OFICINA DE POSTGRADOS

TEMA:

TÉCNICAS DE SEGURIDAD EN REDES DE COMUNICACIONES APLICADAS A LA CUSTODIA DE EVIDENCIA DIGITAL.

Proyecto de investigación previo a la obtención del título de
Magister en Ciberseguridad

Línea de Investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES, SEGURIDAD DE LA INFORMACIÓN

Autor:

Perkins Santiago Haro Parra

Director:

Juan Carlos Santillán Lima M.Eng.

Ambato – Ecuador

Marzo 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

TÉCNICAS DE SEGURIDAD EN REDES DE COMUNICACIONES APLICADAS A LA CUSTODIA DE EVIDENCIA DIGITAL.

Línea de Investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES, SEGURIDAD DE LA INFORMACIÓN

Autor:

PERKINS SANTIAGO HARO PARRA

Juan Carlos Santillán Lima M.Eng. f._____
Firmado electrónicamente por: JUAN CARLOS SANTILLAN LIMA

CALIFICADOR

Darío Javier Robayo Jácome. Ing. Mg. f._____

CALIFICADOR

José Marcelo Balseca Manzano. Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda. Ing. Mg. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villaroel. Dr. f._____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Marzo 2021

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo, **PERKINS SANTIAGO HARO PARRA**, con **CC. 060341197-6**, autor del trabajo de graduación intitulado: "**TÉCNICAS DE SEGURIDAD EN REDES DE COMUNICACIONES APLICADAS A LA CUSTODIA DE EVIDENCIA DIGITAL**", previa a la obtención del título profesional de Magister en Ciberseguridad, de la oficina de posgrados.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, marzo 2021

PERKINS SANTIGO HARO PARRA

CC. 060341197-6

AGRADECIMIENTO

La gratitud es un hermoso valor relativamente fácil de demostrar dentro de la concepción más grande del ser humano, el amor recibido, la dedicación y la paciencia con la que cada día se preocupaban por mis avances y desarrollo de esta tesis es simplemente único y se refleja en la vida de un hijo.

Gracias a mis padres Blanquita y Huguito, por ser los principales promotores de mis sueños siendo la compañía idónea y más completa que se logra tener naturalmente en la vida, a mis hermanos por siempre desear y anhelar lo mejor para mi vida, a toda mi familia, a mis amigos, a mi novia por ser el ingrediente perfecto para poder alcanzar esta dichosa y merecida victoria.

Gracias a mi universidad la Pontificia Universidad Católica del Ecuador sede Ambato por haberme permitido formarme, gracias a todos los docentes que fueron participes en este proceso, a mi tutor de tesis por guiarme apropiadamente con sus conocimientos y experiencia para la culminación de este trabajo.

Gracias a todos ustedes, fueron ustedes los responsables de realizar pequeño aporte, que al dia de hoy se vería reflejado en la culminación de mi paso por esta alma mater.

Muchas gracias

Ing. Perkins Santiago Haro Parra

Maestrante.

DEDICATORIA

El presente trabajo está dedicado a mi querida familia, amigos y a cada una de las personas que directa o indirectamente han formado para de esta formación académica.

RESUMEN

A medida que las nuevas tecnologías, se extienden en las organizaciones con una creciente influencia de transformación digital, los desafíos de seguridad comenzaron a identificar nuevas amenazas y ataques cada vez mayores, la detección de amenazas y vulnerabilidades ha dado a los profesionales de ciberseguridad la adopción de nuevos métodos y técnicas acompañados de herramientas que garanticen la admisibilidad de la evidencia digital a corto y a largo plazo. Este proyecto establece un conjunto de técnicas de seguridad aplicadas en las redes de comunicaciones que aseguren la adecuada custodia digital. Para poder contestar la pregunta de investigación planteada, se planifica realizar un proceso de 4 etapas: investigación del estado del arte, descripción de las metodologías y técnicas de seguridad aplicadas en las redes de comunicación, diagnóstico de las metodologías o técnicas utilizadas por los actores de justicia y la síntesis de las buenas prácticas aplicadas en técnicas adecuadas sobre las redes de la custodia de la evidencia digital. La parte esencial de este proyecto consiste en el diagnóstico realizado a los principales actores del Consejo de la Judicatura de la provincia de Chimborazo lo que muestra que estos actores no cuentan con los conocimientos, metodologías, técnicas y recursos para la preservación y la admisibilidad de la evidencia digital, da paso a la vulnerabilidad muy amplia para los Ciberdelincuentes al acceso a la información, es esta alterada, modificada o a su vez destruida.

Palabras claves: ciberseguridad, admisibilidad, diagnóstico, preservación, ciberdelincuentes.

ABSTRACT

As new technologies spread in organizations with a growing influence of digital transformation, security challenges began to identify new threats and increasing attacks. Threat and vulnerability detection have encourage to cybersecurity professionals new methods and techniques accompanied by tools that guarantee digital evidence's admissibility in the short and long term. This project establishes a set of security techniques applied in communication networks that ensure adequate digital custody. In order to answer the research question, it is planned to carry out a process of four stages: state of the art, description of the security methodologies and techniques applied in communication networks, diagnosis of the methodologies or techniques used by the justice operators and the synthesis of acceptable practices applied with good techniques on the networks of the custody of digital evidence. The essential part of this project consists of the diagnosis made to the main operators of the Judicial Council of Chimborazo Province, which determines that these operators do not have the knowledge, methodologies, techniques, and resources for the preservation and admissibility of the digital evidence, resulting in an extensive vulnerability for Cybercriminals to access the information being it altered, modified or destroyed.

Keywords: *cybersecurity, admissibility, diagnosis, preservation, cybercriminals.*

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

Introducción

En el mundo actual donde la utilización de las redes de comunicaciones son más intensivo a través de dispositivos y medios como el internet, celulares, redes sociales y los nuevos entornos 3.0, *ejemplos de los más utilizados en la actualidad por los usuarios*, y en donde las relaciones personales se encarrilan a través de los medios tecnológicos, electrónicos y telemáticos, es racional que ahora empiece a surgir muchas necesidades de aprobar o acreditar las actuaciones legitimas en casos muy delicados como las transferencias bancarias, declaraciones, impuestos o las conductas ilícitas como fraudes informáticos, el PHISING, las amenazas mediante SMS y los acosos a través de redes sociales.

Durante esta pandemia, los sistemas de información juegan un papel sumamente importante en la administración de los datos y la información a la misma velocidad que se encuentra la situación. Por ello, es una pieza cable para disponer de evidencias para tomar las acciones, decisiones lo más pronto posible que ofrece la automatización de información, beneficios que son útiles para la salud pública. Los dispositivos electrónicos permiten un acceso, intercambio inmediato, muy ágil y coordinado de datos opta la priorización en la atención y respuesta, sobre todo aun la atención a las personas más vulnerables como las personas adultas mayores, personas con discapacidad y personas con desconocimientos tecnológicos. Los datos obtenidos por los miembros de salud y las autoridades en esta emergencia ha sido una pieza clave como evidencia de los actos realizados con los recursos económicos, físicos y materiales del gobierno.

En la pandemia de Covid-19, se ha generado mucha información que logra ser validada como evidencia en los Juicios, en vista que los dispositivos electrónicos están el alcance de la mano y estar conectados a una red es algo muy simple, la información es ahora digital y manipularla es cotidiano. El cierre de las infraestructuras de las unidades educativas, universidades y centros de educación, la educación se vio obligada a readaptarse en clases de formato online, esto ha provocado la generación de mucha información digital, dado que las tareas son en línea y para poder ser calificados o dar una ponderación al trabajo, el estudiante en este caso evidenciará la tarea al cargar a las diferentes plataformas por medio de una foto o por un medio digital.

Toda información generada por los medios electrónicos y telemáticos es de suma importancia puesto que el alcance y uso de estos es a nivel de toda la sociedad, generan evidencia en muchos

delitos muy grabes como pedofilia, pornografía infantil, suplantación de identidad, entre otros, esta información es muy vulnerable a la manipulación y volatilidad de la evidencia digital son muy vulnerables ante alteraciones por el receptor o por quien la dirige, pierden las garantías de originalidad de la evidencia, si bien el avance de la tecnología da una ayuda a solucionar muchos problemas, de igual forma va de la mano con muchas nuevas formas de delinquir, crea un mundo opaco y casi inexplorado, por estas razones los profesionales del derecho, inclusive los profesionales informáticos, se encuentran en problemas al momento que se presentan casos que ameritan su estudio y posterior sanción en el Ecuador.

Las pruebas que se presentan dentro de un proceso judicial son de mucha importancia, debido a que logra aportar elementos que constituyen evidencias para condenar o absolver a los sindicados en una causa; es por ello, que la cadena de custodia es vital importancia para garantizar su conservación y pureza.

Antecedentes teóricos prácticos

En Ecuador (Molina, Santillán, Luna, Lozada, Guaiña, 2019), en su trabajo de investigación "preservación digital y la admisibilidad de las evidencias" impulsan varios modelos para la conservación y la preservación digital, es considerados por las instituciones de investigación criminal, estos modelos fueron creados bajo las características enfocadas en el problema y a la necesidad del usuario.

PRECEDI es un modelo que garantiza la adecuada preservación de le evidencia dado que organiza una mayor admisibilidad de la evidencia digital que se preserva en un repositorio al cumplir los aspectos del modelo, los custodios y los técnicos, especialmente los fiscales y jueves otorgan una importancia alta a PRECEDI.

A nivel internacional (Valencia, Orozco, 2017) hace énfasis de la metodología ISO/IEC – 27000, basado en estándares internacionales con normas establecidas, modela la integración de las normas ISO/IEC 27001, 27002, 27005 y las normas que se desee adaptar bajo la necesidad del usuario. Esta metodología es utilizada para implementar el sistema de gestión de seguridad de la información (SGSI) aplicado a empresas grandes y pequeñas definir el nivel de aceptación de riesgos y la valoración de cada uno de estos.

Situación problemática

Se ha logrado evidenciar con mecanismos de observación directa que la cadena de custodia de los contenidos físicos o digitales de las instituciones de investigación criminal en la provincia de Chimborazo, no cuentan con las herramientas y técnicas necesarias para garantizar la admisibilidad de la evidencia digital.

Al saber que la evidencia digital podría ser vulnerada, alterada, modificada o a su vez destruida los actores principales de las instituciones de investigación criminal demuestran un desconocimiento de herramientas adecuadas y técnicas o metodologías eficientes para la admisibilidad de la evidencia digital.

Los gobiernos de turno han demostrado desinterés de aplicar recursos económicos, espacio físico, estructura o infraestructura de almacenamiento de datos para la evidencia digital.

Planteamiento del problema

¿Como se garantizará la admisibilidad de la evidencia digital en un proceso judicial?

Hipótesis de trabajo

Las técnicas de seguridad aplicadas en las redes de comunicaciones mejoran la custodia de la evidencia digital en la provincia de Chimborazo.

Objetivo general de la investigación

Establecer un conjunto de técnicas de seguridad aplicadas en las redes de comunicaciones que aseguren la adecuada custodia digital.

Objetivos específicos de la investigación

- Realizar un estudio de la situación actual de las investigaciones relacionadas con la aplicación de las técnicas de seguridad en redes de comunicaciones aplicadas a la adecuada custodia de evidencia digital.
- Realizar un estudio comparativo de las diferentes metodologías de seguridad aplicadas en las redes de comunicaciones para garantizar la adecuada custodia de evidencia digital.
- Proponer un conjunto de buenas prácticas con la aplicación de técnicas adecuadas sobre redes de comunicaciones para garantizar la custodia de la evidencia digital en la provincia de Chimborazo.

Metodología

Para poder alcanzar los objetivos planteados, se piensa realizar una planificación de procesos metodológicos basado en 4 etapas que son: Investigación del estado del arte, descripción de metodologías y técnicas de seguridad aplicadas en las redes de comunicaciones en la custodia digital, diagnóstico de las metodologías o técnicas utilizadas por los actores de justicia de la evidencia digital y la redacción de la síntesis de la síntesis de las buenas prácticas aplicadas en técnicas adecuadas sobre las redes de comunicaciones de la custodia de la evidencia digital, estas ayudaran al desarrollo de la investigación propuesta.

Justificación de la investigación

La necesidad de dar soluciones oportunas o construir con la calidad en el servicio para evitar insatisfacciones en el traslado de la evidencia digital, las instituciones de investigación criminal y sus actores principales están obligados a llevar modelos de gestión que permita mejorar los procesos, de allí nace la importancia de buenas prácticas para la seguridad en las redes de comunicaciones para la custodia de la evidencia digital.

La inasistencia o desconocimiento de una metodología o técnica adecuada en territorio para el manejo de la custodia de le evidencia digital, ha incidido directamente en la inseguridad que tiene los actores principales de la custodia de la evidencia digital, al no cumplir con los

parámetros necesarios de seguridad y provoca la incertidumbre y la calidad de la evidencia digital, esta es muy vulnerable a efectos del ciberdelincuente.

De este punto nace la importancia de crear una secuencia de buenas prácticas para la gestión de la preservación y admisibilidad de la evidencia digital, con ello las instituciones de investigación criminal y sus actores principales tendrán una herramienta para ejecutar de mejor forma la custodia de la evidencia digital.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1 La preservación digital

La preservación digital son procesos que da la garantía a los accesos futuros a los archivos y activos digitales o digitales, es un proceso de gestión de archivos digitales las cuales garantizan que se utilizará la información a largo plazo, incluso los formatos de la información y las tecnologías evolucionen con el tiempo. Digital Preservation (DP) por sus siglas en inglés, su objetivo principal es llevar ventaja a las debilidades del soporte físico de la vulnerabilidad y lo anticuado tecnológico, "la capacidad de asegurar que la información digital, se mantiene con las cualidades accesibles y suficientes de autenticidad, que interpretaran en el futuro con uso de una plataforma tecnológica diferente utilizado al momento de su creación" (Ferreira, 2006).

Los contenidos y objetos digitales llegan a ser extremadamente de poca duración de vida, se alcanza a contrarrestar da la atención adecuada para preservarlos en su entera integridad a largo plazo. La autenticidad y confianza en la gestión digital son muy importantes para la integridad digital, debido a que definen si de su origen los documentos digitales serán confiables tanto sea para su acceso como para su preservación a largo plazo (Corrado, 2019). La preservación digital no es algo nuevo, pero cada dia, se vuelve más importante a medida que se generan una gran cantidad de activos digitales y en una gran gama amplia de formatos de archivo a partir de diferentes fuentes de datos. En realidad, es posible que necesite conservar archivos de formato PDF, mensajes de redes sociales, correos electrónicos, grabaciones de voz, mensajes de texto o incluso de sitios web.

La preservación digital no consiste en simplemente realizar durante periodos establecidos las copias de seguridad de los archivos. Tener un buen plan de contingencia es importante, pero hablar de preservación no lo es en su totalidad. Las copias de seguridad no son suficientes para dar una preservación de datos a largo plazo y por lo general no normalizan un formato de archivo.

1.1.1. Análisis de proyectos y modelos de preservación digital

Los proyectos presentados a comprendido diversas áreas, desde la concientización de organismos creadores y preservadores de información a herramientas desarrolladas, además por comités expertos.

Según Molina, Santillán, Luna, Lozada & Guaiña (2019), impulsa varios modelos para la conservación y preservación digital. Estos modelos, se definen hacia un horizonte de preservación digital a largo plazo.

- Modelo de ciclo de vida de conservación. – Realiza una conceptualización de las actividades necesarias a la unidad de custodia.
- INTERPares. – Propuesto por (The International Research on Permanent Authentic Records in Electronic Systems, 2013), desarrolla el principal conocimiento para la preservación de los documentos digitales a largo plazo.
- PLANETS. – Por su sigla en inglés (Preservation and Long-term Access through Networked Services), trata de un proyecto que trata los retos planteados para la preservación digital.
- DAMM. - El objetivo, se guía en extraer las características de estos objetos para la validación hacia un futuro, es la capacidad para identificar los formatos de archivos en riesgo y en necesidad de atención.
- PREMIS. – Basado en el Matadata de OAIS, bajo la forma de un esquema de metadatos enfocados en estrategias de implementación de metadatos de la preservación en archivos digitales.
- NDSA. - Es un conjunto de directrices y prácticas escalonadas con el objetivo de ofrecer, varias instrucciones muy referentes en la preservación de los contenidos digitales en cuarto nivel progresivos a través de las cinco áreas funcionales diferentes. (National Digital Stewardship Alliance, 2015).
- OAIS. – El modelo OAIS, ISO 14721:2003, presenta un modelo de referencia utilizado para la conservación y preservación de archivos digitales.
- PREDECI. – Propone un marco para la comprensión y la mayor conciencia de conceptos inexcusables para la preservación de la evidencia digital para un largo plazo, este modelo aborda funciones de preservación del modelo OAIS incluyen muchos aspectos importantes en el entorno de instituciones de investigación criminal, conserva la

estructura global como la ingesta, administración de la preservación, almacenamiento, administración de datos, plan de preservación y acceso.

Los custodios y los técnicos, especialmente los fiscales y jueces otorgan una importancia alta a PREDECI por sus procesos que garantizan la adecuada preservación de la evidencia pues organiza una mayor admisibilidad de la evidencia digital que se preserva en un repositorio cumplen con todos los aspectos del modelo PREDECI.

Molina, Santillán, Luna, Lozada, & Guaiña (2019) concluyen que el modelo PREDECI tiene algunos de los aspectos no considerados como: - legalidad de la evidencia, - confidencialidad, - control de calidad ingesta, - ingesta parcial, - metadatos de entorno, -transmisión, - museo de herramientas, - garantía de integridad de evidencia originales, - almacenamiento distribuido, - terminología, - certificación de la estrategia, y - aspectos de trazabilidad y continuidad de la preservación; organizadas en cuatro dimensiones los cuales permiten en una forma conjunta mejorar la admisibilidad de la evidencia digital en la corte a largo plazo.

1.1.2. Modelo PREDECI

Es un modelo de referencia con la responsabilidad de custodiar las pruebas a largo plazo para sumar la aceptabilidad de las pruebas digitales en los tribunales, este modelo, también, da las garantías, la fidelidad y la integridad a un largo plazo y responde a un conjunto de responsabilidades especificadas en leyes, regulaciones bajo en el entorno de OAIS.

A continuación, se muestra una clara explicación de la guía, normas y marcos del modelo PRECEDI, en la figura 1.

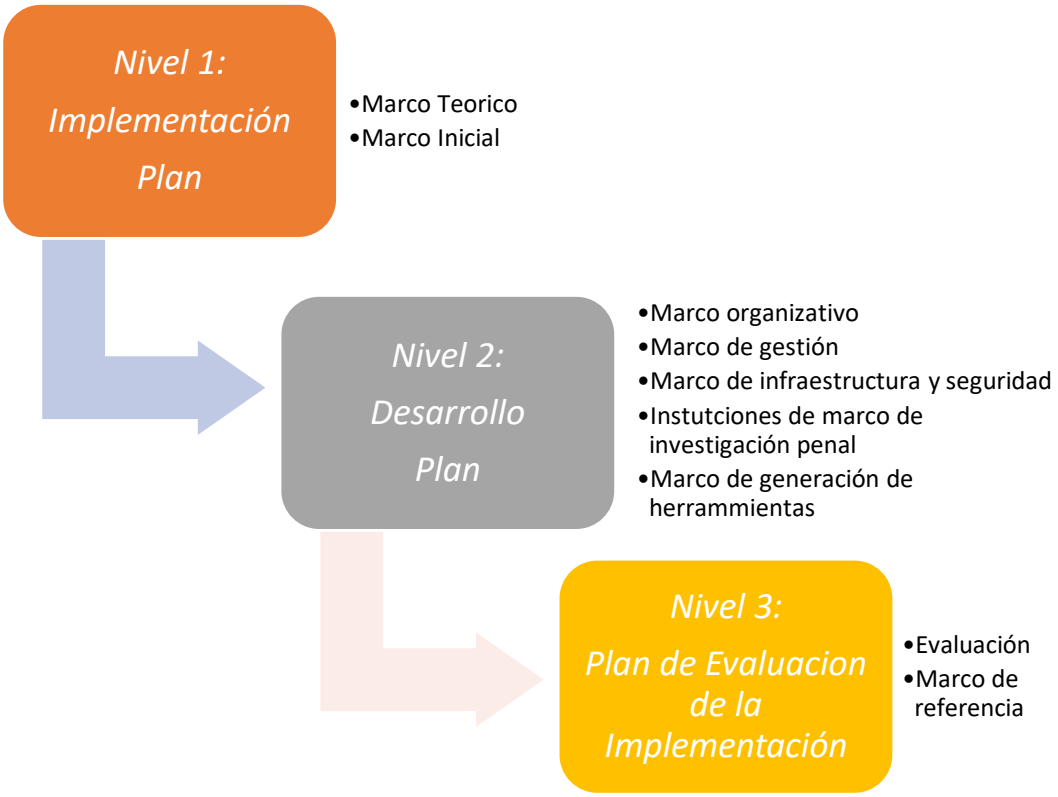

Figura 1. Guía de implementación del modelo PRECEDI
Fuente: Molina Granja, et al 2019

Este modelo PREDECI, conlleva una responsabilidad de proteger las pruebas o evidencias digitales a largo plazo y aumentar la aceptabilidad de estas en los tribunales o la admisibilidad de pruebas a una comunidad. Este modelo PRECEDI, también logra garantizar la fidelidad e integridad a largo plazo y contesta a un conjunto de responsabilidades especificas ante las leyes y regulaciones para este entorno bajo el modelo de preservación OAIS (CCSDS, 2012) y conceptos de los metadatos.

1.1.3. Catálogo de criterios NESTOR para los repositorios digitales

Los recursos digitales con la red de almacenamiento de información digital a largo plazo han emprendido esfuerzos para implementar un catálogo de criterios para repositorios digitales que brinde confianza. Tiene la visión de introducir criterios establecidos para la evaluar los repositorios digitales a largo plazo, cada uno de estos criterios enriquece con explicaciones y

ejemplos detallados precisos y se agrupan en secciones como: organización marco, objeto de gestión e infraestructura y seguridad, integridad de la información (NESTOR, 2006).

NESTOR es compilado para su aplicación principalmente, pero, también se discute y da estándares al contexto internacional. Es importante identificar los criterios validos entre condiciones características nacionales, se ubican en más áreas dentro del marco legal, la provisión de instituciones públicas con recursos financieros y humanos, estructura organizativa nacional y el estado de desarrollo nacional en el campo de la preservación digital a largo plazo.

1.1.3.1. Dimensiones del catálogo NESTOR

Al concluir la evaluación de los repositorios y la certificación, es detallado los parámetros de un repositorio apropiado para un modelo de preservación digital, en conjunto con las aportaciones de los grupos de trabajo, autores de Catálogo de Criterios para Repositorios Digitales Confiables las cuales establecieron condiciones y dimensiones para crear repositorios y archivos digitales seguros, auditables (NESTOR, 2006).

1.1.3.1.1. Marco organizacional

En la figura 2, se observa un resumen del marco organizacional de los criterios de NESTOR.

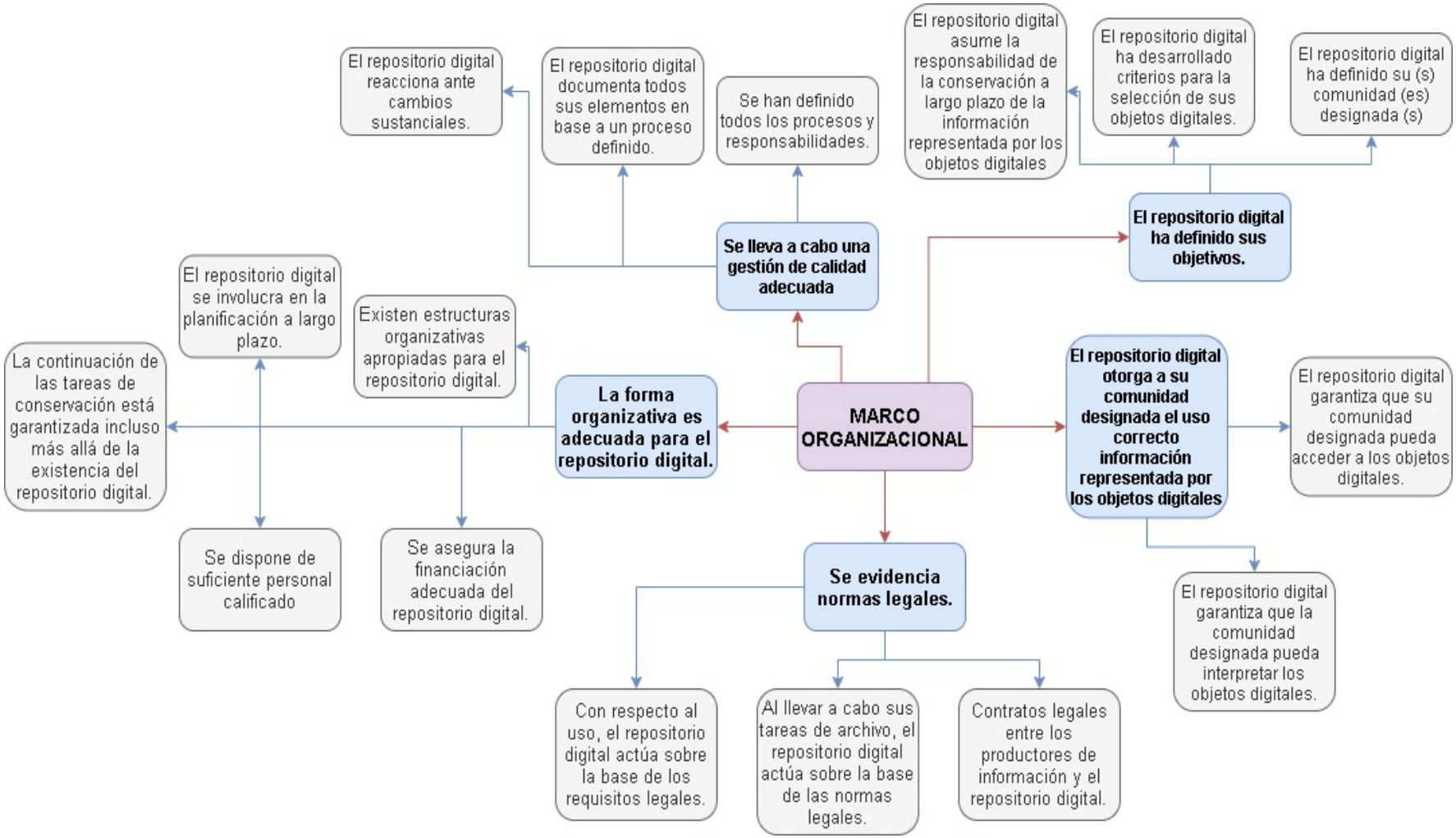

Figura 2. Detalle del marco organizacional.
Fuente: Elaboración propia, 2020

1.1.3.1.2. Gestión de objetos

En las figuras 3 y 4, se observa la gestión de objetos de los criterios de NESTOR.

Figura 3. Detalle de objetos de NESTOR, (1)
Fuente: Elaboración propia, 2020.

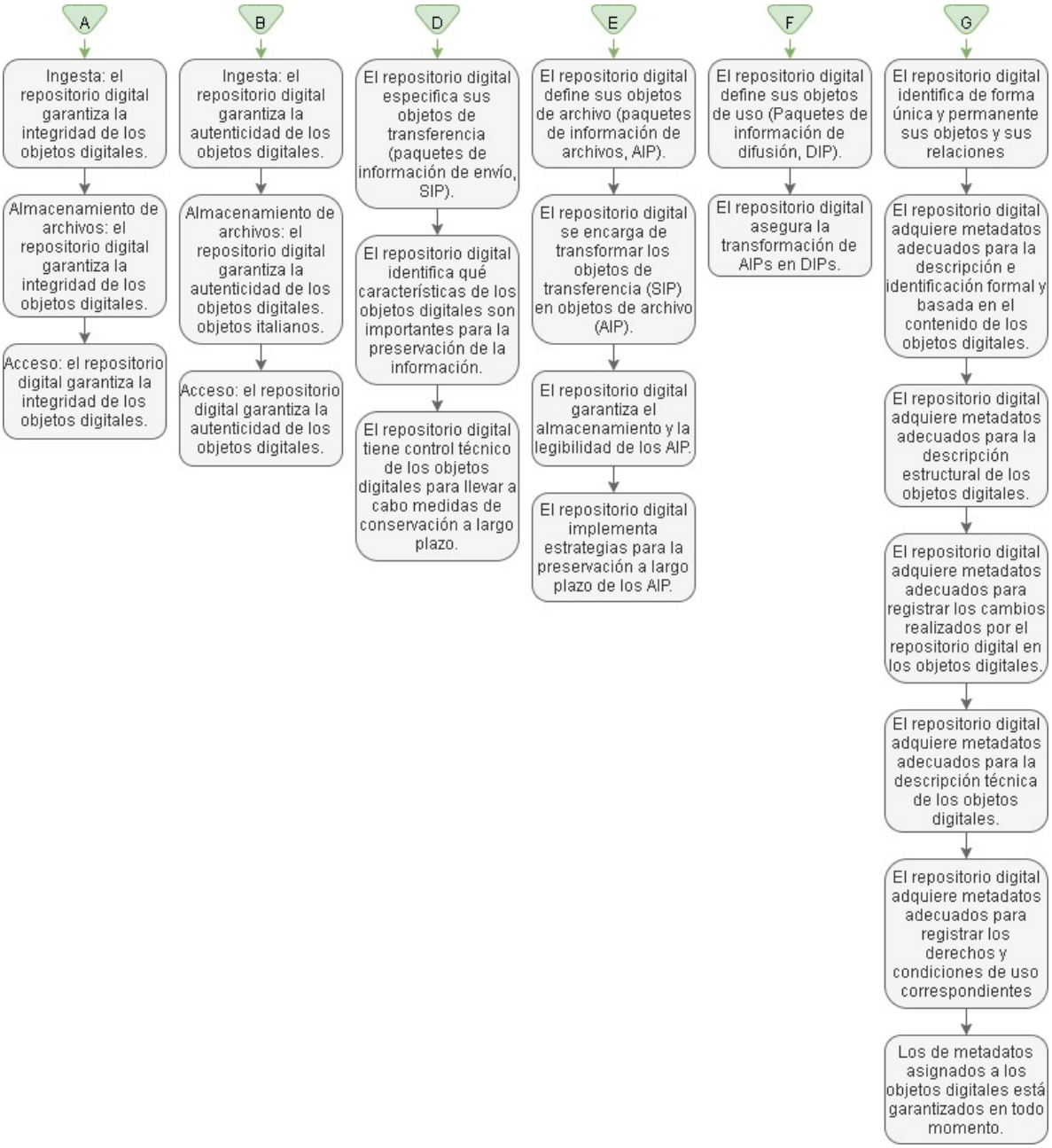

Figura 4. Detalle de gestión de objetos, (2)
Fuente: Elaboración propia, 2020.

1.1.3.1.3. Infraestructura y seguridad

En la figura 5, se observa la gestión de objetos de los criterios de NESTOR.

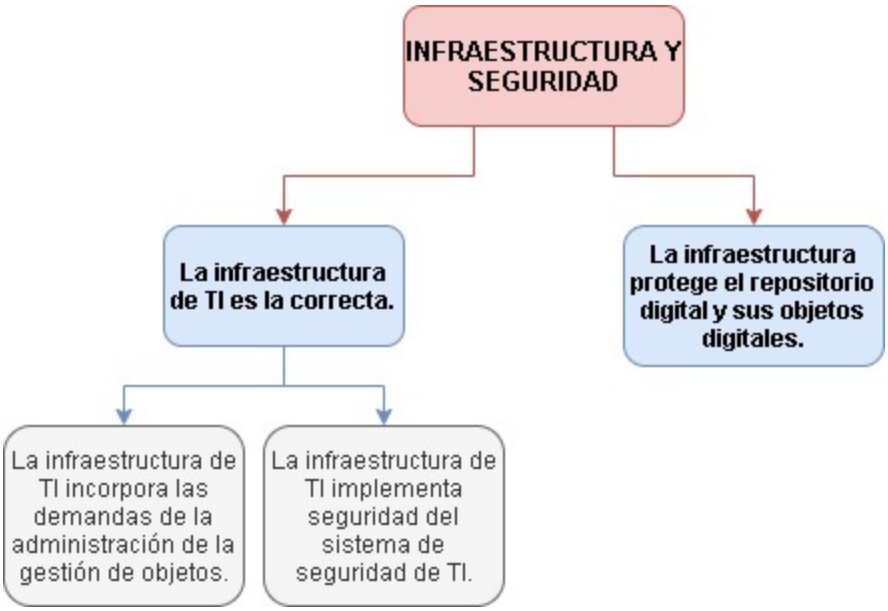

Figura 5. Detalle de infraestructura y seguridad
Fuente: Elaboración propia, 2020.

1.1.3.1.4. Integridad de información

En la figura 6, se observa la gestión de objetos de los criterios de NESTOR.

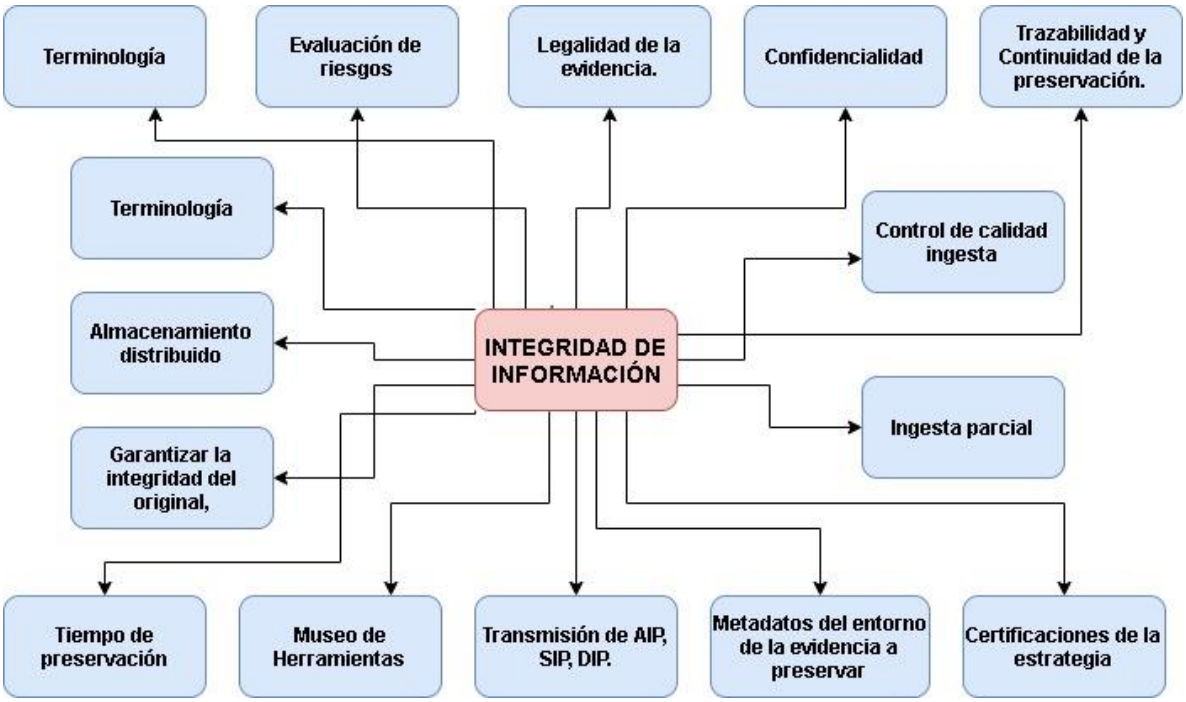

Figura 6. Detalle de integridad de información
Fuente: Elaboración propia, 2020.

Existen diferentes modelos de repositorios, la cuales cumplirán varios requisitos para garantizar los resultados de su funcionalidad a largo tiempo, los estándares muy comunes son:

- TRAC
- DRAMBORA
- NESTOR

Según Ausay, Valle (2019) aseguran que el método más optimo entre las 3 analizados es el método NESTOR debido que cumple con todas las condiciones necesarias para garantizar los resultados de funcionalidad que necesita el usuario a largo tiempo obtiene como resultado de 100% de cumplimento, como se muestra en la tabla 1.

Tabla 1. Porcentaje de cumplimiento de requisitos básicos

	DRAMBORA	TRAC	NESTOR
Condiciones	90%	95%	100%

Autor: Ausay, Valle, 2019.

1.2 Preservación digital en el área judicial

1.2.1. Evidencia digital

Según Amato, Cozzolino, Moscato & Moscato, (2019) la evidencia digital es el elemento principal de cualquier proceso forense. Los datos son hechos elementales, información codificada que necesita una interpretación para adquirir significado y aportar conocimiento. Los datos digitales son una representación en un sistema binario de secuencias de bits no es inmediatamente comprensible para los humanos, por lo que requiere una serie de operaciones a través de las cuales, se realiza una transformación que conducirán a resultados diferentes (mostrados en el monitor en texto representación o como un video, sino, también como una imagen impresa en un trozo de papel).

Señala que, por su naturaleza, los datos digitales son:

- Inmaterial, por lo que necesita un soporte adecuado para contener como CD-ROM, disco duro, memorias USB;
- Volátil, porque se logra dispersar con bastante facilidad;
- Alterable, modificable incluso de manera anónima y / o involuntaria;
- Reproducible en un número potencialmente infinito de copias.

Si supervive una evidencia digital Estupiñan, Mora, Santiago (2019) indica que:

> "La evidencia digital se presenta en diferentes formas y es recopilada de acuerdo con su tipo: volátil, persistente, lógica y física. En el caso de la evidencia volátil y persistente, se realiza directamente sobre la memoria del equipo, pues a diferencia de tipo lógico y físico no implica" (p, 15).

Acurio (2016) presenta la necesidad de la evidencia digital en el COIP y en COGEP que, a continuación, se detalla:

– COIP. - Materias Penales: Comprobar la existencia material de la infracción y la responsabilidad penal de la persona procesada. Generar convicción en el juzgador más allá de toda duda razonable.

- COGEP. - Materias no Penales: A la hora de sustanciar ante cualquier Tribunal de Justicia una cuestión litigiosa hay que tener presente que para que las pretensiones de las partes prosperen no basta con relatar los hechos sucedidos, sino que, también hay que desplegar la actividad probatoria necesaria que acredite probatoria necesaria que acredite la veracidad del relato que se expone (Art. 162, COGEP).

Acurio (2016) indica que existen dos artículos como normas legales de la ley de Comercio Electrónico y Firmas electrónicas del Ecuador, la cual, se detalla:

- Artículo 2, Articulo Jurídico de los Mensajes de Datos. - Los mensajes de datos tendrá igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos, se someterá al cumplimiento de los establecido en esta Ley y su Reglamento.
- Artículo 52, Medios de prueba. - Los mensajes de datos, firmas electrónicas, documentos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación serán considerados medios de prueba. Para su valoración y efecto legales, se observará lo dispuesto en el Código de Procedimiento Civil.

Los mensajes de datos es aquella información generada por medios electrónicos, digitales o similares que son almacenados o intercambiadas por diferentes medios como ejemplo los documentos electrónicos, páginas web, correos electrónicos, telegrama, fax, facsímil e intercambio electrónico de datos.

La Ley de Comercio Electrónico ARCOTEL (2002), se pronuncia que los mensajes de datos "tienen el mismo valor que los documentos escritos en virtud del principio de equivalencia funciona", los mensajes de datos son medios de prueba "el medio probatorio es el camino que designa la ley para ingresar el objeto de prueba al proceso" (p, 8).

Acurio (2016) menciona algunas normas legales las cuales, se van a citar las más importantes para el proceso de entendimiento en la investigación.

- Artículo 147, Validez y eficacia de los documentos electrónicos. - Tendrán la validez y eficacia de un documento físico original, los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos, satelitales o producidos por

nuevas tecnologías, destinadas a la tramitación judicial. Ya sea que contengan actos o resoluciones judiciales. Igualmente, los reconocimientos de firmas en documentos o la identificación de nombre de usuario, contraseñas, claves, utilizados para acceder a redes informáticas. Todo, lo cual, siempre que cumplan con los procedimientos establecidos en las leyes de la materia.

- Código Orgánico Integral Penal, articulo 499.- La prueba documental, se regirá por las siguientes reglas, podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este código.
- Código Orgánico General de Procesos, articulo 196.- producción de las pruebas documentales en audiencia para la producción de la prueba documental en ausencia de juicio, se procederá da siguiente manera: las fotografías, grabaciones, los elementos de prueba audiovisuales, computacionales o cualquier otro de carácter electrónico apto para producir fe, se producirán, también en su parte pertinente en la audiencia y por cualquier medio idóneo para su percepción pro los asistentes.

Bajo las normas legales de COGEP Acurio (2016) sita el artículo 202, documentos digitales producidos electrónicamente con sus respectivos anexos, serna considerados originales para los afectos legales.

- Las reproducciones digitalizadas o escaneadas de documentos públicos o privados que se agreguen al expediente electrónico tienen la misma fuerza probatoria del original.
- Los documentos originales escaneados, serán conservados por la o el titular y presentados en la audiencia de juicio o si la o el juzgador lo solicite.
- Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este código.

Articulo 500 COIP. –

> "El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí." (p,12).

1.2.2. Custodia de la evidencia digital

La Cadena de Custodia (CdC) un concepto ligado ampliamente al ámbito legal y judicial, se le da ese concepto a la recopilación de evidencias de cualquier tipo. Para entender cuál es su verdadera importancia realizaremos un ejemplo muy claro para que el entendimiento sea mejor: un caso de corrupción, si la policía y los investigadores allanan la vivienda del sospechoso bajo la orden del Juez, encuentran una gran cantidad de documentos referente a contratos inflados económicamente para estafar a la Administración Pública, por, lo cual, el sospechoso tiene muchas pruebas en a favor de ser culpable. Ahora el encargado de custodiar esas evidencias es un amigo íntimo del sospechoso y que no se lleva ningún control de trazabilidad sobre la custodia, si las pruebas llegan al Juez, toda esta documentación que antes eran la prueba de un delito ahora es completamente normal y responden a la más absoluta legalidad, por lo tanto, el Juez no tiene más que desestimar la acusación. Con este claro ejemplo para evitar que estas situaciones se produzcan en la realidad, existe el concepto de Cadena de Custodia (Perona, 2016).

La CdC, tiene establecido una serie de mecanismos y procedimientos que dan la seguridad de los elementos probatorios (evidencia, indicios o pruebas) no hayan sufrido alguna alteración, contaminación o a su vez destruido, desde que se realizó su recolección, custodia hasta el momento donde, se presenta como una evidencia ante las autoridades jugadoras. Estos procesos controlan donde y como se ha obtenido la evidencia, como y cuando se ha manejado la evidencia, quienes tienen el acceso a ella, donde se encuentra y quien la tiene, y si es el caso de destrucción, cuando, donde, quien y porque se ha destruido. Todos estos procedimientos tienen un absoluto control rigorosos, de manera que no dará una duda ni por un instante de la validez de la prueba (Perona, 2016).

Bórquez (2011) comprende que la evidencia digital conlleva ciertas peculiaridades con respecto a otros tipos de evidencias, si la información, se consigue presentar como medio de prueba, se logra encontrar en diferentes estados como:

- Almacenada estáticamente.
- Almacenada dinámicamente o en procesamiento.
- En tránsito o desplazamiento.

Si, se habla de CdC, se habla de la preservación de la evidencia material incautada que es relacionada con un delito, pero en la informática ese control material de las pruebas carece de sentido si se habla de las memorias RAM, esa información a veces logra ser muy relevante para resolver una investigación (procesos en ejecución, credenciales de usuarios, etc.), pero esta información se pierde al momento en que este dispositivo donde trabaja la memoria RAM deje de percibir corriente eléctrica. Con ese pequeño ejemplo, se manifiesta que si se habla de CdC no podemos relacionar solo a pruebas o evidencias materiales, al contrario, hay q hablar, también sobre los datos de dispositivos volíteles y que se generan sobre el terreno. Si hablamos de evidencia digital es necesario realizar una copia de dicha información del dispositivo volátil a uno no volátil, este dispositivo generado "in situ" y al ser tratada como tal y aplicar los procedimientos de CdC y dar las garantías de su validez legal (Bórquez, 2011).

En este sentido, podemos mencionar que la CdC en el ámbito de la informática, es un proceso de protocolos de actuaciones relativas a la seguridad y manipulación que se sigue durante el período de vida de una prueba digital, desde que ésta se genera, hasta que se destruye o deja de ser útil o necesaria (Bórquez, 2011).

La norma ISO/IEC 27037:2012 *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, facilita una guía para llevar una actuación pericial en el escenario donde la evidencia es recogida, identificación y secuestro de la evidencia digital. Esta norma viene a sustituir a las antiguas directrices como la RFC 3227, norma más dirigida a dispositivos actuales y más acorde con el estado de la técnica actual (Roatta, Casco, Fogliato, 2017).

Acurio (2016) pronuncia que la custodia luego de recuperar la información y preservar la integridad del contenido digital esta situación planteada por el COIP (código Orgánico Integral Penal) comete un error debido a que "no se logra probar la integridad del contenido digital por medio de cadena de custodia, a causa de que esta sobre los elementos físicos, basados en el principio criminalístico de mismisidad"

El artículo 456 "se aplicará la cadena de custodia a los elementos físicos y al contenido digital" para garantizar la integridad de la evidencia digital esta será a través de un código de integridad

o función HASH, así como lo dispone el artículo 7 del reglamento de la Ley de Comercio Electrónico y Mensaje de Datos (Acurio, 2016).

Según Aishwarya Lakshmi, Honnavali, Rajashree, (2020) la propiedad crucial de una función hash es la resistencia a colisiones, la resistencia a la colisión es propiedad de la función hash criptográfica de modo que encuentra un código inquebrantable de seguridad y así que es impracticable encontrar una entrada que tenga la misma salida. El diseño estándar más común de la función hash, se basa en la construcción Merkel - Damograd, un documento MD5 y SHA1 verifican los valores de un archivo de imagen. Aunque se ha cuestionado el uso de MD5 y SHA1 en función del grado de colisión de resistencia, la posibilidad de que ocurran colisiones hash al azar es improbable debido a el número significativamente grande involucrado, MD5 es un algoritmo hash criptográfico que produce un valor hash de 128 bits para cualquier entrada de longitud arbitraria. SHA1, bajo la familia de SHA160.

1.2.3. Legislación internacional

En lo internacional, los países que cuentan con una legislación apropiada sobre delitos informáticos y preservación de la evidencia, el artículo 9 de la ley de modelo sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) por sus siglas en inglés dice: “Al valorar la fuerza probatoria de un mensaje de datos se habrá de detener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en que la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente” (UNCITRAL, 1966).

En Ecuador, la ley del sistema Nacional de Archivos, se pronuncia que “Es obligación del Estado velar por la conversación de las fuentes históricas y sociológicas del país, así como modernizar y tecnificar la organización y administración de los archivos…”. “Constituye Patrimonio del Estado, la documentación básica que actualmente existe o que en adelante, se produjere en los archivos de todas las instituciones de los sectores públicos y privados, así como la de personas particulares” (Juillard, 2009).

El artículo 456 del (COIP) señala que: “Se aplicará cadena de custodia a los contenidos 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” (Asamblea Nacional del Ecuador, 2014).

1.2.4. La Preservación digital en Chimborazo

En la realidad, toda institución pública o privada genera a cada minuto información digital que bajo a un mandato legal, por responsabilidad social y valor cultural e histórico, se preservarían a largo plazo mediante técnicas o métodos acertados que permitan disponer de una forma técnica a la información digital en un futuro próximo o lejano. En el Ecuador existe un fundamento jurídico que motiva y exige que se dé cumplimento a estas responsabilidades de igual forma con distintos modelos de preservación digital que podrían ser aplicadas (Molina-Granja, 2018).

Las entidades o instituciones del sector privado o público requieren de la preservación de información digital como hospitales, bibliotecas, museos, fiscalías, instituciones de investigación, instituciones de investigaciones penales, instituciones de educación o cualquier entidad que tenga responsabilidad u obligación legal de salvaguardar los datos o información digital generalmente utilizan repositorios digitales (Molina-Granja, 2018).

Bajo la normativa ecuatoriana en la ley de conservación de archivos en los artículos 1 y 2 menciona “la documentación básica que existe actualmente o que se produce en los archivos de todas las instituciones del sector público y privado, así como la de los particulares, se constituirá mediante los siguientes instrumentos:: a) Escritos a mano, tipográficos o impresos, y sean originales o copias; b) Mapas, planos, bocetos y dibujos; c) Reproducciones fotográficas y cinematográficas, y sean negativos, placas, películas y clichés; d) Material sonoro, contenido en cualquier forma; e) Material cibernético y, f) Otros materiales no especificados” (Molina-Granja, 2018).

En la actualidad, la migración de formatos antiguos a formatos actuales, le emulación a través de software actual a software antiguo, metadatos y el más simple la replicación o copia de la información, se ha dado en el transcurso del tiempo, pero ninguno de ellos se sobrepuesto

encima de otros, visto que la conservación digital es un campo aun en desarrollo y no todas las entidades tiene las mismas características y necesidades (Molina-Granja, 2018).

Las instituciones bajo en cualquier ámbito laboral actualmente realizan propuestas de preservación digital utiliza grandes sistemas y costosos, la mayor parte de ellos aplican el modelo OAIS (open archival information system) para la preservación de su información digitales. El modelo actual de referencia de OAIS y PREDECI es adaptable a cualquier institución, pero desde una visión científica propia de la comunidad han planteado la necesidad de documentación complementaria para pequeñas instituciones bajo el nombre de OAIS-LIFE (Molina-Granja, 2018).

Molina-Granja (2018) indica en su investigación que, en la provincia de Chimborazo, se determinó que 63 instituciones fueron analizadas en términos de preservación digital, por lo tanto, el 67% son del sector público y el 22% son del sector privado, bajo el análisis e interpretación indica que el 11% de las instituciones que fueron evaluadas tienen algún método formal de preservación digital aplicada, y el 89% de las demás instituciones almacenan información digital, gráfico 1.

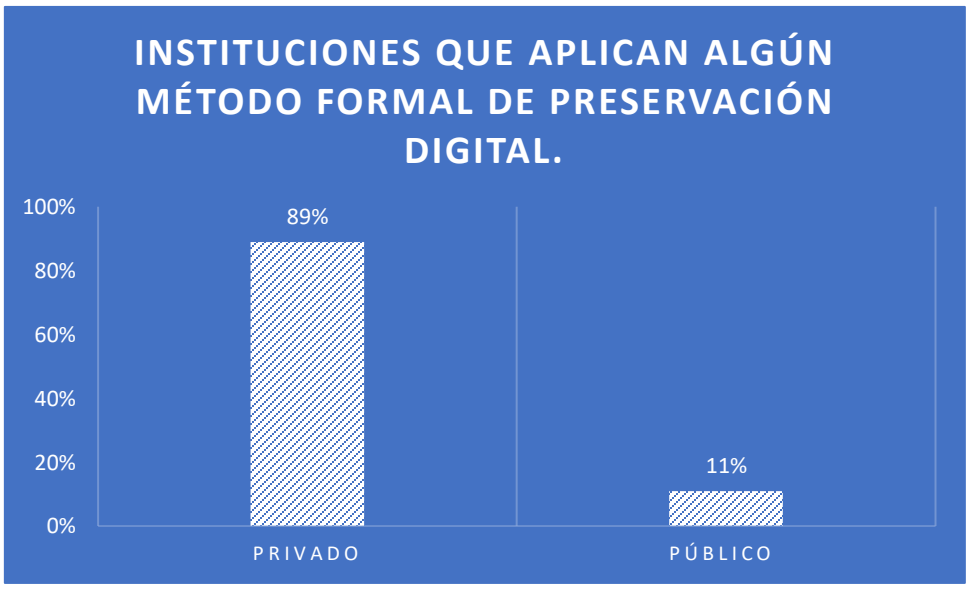

Gráfico 1. Valoración institucional por aspectos evaluados
Fuente: Molina-Granja, 2019.

La preservación digital es un requisito legal en el Ecuador, lo que indica que es responsabilidad de hacer cumplir a nivel público, privado, personal e institucional independientemente el tipo de negocio o actividad que realiza. En el Ecuador la preservación digital de conservarse durante 5 años para algunas acciones legales o patrimoniales y sin límite para todos.

1.3 Admisibilidad

La admisibilidad de evidencia digital ha dado que la ciencia forense considere un elemento importante en el fracaso del enjuiciamiento exitoso de los delitos informáticos. Logra identificar el derecho consuetudinario relacionado con pruebas obtenidas indebidamente y su admisibilidad, la búsqueda de las verdaderas razones de tales fallas reveló que la pugna entre el derecho individual a la privacidad y el acceso investigativo a información digital, jurisdicción, estandarización de métodos, reproducibilidad, confiabilidad de los hallazgos de investigadores forenses y la falta de conciencia entre los técnicos forenses de su lugar y responsabilidades en el sistema de justicia penal tienen funciones importantes entrelazadas (Mison, Davies, Eden, 2020).

Todo modelo digital es capaz de generar información que personal o institucional logra convertirse en evidencia, para que esta información se convierta en evidencia, se aplica adecuadamente los procesos de información forense, esto permite recuperar, analizar, preservar datos que han sido procesos electrónicamente y almacenados en un sistema informático.

Existe una ineficacia jurídica que afectan los aspectos procesales, la cual, se denomina la inadmisibilidad, en otras palabras, es un acto concreto indirectamente, ha despertado cierto interés de parte de las autoridades competentes del país.

Según Gopalakrishnan, Vineti, Mohan, Sethumadhavan, (2018) indica que “La relevancia y la admisibilidad son dos aspectos cruciales que se consideran a la hora de recopilar y analizar pruebas digitales. Ambos aspectos, se cumplirán para tener pruebas contundentes ante el tribunal” (p, 3).

- Relevante: si prueba o refuta hechos en un caso.
- Admisible: Si cumple con todos los requisitos reglamentarios y legales y su adquisición, se adhiere a las mejores prácticas de la ciencia forense digital.

1.3.1. Características de la admisibilidad y la inadmisibilidad

Según Carrasco (2017) indica que:

> "El estudio de la inadmisibilidad de un acto no ha sido enfocado desde el punto de vista de los actos jurídicos procesales a los cuales le es aplicable, pues, se suele aludir a ella sin distinguir el agente generador del acto procesal (actos del órgano jurisdiccional, partes, terceros, auxiliares de la administración de justicia, etc.)" (p,21).

Por otra parte, no solo la inadmisibilidad es aplicada en procedimientos de naturaleza civil, sino que se utiliza para la mayoría de los procedimientos (civil, penal, laboral, familiar, constitucional, administrativo, policial, consumo y entre otros), en secuencia, se trata de una forma de invalidez jurídica trascedente cuyo estudio da el resultado útil para la comunidad jurídica.

El diccionario de la lengua Española de la Real Academia Española contiene dos conceptos para la palabra "admisión": "1. f. Acción y efecto de admitir. 2. f. Der. Trámite en que, atiende aspectos formales, se decide si una demanda, recurso o petición serán tomados en consideración para resolver el fondo". Admitir, se define como "aceptar, permitir". Admisibilidad significa, según el mencionado diccionario, como "cualidad de admisible". En similar sentido la explica Couture al definirla como "acción y efecto de dar entrada, normalmente por parte del juez, a una defensa, petición o documento, debido a su procedencia formal o sustancial"

Características para el cumplimiento de la admisibilidad de la evidencia, según Acurio (2017) recomienda que para tener un cumplimiento de la admisibilidad, se cumplirán los siguientes parámetros:

- Estándares de un Proceso de Operaciones
- Cumplimiento de principios básicos
- Cumplir los principios constitucionales y legales (Teoría de Árbol Envenenado, Secreto a la correspondencia y las comunicaciones)
- Seguir el trámite legal.

Para esto es necesario probar dos situaciones:

- Establecer que el mensaje de datos usado como evidencia digital fue localizado y recuperado del equipo informático del sospechoso y de ningún otro equipo informático perteneciente a alguien más.
- Comprobar que el mensaje de datos usado como evidencia fue creado u originado en el equipo perteneciente al sospechoso más allá de cualquier duda de que dicho mensaje fue puesto o creado ahí por el equipo informático del investigador.

De acuerdo con Carrasco (2017) las características de la inadmisibilidad expresan que la inadmisión de un determinado acto procesal impide que este se despliegue o genere los efectos dispuestos por la ley, en tal sentido, la inadmisibilidad constituye un acto de sanción de invalidez que genera en un juicio de calificación de regularidad o validez inicial de actos que tienen origen en las partes o terceros técnicos que, en un caso de actuar, obstará a que se den efectos propios del acto.

1.3.2. Como se logra la admisibilidad.

Para generar procesos de admisibilidad en la actualidad y no a largo plazo, Kebande, Baror, Parizi, Raymond, Venter (2020) menciona que "La admisibilidad, se logra con la aplicación de los códigos de integridad (Valor HASH) y su comparación", "¨ Es un error verificar la admisibilidad de la evidencia digital (mensajes de Datos) a través de la cadena de custodia." Da como soluciones simples.

Lazareva, Kakhkhorov, Shinkaruk, (2020) llegan a la conclusión sobre la inevitabilidad de introducir nuevas tecnologías digitales en los procesos penales. La información digital almacenado en datos electrónicos ocupa un lugar cada vez más significativo en la estructura de las pruebas procesales penales, la gestión de documentos electrónicos alcanza a cambiar la idea de la esencia de la evidencia, el procedimiento de recolección de evidencia y el concepto de acción investigadora. El resultado es que el concepto de formación de evidencia, finalmente, ha perdido su viabilidad científica. Como resultado de esta investigación, los autores, también mencionan el desarrollo del concepto de evidencia, de formalización del proceso de recolección de evidencia, cambio de opinión sobre la admisibilidad de las pruebas en los procesos penales.

1.3.3. La calificación de la admisibilidad - inadmisibilidad

La admisibilidad de un acto de parte o de terceros en el ámbito técnico esta realizada si quieren ejercer un derecho determinado de incorporar al proceso un determinado acto procesal, al presentar un escrito en los sistemas imbuidos en el acto inspirado en la oralidad, el juez considera calificarlo como admisible o no.

El acto procesal que crean las partes o terceros técnicos no se despliega los efectos por el hecho un propuesto, estos efectos inician en la declaración de la admisibilidad de acto que está contenida implícitamente en una resolución judicial, la inadmisibilidad se trata de una calificación jurídica del acto procesal de partes o de terceros técnicos tan pronto como realizan o incorporan al proceso escrito u oral, en otras palabras, antes que los actos produzcan efectos (Carrasco, 2017).

1.3.4. Modelo para evaluar la admisibilidad de la evidencia

Según Antwi-Boasiako, Venter (2017) analiza un modelo armonizado propuesto para dar una evaluación de la admisibilidad de la evidencia digital y su aplicación en procedimientos judiciales, Desarrolla el modelo conceptual que se muestra en la Figura 6, la cual, proporciona un marco establecido de dependencias y relaciones entre los diversos requisitos y consideraciones de evaluación.

Este modelo conceptual encapsula tres niveles de armonización, denominadas fases, que se integran en el modelo armonizado propuesto para la evaluación de la admisibilidad de la evidencia digital. Las tres fases están integradas, pero difieren entre sí en términos de su relevancia funcional para evaluación de la admisibilidad de la evidencia digital, véase en la figura 7.

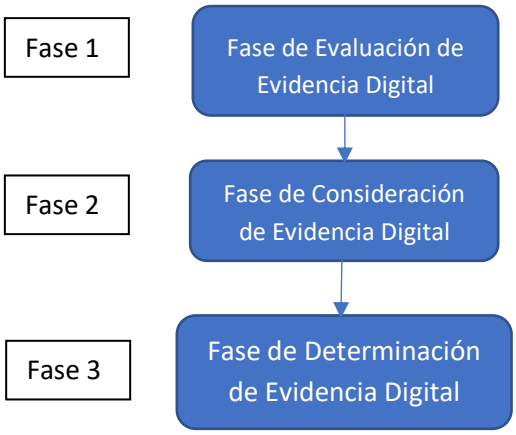

Figura 7. esquema de modelo de evaluación de la admisibilidad de las pruebas digitales
Autor: Antwi-Boasiako, A., & Venter, H. (2017)

Con el avance del tiempo, se esperan avances en informática y en las tecnologías de la información para poder dar un impacto significativo a los requisitos técnicos y legales que proporcionan a la base para la admisibilidad de la evidencia digital. El modelo armonizado propuesto para la evaluación de la admisibilidad de la evidencia digital ha sido creado para asegurar los futuros desarrollos tecnológicos en los campos que están integrados en el proceso forense digital. Como tal, la propuesta del modelo contribuye a los esfuerzos continuos en la estandarización de la ciencia forense digital a cargo de la academia, la industria y las entidades de justicia. Según (Antwi-Boasiako & Venter, 2017).

1.4 Seguridad

1.4.1. Seguridad de la información

La información, se considera actualmente como un activo crítico para la sociedad y las organizaciones, las instituciones educativas de nivel superior no han logrado operar sin información, sin embargo, con el rápido desarrollo de las tecnologías surgen una cantidad de amenazas que ponen bajo riesgo la seguridad de la información. Un extenso nivel de amenazas se encuentra en la plataforma de Internet, que es una ventana informática abierta para los ciber atacantes que utilizan métodos más intrusivos para vulnerar la Seguridad informática (SI). Se

ha generado cuantiosas sumas de dinero para controlar los peligros, pro estas acciones no son las suficientes y suelen sucumbir debido al factor humano, es por eso, que es muy necesario de disponer de mejores herramientas para combatir estas amenazas.

Estupiñan Londoño, Mora Merchán, Santiago (2019) menciona la importancia del monitoreo de red que es muy útil para encontrar fallas en la seguridad de la red, detectar intrusos, capturar paquetes para posteriormente analizarlos y descubrir la posible ruta de acceso y huida de quien realizó las modificaciones en el sistema, la herramienta Wireshark es una herramienta útil para realizar las capturas de paquetes y presenta una ventaja, es multiplataforma lo que hace mucho más fácil el uso de la misma herramienta en los distintos sistemas operativos. La información que pasa en la red es volátil por eso es pertinente encontrar maneras para controlar o reaccionar frente a un incidente y una de las maneras más eficientes es realizar un monitoreo y un análisis de la red, para esto, se cuenta con las herramientas necesarias y las políticas pertinentes para generar una buena infraestructura y así, en el caso de requerirse, lograr generar una evidencia digital que sea admisible ante la corte.

1.4.2. Modelos y técnicas de seguridad de la información

Se ha encontrado muchas técnicas de seguridad de información, la cual, serán referentes para el estudio de esta investigación, son de diferentes actores las cuales sus ideas que presentan sobre seguridad son amigables bajos muchos ámbitos, la cual se describen, a continuación.

- Técnica de ingeniera social

Yupanqui, Oré, (2017) identifican que esta técnica es realizada por los hackers educados, que realizan sus explotaciones bajo tres elementos importantes: 1) Factor humano, 2) aspectos organizativos, 3) controles tecnológicos. Las dimensiones tecnológicas normalmente son software anti pishing, filtros spam, cortafuegos, etc. La dimensión humana es necesario una conciencia y educación muy eficaces para ayudar a fortalecer el "firewall humano" seria idealmente cultivar una cultura de comportamiento de seguridad de la información. En otro lado, realizar medidas organizativas solidas como políticas y procedimientos internos da una base más en la seguridad de la información.

- Metodología ADM-TOGAF

Jaramillo, Cabrera, Abad, Torres & Verdúm (2015) indican el incremento del uso de la nube como espacio de almacenamiento para establecer un framework basado en el método de arquitectura empresarial ADM-TOGAF, la cual, consta de 8 fases y permite una integración fácil con otras normas de Seguridad de la Información, tales como COBIT5, ISO 27001, NIST como se muestra en la figura 8.

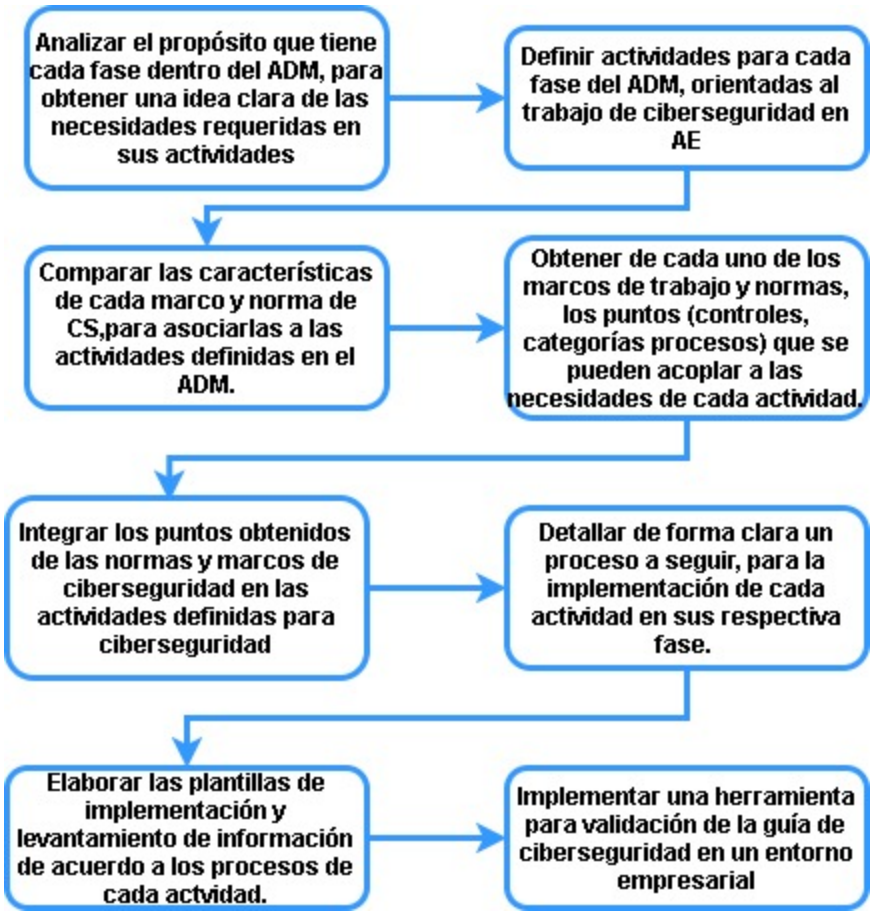

Figura 8. Proceso de elaboración de las fases de ciberseguridad para la arquitectura empresarial
Autor: Jaramillo, Cabrera, Abad Torres, Verdúm, 2015.

Los resultados que obtiene la metodología ADM-TOGAF de dicha integración fueron de un 52% para la fase preliminar, y de un 55% para la fase de visión de arquitectura, lo que da a reflejar un mayor porcentaje de cumplimiento y verifica que estén claros los lineamientos necesarios para iniciar el trabajo de implementación de gestión de riesgos de ciberseguridad.

- Metodología bajo la familia ISO/IEC – 27000

Valencia, Orozco (2017) hace énfasis del modelo metodológico que esté basado en estándares internacionales que cumplan con las normas establecidas. Consecuentemente, diseñan un modelo que integra las normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, que son utilizados para implementar el sistema de gestión de seguridad de información (SGSI), en empresas pequeñas, define el nivel de aceptación de los riesgos y la valoración de estos. Dan una conclusión de que no es necesario implementar un SGSI complejo con toda la familia del estándar ISO/IEC 27000, debido a que sería de gran complejidad para la empresa; solamente son necesarias cuatro fases principales que permiten establecer de manera sólida el proyecto, la tabla 2 de las fases, se muestran, a continuación.

Tabla 2. Las 4 fases de implantación de SGSI y la relación con las normativas ISO/IEC 27000

Fases 27003:2010	Etapas	Numerales de la norma ISO/ IEC 27001:2013 relacionados
Obtener la aprobación de la Dirección para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI	4.1. Conocimiento de la organización y de su contexto.
	Definir el alcance preliminar del SGSI	4.2. Comprensión de las necesidades y expectativas de las partes interesadas.
	Creación del plan del proyecto para ser aprobado por la Dirección	5.1. Liderazgo y compromiso 7.1. Recursos
Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites del SGSI	4.3. Determinación del alcance del sistema de gestión de seguridad de la información.
	Definir el alcance y los límites de las Tecnologías de Información y Comunicaciones	
	Definir el alcance y los límites físicos	
	Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI	
	Desarrollar la política del SGSI y obtener la aprobación de la Dirección	5.1. Liderazgo y compromiso 5.2. Política 6.2. Objetivos de seguridad de la información y planes para lograrlos.
	Definición de roles, responsabilidades del SGSI	5.3. Roles, responsabilidades y autoridades en la organización. 7.2. Competencia 7.3. Toma de conciencia
Realizar el análisis de los requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso SGSI	4.2. b) La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información.
	Identificar los activos dentro del alcance del SGSI	
	Realizar una evaluación de la seguridad de la información	6.1.2. Valoración de riesgos de seguridad de la información.
Realizar la valoración de riesgos y planificar el tratamiento de riesgos	Realizar la valoración de riesgos	6.1.2. Valoración de riesgos de seguridad de la información.
	Seleccionar los objetivos de control y los controles	6.1.3. Tratamiento de riesgos de la seguridad de la información. 6.2. Objetivos de seguridad de la información y planes para lograrlo.
	Obtener la autorización de la Dirección para implementar y operar el SGSI	5.1. Liderazgo y compromiso

Fuente: Valencia, Orozco, 2017.

- Metodología MAGERIT

La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2015), crean la metodología (MAGERIT) sigue la metodología de la normativa ISO 31000, responde al denominado "Procesos de Gestión de Riesgos", la cual implanta procesos de Gestión de Riesgos dentro de un marco de trabajo para que los organismos de gobiernos o entidades públicas tomen decisiones toman en cuenta los riesgos derivados del uso de las tecnologías de la información. Hay muchas aproximaciones al momento de analizar los riesgos que soportan las áreas de TIC: guías formales, aproximaciones metódicas y herramientas de soporte, todas estas buscan dar un objetivo al análisis de gestión de riesgos para indicar si es seguro o inseguros el o los sistemas, el gran reto es la complejidad del problema al que se enfrentan y esa complejidad es la gran cantidad de elementos que tiene que considerar. En ese sentido Magerit persigue una a proximidad metódica para no dejar a la improvisación, independencia de la arbitrariedad del analista.

MAGERIT ha buscado los objetivos que se muestran en la figura 9, a continuación.

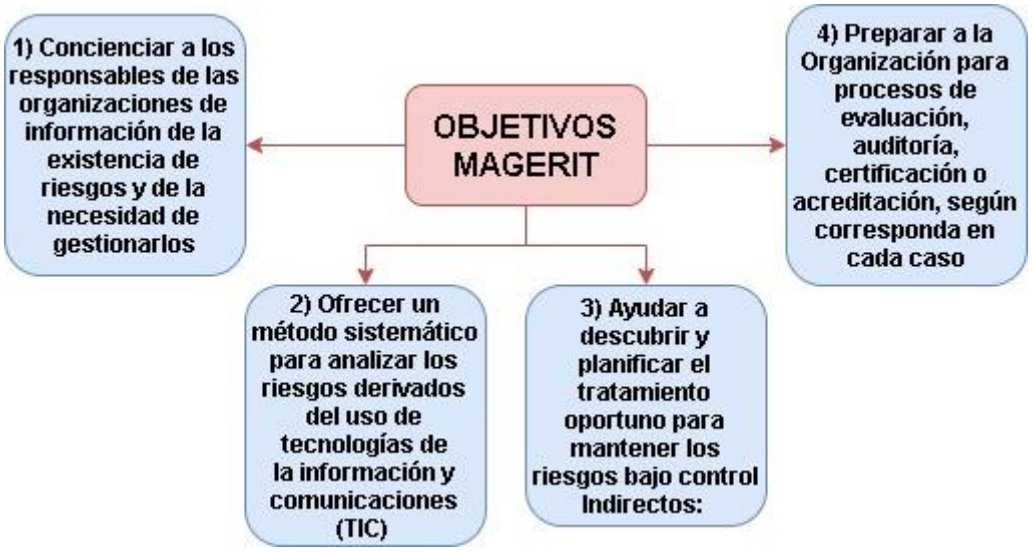

Figura 9. Objetivos de la metodología de MAGERIT
Autor: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2015.

- Metodología CRAMM.

CCTA Risk Analysis and Management Method (CRAMM) por sus siglas en inglés, es una metodología de análisis y riesgo que fue desarrollada por la Agencia Nacional de Telecomunicaciones del Gobierno del Reino Unido por el centro de informática, SCRAMM logra definirse como una metodología muy robusta debido a que analiza y gestiona los riesgos. Está enfocada a proteger la confidencialidad, la integridad y la disponibilidad de un sistema y sus activos, esta metodología es compatible con las normas ISO 27001 y es aplicable a todo tipo de sistemas y redes de información bajo la etapa de estudio de factibilidad, da un alto nivel de riesgo es requerido para identificar los requisitos de seguridad general, los costos y la contingencia asociados de las distintas opciones (Cordero, 2015).

Según Cordero (2015), la metodología CRAMM se divide en tres etapas las cuales son detalladas en la figura 10.

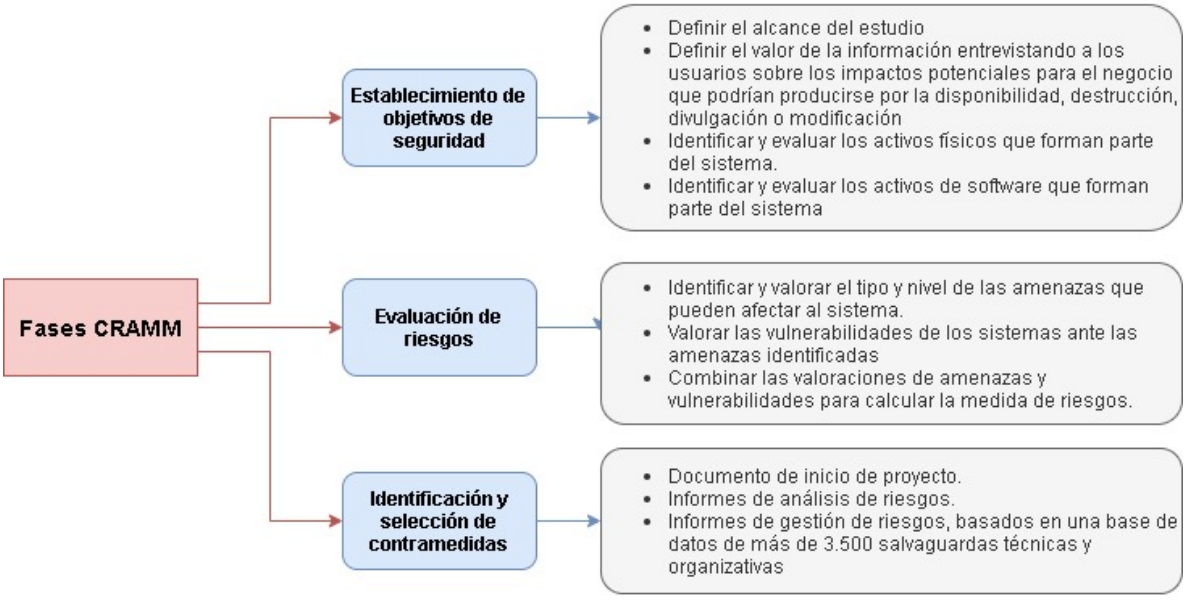

Figura 10. Fases para realizar el análisis de riesgos CRAMM
Autor: Cordero, 2015.

1.4.3. Definición e implantación de las políticas de seguridad

Según Contero (2019) analiza los conceptos de seguridad de la información de muchas publicaciones y el maneja de la siguiente manera como se explica en la figura 11.

Figura 11. Jerarquia en los conceptos de seguridad de la información
Fuente: Contero, 2019.

CIA: Son los objetivos fundamentales de la Gestión de la seguridad de la Información (Confidencialidad, Integridad y Disponibilidad)

Políticas de Seguridad: Se define como política como *declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.*

Plan de seguridad: Son las decisiones para realizar acciones futuras y los medios que se utilizan para actuar las mismas.

Procedimiento de Seguridad: Es el detalle de los pasos que se siguen para ejecutar las tareas determinadas; procedimientos de seguridad que aplican políticas de seguridad en una empresa u organización.

Este procedimiento de seguridad se divide en tareas y operaciones específicas y estas realizaran o generar registros o evidencias.

La seguridad de la información es la disciplina que abarca los sistemas de protección física, la prevención de accidentes o la prevención de actividades desleales por parte de los empleados de una organización o empresa.

(Recio, 2012) “El punto de inicio para establecer y mantener con garantías de éxito la seguridad de la información, es la definición de los objetivos de una manera clara y entendible, a partir de los cuales podrían desarrollar las políticas y procedimientos que definan un marco referencial para DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR “ situar las medidas de seguridad a implantar, tiene en cuenta los aspectos legales que rigen la seguridad del espacio físico donde se sitúa una empresa”.

“Los objetivos de la seguridad de la información, se fundamentan en los tres principios a cumplir un sistema informático”.

1.4.4. Seguridad en redes de comunicación

La seguridad en las redes de comunicación da las garantías de integridad, disponibilidad y el rendimiento de una organización proponer la protección de los activos de TI contra las amenazas como el malware, ransomware y ataques de denegación de servicio. Las soluciones de seguridad es un componente esencial de la optimización de la red, ha dado la ayuda de prevenir onerosos ataques y ha aumentado la productividad de empresas, a consecuencia de que aseguran un correcto funcionamiento de las redes (Jiang, 2020).

Tener un programa de seguridad en la red aborda una serie de políticas de seguridad de datos, un plan de contingencia ante eventos peligrosos, además de la necesidad de realizar un análisis de vulnerabilidades y pruebas de pentesting regulares. Mediante de un ataque simulado a la red las pruebas ayudaran a evaluar la eficacia de sus procesos y controles de seguridad, así como el comportamiento y la actuación del personal de TI en respuesta antes estos incidentes (Huang, 2020).

Ahora bien, Juan Rodríguez (2020) realiza una pregunta ¿Qué manera se interconectan estos dispositivos?, como no es de otra manera, se realizan la conexión a través de redes de comunicaciones que varían en su ámbito de actuación como son: Wide Área Networks (WAN) o las Local Área Network (LAN). Dichas redes tendrán infraestructura definida o no, donde exista diferentes dispositivos de control las cuales supervisan y facilitan el intercambio de información entre los usuarios conectados o nodos finales de la red. Las redes LAN en ejemplo

donde es común la existencia de dispositivos enrutador encargado de encaminar información entre los propios dispositivos que conforman la red.

El análisis forense de redes es extensión del modelo de seguridad de redes, que tradicionalmente enfatiza la prevención y detección de ataques a la red. Esto aborda la necesidad de una clara investigación dedicada a las capacidades para la investigación de comportamientos maliciosos en redes, los atacantes de hoy en día tienden a utilizar sofisticadas técnicas de ataque de múltiples etapas y múltiples hosts y herramientas antiforense para cubrir las huellas de ataque. Debido a las limitaciones actuales de detección de intrusos y herramientas de análisis forense, reconstruir escenarios de ataque desde La evidencia dejada por los atacantes de un sistema empresarial es desafiante. En particular, la reconstrucción de escenarios de ataque utiliza la información de las alertas de IDS y los registros del sistema que tienen un gran número de falsos positivos es un gran desafío (Singhal, Lui, Wijesekera, 2015).

1.4.5. Metodologías y técnicas de seguridad en las redes de comunicaciones

Se ha identificado muchas técnicas de seguridad en las redes de comunicación, las cuales se hacen referencia para el estudio de esta investigación tratan de comparar y analizar cuál de estas técnicas es la mejor para el uso de los actores de las entidades de criminología.

- Técnica de Encriptación en las Redes WSN (Wireless Sensor Networks).

Según Valencia, Guarda, Luna, Ninahualpa, (2019) menciona que la criptología que trabaja con nodos de bajos recursos en procesamientos para garantizar la integridad y disponibilidad, se considera que no enfatiza en la confidencialidad, en este caso se plantea los siguientes procedimientos, el Gateway al recibir la información censada corroborara que la intimación se encuentra acorde con el valor HASH, caso contrario descartara el paquete y se encontrará a la espera de una nueva muestra como se muestra en la figura 12, es decir, no procesara la información basura.

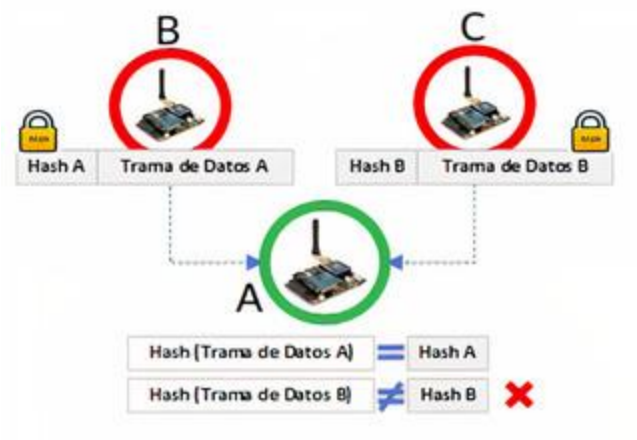

Figura 12. Aplicación HASH en la información transmitida por los nodos finales
Fuente: Valencia, Guarda, Luna, Ninahualpa, 2019.

La función HASH que se propone es aplicar un MD5, la cual da un código de 32 caracteres hexadecimales, se aplica este método para considerar que el tiempo de ejecución es menor frente a SHA-1 con tiempos menores de 100ms suman el tiempo de demora la transacción del nodo final al Gateway para los sistemas de medición. Realizar este método, se busca que el Gateway garantice la integridad de la información transmitida por cada uno de los nodos, evitan el ataque a los paquetes. Para el manejo de las llaves públicas y privadas, es recomendado la distribución de las entidades especializadas como el Ministerio de Obras Publicas en el Ecuador, la cual, es considerado como autoridad de gobierno observar la figura 13 (Valencia, Guarda, Luna & Ninahualpa, 2019).

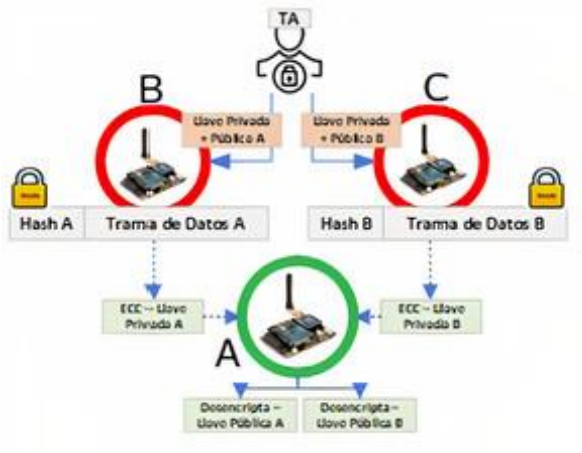

Figura 13. Encriptación asimétrica ECC en la información transmitida por los nodos finales
Fuente: Valencia, Guarda, Luna, Ninahualpa, 2019.

Esta técnica encriptara la información con la llave privada única por cada nodo, de manera que el objetivo es de una integridad complementaria a la información sin dejar que ningún atacante externo a la red incluirán información (Valencia, Guarda, Luna & Ninahualpa, (2019).

- Técnicas de Tunelizado o “Tunneling”

Martínez (2019) indica en su investigación la técnica Tunneling, la cual, consistente en la comunicación de los datos que se envían, estas van a ir encapsulados con un protocolo de red cifrado para viajar sobre la red de comunicación mediante un túnel, este proctólogo encapsula un paquete IP “pasajero” sobre otro “portador” para poder utilizar redes públicas y establecer sobre ellas enlaces que permitan conectar otras redes con direccionamiento diferente, en la figura 14, se indica un ejemplo de Tunnleing.

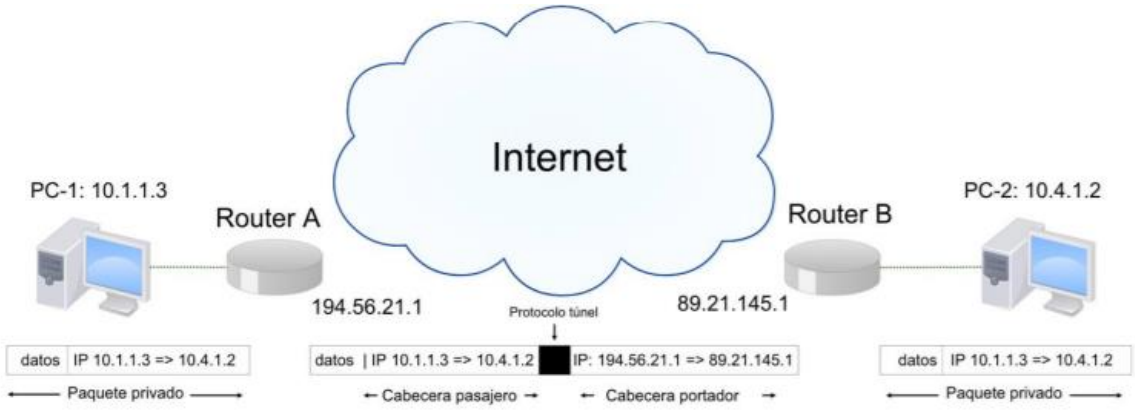

Figura 14. Técnica de tunelizado
Fuente: Martínez, 2019.

Como se muestra en la figura N° 14, el Router A encapsula el paquete privado con cabeceras IP públicas que podrían ser enrutadas sobre Internet. Posteriormente, el Router B elimina las cabeceras IP públicas del paquete recibido y devuelve el paquete original a la red privada.

La información cifrada viaja dentro de la unidad de datos del protocolo de comunicación (PDU), estos nodos que participan en la comunicación interactuar con el paquete, pero al final de la comunicación la información es desencapsulada y descifrada para su uso, de esta manera el túnel, se establece entre los puntos de extremo a extremo de la comunicación y el protocolo que se Utilice y este es de los más populares es SSH (Martínez, 2019).

- Técnica de Seguridad en la Implementación de Servicios Sobre IPv6.

Según Bareño, Navarro, Cárdenas, Sarmiento, Duarte (2016) busca la mitigación de los posibles ataques o problemas en el proceso de autenticación, integridad y confidencialidad de usuarios locales o remotos a través de diversas redes con resultados de implementación confiable y seguros. Da la utilidad el protocolo nativo IPSEC en IPV6 de host a host en lugar de punto a punto como se hace en IPV4, ll encabezado de autenticación, se utiliza para garantizar la integridad y ataques de no repudio, ESP (Carga de Seguridad Encapsulada) para la confidencialidad e integridad, Para el escenario de las pruebas, se ha determinado realizarlo en máquinas virtuales y un analizador de paquetes o Sniffer como Wireshark, para el fin de determinar en cuestiones de seguridad de los datos en cuanto a confidencialidad, integridad, autenticación y no repudio. Finalmente, la implementación y revisión de la seguridad de los servicios analizados en entornos integrados bajo IPV6 será un proceso continuo en el que diariamente aparecen nuevas vulnerabilidades y riesgos de seguridad, es importante mantener una buena formación en los protocolos utilizados, porque hacia el futuro existirán nuevos riesgos en medida de seguridad, si se incremente la utilización del protocolo IPV6.

- Metodología OWASP

Por sus siglas en inglés (Open Web Application Security Project), esta metodología centra las funciones en aplicaciones web y a las seguridades que presenta para resguardar su seguridad, la función principal de esta metodología de análisis es la de asistir a organizaciones en la forma de decisiones evidencian las vulnerabilidades y riesgos que existieran. OWASP es una herramienta muy utilizada en las organizaciones para identificar e informar los posibles riesgos que se presentarían en la página web, detecta incidentes ajenos al uso habitual e informar sobre lo encontrado (Delgado 2020).

OWASP presenta un plan de ejecución ordenado, la cual, recorre las distintas áreas vulnerables de forma sistemática de una aplicación web, analiza toda posibilidad que tiene la organización de ser víctima de un ataque, cabe recalcar que es una herramienta de análisis de uso gratuito identificada para mejorar de las aplicaciones web debido que los ciber atacantes utilizan diferentes rutas para materializar y causar pérdidas cuantiosas a las organizaciones (Delgado 2020).

La metodología OWASP maneja el top 10 de vulnerabilidades más comunes que se muestra en la figura 15.

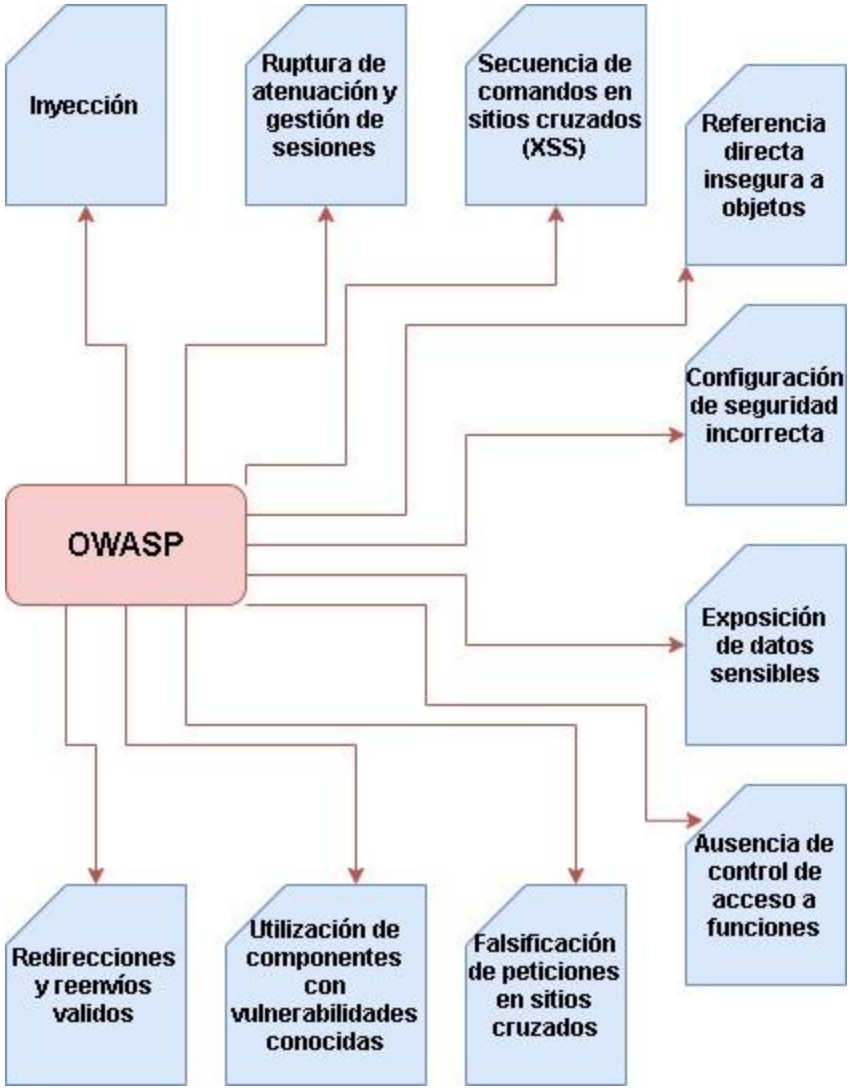

Figura 15. Top 10 de vulnerabilidad de OWASP
Fuente: Delgado,2020.

- Metodología CVSS 3.0

La metodología CVSS por sus siglas en inglés (Common Vulnerability Scoring System) es un framework abierto y es utilizado universalmente, la cual establece métricas de comunicación de características, impacto y severidad de las vulnerabilidades que afectan a los elementos de entorno de seguridad, este sistema de puntuación proporciona un método estándar de código abierto para estimar el impacto de una vulnerabilidad, la cual se compone de tres grupos

principales métricas: BASE, TEMPORAL y ENTORNO, cada uno cuenta con sus métricas (Sánchez, Vivero, & Baroja, 2018).

Sánchez, Vivero, & Baroja (2018) explica de una forma más amigable los grupos que utiliza la metodología CVSS 3.0.

Grupo Base: Encapsula las cualidades intersecan de una vulnerabilidad y son independientes en el tiempo y el entorno:

- **Access Vector (AV). Valores:** [L, A, N] (Local, Adjacent, Network)
- **Access Complexity (AC). Valores:** [H, M, L] (High, Medium, Low)
- **Authentication (Au). Valores:** [M, S, N] (Multiple, Single, None)
- **Confidenciality Impact (C). Valores:** [N, P, C] (None, Partial, Complete)
- **Integrity Impact (I). Valores:** [N, P, C] (None, Partial, Complete)
- **Availability Impact (A). Valores**: [N, P, C] (None, Partial, Complete)

Grupo Temporal: Características de la vulnerabilidad que cambian en el tiempo y se aplican tres métricas:

- **Exploitability (E). Valores:** [U, POC, F, H, ND] (Unproven, Proof-of-Concept, Functional Exploit, High, Not Defined)
- **Remediation Level (RL). Valores:** [OF, TF, W, U, ND] (Official Fix, Temporary Fix, Workaround, Unavailable, Not Defined)
- **Report Confidence (RC). Valores:** [UC, UR, C, ND] (Unconfirmed, Uncorroborated, Confirmed, Not Defined)

Grupo Environmental: Las características de la vulnerabilidad relacionadas con el entorno del usuario. En este caso los factores que se evalúan son:

- **Collateral Damage Potential (CDP). Valores:** [N, L, LM, MH, H, ND] (None, Low, Low Medium, Medium High, High, Not Defined)
- **Target Distribution (TD). Valores:** [N, L, M, H, ND] (None, Low, Medium, High, Not Defined)
- **Security Requirements (CR, IR, AR). Valores:** [L, M, H, ND] (Low, Medium, High, Not Defined)

Para un mejor entendimiento, se muestra en le figura 16 los grupos de la metodología CSVV 3.0.

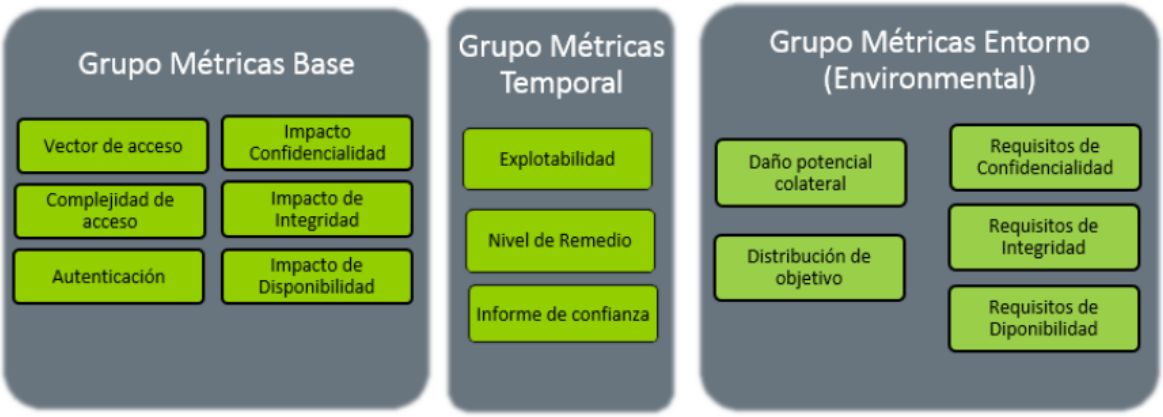

Figura 16. Métricas CSVV 3.0
Fuente: Sánchez, Vivero, & Baroja, 2018.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de la investigación

Para encontrar la metodología y establecer el modelo, está compuesta por varias actividades que ayudaran a establecer responsabilidades en cada una de las etapas de su desarrollo resuelve un análisis cualitativo y cuantitativo que permite lograr procesos bien definidos a la investigación.

La elaboración de esta metodología permite visualizar un proceso de investigación por etapas y su tratamiento efectivo en cada una de ellas, las herramientas a utilizar serán reconocidas en cada una de las etapas de acuerdo con la noción que corresponde a la estructura de construcción del proceso.

Para una mejor investigación y determinación de los datos adquiridos para el análisis, se consideró trabajar con las siguientes características:

Tipo de Investigación: Tipo Experimental, Prospectivo, Transversal

En este estudio, se utilizó la investigación experimental con la finalidad de descubrir las causas en las cuales las técnicas no dan las garantías para la admisibilidad de la evidencia digital, por otra parte, la investigación prospectiva ayudará en establecer mejores técnicas sobre la preservación digital y el manejo de la evidencia digital por los actores principales de justicia y para complementar la investigación transversal que analizará los datos de variables recopiladas en el periodo de tiempo en la población aplicada la investigación.

Diseño de Investigación: Descriptivo - Correlacional

Con el diseño descriptivo, se puntualizó las características del Consejo de la Judicatura como actores principales de la investigación, en complemento de estudio la correlacional entenderá y avaluará la relación estadística de los datos recolectados por la encuesta NESTOR, la cual va a hacer aplicada para esta investigación.

Población: 28 actores de justicia de la provincia de Chimborazo, distribuidos en Custodios de Evidencia, Jueces, Peritos, Fiscales y Técnicos.

Muestra: Igual a la que se muestra en la población.

Tipo de Recolección de la Información: La técnica para recolectar información para el procesamiento y análisis es la encuesta NESTOR: Network of Expertise in Long-term Storage of Digital Resources y su instrumento el cuestionario, esta encuesta está basada en un catálogo de criterios para los repositorios digitales.

2.2. Caracterización del consejo de la judicatura

El Consejo de la Judicatura es pertenece como servicio público de gobierno, de administración, vigilancia y disciplinario de la Función Judicial (poder judicial ecuatoriano). Este órgano no es jurisdiccional, por lo que no se consigue administrar justicia como la Corte Nacional de Justicia, las cortes provinciales o los juzgados de primera instancia, las funciones están limitadas a la administración y mantenimiento de las demás instituciones u órganos de la Función Judicial, establecer evaluaciones a los jueces y otros operadores de justicia (funcionarios públicos de la Función Judicial), realizar gestiones y supervisión a los concursos de méritos y oposición para la selección del nuevo personal de los órganos, e imponer sanciones por malas actuaciones de los funcionarios públicos.

El Consejo de Judicatura posiciona a la planificación para el desarrollo como una obligación primordial del estado, a la vez, determina que el plan Nacional de Desarrollo es el instrumento al que se sujetaran las políticas, programas y proyectos públicos; la programas y ejecución del presupuesto del estado, la inversión y la asignación de los recursos públicos.

De acuerdo con lo estipulado en el artículo 179 de la Constitución ecuatoriana vigente, el Consejo de la Judicatura está integrado por nueve vocales principales con sus respectivos alternos, los vocales duran en sus funciones por un período de seis años sin posibilidad de reelección. Uno de los lineamientos que propone la Constitución es la paridad de género (mismo número de hombres y mismo número de mujeres en la composición de asambleas, consejos, entre otros), por lo que, también, se procura que la cantidad de hombre y mujeres sea lo mayor pareja posible. El vocal elegido de la terna enviada por la Corte Nacional de Justicia presidirá el Consejo.

El Plan Estratégico de la Función Judicial (PEFJ) 2019- 2025, el cual, contó con la efectiva participación de las autoridades y órganos del Consejo de la Judicatura, Corte Nacional de

Justicia, Defensoría Pública y Fiscalía General del Estado; permite así tener la hoja de ruta para la Función Judicial en base a cuatro ejes.

La primera sección abarca lo realizado en torno al Eje #1 del PEFJ, que promueve la "Lucha contra la corrupción", describe las gestiones implementadas en lo concerniente al Objetivo Estratégico 1 que busca "Institucionalizar la transparencia e integridad en la Función Judicial, facilitar el control social y asegurar el óptimo acceso a los servicios de justicia" en los siguientes ámbitos: políticas y acciones encaminadas a la lucha contra la corrupción, investigación de presuntos actos de corrupción, procesos de transparencia, y convenios con demás instituciones y organizaciones de la sociedad civil para hacer frente a la lucha contra la corrupción. Las acciones ejecutadas en relación con el Eje #2 del PEFJ, constan en la segunda sección sobre el "Fortalecimiento institucional a través de la capacitación, evaluación y tecnificación de los servidores judiciales", cuyo objetivo es "Fortalecer la gestión institucional y modernizar los procesos y servicios judiciales con prioridad en capacitación, evaluación y tecnificación de servidores judiciales". En este ámbito, se analiza el fortalecimiento de las capacidades de las y los servidores administrativos, jurisdiccionales y personas vinculadas al sector judicial, la promoción y evaluación de servidores jurisdiccionales, la modernización y mejora en la prestación de los servicios de justicia, promoción de la justicia de paz y de los métodos alternativos de resolución de conflictos, y la garantía de la provisión y optimización de infraestructura.

La sección tercera aborda las acciones realizadas en cuanto al Eje #3 del PEFJ referente a la garantía de la "Independencia interna y externa" de la Función Judicial; a su vez contempla el Objetivo Estratégico 3 sobre el mismo ámbito. En este marco, se exponen los mecanismos permanentes de control disciplinario en la Función Judicial y cada una de las medidas que se han implementado en 2019 para este fin. Los avances alcanzados en cuanto al Eje #4 del PEFJ referente al "Fortalecimiento de los mecanismos de investigación y sanción en casos de violencia sexual contra niños, niñas, adolescentes y mujeres", y que enmarcan el Objetivo Estratégico 4 que señala "Fortalecer los mecanismos de investigación y sanción de la violencia en todos los ámbitos y garantizar la protección a las víctimas y su entorno familiar, mediante procesos justos y eficientes" constan en la sección cuarta. En ésta, se describen las acciones destinadas a implementar la Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres, los planes institucionales que aportan a este proceso y los principales logros

alcanzados en cuanto a la implementación de esta norma. (*Consejo de la Judicatura | Consejo de la Judicatura*, s. f.).

Con mecanismos de observación directa, se ha logrado identificar que la cadena de custodia de los contenidos físicos o digitales no cuentan con las herramientas y técnicas necesarias para garantizar la admisibilidad de la evidencia digita a corto o a largo plazo, los diferentes actores en la cadena de custodia como los jueces, fiscales, peritos, custodios y los técnicos de sistemas funcionarios públicos del Consejo de la Judicatura de la provincia de Chimborazo no cuentan con las herramientas ni las técnicas adecuadas para la ingesta, traslado y recepción de la evidencia digital hacia la autoridad juzgadora, lo que provoca que la evidencia digital sea altamente vulnerada, modificada o a su vez destruida por los ciberdelincuentes.

2.3. Metodología de desarrollo.

Para poder alcanzar los objetivos propuestos, se planifica un proceso metodológico que se detalla, a continuación:

Primera etapa: investigación del estado del arte.

En esta fase de la investigación, se realizará una recopilación detallada de toda información, con la finalidad de definir el estado del arte sobre diferentes temas las cuales van a ser como referencia de estudio para este trabajo como: la preservación digital, prevención digital en el área judicial, la admisibilidad de la información digital, seguridad de la información y seguridad de redes de comunicaciones, fundamentada en una adecuada bibliografía que a través de artículos, trabajos publicados y tesis relacionados en varias conferencias y revistas.

Se basará en la búsqueda de información en las diferentes plataformas de alto nivel de estudio de publicaciones e investigaciones como SCOPUS, Google Académico, SpringerLink, ScienceDirect, entre otros, toda esta primera etapa, se ha cumplido dentro de la elaboración en el capítulo 1 del presente documento.

Segunda etapa: describir las metodologías y técnicas de seguridad aplicadas en las redes de comunicaciones en la custodia digital.

Se realizará el análisis de lo siguiente:

- Análisis sobre las metodologías y técnicas de seguridad aplicadas a la información.

Este subíndice de esta etapa, se identificará las diferentes metodologías y técnicas sobre la seguridad de la información, en la actualidad existe mucha información sobre temas relacionados, pero, se dará más relevancia a las que son más relacionadas al tema de estudio de investigación de desarrollo.

- Determinar cuáles son las metodologías y técnicas de seguridad en las redes de comunicaciones necesarias para un modelo de preservación digital.

Este subíndice de esta etapa, se analizará las diferentes metodologías y técnicas de seguridad en el ámbito de las redes de comunicación, estas metodologías y técnicas realizan estudios de seguridad en las diferentes etapas de una comunicación de diferentes actores que analizan sus estudios bajo muchas dependencias a las necesidades de los actores y al escenario de estudio.

- Requerimientos legales y políticas de preservación de datos en instituciones de investigación criminal.

La evidencia digital dentro de un proceso judicial es de especial importancia, porque a medida de ella se logra confirmar o desvincular una hipótesis o afirmación de precedente, el objetivo de todo el proceso se dirige hacia la averiguación de la verdad formal, los requerimientos legales y políticas de preservación de la evidencia, se investigará bajo las leyes vigentes dentro a la constitución de la Republica del Ecuador.

Tercera etapa: diagnóstico de las metodologías o técnicas utilizadas por los actores de justicia de la evidencia digital.

En esta etapa, se realizará el diagnóstico de la situación actual de los modelos utilizados por los actores principales en la preservación y admisibilidad de la evidencia digital, mediante una encuesta basada en las dimensiones de confianza propuestas en el modelo y la encuesta NESTOR, dicha encuesta está compuesta en un formato de 98 preguntas con opciones de selección múltiple, en primera instancia, se encuentra la parte de identificación del encuestado, la segunda instancia está compuesta por las preguntas con ponderación a escala de valoración donde:

- (1) significa que cumple completamente el requerimiento implementado en un modelo formal y sistémico.
- (2) significa que la institución alcanza a cumplir ese requerimiento, pero es un proceso o procedimiento aislado y no forma parte de un modelo formal o sistémico, o no forma parte de un aplicativo, o que tiene un modelo implementado, pero no cumple ese requerimiento completamente.
- (3) significa que la institución no cumple con ese requerimiento y no tiene un modelo implementado.

Esta encuesta, se la aplico a todos los actores principales de la custodia de la evidencia digital del Consejo de la Judicatura de la provincia de Chimborazo, enviada por los medios de comunicación como la aplicación más popular como WhatsApp y correo electrónico, de igual forma se ha realizado una llamada previa a estos actores para su apertura a la encuesta. La encuesta se la aplico mediante la plataforma de Googleforms, bajo la autorización del director del Consejo de la Judicatura de la provincia de Chimborazo.

Es una encuesta que se realizó en línea, la encuesta se la realizo de manera amigable gráficamente con una duración de aproximadamente de 12 a 15 minutos, en anexos, se observa más detallado la encuesta Anexo 1.

En bases a este diagnóstico con la encuesta NESTOR realizada a los actores principales del Consejo de la Judicatura de la provincia de Chimborazo, se realizará el conjunto de las buenas prácticas.

Cuarta etapa: redacción de la síntesis de las buenas prácticas aplicadas en técnicas adecuadas sobre las redes de comunicaciones de la custodia de la evidencia digital.

En esta etapa, se la realiza de forma simultánea con las etapas anteriores, se realizará el análisis y los datos recolectados por medio de la encuesta NESTOR realizada a los actores principales de la evidencia digital del Consejo de la Judicatura de la provincia de Chimborazo.

En conjunto con el paso anterior, los datos serán tabulados bajo la metodología y encuesta NESTOR da un diagnóstico sobre la metodología, la cual, usa actual mente estos actores al momento de la manipulación de la evidencia digital en el escenario donde se encuentren.

Se redactará el conjunto de las buenas prácticas con aplicación de técnicas de seguridad a las redes de comunicación que serán utilizados previo el análisis y el resultado de la encuesta NESTOR, hacia los actores principales del Consejo de la Judicatura de la provincia de Chimborazo.

Esta metodología presenta una secuencia ordenada en la investigación, con productos de cada fase que serán utilizados en la siguiente etapa y que cada uno en sí resuelven los problemas planteados con anterioridad y por tanto permite realizar el seguimiento y cumplimiento de actividades.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Interpretación de los datos alcanzados por la encuesta NESTOR

Los principales actores del manejo de la evidencia digital del Consejo de la Judicatura de la provincia de Chimborazo llevaron a cabo un cuestionario previamente diseñado al escenario donde se encuentra esta institución de investigación criminal, compuesto por 99 elementos o variables, mide el nivel de importancia de los aspectos que la institución tendrán en cuenta al aplicar técnicas o buenas prácticas de preservación en la evidencia digital. El nivel de importancia se mide a través de la guía de evaluación de desempeño.

El cuestionario, se dividió en cinco partes siguientes las cuales van a verificar la importancia de los aspectos. (a) Infraestructura Organizativa, se determinará si las políticas de preservación que actúa dentro de un marco organizativo determinado por los objetivos definidos, las condiciones legales y los recursos financieros disponibles, (b) Administración de Objetos Digitales, en este punto, se pretende verificar si las políticas de aplicación de técnicas o modelos de preservación digital analizan los objetivos y estrategias, y especifican todos los requisitos relacionados con la gestión de objetos digitales durante el ciclo de vida. (c) Gestión de Riesgos de Infraestructura y Seguridad, se analizará los aspectos técnicos y de seguridad del sistema en general, (d) Aspectos de Gestión de la Integridad de las Instituciones de Investigación Penal.

3.1.1. Análisis e interpretación de datos

Tras la consolidación y análisis estadístico de los datos, obtenemos:

Se determina que 28 actores fueron encuestados y evaluados las cuales como resultado muestra que el 75% pertenecen en el sector público y el 25% al sector privado (véase el gráfico 2).

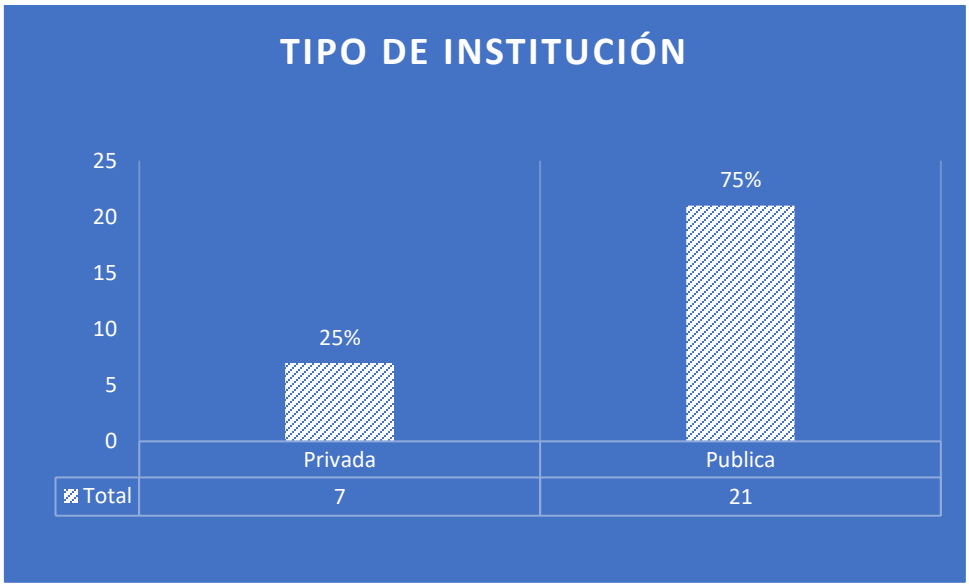

Gráfico 2. Instituciones analizadas en la encuesta NESTOR
Fuente: Elaboración propia,2020.

En un total de 28 actores encuestados en los cargos que desempeñan, un 42.9% son respuestas de los peritos, el 28.6% son técnicos de sistemas, 17.9% son fiscales y en un 10.7% son custodios, todos ellos son actores principales del Consejo de la Judicatura de la provincia de Chimborazo. (véase el gráfico 3).

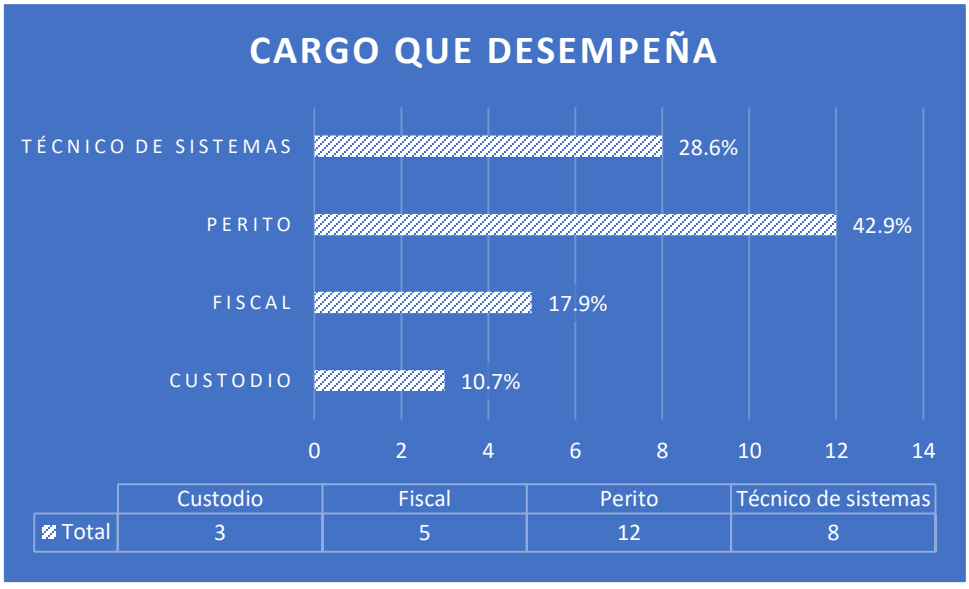

Gráfico 3. Cargos que desempeñan los actores del Consejo de la Judicatura en la encuesta NESTOR
Fuente: Elaboración propia,2020.

Durante la evaluación y tabulación de la encuesta NESTOR, los actores del Consejo de la Judicatura de la provincia de Chimborazo indica que un 50% si manejan un repositorio digital donde almacenan la información de la evidencia digital, el 28.57% manejan un repositorio digital y físico para el almacenamiento de la evidencia digital y el 21.43% manejan un repositorio físico para el almacenamiento de la evidencia digital. (véase el gráfico 4)

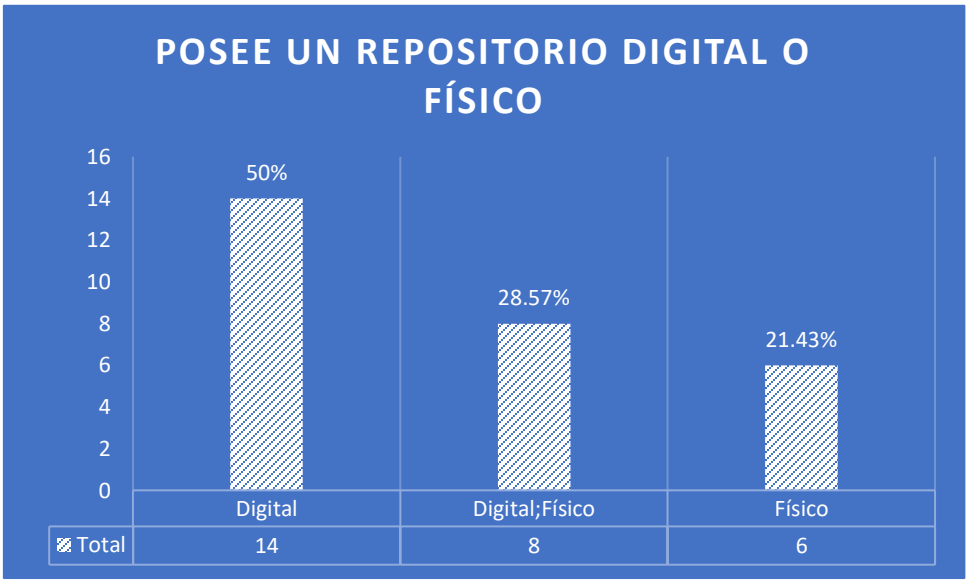

Gráfico 4. Tabulación de los actores si poseen un repositorio digital o físico con la encuesta NESTOR
Fuente: Elaboración propia,2020.

En el punto (a) Infraestructura Organizativa, identificamos que dentro de las 21 preguntas que conlleva este punto, indica en (**cumple)** se obtiene un 0.68% con un valor medio de 0.19, en (**cumple parcialmente)** se obtiene un 44.89% con un valor medio de 12.57 y en (**no cumple)** se obtiene un 54.25% con un valor de 15.19, da como resultado un nivel bajo de cumplimiento. (véase el gráfico 5)

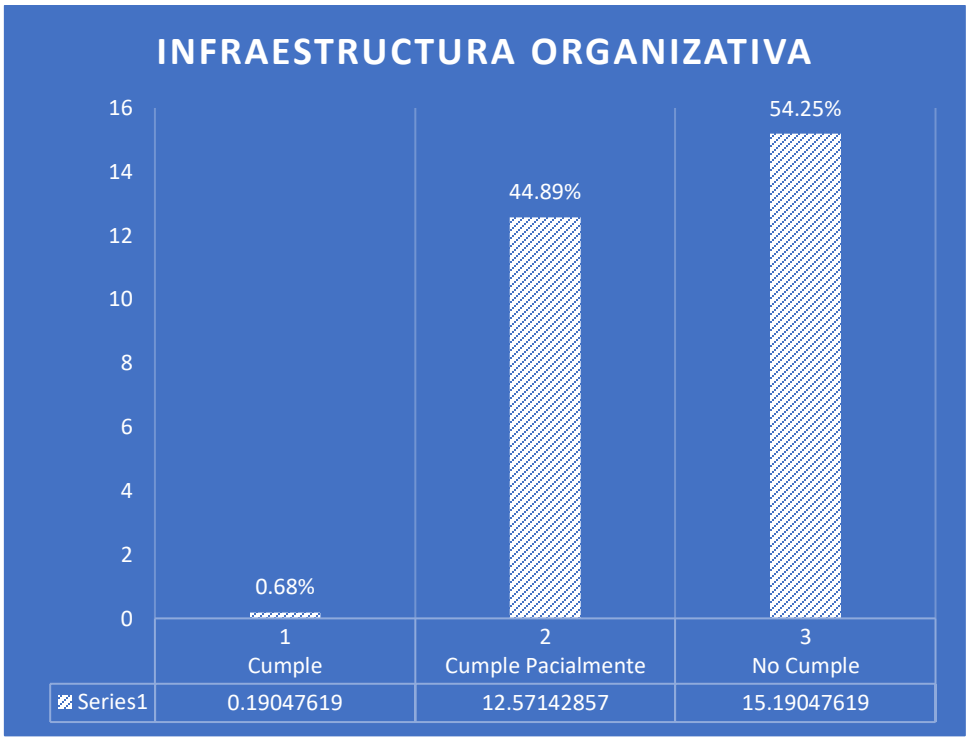

Gráfico 5. Tabulación de infraestructura organizativa con la encuesta NESTOR
Fuente: Elaboración propia,2020.

En el punto (b) Administración de Objetos Digitales, en este punto, se identifica 19 preguntas de la encuesta NESTOR aplicada a actores principales del Consejo de la Judicatura de la provincia de Chimborazo, la cual demuestra que en (**cumple)** tenemos un 0.37% con un valor medio de 0.10, en (**cumple parcialmente)** con un valor medio de 12.68 y en (**no cumple)** un 54.32% con un valor de 54.32%, da como resultado que en este punto existe un bajo nivel de cumplimiento. (véase el gráfico 6).

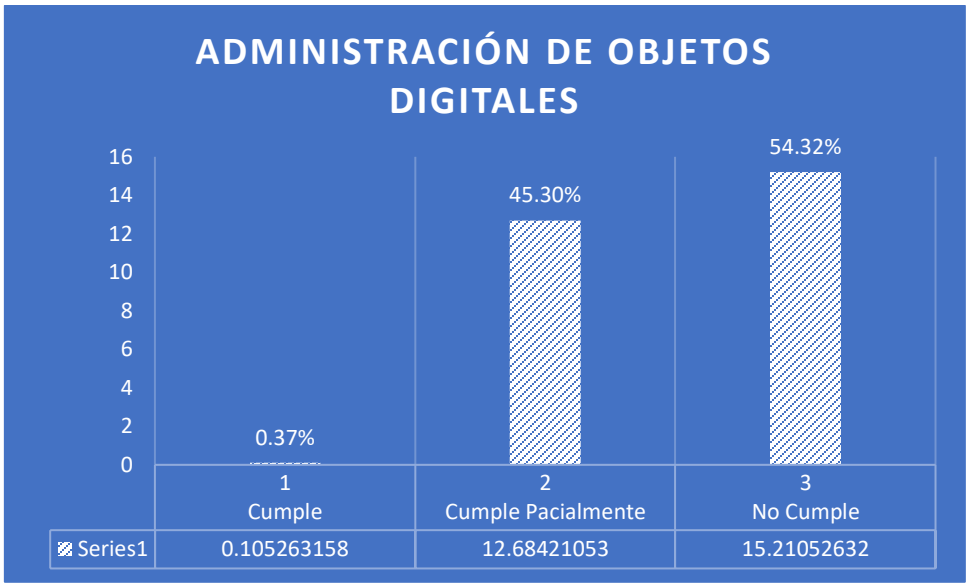

Gráfico 6. Tabulación de la administración de objetos digitales con la encuesta NESTOR
Fuente: Elaboración propia, 2020.

En este punto (c) Gestión de Riesgos de Infraestructura y Seguridad, se ha identificado 10 preguntas en la encuesta NESTOR hacia los actores del Consejo de la Judicatura de la provincia de Chimborazo, lo cual, demuestra que el indicador (**cumple**) encontramos un 0% con un valor medio de 0, en el indicador (**cumple parcialmente**) indica un 47.85% con un valor medio de 13.4 y en el indicador (**no cumple)** un 52.14% con un valor medio de 14.6, da como resultado que tiene un bajo nivel de cumplimiento. (véase el gráfico 7).

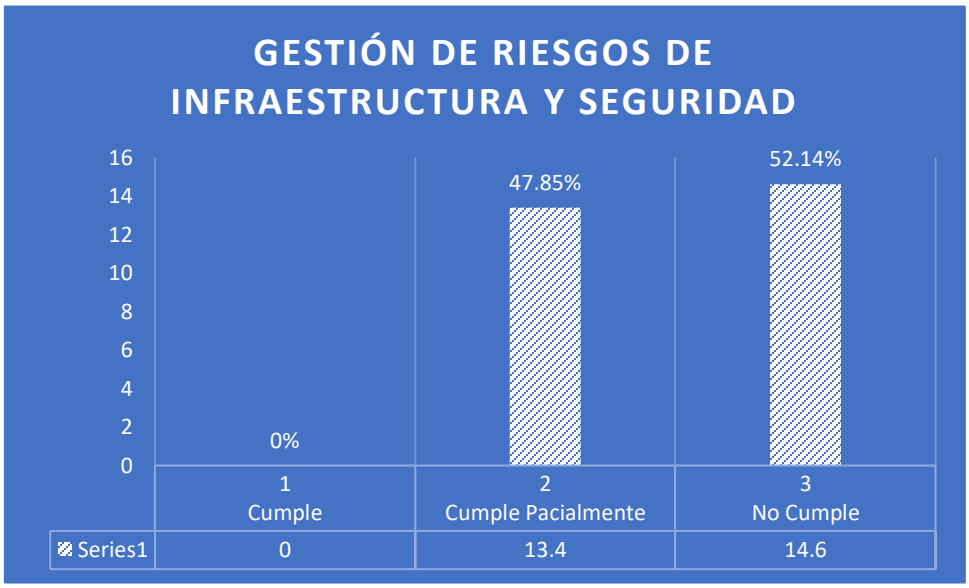

Gráfico 7. Tabulación de gestión de riesgos de infraestructura y seguridad con la encuesta NESTOR
Fuente: Elaboración propia, 2020.

En el punto (d) Aspectos de Gestión de la Integridad de las Instituciones de Investigación Penal, se pudo identificar un total de 38 preguntas que fueron aplicada a los actores del Consejo de la Judicatura de la provincia de Chimborazo, señala en el indicador (**cumple)** tiene un 1.12% con un valor medio de 0.31, en el indicador (**cumple parcialmente)** un 45.58% con un valor medio de 12.76 y en el indicador (**no cumple)** un 53.28% con un valor medio de 14.92, dándonos un resultado que el nivel de cumplimiento es bajo. (véase el gráfico 8)

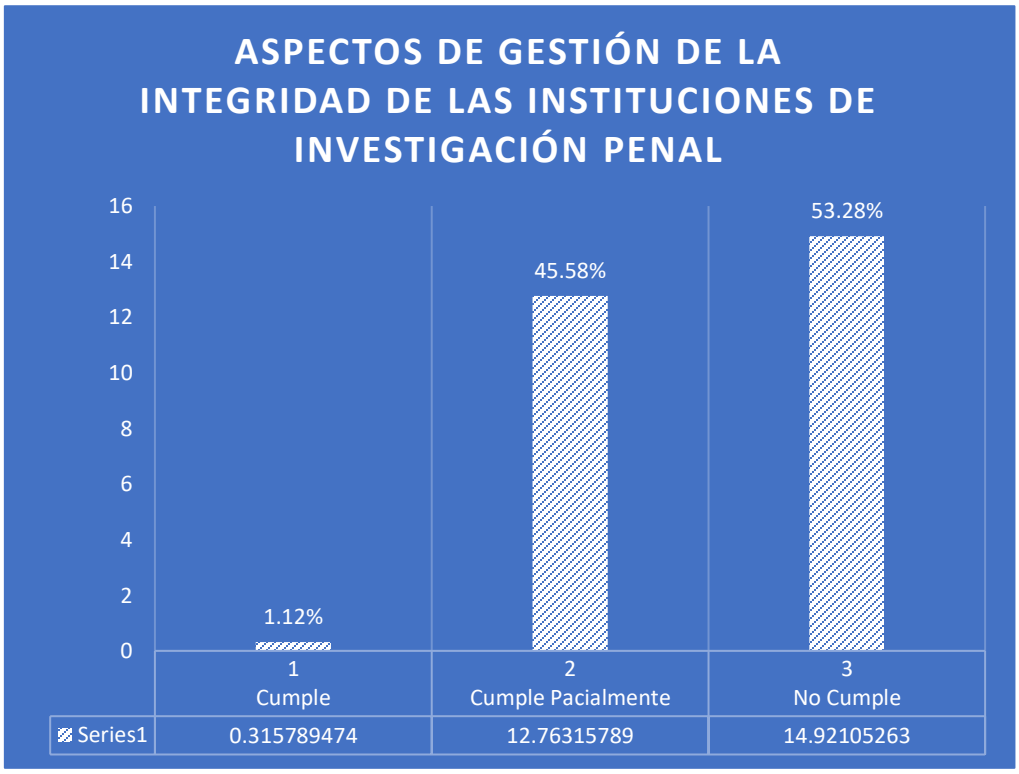

Gráfico 8. Tabulación de aspectos de gestión de la integridad de las instituciones de investigación penal con la encuesta NESTOR
Fuente: Elaboración propia, 2020.

Como resultado final, se determina que se obtiene un valor de un 54% para el aspecto de la Infraestructura Organizativa, para el aspecto de la Administración de Objetos Digitales un valor de 54%, para el aspecto Gestión de Riesgos de Infraestructura y Seguridad un valor de 52%, y en el aspecto de Gestión de la Integridad de las Instituciones de Investigación Penal un valor de

53% todos ellos bajo el porcentaje de 100% como máxima de cumplimiento. Esta evaluación determina un bajo nivel de cumplimiento en los aspectos de preservación digital en el manejo de la evidencia digital. (véase el gráfico 9).

Este resultado muestra una importancia baja para los procesos de preservación y admisibilidad de la evidencia digital, esto corresponde a la disponibilidad de recursos, formación formal o ignorancia de la ley; en cualquier caso, se trata de datos que demuestran el tratamiento inadecuado de la información digital, por lo tanto, una alta posibilidad de que a corto y a largo plazo esa información sea inaccesible, provoca desde el punto de vista cultural, histórico y jurídico una pérdida de información.

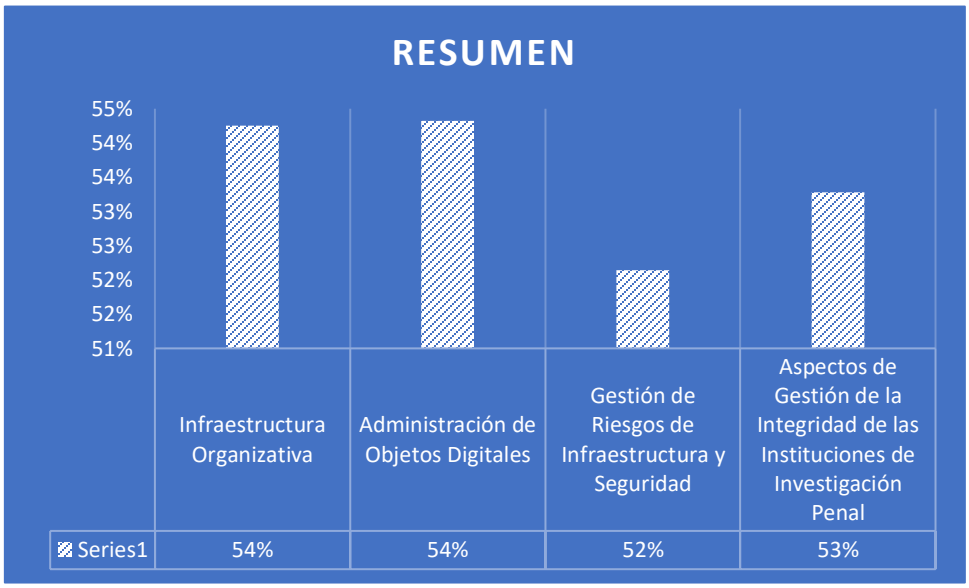

Gráfico 9. Resumen de los datos de tabulación con los 4 aspectos relacionados con la encuesta NESTOR
Fuente: Elaboración propia, 2020.

3.2. Análisis entre los métodos y técnicas de seguridad de la información y seguridad en las redes de comunicación aplicadas en la preservación digital

Las diferentes técnicas y metodologías de seguridad de la información y seguridad en las redes de comunicación han venido modificándose en el transcurso de los años y en el avance de la tecnología para dar una mejora en la seguridad de la información en que la maneja las instituciones públicas y privadas que adoptan una de ellas. Los ciberdelincuentes con la facilidad

de la tecnología desarrollan dia a dia técnicas para realizar los ataques y las herramientas utilizadas por ellos cada vez son más robustas.

Se ha identificado 5 metodologías y técnicas de seguridad de la información relevantes al análisis, a continuación, en la tabla 3, se muestra un resumen de las técnicas y metodologías de seguridad aplicadas a la información más utilizadas por el sector público y privado.

Tabla 3. Metodología y técnicas de seguridad aplicadas a la información

N°	NOMBRE	MÉTODO	RESUMEN
1	Ingeniería Social	Técnica	Identificada por los hackers educados las cuales explotan bajo tres elementos importantes como factor humano, aspectos organizativos y control tecnológico.
2	ADM-TOGAF	Metodología	Consta de 8 fases y permite una integración fácil con otras normas de seguridad de la información.
3	ISO/IEC – 2700	Metodología	Hace énfasis a todos los modelos de la familia ISO e integra a su naturalidad de la investigación las normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005.
4	MAGERIT	Metodología	Sigue a las normativas ISO 31000, la cual responde a los Procesos de Gestión de riesgos, la cual implanta procesos de gestión de riesgos dentro de un marco de trabajo para que se tomen decisiones en cuenta de riesgos.

5	CRAMM	Metodología	Es una metodología que analiza y gestiona los riesgos, enfocado a la protección de la confidencialidad, integridad, y disponibilidad de un sistema y sus activos. Es compatible con las normas ISO 27001.

Fuente: Elaboración propia,2020.

Se ha identificado de igual forma 5 metodologías y técnicas de seguridad de redes de comunicación relevantes al análisis, en este ámbito, se identifica en la tabla N° 4 las metodologías y técnicas más utilizadas en el sector público y privado.

Tabla 4. Metodologías y técnicas de seguridad aplicadas a las redes de comunicación

N°	NOMBRE	MÉTODO	RESUMEN
1	Encriptación en las Redes WSN (Wireless Sensor Networks).	Técnica	Realiza la encriptación a los nodos de bajos recursos en procesamiento, la cual, da las garantías de integridad, disponibilidad, pero no enfatiza con la confidencialidad, al recibir información esta viene con un valor HASH y si no, se encuentra con este valor, se descarta el paquete.
2	Tunelizado o “Tunneling”	Técnica	Los datos de comunicación se envían encapsulados utiliza un protocolo de red cifrada mediante un túnel, los routers eliminan las cabeceras IP públicas de paquete y devuelve el paquete original.

3	Implementación de Servicios Sobre IPv6.	Técnica	Mitiga los posibles ataques o problemas en el proceso de autenticación, integridad y confidencialidad de los usuarios locales o remotos a través de diversas redes con resultados de implementación confiable y segura.
4	OWASP	Metodología	Esta metodología realiza las funciones en aplicaciones web y a las seguridades que presentan para resguardar su seguridad, la función principal es el análisis de asistir a organizaciones evidencia las vulnerabilidades y riesgos que existirán.
5	CVSS 3.0	Metodología	Es un framework abierto y es utilizado para establecer métricas de comunicación de características, impacto y severidad de las vulnerabilidades que afectan los elementos de entorno de seguridad, esta proporciona un código abierto para estimar el impacto de una vulnerabilidad.

Fuente: Elaboración propia,2020.

La información del sector público por estar conectada directamente al gobierno y a la ciudadanía, se convierte en un bien público que la obligación es ser protegido, a esta información generada, se conservarían su confidencialidad, integridad y disponibilidad. Es de suma importancia la aplicación de la seguridad en la información pública y privada, puesto que así se podrá preservar y proteger ante las diferentes amenazas y situaciones que llegaran afectarla,

genera confianza en la ciudadanía y en las personas que proporcionan y/o usan este tipo de información, contribuye a mejorar la transparencia en el ejercicio de la administración pública de las entidades del Estado. La implementación de sistemas de gestión de seguridad de la información se hace importante dado que ayuda a preservar la seguridad y la privacidad de la información en el sector público y privado, previene así que la información sea utilizada en ambientes inseguros que la pondrán en riesgo frente amenazas, que desestabilizaran la continuidad de los procesos y el cumplimiento de objetivos en la gestión administrativa.

Es por ello por lo que las diferentes técnicas y metodologías fueron adoptadas por las empresas bajo a la necesidad y el escenario que sean utilizadas, a continuación, se hace una comparación de estas diferentes técnicas en las siguientes tablas.

Tabla 5. Ventajas y desventajas de la técnica de ingeniería social

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Técnica de Ingeniería Social	Capacitación al personal sobre seguridad informática e ingeniería social.	Poco entendimiento por partes de las personas mayores a 50 años.	Es aplicado en toda empresa a media y gran escala, da la seguridad a sus colaboradores.
	Es de costo menor.	Depender de una sola contraseña para ingresar a las diferentes cuentas.	
	Identificación a los posibles ingenieros sociales.	No tener identificado o conocer las herramientas instaladas en la maquinas.	
	Instalación de softwares y hardware a las máquinas de uso de los colaboradores.	No identificar los puertos abiertos que se encuentran en la infraestructura de red.	

	Bloqueo de redes sociales y medios de fácil ataque.		
	Bloqueo y seguridad de puertos en toda la infraestructura de red.		

Fuente: Elaboración propia, 2020.

Tabla 6. Ventajas y desventajas de la metodología ADM-TOGAF

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Metodología ADM-TOGAF	• Reducción de Costos. Al mejorar tiempos de mercado de proyectos TI, incrementa la calidad y mejorar funcionalmente las aplicaciones, el efecto es beneficioso en términos de costos.	Permite un nivel alto de personalización que a menudo alcanza a convertirse en un problema.	Desarrollado para una arquitectura empresarial que cumpla con las necesidades empresariales y de tecnología de la información de una organización
	• Reducción de Riesgos: Identifica los drivers y objetivos de negocio, así como los involucrados en los dominios de arquitectura, facilita la identificación de los riesgos y enfatiza en su mitigación.	La documentación tiene un lenguaje inadecuado que complica el entendimiento.	

	• Identificación de Oportunidades: Si, se aplica esta metodología, se alcanza a descubrir en cada escenario donde lo es aplicada oportunidades en el ámbito TI.	No tiene una especificación de meta-dato.	
	• Flexibilidad y Adaptación: La gestión de requisitos, centro de la metodología es la clave para flexibilizar proyectos sin perder en las arquitecturas diseñadas.	Una inadecuada clasificación de los artefactos no asegura la coherencia de la arquitectura.	
	• Lenguaje Común: La metodología da un amplio repositorio de documento y modelos que adoptan la visión de la empresa a los diferentes involucrados.	No cumple con la elaboración de un documento de especificación que describan los resultados de las fases.	
		No especifican quienes cumplirían los diferentes roles en las etapas del modelo.	

Fuente: Elaboración propia, 2020.

Tabla 7. Ventajas y desventajas de la metodología bajo la familia ISO/IEC-27000

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el medio.
Metodología bajo la familia ISO/IEC – 27000	Tiene una gran compatibilidad con la ISO 9000.	Se trata de una abstracción y un elevado nivel, por lo que no está muy detallado.	Para empresas de diferentes tamaños y sectores, colocaran en marcha prácticas y acciones para obtener la ISO 27000. En razón, la empresa grande, media o pequeña sea cual sea su tamaño o la rama de su actividad, será percibida de una forma distinguida debido la conquista del sello, emitido por una organización internacional de normalización.
	Trata todos los requisitos necesarios del Sistema de Gestión de Seguridad de la Información (SGSI).	Los requisitos parecerán difíciles de interpretar, porque existen nuevos conceptos.	
	Obedece los reglamentos relacionados con la protección de datos, privacidad y gestión de tecnología de la información, como es el caso de las entidades en el sector financiero o sector salud.	No, se hace mención del modelo PHVA (Planificar, Hacer, Verificar y Actuar).	
	Desde el punto de LGPD (Ley General de Protección de Datos), la ISO 27000 tiene un valor distinguido extra. Pues, prácticamente toda empresa trabaja con algún tipo de información confidencial (direcciones,	No, se menciona en ningún momento la política del Sistema de Gestión de Seguridad de la Información.	

	teléfonos, emails, números de documentos de identificación, datos bancarios).		
		No existe una descripción detallada a la hora de identificar los riesgos.	

Fuente: Elaboración propia, 2020.

Tabla 8. Ventajas y desventajas de la metodología MAGERIT

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Metodología MAGERIT	Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.	El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.	Fue creada para instituciones de gobierno, pero logra ser adoptada para grandes empresas
	Alcance completo en análisis y gestión de riesgos.	En su modelo no involucra los procesos, recursos, ni vulnerabilidades.	
	Es bien documentada en cuanto a recursos de información, amenazas y tipos de activos.	Posee falencias en el inventario de políticas.	

	Utiliza un completo análisis de riesgos cuantitativo y cualitativo.	Se considera una metodología costosa en su aplicación.	
	Es libre y no necesita autorización para su uso.		
	Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo.		
	Se centra en tres objetivos: concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrece en método sistemático para analizar tales riesgos, ayudar a describir y planificar las medidas oportunas para mantener los riesgos bajo control.		
	Preparar la organización para procesos de evaluación, auditoria, certificación o acreditación.		

	Permite que el proceso este bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riesgos efectiva.		
	Posee una buena base documental en tres libros: el método, catálogo de elementos y guía de técnicas, que son de acceso público.		
	Posee herramientas para el análisis de riesgos PILAR.		

Fuente: Elaboración propia, 2020.

Tabla 9. Ventajas y desventajas de la metodología CRAMM

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Metodología CRAMM.	Aplica los conceptos de manera formal, estructurada y disciplinada protegido los principios de seguridad y sus activos.	En su medo leo no tiene contemplados elementos como los procesos y los recursos.	Organizaciones públicas y privadas.
	Realiza un análisis de riesgos cualitativo y cuantitativo.	El costo para una compañía comercia es de 3.765 dólares más 1.143 dólares de mantenimiento.	

	Es aplicable a todo tipo de sistemas y redes de información y se logra utilizar en todas las etapas de ciclo de vida del sistema de información desde la planificación y viabilidad, por medio del desarrollo e implantación.	El costo para sector público es de 1.189 dólares más el consto de mantenimiento anual es de 1.143 dólares.	
	Se consigue usar siempre que sea necesario para identificar la seguridad y los requisitos de contingencia para un sistema de información o de la red.		
	Identifica y clasifica los activos de TI.		
	Evalúa el impacto empresarial.		
	Identifica y evalúa amenazas y vulnerabilidades, evalúa los niveles de riesgo e identidad los controles requeridos.		
	Compuesta por más de 4000 contramedidas reunidas en grupos y subgrupos con los mismos aspectos de seguridad, incluye activos de software y protecciones medioambientales.		

	Combina análisis y evaluación de riesgos.		

Fuente: Elaboración propia, 2020.

Tabla 10. Ventajas y desventajas de la técnica de encriptación en las redes WSN (Wireless Sensor Networks).

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Técnica de Encriptación en las Redes WSN (Wireless Sensor Networks).	Tiempo de vida	Alto consumo de energía y potencia.	Se aplica en muchos medios como:
	Una amplia cobertura.	Alta capacidad de memoria y recurso informáticos.	Militares
	Bajos costos y facilidad de la instalación.	Redes desentendidas, con alta probabilidad de fallo, lo cual, se desea aminorar con el monitoreo de estas.	Medioambientales
	Un corto tiempo de respuesta.		Aplicaciones médicas.
	Precisión y frecuencia de las mediciones.		Aplicaciones en hogares y edificios.
	Introducción de algoritmos criptográficos que proveen de seguridad y eficiencia a la red.		Aplicaciones industriales.
			Aplicaciones turísticas.

			Aplicaciones en desastres naturales.

Fuente: Elaboración propia, 2020.

Tabla 11. Ventajas y desventajas de las técnicas de tunelizado o "tunneling"

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Técnicas de Tunelizado o " Tunneling"	Permite solo el tráfico necesario para el acceso a los servicios públicos necesarios por los usuarios.	Problemas para resolver direcciones privadas con públicas.	Es aplicada para empresas pequeñas, medias y grandes empresas como seguridad.
	Alta velocidad y ancho de banda para los servicios relevantes dentro de la empresa.	No atraviesa firewalls a causa de que tiene problemas con la NAT.	
	Acceso irrestricto a servicios públicos, son amenazas de seguridad a la empresa.	Algunas aplicaciones son de pago.	
	Acceso restringido para precautelar la saturación de canales de comunicación, posibles ataques, robos de información, registro en black list y vaneo de IPs.	Exige mayor rendimiento del firewall por la configuración de la VPN.	
	Bajos costos de implementación.	No, se tiene hardware especializado en encriptación	

Fuente: Elaboración propia, 2020.

Tabla 12. Ventajas y desventajas de la técnica de seguridad en la implementación de servicios sobre IPv6

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Técnica de Seguridad en la Implementación de Servicios Sobre IPv6.	Es compatible con Server Windows 2008, Server Windows 2012 R2, Server Linux Debian, Server Ubuntu.	Soporte permanente.	Es implantado para grandes compañías o empresas para la migración de IPV6
	Soporta los parámetros de configuración de nivel de dificultad.	Es necesario una dirección IPv4 o algún tipo de NAT en los routers pasarela.	
	Soporta Ipsec.	Problemas restantes de arquitectura.	
	Soporta VPN.	Más difíciles de memorizar.	
	Autenticación clave compartida y certificado digital, RSA, DSA, PSK.	La mayoría de las redes son ipv4 entonces la implementación total de ipv6 sería muy costosa y tardaría mucho en implementarlas.	
	Confidencialidad entre 56 y 128 bits y soporta DES, AES.		
	Integridad MD5, SHA.		

Fuente: Elaboración propia, 2020.

Tabla 13. Ventaja y desventaja de la metodología OWASP

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Metodología OWASP	No es necesario una tecnología que lo soporte.	Consumo de mucho tiempo.	Es de código libre por, lo cual, es utilizado para todo tipo de empresa o emprendimiento.
	Es aplicada a una variedad de situaciones	No existe siempre material de soporte	
	Es muy flexible.	Requiere de un conocimiento humano y habilidades significantes para ser efectivos.	
	Promueve trabajar en equipo.	Se requiere desarrolladores de seguridad muy capacitados.	
	Es tempranamente en el clico de desarrollo de software.	Se logra perderse los problemas en librerías compiladas.	
	Es muy completo y efectivo en el código fuente.	No alcanza a detectar errores en modelo de ejecución	
	Rápido (para revisiones competentes)	El código fue publicado y da a diferir del que está es analizado.	
	Requiere un relativo nivel de conocimientos para la revisión de código fuente.		

	Existen muchos revisores de instrucción en aplicaciones web disponibles.		
	Prueba de código que está es expuesto en realidad.		

Fuente: Elaboración propia, 2020.

Tabla 14. Ventajas y desventajas de la metodología CVSS 3.0

Metodología / Técnica	Ventaja	Desventaja	Aplicación en el Medio.
Metodología CVSS 3.0	Puntuaciones estandarizadas de la vulnerabilidad: Las organizaciones estandarizan las puntuaciones de vulnerabilidad, y se reflejan en política que aprovecha de gestión, establecer la rapidez con la vulnerabilidad seria validad y remediada.	Poca información para la implementación de la metodología para empresas que quieren implementarse por primera vez.	Muchas organizaciones están utilizan CVSS, y cada una de ellas encuentran valor de diferentes maneras. A continuación, algunos ejemplos.
	Marco abierto: Dentro de la utilización del estándar CVSS, se proporciona usuarios de detalles sobre los parámetros usados en la generación de la puntualización de la vulnerabilidad analizada, permite comprender al	Muchos recursos informáticos para la implantación.	Proveedores de Boletines sobre Vulnerabilidades

	usuario el razonamiento que sustenta la puntuación.		
	Riesgo priorizado: Al establecer la puntuación de la vulnerabilidad, el estándar de CVSS permite detectar y conocer el riesgo de la vulnerabilidad con la solución, permite al usuario conocer la importancia de la vulnerabilidad en la relación con otra en su arquitectura, se identifica como riesgo bajo, medio y alto.	El costo varía depende a que escenario será implementado, los costos son elevados.	Proveedores del Software de Aplicación.
	Configuraciones específicas (complejidad de ataque)		Organizaciones de usuarios:
	La diferencia más significativa entre las versiones 3.0 y 3.1 de CVSS es un cambio en la definición de Attack Complexity, en la versión 3.0, Attack Complexity, se consideró si el sistema atacado solo podría explotarse si estaba en una determinada configuración. Si es así, la complejidad del ataque es alta. En la versión 3.1, si se requiere una configuración		Gestión y Escaneo de Vulnerabilidades.

	específica para que un ataque tenga éxito, se asume que el sistema atacado está en esa configuración a los efectos de la puntuación.		
			Investigaciones

Fuente: Elaboración propia, 2020.

3.3. Desarrollo del conjunto de las buenas prácticas con aplicaciones sobre las seguridades y garantizar la evidencia digital

Al realizar el análisis de los datos recolectados por la encuesta NESTOR, Se desarrolla el conjunto de las buenas prácticas bajo los 5 aspectos identificados previamente.

3.3.1. Infraestructura organizativa.

Se recomienda buenas prácticas en el ámbito de las políticas de preservación digital posibles utilizados dentro el marco organizativo de los objetivos definidos, condiciones legales y recursos disponibles financieros o físicos.

- *Crear un repositorio digital bajo las credenciales y la seguridad*.

El valor que tiene la evidencia digital es muy alto para resolver un evento de juicio, lo cual, organizarlo, recuperarlo, preservarlo y darle un mayor uso es muy necesario a corto o a largo plazo.

- *Crear unas políticas al repositorio que refleje una misión en la preservación digital a largo plazo.*

Crear compromisos de preservación y gestión de acceso de la información, elaborar un plan estratégico que defina el enfoque que tiene el repositorio que especifique el tipo de información a preservar, almacenar, administrar y proporcionar el acceso.

- *Establecer tareas y personal profesional en el repositorio de la evidencia digital.*

El repositorio identificará y establecerá tareas a realizar y tener disponible un número adecuado de personal para apoyar las funciones y los servicios bajo un desarrollo de programa que permita la personal desarrollar habilidades, destrezas y conocimientos.

- *Crear una herramienta en el repositorio que permita la transparencia, historial y rendición de cuentas de todas las acciones realizadas en un determinado tiempo.*

Establecer una herramienta, la cual despoje un historial documentado de los cambios en sus operaciones, procedimientos, software y hardware, y cada cierto tiempo una rendición de cuentas de todas las acciones que apoya así las operaciones y administración del repositorio que afectan la preservación de contenido digital en el tiempo.

- *Disponer funciones en el repositorio.*

Proporcionar funciones al repositorio para definir, recoger, rastrear y proporcionar información de integridad y comprometerse a un horario regular de auto elevación y certificación externa.

- *Establecer en el repositorio practicas financieras y procedimientos de transparencia.*

Disponer de procesos de planificación y presupuesto a corto y largo plazo, realizar prácticas financieras y procedimientos que son transparentes cumple con normas de contabilidad y auditoría por terceros conforme a los requisitos legales territoriales, también, realizar un repositorio de procesos continuos para analizar e informar sobre riesgos financieros, beneficios, inversión y gastos

- *Disponer en el repositorio de contratos apropiados o acuerdos para rastrear y administrar los derechos de propiedad intelectual.*

Disponer de contratos apropiados o acuerdos para materiales digitales que administra, preserva y a los que proporciona el acceso, también, disponer un rastreo y administración a los derechos de propiedad intelectual y disponer restricciones sobre el uso del contenido del repositorio según lo requerido por el contrato de depósito o licencia.

- *Establecer procedimientos de identificación de contenido y propiedades de la información.*

El repositorio tendrá que disponer de procedimientos para identificar la información de contenido y las propiedades de la información que la preservará, dar especificaciones y

disposición de la información que necesita para ser asociado con contenido especifico de la información en el momento del depósito.

3.3.2. Administración de objetos digitales.

Se verifica si las políticas de aplicación de técnicas o modelos de preservación digital analizan los objetivos, estrategias y alcance para especificar si todos los requisitos relacionados con la gestión de objetos digitales durante el ciclo de vida se cumplen.

- *Disponer de control y registros de objetos digitales.*

El repositorio tiene que disponer de registros contemporáneos de acciones y procesos de administración que sean relevantes para la adquisición de contenidos, también, disponer de un control suficiente sobre los objetos digitales para la preservación de la evidencia digital.

- *Descripcion y construcción de AIP (paquete de información del archivo)*.

Tendrían que disponer para cada AIP (paquete de información del archivo) o clases de AIPS preservada, una definición y construcción asociada que sea adecuada para el análisis y que sea apto para las necesidades de conservación a largo plazo.

- *El repositorio tendrá acceso a herramientas y estándares persistentes para los AIPS.*

Disponer de acceso a las herramientas necesarias y los recursos para proporcionar información de presentación autorizada para los objetos digitales que contiene en el repositorio, utilizar estándares que genera identificadores persistentes y únicas para todos los AIPS.

- *Asegurar, verificar, proporcionar independencia en los repositorios.*

El repositorio asegurará que la información del contenido de las AIPS sea comprensible para la comunidad designada al momento de la creación, dar integridad y exactitud para cada AIP, proporcionar un mecanismo independiente para verificar la integridad de la colección del repositorio.

- *Disponer mecanismos de monitorio en el entorno de preservación.*

Se tendrá que implementar estrategias de documentación de preservación correspondiente a los participantes, mostrar la efectividad de sus actividades de preservación.

- *Almacenamiento y preservación de las AIPS (paquete de información del archivo).*

Disponer de especificaciones para que las AIPS, se almacenen hasta el nivel de bits con registros contemporáneos de acciones y procesos de administración que son relevantes para el almacenamiento y preservación de las AIPS.

Especificar los requisitos de información minia para permitir a la comunidad designada a descubrir e identificar los materiales de interés.

3.3.3. Gestión de riesgos de infraestructura y seguridad.

Se propone el análisis de los aspectos técnicos de seguridad del sistema en general, da como una prioridad dar una solución y resolver un ataque a la vulnerabilidad de la evidencia digital.

- *Disponer suficiente hardware y software de soporte para el repositorio.*

El repositorio tendrá mecanismos eficaces para detectar la pérdida o corrupción de bit y de disponer de hardware y software de soporte para la copia de seguridad del contenido del repositorio y seguimiento de las funciones del repositorio, define procesos de cambio de medio de almacenamiento como refrescar y migrar los datos.

- *El repositorio tendrá el compromiso de permitir, reaccionar, identificar procesos.*

Se permitirá que el repositorio registrara y reaccionara a la disponibilidad de nuevas actualizaciones de seguridad basadas en la evolución del riesgo / beneficio, identificar y documentar los procesos críticos que afectan su capacidad para cumplir con sus responsabilidades obligatorias.

- *Disponer de análisis de factores de riesgo de seguridad.*

El repositorio permitirá gestionar la ubicación de copias de todos los objetos digitales, dispone de un análisis sistemático de los factores de riesgo de seguridad asicados con datos, sistemas, personal y planta física.

- *Definir roles, responsabilidades y autorización al personal del repositorio.*

Implementar controles para responder adecuadamente a cada uno de los riesgos de seguridad definidos, el personal que maneja el repositorio tendrá definido los roles, responsabilidades y autorizaciones relacionadas con el implemento de cambios del sistema da una adecuación una

preparación escrita y planes de recuperación, incluye al menos una copia de seguridad de la información preservada junto con una copia de los planes de recuperación.

3.3.4. Aspectos de gestión de la integridad de las instituciones de investigación penal.

Se recomienda los análisis legales para los repositorios de la evidencia digital que cumplan con las disposiciones bajo a la ley existentes en el escenario donde se va a aplicar.

- *Establecer un documento legal para la preservación*

Establecer un documento autorizado legal que dispone la preservación de la evidencia, controlar que la evidencia cumpla las disposiciones legales para la preservación.

- *Tener en el repositorio un control de ingreso y acceso a la evidencia*

El repositorio permitirá el nombre de la autorización del documento con el usuario autorizado, determinar el o varios usuarios permitidos para el ingreso y acceso a la evidencia da el control de uso del aplicativo con un registro de usuarios autorizados.

El repositorio emitirá una alerta de seguridad al intentar acceder a la evidencia no permitida.

- *Añadir un sistema de verificación de la evidencia.*

El sistema del repositorio dispondrá de un mecanismo de verificación de la evidencia ingresada, como una forma de backup el sistema realice una copia de la información adicional relacionada con el contenido de la evidencia solicita la verificación antes de ejecutar el proceso de preservación.

- *Añadir un sistema de incremento de evidencia.*

El repositorio contará con un sistema que permite incrementar la evidencia a un caso específico, da un listado del ingreso de la evidencia cronológicamente organizada. El sistema del repositorio permitirá almacenar la herramienta de creación, de recogida y de preservación de la evidencia.

- *Emisión de reportes de la evidencia a preservar.*

Establecer en el sistema del repositorio la emisión de reportes de los metadatos de le evidencia a preservar, el sistema emitirá reportes de los procesos y actividades de la preservación de la evidencia dentro del repositorio.

- *Disponer mecanismo de verificación de integridad de la evidencia.*

El sistema del repositorio realiza un reporte de ubicación de la evidencia original y de las copias realizadas que mantiene el sistema, realizar un mecanismo de verificación de integridad de la evidencia bajo el código Hash.

- *Emisión de alertas en el repositorio.*

El repositorio emitirá alertas de seguridad, errores de operación, de cumplimiento de políticas de preservación, de cumplimento del tiempo de preservación, permite la definición del tiempo y modificación de preservación de la evidencia.

CONCLUSIONES

- La realización del estudio de la situación actual, en investigaciones relacionadas con la aplicación de técnicas de seguridad, en redes de comunicaciones aplicadas a la adecuada custodia de evidencia digital, permitió conocer las diferentes metodologías y técnicas, e identificar la situación actual de las instituciones criminales que no utilizan una metodología o una técnica adecuada para preservar la evidencia digital, esto apertura a la vulnerabilidad de la evidencia digital.
- La realización del estudio comparativo de las diferentes metodologías de seguridad aplicadas, en las redes de comunicaciones que garantiza, la adecuada custodia de evidencia digital, determinó que las metodologías y técnicas encontradas para la seguridad aplicadas a las redes de comunicación, la más adecuadas es la metodología bajo la familia ISO/IEC – 27000, puesto que es compatible con toda con la ISO 9000 y lo más importante que cada norma tiene reservado un numero dentro de una serie que van desde 27000 hasta la 27019 y de 27030 a 27044, cada una tiene las certificaciones de toda la familia que permite establecer las estrategias y controles que dan seguridad a una permanente protección y salvaguardia de la información bajo los beneficios de múltiples mejoras, gestión de comunidad, reducción de riesgos y conformidad con la legislación.
- Los actores principales en el manejo de la custodia de la evidencia digital no cuentan con los conocimientos y las técnicas o metodologías adecuadas para la preservación de la evidencia digital, da como una vulnerabilidad muy abierta para los ciberdelincuentes al acceso a la información, de igual forma cabe mencionar que las instituciones de gobierno no brindan un espacio de capacitación o de recursos notables eficientes para tener un repositorio virtual para la evidencia digital, obtiene como resultado una gran vulnerabilidad para la evidencia digital ante los atacantes, pierde así la admisibilidad antes de llegar a la autoridad juzgadora.
- La propuesta del conjunto de buenas prácticas, con la aplicación de técnicas adecuadas sobre redes de comunicaciones, que garantizan la custodia de la evidencia digital en la provincia de Chimborazo, permite concluir que la Infraestructura Organizativa abarca como una de las más importantes dentro los 4 aspectos mencionados debido a que se

rige en el ámbito de las políticas de preservación digital posible utilizados dentro del marco organizativo de los objetos definidos, condiciones legales y recursos disponibles, financieros o físicos de la organización o institución donde se desee implementar.

- El diagnóstico realizado por medio de la encuesta NESTOR, concluye que los actores principales que manejan la custodia de la evidencia digital del Consejo de la Judicatura de la provincia de Chimborazo muestra una importancia muy baja para los procesos de preservación y admisibilidad de la evidencia, esto corresponde a la disponibilidad de recursos, formación personal o ignorancia de la ley, en sí, se trata de datos que muestra que existe un tratamiento inadecuado de la información digital, por lo tanto, esto tomaría una alta posibilidad de que a corto o a largo plazo la información se inaccesible.

RECOMENDACIONES

- Aplicar las buenas prácticas detalladas en esta investigación bajo a la necesidad y escenario donde se encuentre la institución o usuario que maneja la custodia de la evidencia digital.
- Es muy importante realizar más investigaciones sobre la preservación de la evidencia digital para tener una segunda o varias guías para la preservación y admisibilidad de la evidencia digital, en conjunto con el avance de la tecnología y las nuevas formas de ingesta de la evidencia digital.
- Realizar amplias investigaciones sobre la admisibilidad de la evidencia digital a corto y a largo plazo da énfasis a los repositorios en la nube, tecnología que en el trascurso de los días son más utilizados y a la vez muy vulnerables por los ciberdelincuentes.

BIBLIOGRAFÍA

Acurio, S. (2016). *Evidencia Digital en el Proceso Judicial* [Diapositivas]. http://www.oas.org/en/information_center/default.asp. https://www.sites.oas.org/cyber/Documents/2016%20%20Evidencia%20Digital%20en%20el%20Proceso%20Judicial-Santiago%20Acurio.pdf

Acurio, S. (2017, octubre). *Introducción a la Informática For*. http://www.criptored.upm.es/guiateoria/gt_m592b.htm. http://www.criptored.upm.es/guiateoria/gt_m592b.htm

Aishwarya Lakshmi, K., Honnavali, P. B., & Rajashree, S. (2020). Ensure the validity of forensic evidence by using a hash function. *Lecture Notes in Networks and Systems*, 341-346. https://doi.org/10.1007/978-981-15-7345-3_28

Amato, F., Cozzolino, G., Moscato, V., & Moscato, F. (2019). Analyse digital forensic evidences through a semantic-based methodology and NLP techniques. *Future Generation Computer Systems*, 297-307. https://doi.org/10.1016/j.future.2019.02.040

Antwi-Boasiako, A., & Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. *Advances in Digital Forensics XIII*, 23-38. https://doi.org/10.1007/978-3-319-67208-3_2

ARCOTEL. (2002). *2002-67 Ley de Comercio Electrónico, Firmas y Mensajes de Datos | Ecuador - Guía Oficial de Trámites y Servicios*. https://www.gob.ec/regulaciones/2002-67-ley-comercio-electronico-firmas-mensajes-datos.

https://www.gob.ec/regulaciones/2002-67-ley-comercio-electronico-firmas-mensajes-datos

Asamblea Nacional del Ecuador. (2014, 10 febrero). *CÓDIGO ORGÁNICO INTEGRAL PENAL*. https://tbinternet.ohchr.org/. https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Bareño Gutierrez, R., Navarro Núñez, W., Cárdenas Urrea, S., Sarmiento Osorio, H., & Duarte Acosta, N. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *INGE CUC*, *12*(1), 86-93. https://doi.org/10.17981/ingecuc.12.1.2016.09

Bórquez V, P. (2011). Importancia de la cadena de custodia de evidencias. *Revista médica de Chile*, *139*(6), 820-821. https://doi.org/10.4067/s0034-98872011000600020

Carrasco, J. (2017). *La inadmisibilidad como forma de invalidez de las actuaciones de parte y de terceros técnicos en el Código de Procedimiento Civil*. https://www.redalyc.org/. https://www.redalyc.org/jatsRepo/197/19758807013/index.html

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional |. (s. f.). COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. https://uncitral.un.org/es

Consejo de la Judicatura | Consejo de la Judicatura. (s. f.). https://www.funcionjudicial.gob.ec/. https://www.funcionjudicial.gob.ec/index.php/es/inicio.html

Contero, W. M. (2019, marzo). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR*. https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf. https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Cordero, G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información*. http://dspace.uazuay.edu.ec/. http://polux.unipiloto.edu.co:8080/00000744.pdf

Corrado. (2019, 8 marzo). *Bringing Content into the Picture: Proposing a Tri-Partite Model for Digital Preservation*. Biblioteconomía. http://blog.bne.es/biblioteconomia/2018/03/07/bringing-content-picture-proposing-tri-partite-model-digital-preservation/

Delgado, J. (2020). *Análisis de seguridad mediante la metodología OWASP a redes inalámbricas en «Universidad laica Eloy Alfaro de Manabí extension el Carmen»"*. https://repositorio.uleam.edu.ec. https://repositorio.uleam.edu.ec/bitstream/123456789/2068/1/ULEAM-INFOR-0044.pdf

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis*

y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Ministerio de Hacienda y Administraciones Públicas, España. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Esparza, D. E. I., Diaz, F. J., Echeverria, T. K. S., Hidrobo, S. R. A., Villavicencio, D. A. L., & Ordonez, A. R. (2020). Information security issues in educational institutions. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1. https://doi.org/10.23919/cisti49556.2020.9141014

Estupiñan, A. D. C. A. (2013, 25 noviembre). *Análisis de riesgos en seguridad de la información | Ciencia, Innovación y Tecnología*. https://www.jdc.edu.co/revistas/index.php/rciyt/index. https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121

Estupiñan Londoño, T. V., Mora Merchán, K. T., & Santiago, C. (2019). Importancia de la Forensia en Redes para la Recopilación de Evidencia Digital. *Proceedings of the 17th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Industry, Innovation, and Infrastructure for Sustainable Cities and Communities"*, 1. https://doi.org/10.18687/laccei2019.1.1.479

Estupiñan Londoño, T. V., Mora Merchán, K. T., & Santiago Cely, C. P. (2019). Importancia de la Memoria como Evidencia Digital en la Informática Forense. *Proceedings of the 17th LACCEI International Multi-Conference for Engineering, Education, and*

Technology: "Industry, Innovation, and Infrastructure for Sustainable Cities and Communities", 1. https://doi.org/10.18687/laccei2019.1.1.477

Ferreira, M. (2006). *Introdução à preservação digital – Conceitos, estratégias e actuais consensos*. Escola de Engenharia da Universidade do Minho.

FM Granja y GD Rodríguez Rafael, "Preservación de evidencia digital: Aplicación en la investigación criminal", *Conferencia de Ciencia e Información (SAI)* 2015, Londres, Reino Unido, 2015, págs. 1284-1292, doi: 10.1109 / SAI.2015.7237309.

Gopalakrishnan, A., Vineti, E., Mohan, A. K., & Sethumadhavan, M. (2018). The Art of Piecewise Hashing: A step toward better evidence provability. *Journal of Cyber Security and Mobility*, 109-130. https://doi.org/10.13052/jcsm2245-1439.719

Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1. https://doi.org/10.1504/ijesdf.2017.081749

Granja, F. M., Rafael, G. D. R., Cabezas, E., & Lozada, R. Y. (2019). Implementation of the PREDECI model in the prosecution of Chimborazo in Ecuador: a case study evaluation. *International Journal of Electronic Security and Digital Forensics*, *11*(1), 29. https://doi.org/10.1504/ijesdf.2019.096526

Granja, M. F. T. (2019, 6 abril). *Repositorio Digital UNACH: Aplicación de un Modelo de Preservación Digital para Garantizar la Integridad al Largo Plazo de la Información*

de Archivos del GADM-Riobamba. http://dspace.unach.edu.ec/handle/51000/5577. http://dspace.unach.edu.ec/handle/51000/5577

Huang, L. (2020). Computer network security hazards and preventive strategies. *Advances in Intelligent Systems and Computing*, 180-185. https://doi.org/10.1007/978-3-030-53980-1_27

Jaramillo, H., Cabrera, S., Abad, E., Torres, V., & Verdúm, J. (2015). Definition of Cybersecurity Businness Framework based on ADM-TOGAF. *2015 X Congreso Ibérico de Sistemas y Tecnologías de la Información (CISTI)*, 1. https://doi.org/10.1109/CISTI.2015.7170391

Jiang, B. (2020). Computer Security Vulnerabilities and Preventive Measures. *Advances in Intelligent Systems and Computing*, 752-759. https://doi.org/10.1007/978-3-030-51431-0_109

Juillard, G. (2009). *Ley del Sistema Nacional de Archivos*. https://www.quito.gob.ec/. https://www.quito.gob.ec/lotaip2011/a2/Ley_del_Sistema_Nacional_de_Archivos.pdf

Kebande, V. R., Baror, S. O., Parizi, R. M., Choo, K.-K. R., & Venter, H. S. (2020). Mapping digital forensic application requirement specification to an international standard. *Forensic Science International: Reports*, *2*, 100137. https://doi.org/10.1016/j.fsir.2020.100137

Lazareva, V. A., Kakhkhorov, D. G., & Shinkaruk, V. V. (2020). Digitalization of criminal procedure as a development factor of its competition and competitiveness. *Springer*, 475-482. https://doi.org/10.1007/978-3-030-45913-0_56

Magán-Carrión, R. (2020, 22 octubre). *Líneas de defensa y seguridad en redes ad hoc: un estudio sistemático.* https://rodin.uca.es/. https://rodin.uca.es/xmlui/handle/10498/23796

Manual de Manejo de Evidencias Digitales y Entornos Informáticos. (2009, diciembre). http://www.criptored.upm.es/guiateoria/gt_m592e.htm. http://www.criptored.upm.es/guiateoria/gt_m592e.htm

Martínez, C. L. M. (2019, 28 septiembre). *RUA: Red de comunicaciones para una entidad con 2 centros de cálculo y 200 sedes*. https://www.ua.es/. http://rua.ua.es/dspace/handle/10045/96688

Mison, A., Davies, G., & Eden, P. (2020). The future direction of cybercrime and the difficulties of digital investigations: A rationale for a review of digital investigation specialist education. *SCOPUS*, 1. https://doi.org/10.34190/EWS.20.095

Molina, F. T., Santillán, J. C., Luna, W. G., & Lozada, R. M. (2020). *Predeci - Modelo de preservación de evidencia digital*. Cidepro Editorial. https://doi.org/10.29018/978-9942-823-46-5

Molina Granja, F. T., Santillán Lima, J. C., Luna Encalada, W., Lozada Yañez, R., & Guaiña Yungán, J. (2019). Preservación digital y la admisibilidad de las evidencias. *Ciencia Digital*, *3*(1.1), 118-130. https://doi.org/10.33262/cienciadigital.v3i1.1.364

Molina-Granja, F. (2018). The Digital Preservation in Chimborazo: A Pending Responsibility. *Advances in Intelligent Systems and Computing*, 116-126. https://doi.org/10.1007/978-3-030-02828-2_9

Molina-Granja, F., Rodríguez Rafael, G. D., Luna, W., Lozada-Yanez, R., Vásconez, F., Santillan-Lima, J., Guerrero, K., & Rocha, C. (2018). PREDECI Model: An Implementation Guide. *Advances in Intelligent Systems and Computing*, 1196-1211. https://doi.org/10.1007/978-3-030-01177-2_86

NESTOR. (2006). *Catálogo de criterios para repositorios digitales confiables*. https://www.researchgate.net/. https://www.researchgate.net/publication/265851813_Catalogue_of_Criteria_for_Trusted_Digital_Repositories

Perona, E. (2016, 10 febrero). *Análisis Forense. Cadena de Custodia de la evidencia digital*. Security Art Work. https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/

Poblete, C. J. (2017, 28 marzo). *The inadmissibility as a form of invalidity of legal acts emanating from the parties and third parties*. https://scielo.conicyt.cl/scielo.php?lng=es. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122018000100497&lng=en&nrm=iso&tlng=en

Recio, M. J. (2012, septiembre). *De la seguridad informática a la seguridad de la información*. https://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128. https://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128

Roatta, S., Casco, M. E., & Fogliato, M. (2017). El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. *sedici.unlp.edu.ar*, 2. http://sedici.unlp.edu.ar/bitstream/handle/10915/46243/Documento_completo.pdf?sequence=1&isAllowed=y

Rodríguez, J. (2020). *Protocolos de red*. https://sites.google.com/site/maestrojuanrodriguezlara/semestre-enero-julio-2012/01-int-redes. https://sites.google.com/site/maestrojuanrodriguezlara/semestre-enero-julio-2012/01-int-redes/004-proyecto-de-investigacion/23---protocolos-de-red

Sánchez, F., Vivero, J., & Baroja, D. (2018). Aplicación de una metodología de seguridad avanzada en redes inalámbricas. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 24-38. http://www.risti.xyz/issues/ristie15.pdf

Santillán-Lima, J., Rocha-Jacome, C., Guerrero-Morejón, K., Llanga-Vargas, A., & Vásconez-Barrera, F. (2017). EL IMPACTO DE LOS SERVICIOS DE TELECOMUNICACIONES Y LAS TICS EN LAS NECESIDADES DE LA EDUCACIÓN SUPERIOR. *IV Congreso Internacional de Ciencia Tecnología*

Innovación y Emprendimiento CITE 2017, *4*, 1. https://scholar.google.com/scholar?cluster=16536690886512763078&hl=en&oi=scholarr

Singhal, A., Lui, C., & Wijesekera, D. (2015). A logic based network forensics model for evidence analysis. *Proceedings of the ACM Conference on Computer and Communications Security*, 1677. https://doi.org/10.1145/2810103.2810106

UNCITRAL. (1966). *Comisión de las Naciones Unidas para el Derecho Mercantil Internacional* |. https://uncitral.un.org/es. https://uncitral.un.org/es

Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 73-88. https://dialnet.unirioja.es/servlet/articulo?codigo=6672188

Valencia, L., Guarda, T., Luna, G., & Ninahualpa, G. (2019). Seguridad de la Información en WSN aplicada a Redes de Medición Inteligentes basado en técnicas de criptografía. *Revista Ibérica de Sistemas e Tecnologías de Información*, 393-406. https://media.proquest.com/media/hms/PFT/1/mKDZ8?_s=ANJNDdoDr3quF59jrO%2BQ2mkyV%2BE%3D

Vásconez, F., Molina, F., Santillan-Lima, J., Cabezas, E., & Gálvez, A. (2017, agosto). *AUDITORIA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO "FERNANDO DAQUILEMA", APLICANDO EL MARCO DE TRABAJO COBIT* (4.ª ed., Vol. 4). Escuela Superior Politécnica de Chimborazo.

Yupanqui, J. R. A., & Oré, S. B. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *25*, 112-134. https://doi.org/10.17013/risti.25.112-134

ANEXO 1

Preguntas de la encuesta NESTOR

Tipo de institución

- ○ Publica
- ○ Privada

Cargo que desempeña

- ○ Juez
- ○ Fiscal
- ○ Perito
- ○ Custodio
- ○ Técnico de sistemas de la función judicial

Fecha de encuesta

Fecha

dd/mm/aaaa

Posee un repositorio (lugar donde se guarda o almacena la información) digital o físico

- ☐ Digital
- ☐ Físico

¿El repositorio tiene una misión que refleja un compromiso con la preservación gestión y acceso a la información digital en el largo plazo?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone un plan estratégico de preservación que define el enfoque que tiene el repositorio en el apoyo a largo plazo de su misión?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de una política de colección u otro documento que especifica el tipo de información a preservar, almacenar, administrar y proporcionar acceso?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene identificado y establecido las tareas que debe realizar?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone del número adecuado de personal para apoyar todas las funciones y servicios?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene un programa de desarrollo profesional que ofrece personal desarrollar habilidades y conocimientos?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio ha definido su comunidad y tiene definiciones apropiadamente accesibles?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de políticas de preservación propias para cumplir su Plan estratégico de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de un historial documentado de los cambios en sus operaciones, procedimientos, software y hardware?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de herramientas de transparencia y rendición de cuentas en todas las acciones apoyando la operación y administración del repositorio que afectan la preservación de contenido digital en el tiempo?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de funciones para definir, recoger, rastrear y proporcionar información de integridad?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de funciones para comprometerse a un horario regular de autoevaluación y certificación externa?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de procesos de planificación y presupuesto a corto y largo plazo?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone información sobre prácticas financieras y procedimientos que son transparentes, cumple con las normas de contabilidad y permite ser auditados por terceros conforme a los requisitos legales territoriales?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene un proceso continuo para analizar e informar sobre riesgos financieros, beneficios, inversión y gastos (incluyendo licencias, activos y pasivos)?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de contratos apropiados o acuerdos para materiales digitales que administra, preserva, o a los que proporciona acceso?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone rastrear y administrar los derechos de propiedad intelectual y dispone restricciones sobre el uso del contenido del repositorio según lo requerido por el contrato de depósito o licencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de un procedimiento para identificar la información de contenido y las propiedades de la información que preservará el repositorio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone específica y claramente la información que necesita para ser asociado con contenido específico de la información en el momento de su depósito?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de las especificaciones adecuadas que permiten el reconocimiento y análisis de los SIP?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de mecanismos para verificar adecuadamente la identidad del productor de todos los materiales?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de un control suficiente sobre los objetos digitales para preservarlos?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de registros contemporáneos de acciones y procesos de administración que son relevantes para la adquisición de contenidos?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene para cada AIP (paquete de información del archivo) o clase de AIPs preservada por el repositorio una definición asociada que es adecuada para el análisis de la AIP y apto para necesidades de conservación a largo plazo?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de una descripción de cómo se construyen AIPs?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone documentar la disposición final de todos los DIP's?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene y utiliza una estándar que genera identificadores persistentes, únicos para todos AIPs?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene acceso a las herramientas necesarias y los recursos para proporcionar información de representación autorizada para todos los objetos digitales que contiene?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio ha documentado los procesos para adquirir información de descripción de preservación (PDI) por su contenido e información asociada?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio se asegura de que la información de contenido de las AIPs es comprensible para su comunidad designada en el momento de la creación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio verifica cada AIP para integridad y exactitud en el momento que se crea?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio proporciona un mecanismo independiente para verificar la integridad de la colección/contenido del repositorio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio ha documentado estrategias de preservación correspondientes a sus participaciones?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de mecanismos para monitorear el entorno de su preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone proporcionar evidencia de la efectividad de sus actividades de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de las especificaciones de cómo las AIPs se almacenan hasta el nivel de bits?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de registros contemporáneos de acciones y procesos de administración que son relevantes para el almacenamiento y preservación de las AIPs?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio especifica los requisitos de información mínima para permitir a la comunidad designada descubrir e identificar los materiales de interés?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio permite crear información descriptiva y asegurar de que está asociada con el AIP?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de vínculos bidireccionales entre cada AIP y su información descriptiva?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio verifica el cumplimiento de las directivas de acceso?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone seguir las políticas y procedimientos que permiten la difusión de objetos digitales que son trazables a los originales, con evidencias que apoyen su autenticidad?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio emplea tecnología de notificación de vigilancia tecnológica?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de suficiente hardware y software de soporte para la de copia de seguridad del contenido del repositorio y seguimiento de las funciones del repositorio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de mecanismos eficaces para detectar la pérdida o corrupción de bit?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de suficiente hardware y software de soporte para la de copia de seguridad del contenido del repositorio y seguimiento de las funciones del repositorio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de mecanismos eficaces para detectar la pérdida o corrupción de bit?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio permite registrar y reaccionar a la disponibilidad de nuevas actualizaciones de seguridad basada en una evaluación del riesgo / beneficio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio ha definido procesos de cambio de medio de almacenamiento (por ejemplo, refrescar, migrar)?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene identificado y documentado los procesos críticos que afectan su capacidad para cumplir con sus responsabilidades obligatorias?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio permite gestionar el número y la ubicación de copias de todos los objetos digitales?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio dispone de un análisis sistemático de los factores de riesgo de seguridad asociados con datos, sistemas, personal y planta física?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene implementado controles para responder adecuadamente a cada uno de los riesgos de seguridad definidos?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El personal del repositorio tiene definido roles, responsabilidades y autorizaciones relacionadas con implementar cambios dentro del sistema?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio tiene adecuada preparación escrita y planes de recuperación, incluyendo al menos una copia de seguridad de toda la información preservada junto con una copia de los planes de recuperación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El repositorio controla que la evidencia cumpla la disposición legal para la preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿Existe un documento legal que dispone la preservación de la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿Se permite almacenar el documento de autorización?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿Permite validar el nombre de la autorización del documento con el usuario autorizado en el repositorio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

Permite determinar el o los usuarios permitidos para el ingreso y acceso a la evidencia.

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿Existe control de uso del aplicativo, con el debido registro de usuario autorizado?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿Emite una alerta de seguridad al intentar acceder a evidencia no permitida?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema dispone de un mecanismo de verificación de la evidencia ingresada?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema guarda información adicional relacionada con el contenido de la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema solicita verificación de la evidencia a preservar antes de ejecutar el proceso de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite incrementar evidencia a un caso específico?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema mantiene un listado del ingreso de la evidencia cronológicamente organizada?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite preservar datos técnicos y descriptivos adicionales sobre el entorno de adquisición de la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite almacenar la herramienta de creación, de recogida y de preservación de la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite un reporte de los metadatos de la evidencia a preservar?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite un reporte del proceso de preservación de la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema genera un reporte de la actividad de la evidencia dentro del repositorio?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite acceder a la evidencia y a las herramientas vinculadas para su recreación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite un reporte sobre el entorno hardware en el que fue generada a evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema reporta la ubicación de la evidencia original y de las copias que mantiene el sistema?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

El sistema tiene un mecanismo de verificación de integridad de la evidencia (código hash)

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema reporta actividad sobre los objetos digitales preservados?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite dirigir el almacenamiento de la información a preservar?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite acceder a evidencia almacenada en otros repositorios vinculados?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema mantiene un listado de términos utilizados en el aplicativo?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite acceder a las definiciones e interpretaciones de los términos?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite incrementar la interpretación de términos?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite alertas de seguridad?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite alertas de errores de operación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite alertas de cumplimiento de políticas de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite definir el tiempo de preservación de la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite una alerta de cumplimiento del tiempo de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite modificar el tiempo de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema permite una verificación de la técnica de preservación aplicada a la evidencia?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema genera una certificación de garantía de proceso de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema mantiene un monitoreo del acceso a la evidencia durante el periodo de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El sistema emite un reporte periódico de la actividad sobre una evidencia o caso durante el periodo de preservación?

	1	2	3	
Cumple Totalmente	○	○	○	No Cumple

¿El usar técnicas de seguridad de la transmisión al subir un archivo de evidencia digital en la nube, en este caso específico, usted considera que la admisibilidad se elevaría o disminuiría?

- ◯ Se eleva la admisibilidad
- ◯ Contribuye parcialmente
- ◯ Disminuye la admisibilidad

¿El usar técnicas de seguridad de la transmisión al descargar o visualizar un archivo de evidencia digital en la nube, en este caso específico, usted considera que la admisibilidad se elevaría o disminuiría?

- ◯ Se eleva la admisibilidad
- ◯ Contribuye parcialmente
- ◯ Disminuye la admisibilidad

¿Al usa un aplicativo que cumpla las características mencionadas con anterioridad para preservación de la evidencia digital, en este caso específico, usted considera que la admisibilidad se elevaría o disminuiría?

- ◯ Se eleva la admisibilidad
- ◯ Contribuye parcialmente
- ◯ Disminuye la admisibilidad