar las fotos que servirán como evidencia	Aceptable
Corrupción de los datos	A.10.5.1 Copias de seguridad de la información ISO TR 15801 / Suma de comprobación calculada después de captura de información - Herramientas de almacenamiento sincronizado en linea Mantenimiento periódico de las tarjetas - Herramientas de recuperación de archivos - Planes corporativos de los celulares que utilicen los ACT para capturar las fotos que servirán como evidencia	Aceptable
Error en el uso	A.5.1.1 Publicar y distibuir a todos los empleados de la EMOV y terceros afectados el Documento de Política de Seguridad. A.5.1.2 Revisión de la política de seguridad de la información A.8.1.1 Funciones y Responsabilidades A.8.2.1 Respondabilidad de la Dirección A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.10.1.1 Documentación de los procedimientos de operación	Aceptable
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad	Aceptable

Tabla 90 Riesgo residual: Videos

Amenaza	Controles implementados	Riesgo residual
Hurto de medios o documentos	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.10.5.1 Copias de seguridad de la información	Aceptable
Divulgación	A.7.2.1 Directrices de clasificación A.7.2.2 Etiquetado y manejo de la información A.8.2.2 Concienciación, formación y capacitación en seguridad de la información	Tolerable
Manipulación con software	A.10.5.1 Copias de seguridad de la información - Verificar la información de la metadata para confirmar su integridad mediante herramientas de software - Planes corporativos de los celulares que utilicen los ACT para capturar los videos que servirán como evidencia	Aceptable
Corrupción de los datos	A.10.5.1 Copias de seguridad de la información ISO TR 15801 / Suma de comprobación calculada después de captura de información - Herramientas de almacenamiento sincronizado en linea - Mantenimiento periódico de las tarjetas - Herramientas de recuperación de archivos - Planes corporativos de los celulares que utilicen los ACT para capturar los videos que servirán como evidencia	Aceptable
Error en el uso	A.5.1.1 Publicar y distibuir a todos los empleados de la EMOV y terceros afectados el Documento de Política de Seguridad. A.5.1.2 Revisión de la política de seguridad de la información A.8.1.1 Funciones y Responsabilidades A.8.2.1 Respondabilidad de la Dirección A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.10.1.1 Documentación de los procedimientos de operación	Aceptable
Negación de acciones	A.10.10.1 Registro de auditorías A.10.10.2 Supervisión del uso del sistema	Aceptable
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema, soborno de la información	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.11.6 Control de Acceso a las aplicaciones y a la información A.11.6.2 Aislamiento de sistemas sensibles A.12.6.1 Control de las vulnerabilidades técnicas A.13.1 Notificación de eventos de seguridad de la información A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad	Aceptable

Tabla 91 Riesgo residual: Partes contravenciones – Delitos de tránsito

Amenaza	Controles implementados	Riesgo residual
Divulgación	A.7.2.2. Etiquetado y manejo de la información	Aceptable
Abuso de derechos	A.10.1.3 Segregación de Tareas A.10.10.1 Registro de auditorías A.10.10.2 Supervisión del uso del sistema A.11.2.4 Revisión de los derechos de acceso de usuario	Aceptable
Negación de acciones	A.10.10.1 Registro de auditorías A.10.10.2 Supervisión del uso del sistema	Aceptable
Intrusión, accesos forzados al sistema, acceso no autorizado al sistema	A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.11.6 Control de Acceso a las aplicaciones y a la información A.11.6.2 Aislamiento de sistemas sensibles A.12.6.1 Control de las vulnerabilidades técnicas A.13.1.1 Notificación de eventos de seguridad de la información A.13.1.2 Notificación de los puntos débiles de seguridad	Aceptable
Soborno de la información (Interno)	A.8.1.2 Investigación de antecedentes A.8.1.3 Términos y condiciones de contratación A.8.2.1 Responsabilidades de la Dirección A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.8.2.3 Proceso disciplinario	Aceptable

CONCLUSIONES

1. Mediante las entrevistas al personal involucrado en el manejo de las evidencias digitales, se identifica la falta de controles en la gestión de la cadena de custodia que garantice la autenticidad e integridad de las evidencias y puedan tener un valor probatorio en un proceso judicial.

2. Se determina los requerimientos de las áreas implicadas a partir de la gestión de riesgo, en donde se aplica una metodología que permite identificar y clasificar los activos de información del subproceso que trata las evidencias digitales, identificar y evaluar el riesgo, y su correspondiente tratamiento. Como resultado de este análisis, se detecta que existen activos con un riesgo inherente no tolerable, en donde es necesario aplicar controles a corto plazo para reducir y mitigar el riesgo.

3. Con la implementación de un esquema de seguridad que consta de controles, procedimientos y herramientas que soporten el proceso de gestión de la cadena de

custodia, se logra un mayor grado de confiabilidad en la identificación, recolección, análisis, preservación, presentación y eliminación de la evidencia digital.

4. A partir del análisis de resultados y de la evaluación de riesgos posterior a la implementación de los controles recomendados, se identifica la reducción de riesgos inherentes, sin embargo existen riesgos residuales, los cuales son aceptados por la empresa, con el compromiso del correspondiente monitoreo y mejora continua.

RECOMENDACIONES

1. Se debe socializar a todo el personal de la empresa los controles y procedimientos implementados, utilizando diferentes medios y herramientas que permitan su adopción (correos electrónicos, carteleras informativas, sesiones grupales), con el fin de que estos puedan ser aplicados correctamente y generen una cultura de seguridad de la información, que contribuya a la adecuada gestión de las evidencias digitales.

2. Es prioritario tratar los activos con nivel de riesgo no tolerable y ejecutar un plan de acción a corto plazo. Los activos con riesgo tolerable deben ser tratados a mediano plazo, y por último, para aquellos que tienen riesgos aceptables se debe considerar el cambio de estado que puedan tener a futuro. La metodología de gestión de riesgo aplicada en este subproceso debería ser replicada en los demás procesos de la empresa, para mantener la seguridad de la información en la misma.

3. Para que la implementación de los controles internos obtenga una funcionalidad efectiva, es necesaria la participación del directorio en conjunto con los responsables de las diferentes áreas de la empresa para la revisión, aprobación y difusión de los mismos. Se debe designar a los responsables, con las actividades requeridas para dar cumplimiento a la aplicación de los controles.

4. Es necesario realizar un seguimiento, mantenimiento y mejora continua de los controles internos, por lo que se debe aplicar auditorías, revisiones, monitoreos y mediciones para comprobar el nivel de eficacia de los controles implementados y validar su estado, para determinar si se requiere un cambio, o no, de tratamiento, con el fin de que contemplen los nuevos escenarios que puedan presentarse.

BIBLIOGRAFÍA

[1] Comisión de Derechos Humanos, Declaración Universal de Derechos Humanos, París: Dharana, 1948.

[2] Asamblea Nacional Constituyente del Ecuador, Constitución de la República del Ecuador, Montecristi: Editorial Jurídica del Ecuador, 2008.

[3] Congreso Nacional del Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, Quito: Editorial Jurídica del Ecuador, 2005.

[4] Ministerio de Justicia, Derechos Humanos y Cultos, Subsecretaría de Desarrollo Normativo, Código Orgánico Integral Penal, Quito: Gráficas Ayerve C. A., 2014.

[5] Congreso Nacional del Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, Quito: Editorial Jurídica del Ecuador, 2002.

[6] ISO/IEC - adoptada por el INEN, Norma NTE INEN-ISO/IEC 27001, Quito, 2011.

[7] ISO/IEC - adoptada por el INEN, Norma NTE INEN-ISO/IEC 27002, Quito, 2009.

[8] ISO/IEC - adoptada por el INEN, Norma NTE INEN-ISO/IEC 27005, Quito, 2012.

[9] ISO/IEC, ISO/IEC 27037, Switzerland, 2012.

[10] Fiscalía General del Estado , Manual de Cadena de Custodia, Quito: Editorial Jurídica del Ecuador, 2014.

[11] EMOV EP, Manual de Funciones y Perfiles de Cargo, Cuenca, 2016.

[12] EMOV EP, Manual de normas básicas sobre infracciones de tránsito y su procedimiento, Cuenca, 2014.

[13] Moreno, F. (Juez de Tránsito), Criterios de Valoración y Aceptación de las Pruebas. [Entrevista]. 3 Mayo 2017.

[14] Presidencia Constitucional del Ecuador, Decreto Ejecutivo 988, Quito, 2012.

[15] Asamblea Nacional Constituyente, Ley Orgánica de Transporte Terrestre y Seguridad Vial, Quito, 2008.

[16] EMOV EP, Normas para el Uso de los Recursos Informáticos de la Empresa Pública Municipal de Movilidad de Tránsito y Transporte de Cuenca, Cuenca, 2015.

ANEXOS

Anexo “A”. Cuestionario de identificación de activos de información

Cuestionario de Identificación de Activos de Información

Entrevistado:		**Fecha de Entrevista:**	
Cargo:			
Área:		**Código de Entrevista:**	
Teléfono:			
Correo Electrónico:		**Entrevistador:**	

Objetivo: Ejecutar el inventario y clasificación de los activos de información de los procesos que intervienen en la Cadena de Custodia de Evidencias Digitales que gestiona la EMOV.

1. Identificación del Activo de Información

1.1 ¿Qué información necesita para la ejecución de su trabajo?

1.2 ¿A partir de la ejecución de su trabajo qué información genera?

1.3 Nombre del Activo
Nombre que identifica al activo

1.4 Tipo de Activo

1. **Procesos, subprocesos, actividades del negocio** (cumpla con los requisitos contractuales, legales o reglamentarios)
2. **Información estratégica**, de alto costo (recolección, almacenamiento, procesamiento y transmisión exigen tiempo y dinero)
3. **Hardware:** Equipos de procesamiento de datos, móvil, fijo, periféricos para procesamiento, medios para datos, medio electrónico, otros medios (papel, dispositivas, documentación, fax)
4. **Software:** Programas que contribuyen al procesamiento de datos (SO; Servicio, mantenimiento o administración; paquetes de software, software estándar; aplicaciones del negocio)
5. **Redes:** Dispositivos de telecomunicaciones que interconectan varias pcs o elementos de un SI (medios y soportes, transmisión pasiva o activa, interfaz de comunicación)
6. **Personal:** Persona a cargo de la toma de decisiones, usuarios, personal de operación/mantenimiento, desarrolladores)
7. **Ubicación:** Todos los lugares que contienen el alcance y los medios físicos que se requieren

para su funcionamiento. (Ambiente externo, instalaciones, zona, servicios esenciales, servicios públicos).

8. **Estructura de la organización:** Todas las estructuras del personal asignado a una labor y los procedimientos (autoridades, estructura de la organización, organización del sistema o el proyecto, subcontratistas/proveedores/fabricantes)

1.5 Descripción del Activo

Detalles relevantes y adicionales del activo; se determina si el activo comprende otros activos que podrían ser suministrados por otras áreas.

2. Ubicación del Activo de Información

2.1 Propietario del Activo

Parte de la organización, persona, cargo, proceso o grupo de trabajo que tiene la responsabilidad de la correcta gestión del activo durante todo su ciclo de vida. Asegurar que sea inventariado, clasificado y protegido, definir y revisar periódicamente las restricciones de acceso, garantizar el manejo adecuado cuando es eliminado o destruido.

2.2 Custodio (s) del Activo

Área designada de la entidad, cargo, proceso, o grupo de trabajo, que tiene la responsabilidad de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido (copias de seguridad, asignación privilegios de acceso, modificación y borrado), salvaguarda la información.

2.3 Usuario (s)

Persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

2.4 Medio de Soporte

Físico – Digital-Físico/Digital

2.5 Acceso

Tipo de acceso que tiene autorizado el usuario: Lectura, Escritura, Modificación, Eliminación.

2.6 Formato

Identifica la forma, tamaño o modo de presentación del activo de información: Imagen .jpg .gif .png .tif. ttf - Video .avi .mpeg .mov - Audio .wav .mid. .mp3 .mp4 .ogg - Texto .doc .txt .rtf .pdf - Base de Datos .mdb .sql – otro.

2.7 Ubicación de la Información

Disponible, publicada; Física: Lugar exacto (edificio, piso, costado, área, archivador y sector) donde se encuentra el activo, bajo custodia del Custodio de la información; Electrónica:

Computadores, dispositivos de almacenamiento internos y externos, carpeta pública o privada, sistema de información, equipo de escritorio (dirección IP), nombre del servidor (base de datos, aplicaciones) o url.

2.8 Frecuencia de Actualización

Periodicidad de tiempo en el que se actualiza el activo de acuerdo a su naturaleza y a la normativa aplicable.

2.9 Respaldo (Si – No)

Si, si el activo de información cuenta con un respaldo o copia, el cual podría ser restaurado en caso de requerirse. NO, si la información no cuenta con un respaldo.

3. Seguridad del Activo de Información

3.1 Atributos

Confidencialidad

3.1.1 (A1) El activo de información debe ser restringido a un número limitado de personas.

3.1.2 (A2) La divulgación del activo de información causaría un daño irreparable, grave o de difícil reparación

3.1.3 (A3) El activo de información debe ser protegido de personas externas

Integridad

3.1.4 (A4) La alteración del activo de información causaría un incumplimiento legal o normativo para la institución.

3.1.5 (A5) La alteración del activo de información es de fácil identificación, su corrección es sencilla y no causa daños en las operaciones de la institución.

3.1.6 (A6) El activo de información puede ser alterado o comprometido para fraudes o corrupción

Disponibilidad

3.1.7 (A7) La falta de acceso oportunamente al activo de información por personal autorizado podría afectar la seguridad pública o seguridad nacional.

3.1.8 (A8) La falta de acceso al activo de información por personal autorizado por más de 10 horas ocasiona la interrupción parcial de las operaciones, sin embargo no ponen en riesgo el cumplimiento de algún compromiso institucional.

3.1.9 (A9) El tiempo de tolerancia para el acceso al activo de información sin ocasionar ninguna consecuencia para el proceso o la institución se encuentra entre 30 a 60 minutos.

3.2 Valor

Según las propiedades de confidencialidad, integridad y disponibilidad los activos de información pueden estar expuestos a daños que comprometen la misión de la entidad. Se asigna un valor

cualitativo, que permita posteriormente realizar el análisis de riesgos de cada activo, de acuerdo con la siguiente escala:

A: Alto, M: Medio, B: Bajo

Alto: Afecta a los procesos del negocio.

Medio: Afecta a los procesos de apoyo del negocio.

Bajo: Afecta a los procesos de manera leve sin causar ningún daño considerable a la institución**.**

4. Clasificación del Activo de Información

Cada nivel de clasificación posee características propias de protección, manejo y tratamiento del activo de información.

Uso público: Información que ha sido declarada de conocimiento público de acuerdo con alguna norma jurídica o por parte de las autoridades de la institución. Información que puede ser conocida y utilizada sin autorización por cualquier persona. Se encuentra en registros públicos o en fuentes de acceso al público. LOTAIP Art. 7

Uso Interno: Información que puede ser conocida y utilizada por todos los funcionarios de la entidad, cuya divulgación y uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad o a terceros.

Uso Restringido: Información que solo puede ser conocida y utilizada por un grupo muy reducido de empleados debidamente autorizados por el propietario de la información, generalmente de la alta dirección, su divulgación o uso no autorizados podría ocasionar pérdidas graves a la institución como impactos financieros, daño a la seguridad pública, problemas judiciales o penales.

Fundamento Legal
Norma, Ley, artículo, otros.

Anexo “B”. Matriz de inventario y clasificación de activos de información

Inventario y Clasificación de Activos de Información

Entrevistado:
Area:
Fecha:

Identificación del Activo de Información				Ubicación del Activo de Información									
Código Activo	Nombre del Activo	Tipo de Activo 1 Actividades y procesos del negocio 2 Información 3 Hardware 4 Software 5 Redes 6 Personal 7 Ubicación 8 Estructura de la Organización	Descripción	Propietario del Activo	Custodio(s) del Activo	Usuario(s)	Medio de Soporte 1 Físico 2 Digital	Acceso 1 Lectura 2 Escritura 3 Modificación 4 Eliminación	Formato (Imagen .jpg .gif .png .tif. ttf Video .avi .mpeg .mov Audio .wav .mid. .mp3 .mp4 .ogg Texto .doc .txt .rtf .pdf Base de Datos .mdb .sql Correo Electrónica y otros)	Ubicación de la Información Disponible/Publicada		Frecuencia de Actualización	Respaldo 1 Si 2 No
										Física	Electrónica		

Seguridad del Activo de Información														Clasificación del Activo de Información				
Atributos										Valor				Uso Público	Uso Interno	Uso Restringido	Fundamento Legal	Observaciones
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	Confidencialidad	Integridad	Disponibilidad	Valor Absoluto					

Anexo “C”. Matriz de análisis de riesgo

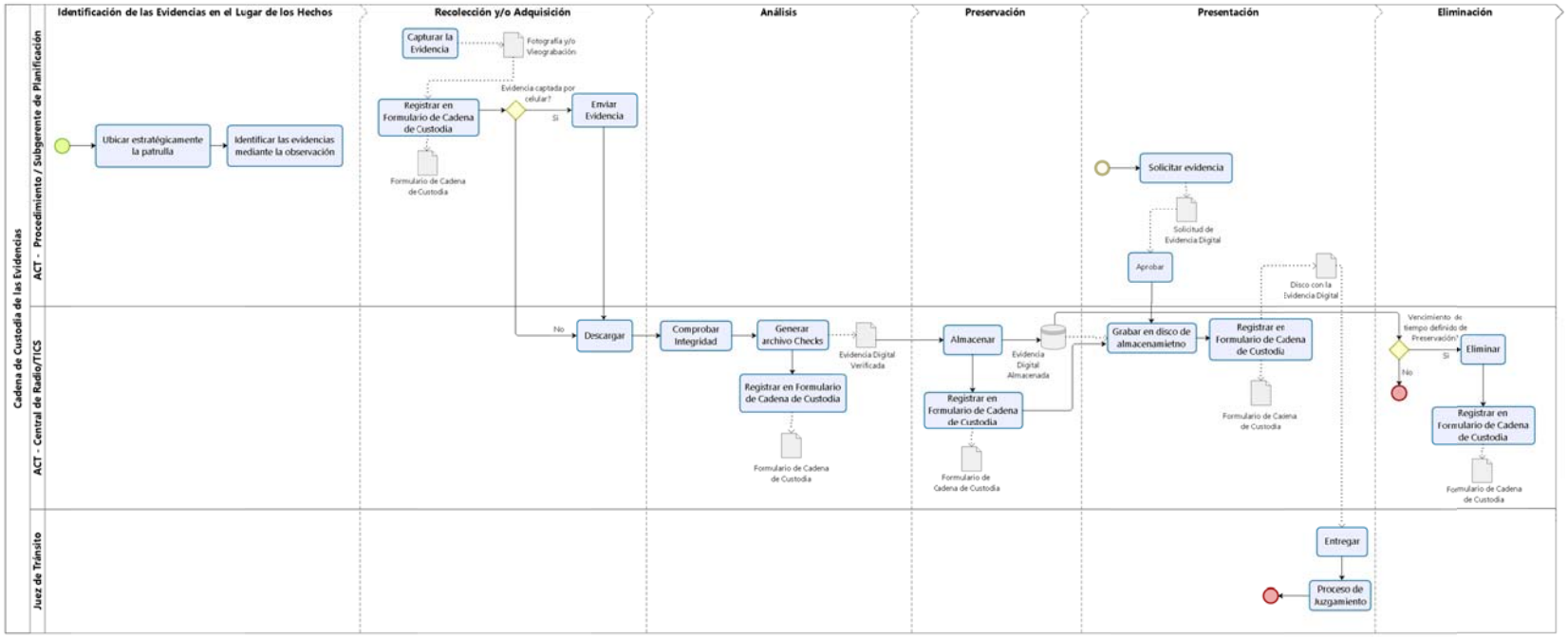
Análisis de Riesgos de los Activos de Información

Activo:
Impacto:

TIPO	Amenaza	Origen: D - deliberadas A - accidentales E - ambientales	Controles		Vulnerabilidad	Consecuencias		Riesgo Actual				
			Existentes	Funcionalidad		Escenarios del incidente	Consecuencia / Impacto	Probabilidad		Riesgo	Nivel de Riego	

Medidas de Respuesta del Riesgo	Controles	Observaciones	Riesgo Residual				
	Recomendados		Frecuencia		Riesgo	Nivel de Riesgo	

Anexo “D”. Diagrama de procedimiento de cadena de custodia de la evidencia digital



Anexo “E”. Formulario de cadena de custodia

EMOV-EP	FORMULARIO DE CADENA DE CUSTODIA
	Número de formulario :

1. RECOLECCIÓN / ADQUISICIÓN

1.1 Información del Agente Civil de Tránsito que captura la evidencia

Nombres y Apellidos	Número de cédula	Firma

1.2 Información del incidente

Tipo	Lugar	Fecha y hora

1.3 Tipo de evidencia : ☐ **FOTOS** ☐ **VIDEOS**

1.4 Información del equipo o dispositivo

Medio	Marca	Modelo	Número de patrulla

1.5 Información del Agente Civil de Tránsito que recibe y descarga la evidencia

Nombres y Apellidos	Número de cédula	Firma

1.6 Fecha y hora de la descarga :

2. ANÁLISIS

2.1 Información del archivo de checksum

Nombre del archivo	Hash

2.2 Detalle de las evidencias

Número	Nombre del archivo	Tipo (Foto / Video)	Hash	Información adicional

3. PRESERVACIÓN

3.1 Información del repositorio

Nombre del equipo	Ruta de almacenamiento	Tiempo mínimo

4. PRESENTACIÓN

4.1 Información general

Número de parte	Número de citación	Fiscal / Juez

4.2 Información del Agente Civil de Tránsito que recibe la evidencia

Nombres y Apellidos	Número de cédula	Firma

4.3 Fecha y hora de entrega : **4.4 Tipo de medio (CD, DVD, etc.) :**

5. ELIMINACIÓN

5.1 Información general

Fecha y hora :

5.2 Información del responsable

Nombres y Apellidos	Número de cédula	Firma

Anexo “F”. Manual de uso de herramientas FastCopy y HashCheck

En la pantalla principal de ***FastCopy***, lo primero que se debe seleccionar es la carpeta origen de los archivos que se necesita copiar**,** para eso se debe dar click en el botón ***Source***, como se ve en la figura 1.

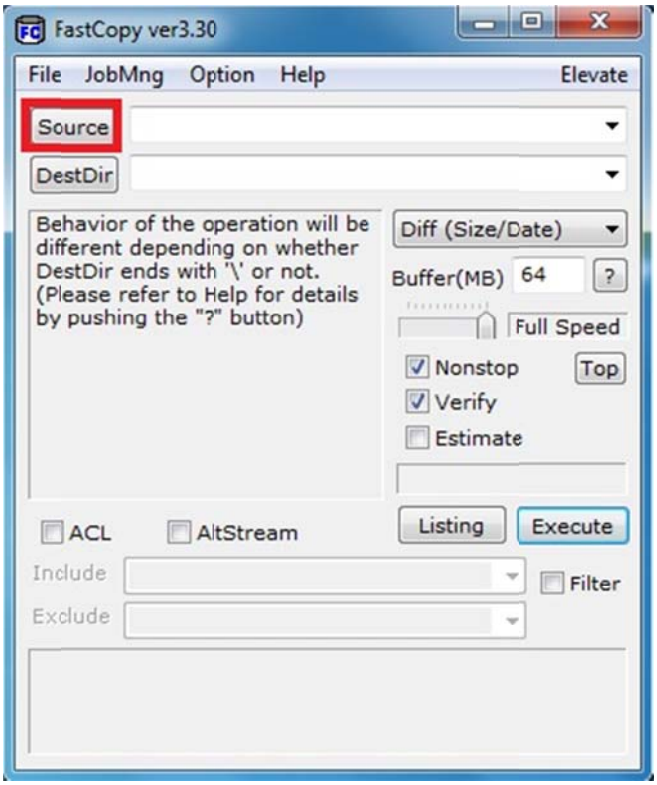


Figura 1 Botón Source

A continuación se abre una ventana donde se puede seleccionar la carpeta origen para la copia, pero adicionalmente hay un botón ***Select files***…en la parte superior (figura 2).

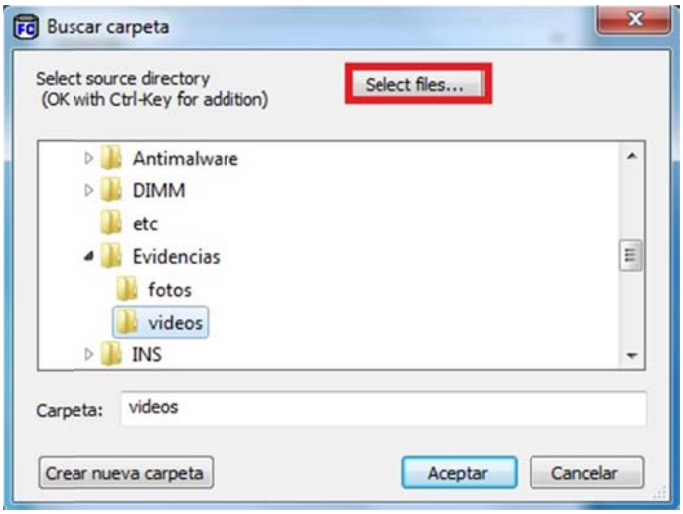


Figura 2 Selección de archivos

Si se presiona este botón, el programa da la posibilidad de seleccionar cuáles son los archivos, dentro de la carpeta, que se desean copiar.

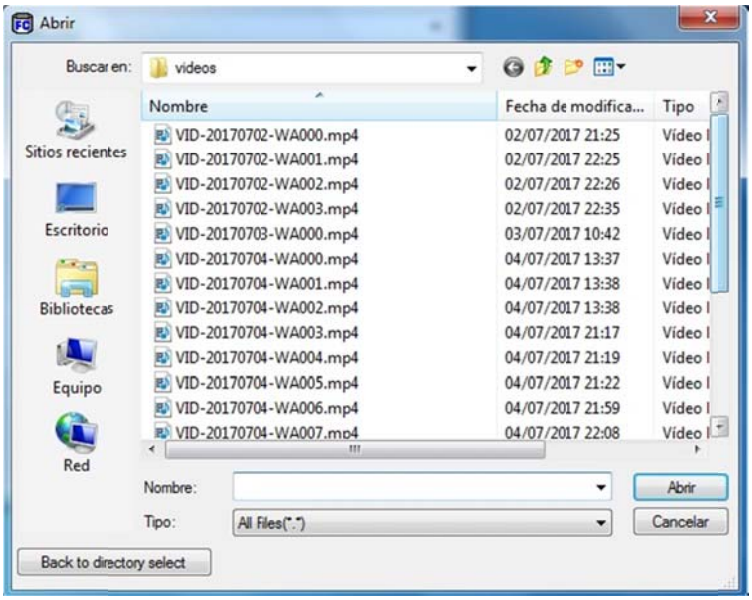


Figura 3 Archivos a copiar

Para este ejemplo se va a copiar la carpeta completa, por lo que se regresa a la ventana anterior, ya sea presionando el botón ***Cancelar*** o el botón ***Back to directory select.*** Luego de seleccionar la carpeta se debe presionar el botón ***Aceptar.***

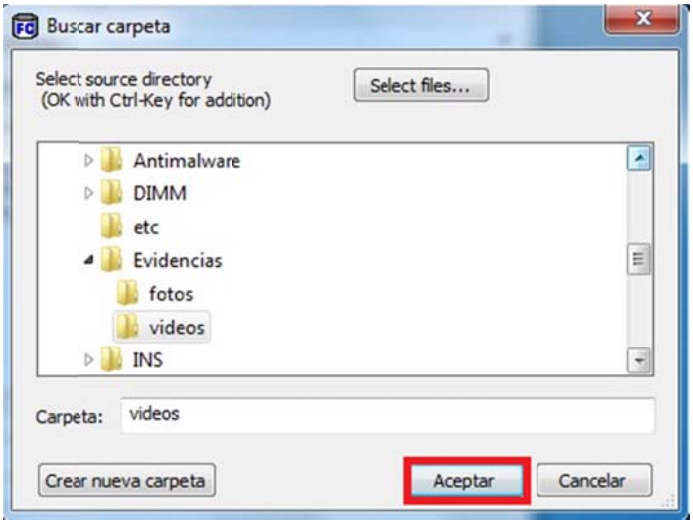


Figura 4 Carpeta origen

Una vez seleccionada la carpeta origen, se regresa a la pantalla principal, donde se muestra la ruta completa de la carpeta.

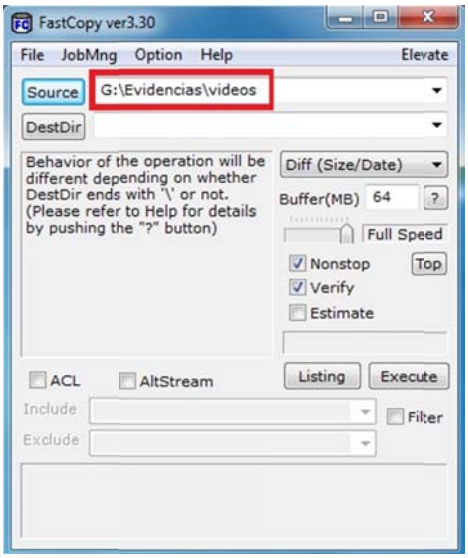


Figura 5 Ruta de la carpeta origen

A continuación se debe seleccionar la carpeta destino, para esto se debe dar click en el botón ***DestDir.***

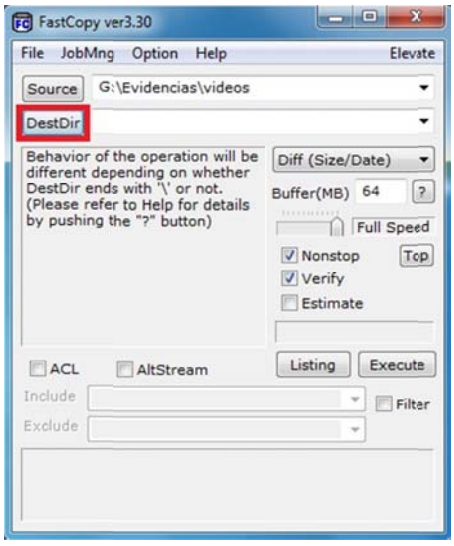


Figura 6 Botón DestDir

Se selecciona la carpeta destino y se presiona el botón ***Aceptar.***

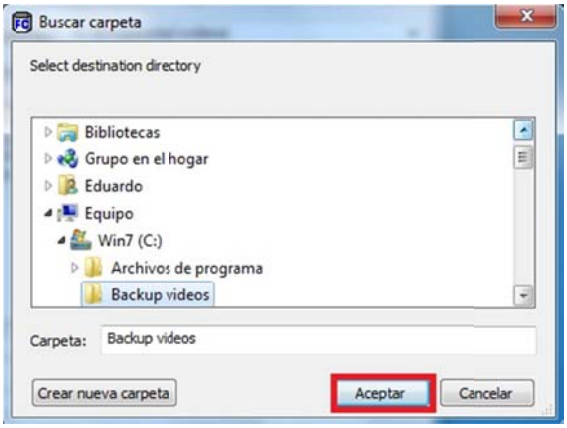


Figura 7 Búsqueda de carpeta destino

Asimismo se presentará la ruta completa donde se realizará la copia

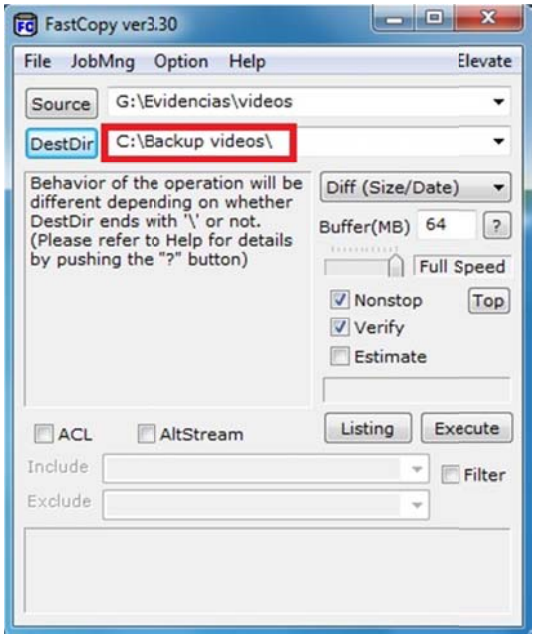


Figura 8 Ruta de carpeta destino

Hay que tomar en consideración que la ruta destino incluye un \ al final, lo que indica que dentro de esta ruta se creará una nueva carpeta con el nombre de la carpeta origen y sobre esta nueva carpeta se realizará la copia.

Si se desea que la copia se realice usando como raíz la carpeta destino seleccionada, como en este ejemplo, se debe eliminar el caracter \. A este comportamiento se refiere la leyenda que se presenta: ***Behavior of the operation will be different depending on whether DestDir ends with '\' or not.***

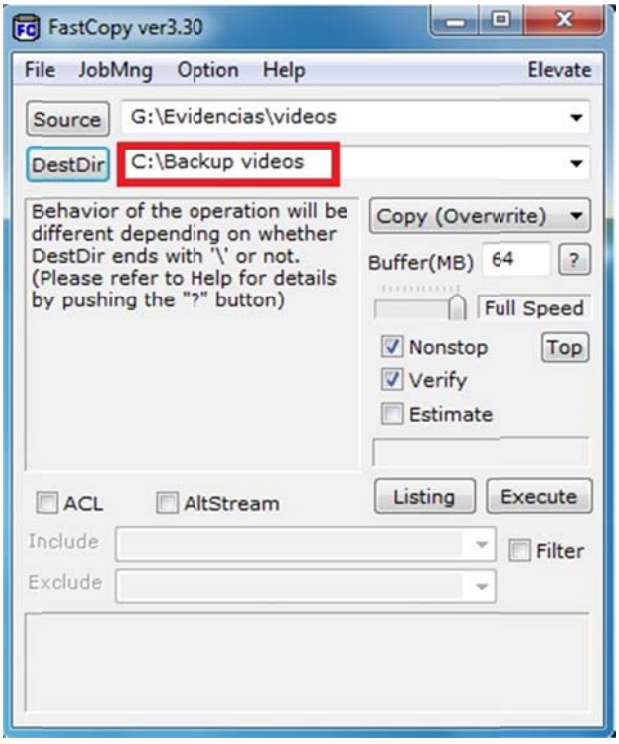


Figura 9 Ruta de carpeta destino

Para continuar con el proceso se debe seleccionar la opción ***Copy (Overwrite).*** Esto le indica al programa que copie todo el contenido, y que si alguno de los archivos origen ya existe en la carpeta destino, lo sobrescriba.

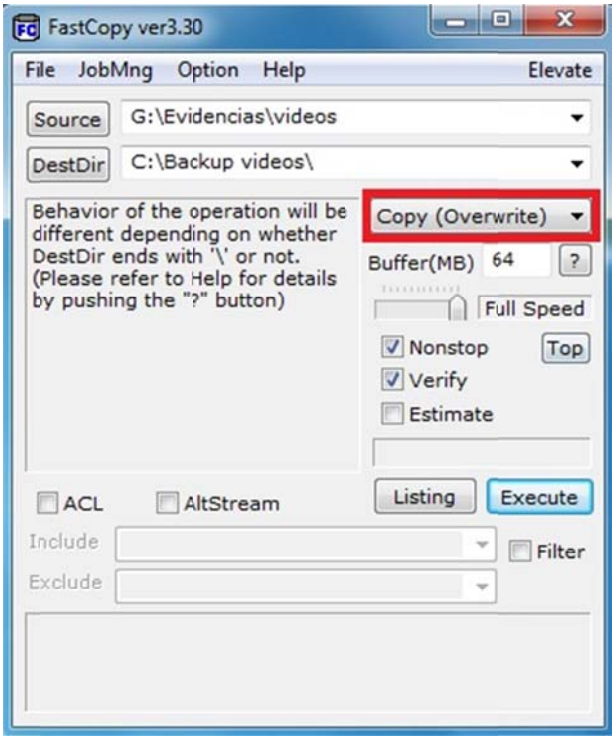


Figura 10 Botón Copy (Overwrite)

Una vez parametrizada la copia a realizar se debe presionar el botón ***Execute.***

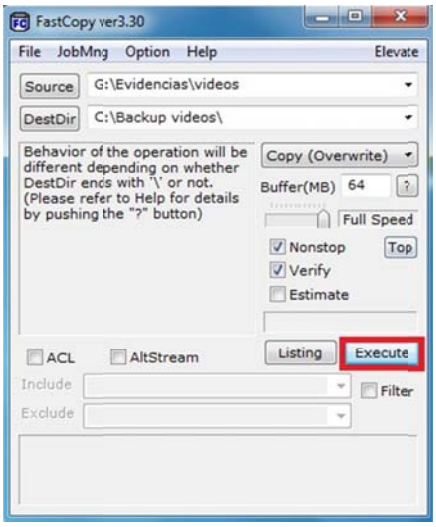


Figura 11 Botón Execute

En el cuadro de información se irá presentando las estadísticas de la copia mientras esta se realiza y en el cuadro inferior presentará el nombre del archivo que se está copiando.

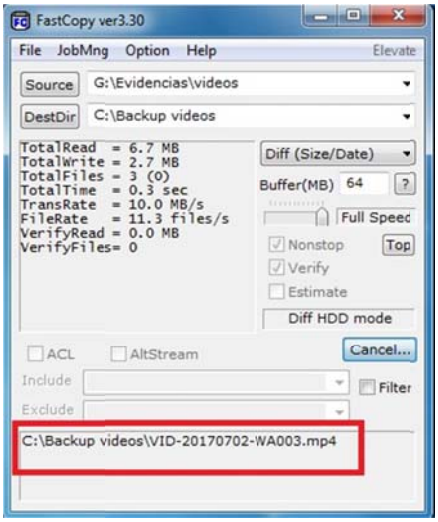


Figura 12 Inicio de ejecución del proceso

Al finalizar la copia se presentará información como la cantidad de archivos, el tiempo que tomó la copia, etc., y en el cuadro inferior mostrará un mensaje que indica la finalización del proceso.

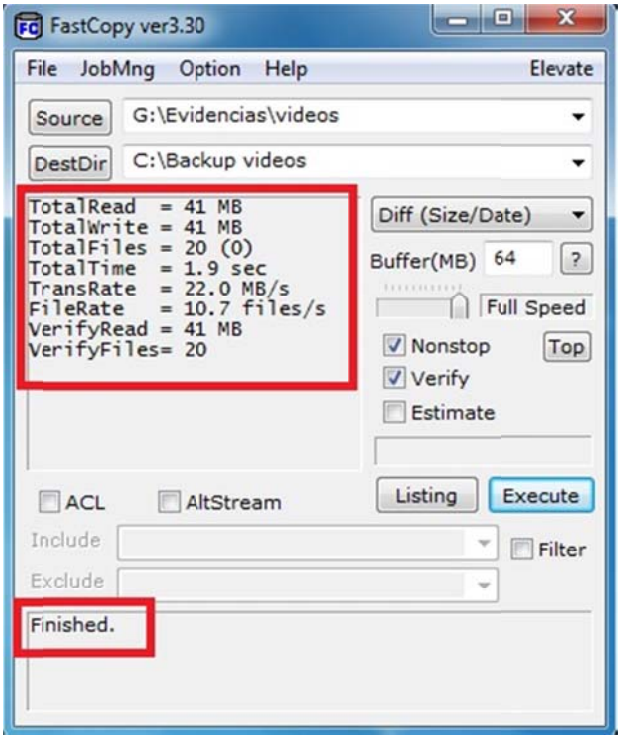


Figura 13 Fin de ejecución del proceso

En la carpeta del programa se crea una subcarpeta llamada ***Log***, y dentro de esta se irán generando los logs de las copias realizadas. El nombre de los archivos creados estará conformado por la fecha y la hora del proceso.

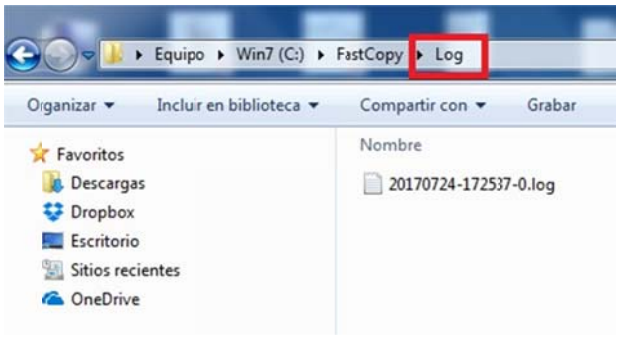


Figura 14 Carpeta Log

Como se puede verificar en la figura 15, en el contenido del archivo generado se detalla la carpeta origen, la carpeta destino, el nombre del archivo con su tamaño y el hash tipo SHA-1.

```
1  ----------------------------------------------
2  FastCopy(ver3.30) start at 2017/07/24 17:25:37
3
4  <Source>  G:\Evidencias\videos
5  <DestDir> C:\Backup videos
6  <Command> Diff (Size/Date) (with Verify)
7  ------------------------------------------------
8  + C:\Backup videos\VID-20170702-WA000.mp4   <20170702-212530 563,780 sha1=0c29a673a31a13dc109e9db147df73ff8b5c466f>
9  + C:\Backup videos\VID-20170702-WA001.mp4   <20170702-222522 604,035 sha1=4a66ff2499ea6da6bdbc2cfade7a3c75db0e0de0>
10 + C:\Backup videos\VID-20170702-WA002.mp4   <20170702-222644 1,616,034 sha1=2741d219afd1e1541c3c52f827871e5fa37f4f8d>
11 + C:\Backup videos\VID-20170702-WA003.mp4   <20170702-223534 15,000,386 sha1=a572e0711e4bf39ae554e1c0785d7aaee2811f93>
12 + C:\Backup videos\VID-20170703-WA000.mp4   <20170703-104244 190,454 sha1=9a68ffcb27b7f4ea6595274e14fb85639ad451a5>
13 + C:\Backup videos\VID-20170704-WA000.mp4   <20170704-133706 380,755 sha1=4a8b1a1f1cd30eb87f4ed64dcb612cfe1245201c>
14 + C:\Backup videos\VID-20170704-WA001.mp4   <20170704-133810 1,080,966 sha1=9951984a30c184c47628f92533194caa05acb4f4>
15 + C:\Backup videos\VID-20170704-WA002.mp4   <20170704-133840 291,717 sha1=2e2c0b1c9ad1903ddc6fff65705b5b9936f758f1>
16 + C:\Backup videos\VID-20170704-WA003.mp4   <20170704-211738 728,215 sha1=8e1107d9e6595fe487ec4affdc5bd762961fa1e3>
17 + C:\Backup videos\VID-20170704-WA004.mp4   <20170704-211946 1,152,008 sha1=d322ca26c7d20fd549c11fea9998290588f21466>
18 + C:\Backup videos\VID-20170704-WA005.mp4   <20170704-212234 1,070,245 sha1=4e5c79e581c109b2b95eaf11d62362a95757f64c>
19 + C:\Backup videos\VID-20170704-WA006.mp4   <20170704-215940 3,769,459 sha1=9706f1aa8d62ee936b75c84885031606d8afcdd5>
20 + C:\Backup videos\VID-20170704-WA007.mp4   <20170704-220818 556,697 sha1=1d3bf7710576970b9543e264584081280002c641>
21 + C:\Backup videos\VID-20170704-WA008.mp4   <20170704-222724 5,639,628 sha1=a5a2044946d33946f665d333a8cf49f89e06ea7c>
22 + C:\Backup videos\VID-20170704-WA009.mp4   <20170704-223148 5,644,288 sha1=d9f979f6f8314d90ef8c3f3879735cdb1e086057>
23 + C:\Backup videos\VID-20170705-WA000.mp4   <20170705-142850 219,525 sha1=9d7c7d7b5f1a7c1eccb7746e82d19fbb58f51b70>
24 + C:\Backup videos\VID-20170705-WA001.mp4   <20170705-142958 504,011 sha1=fb93e91efa90ae0624cdbd2f27861a3800cccb4b>
25 + C:\Backup videos\VID-20170705-WA002.mp4   <20170705-193804 1,061,664 sha1=aa07390adc37ed28454fca79a71142bb31e2dce2>
26 + C:\Backup videos\VID-20170705-WA003.mp4   <20170705-193956 2,193,826 sha1=f5cbb3f8c30cc21e3b700b83da61608ced5acfad>
27 + C:\Backup videos\VID-20170705-WA004.mp4   <20170705-202216 1,012,241 sha1=851d59b93394deaab4fd6a8d29ece08b8224080f>
28
29 No Errors
```

Figura 15 Archivo log

Al final del archivo se presenta una leyenda que dice ***No Errors***, lo cual indica que no hubo errores en el proceso, y también presenta el resumen que se presentó anteriormente en la pantalla.

```
28
29   No Errors
30
31  TotalRead  = 41 MB
32  TotalWrite = 41 MB
33  TotalFiles = 20 (0)
34  TotalTime  = 1.9 sec
35  TransRate  = 22.0 MB/s
36  FileRate   = 10.7 files/s
37  VerifyRead = 41 MB
38  VerifyFiles= 20
39
40  Result : (ErrFiles : 0 / ErrDirs : 0)
41
```

Figura 16 Resumen del archivo log

A diferencia del software anterior, este no tiene una interface propia, sino que agrega funcionalidades al sistema de archivos de Windows.

Continuando con el ejemplo anterior, se selecciona la carpeta destino, se da click derecho sobre ella y por último se selecciona la opción ***Propiedades.***

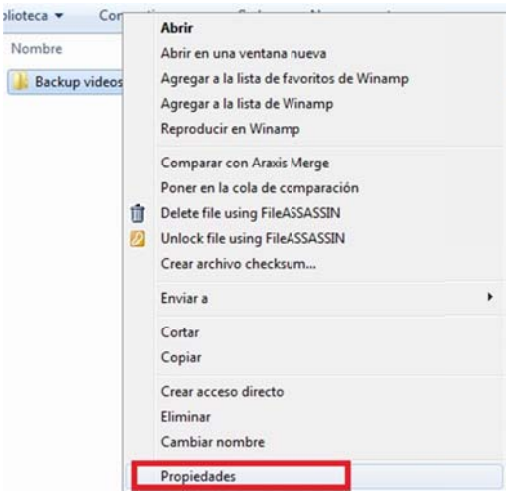


Figura 17 Propiedades de carpeta

Como se puede observar en la figura 18, se agregó a las propiedades una pestaña llamada ***Checksum.***

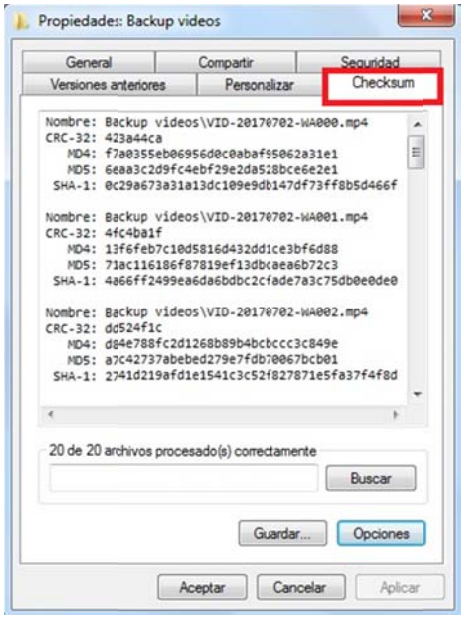


Figura 18 Pestaña Checksum

Esta nueva pestaña contiene la lista de archivos de la carpeta, además de cuatro tipos de suma de comprobación para cada uno de ellos:

- CRC-32
- MD4
- MD5
- SHA-1

En la parte inferior presenta también la cantidad de archivos que contiene la carpeta.

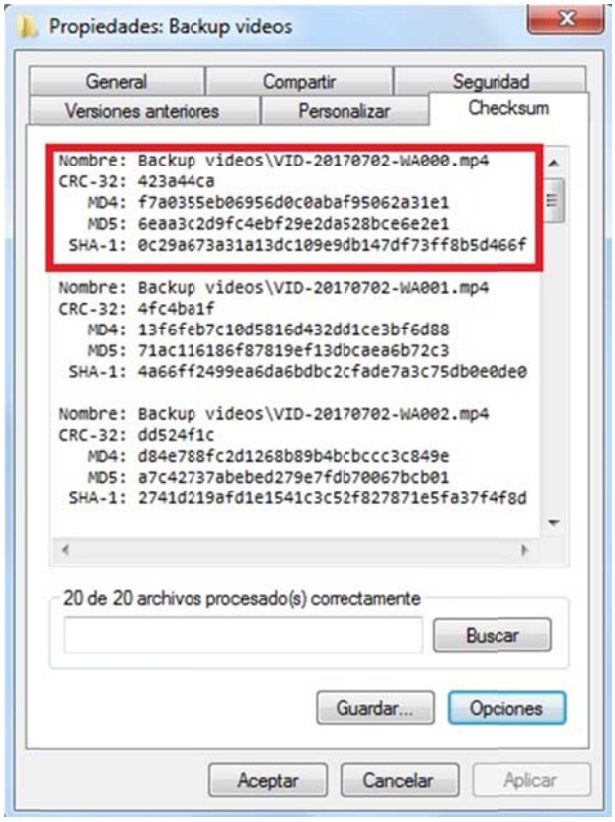


Figura 19 Hashes del archivo

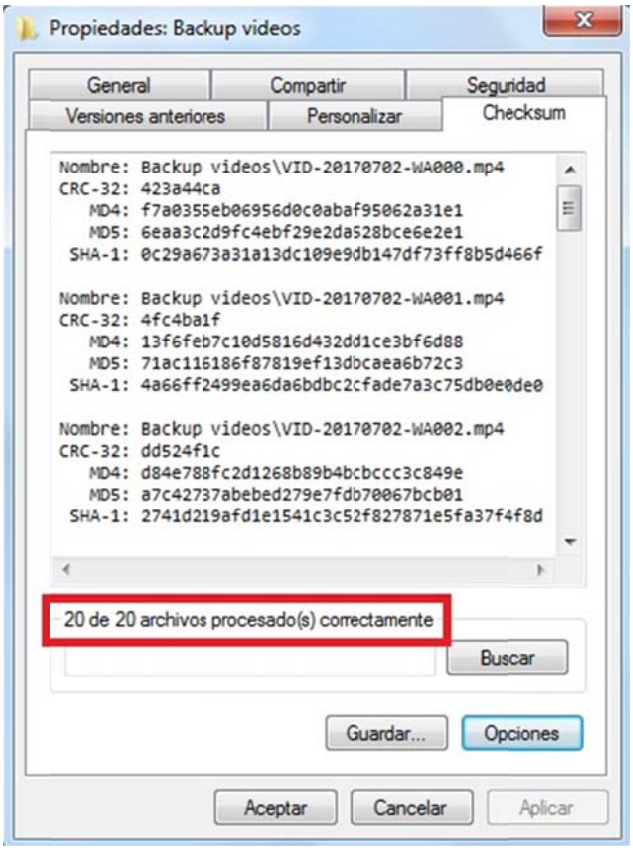


Figura 20 Archivos procesado

La obtención del código hash se realiza por medio de una lógica estándar, por lo que no importa con qué programa se calcule, el resultado debe ser siempre el mismo. En la figura 21 se muestra como ejemplo uno de los archivos de la carpeta: del lado izquierdo se puede observar el SHA-1 calculado por ***HashCheck*** y del lado derecho se verifica este mismo hash en el archivo generado por ***FastCopy.***

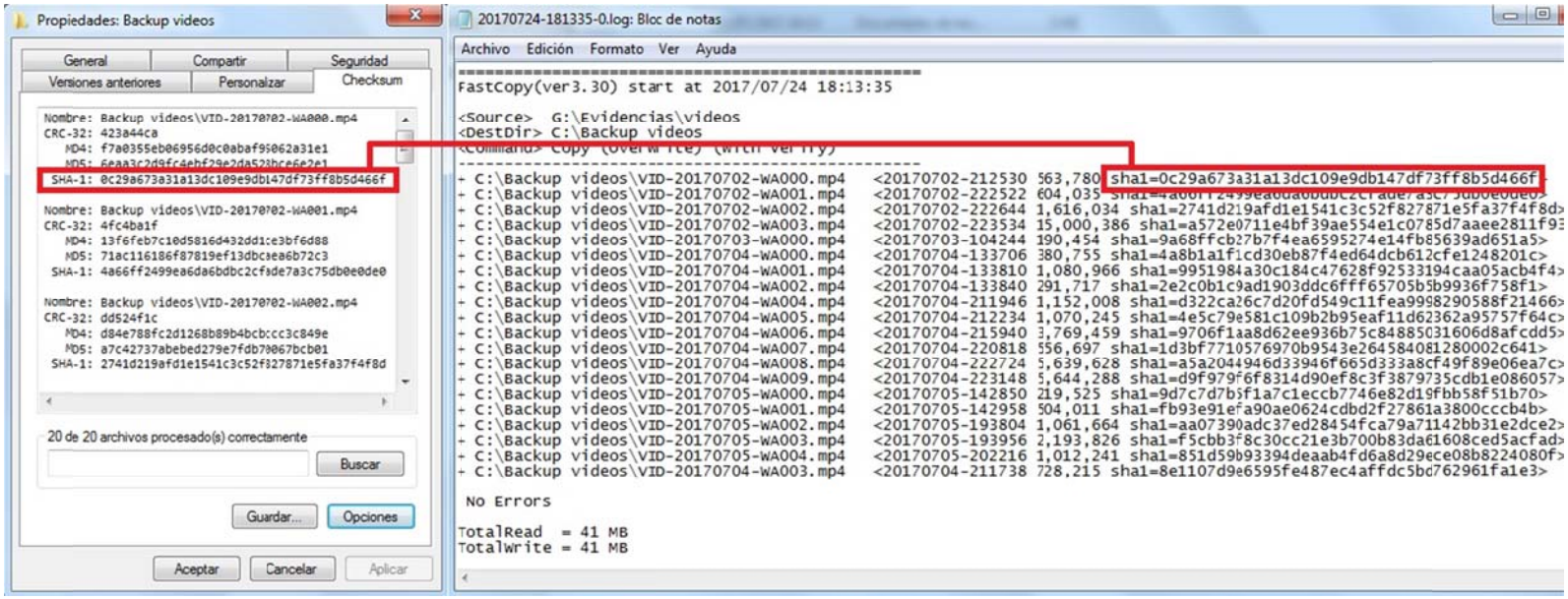


Figura 21 Comparación de hash – HashCheck / FastCopy

El programa da la posibilidad de generar un archivo checksum para la carpeta seleccionada, para esto se debe dar click en el botón ***Guardar***…. A continuación se presenta la ventana de diálogo común y corriente de Windows para grabar archivos, en la cual nos permite elegir entre cuatro tipos de archivos (uno por cada tipo de hash):

Tabla 1 Tipos de archivos hash

Tipo de Hash	Tipo de archivo
CRC-32	sfv
MD4	md4
MD5	md5
SHA-1	sha1

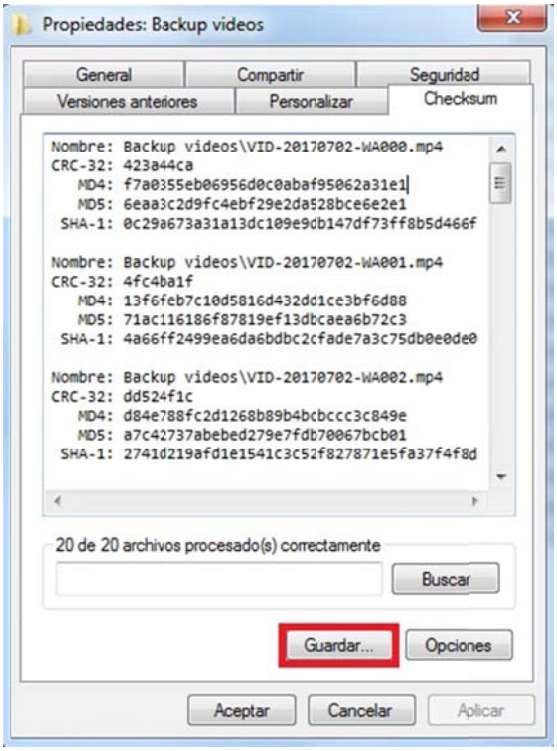


Figura 22 Guardar archivo checksum

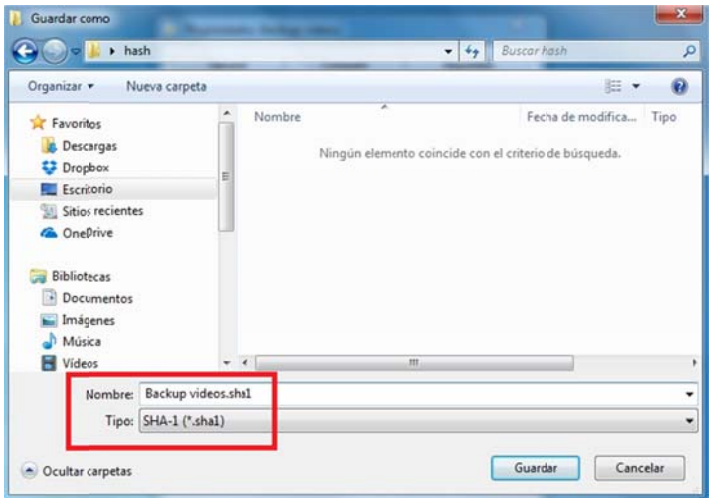


Figura 23 Tipo archivo sha1

Después de seleccionar la ruta donde se guardará este archivo e ingresar el nombre que se le dará, se debe seleccionar ***SHA-1 (*.sha1)*** en el campo ***Tipo*** y presionar el botón ***Guardar.***

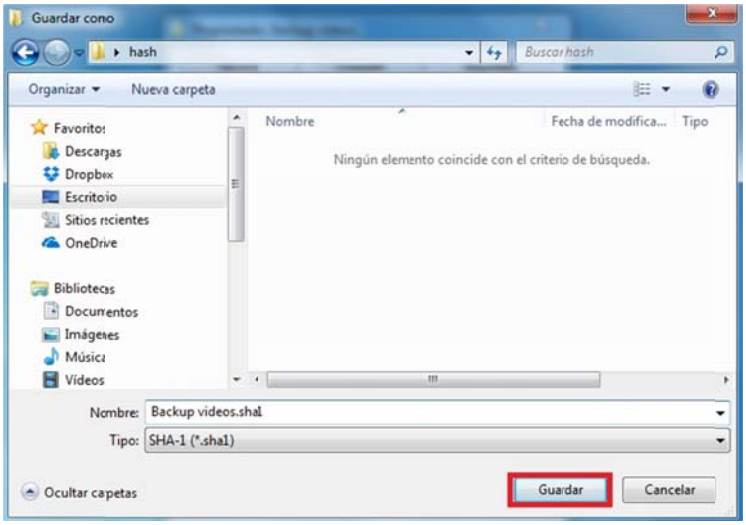


Figura 24 Guardar archivo sha1

Para este caso se ha generado un archivo de checksum tipo sha1.

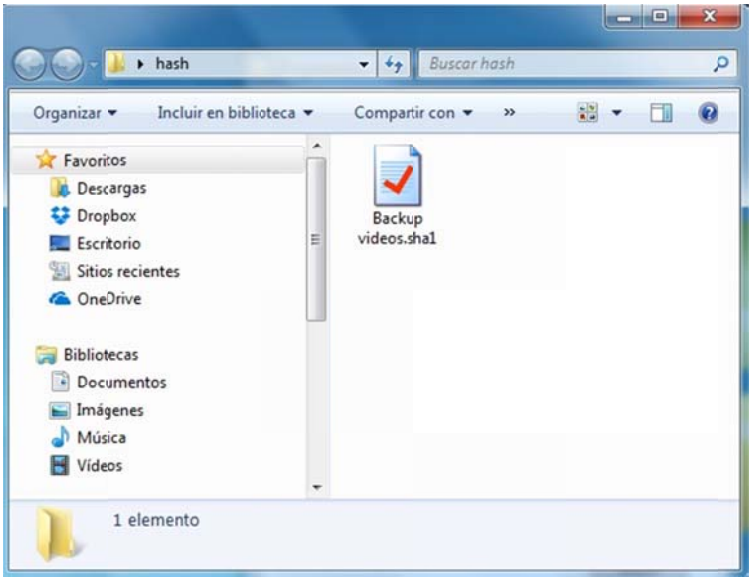


Figura 25 Archivo sha1

Al dar doble click en el archivo generado se abre una ventana donde muestra la lista de archivos existentes al momento de la generación con sus respectivos códigos hash. El programa ***HashCheck*** es el que permite tener este tipo de visualización del archivo, es decir, si este archivo se abre en una computadora en la que no esté instalado el ***HashCheck*** no se podrá ver su contenido con este formato, sin embargo éste podrá ser abierto de forma legible con cualquier editor de texto.

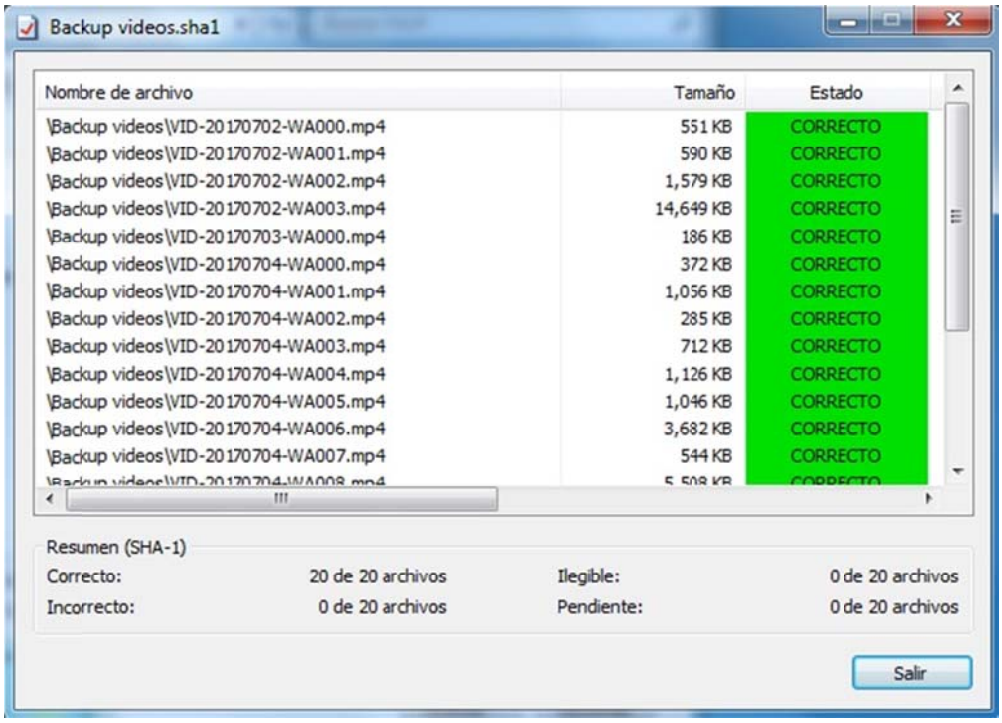


Figura 26 Contenido del archivo checksum (estados)

Además de listar los archivos, el programa verifica que la información contenida en él corresponda exactamente con el contenido de la carpeta desde la cual fue generado. Esto es muy necesario para a futuro comprobar que en esta carpeta no se eliminaron ni modificaron archivos. Si todo está correcto se presentará la columna ***Estado*** en verde y con una leyenda que dice ***CORRECTO.***

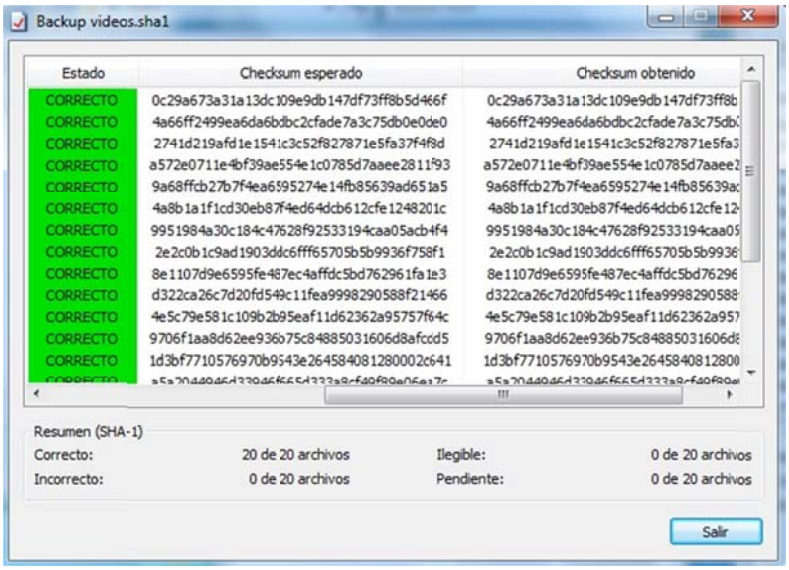


Figura 27 Contenido del archivo checksum (hashes)

A continuación se renombrará uno de los archivos de la carpeta, como se muestra en la figura 28, y luego se abrirá nuevamente el archivo checksum, el cual indicará que el archivo (el original) no fue encontrado, mostrando ***ILEGIBLE*** en la columna ***Estado***, en color amarillo.

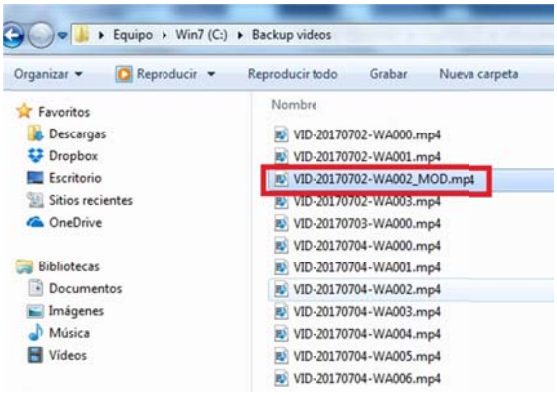


Figura 28 Modificación de nombre de archivo copiado

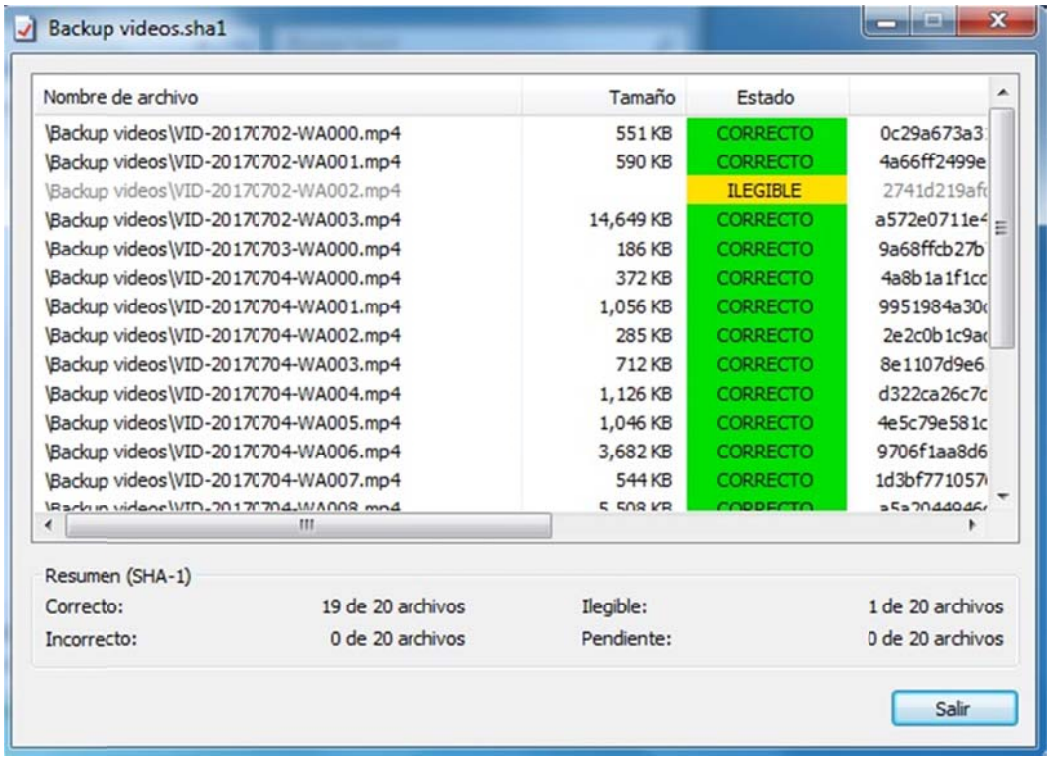


Figura 29 Verificación de archivo checksum (ilegible)

A continuación se altera el contenido del archivo VID-20170704-WA009.mp4 y se guardan los cambios, por ende su hash cambia. Este cambio es advertido por el programa, el cual muestra ***INCORRECTO*** en la columna ***Estado*** del archivo y en color rojo.

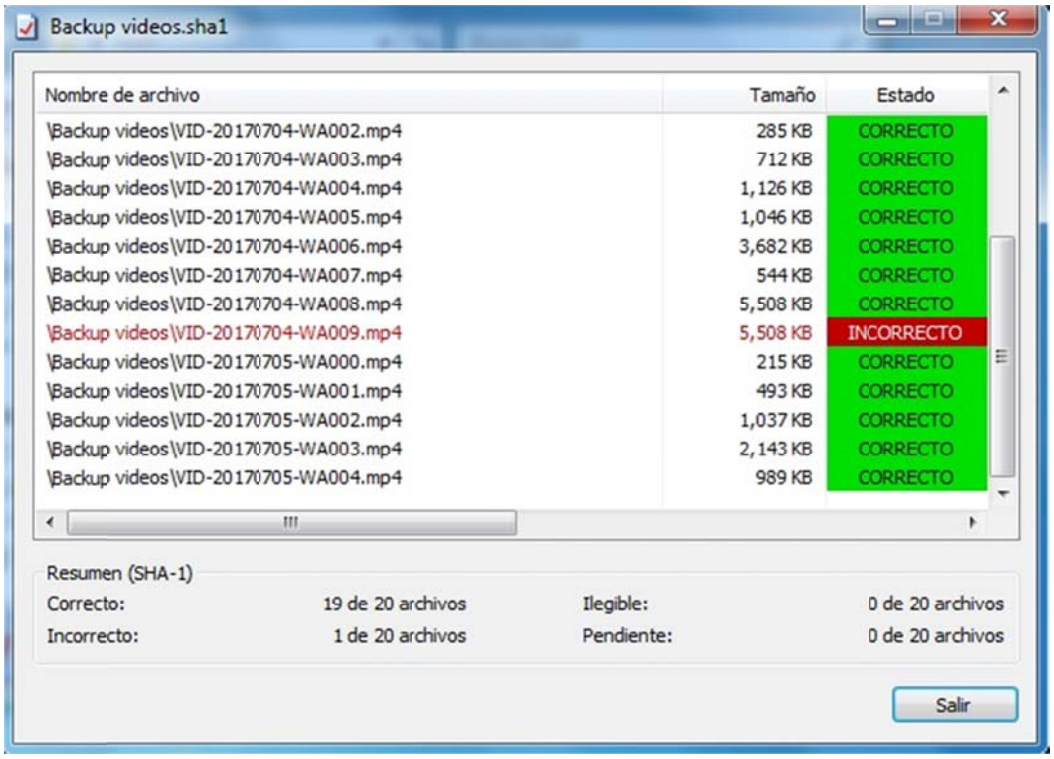


Figura 30 Verificación de archivo checksum (incorrecto)

Al verificar las columnas de hash se puede comprobar que son diferentes, la columna ***Checksum esperado*** muestra el hash antes de los cambios y la columna ***Checksum obtenido*** muestra el hash después de modificar el archivo.

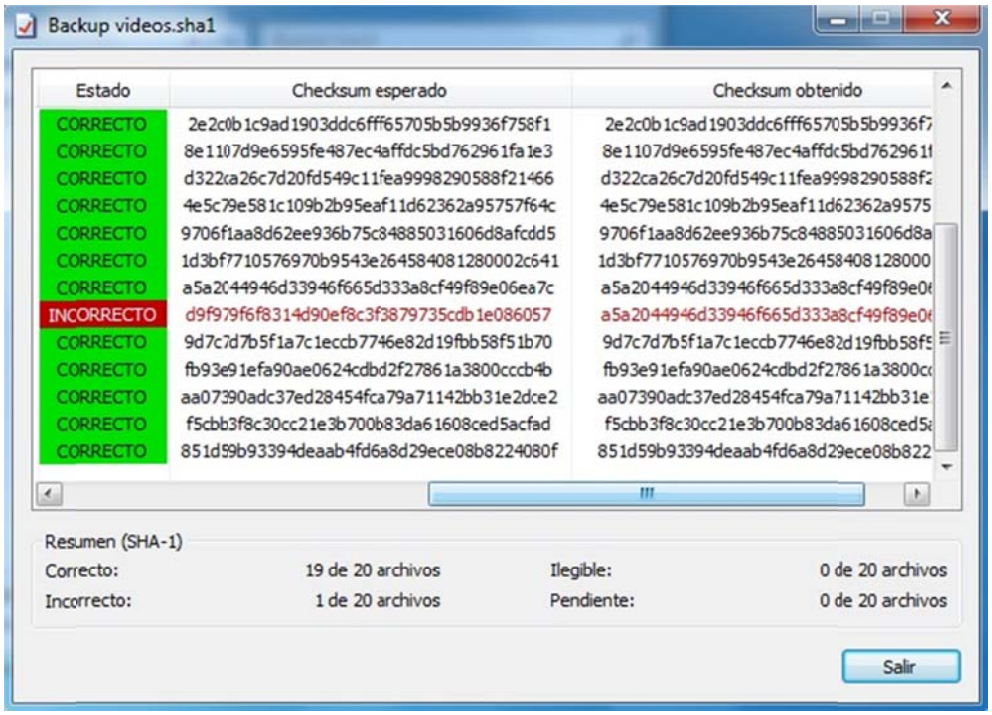


Figura 31 Verificación de archivo checksum (hash incorrecto)