Ciencia Digital
www.cienciadigital.org

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

Preservación digital y la admisibilidad de las evidencias

Digital preservation and the admissibility of the evidence

Fernando Tiberio Molina Granja[1], Juan Carlos Santillán Lima[2],Washington Luna-Encalada [3] , Raúl Lozada-Yañez[4] & Jonny Guaiña-Yungán [5]

Recibido: 10-02-2019 / Revisado: 15-02-209 /Aceptado: 04-03-2019/ Publicado: 14-06-2019

Abstract. **DOI:** https://doi.org/10.33262/cienciadigital.v3i1.1.364

Currently, every institution generates digital information that by legal mandate, by social responsibility, cultural and historical value should be preserved in the long term by means of techniques, methods or appropriate models that allow a technical way to have digital information accessible and informationally useful in a near and far way. In the world and in Ecuador there is a legal basis that motivates and demands that this responsibility be fulfilled, as well as several models of digital preservation. This research intends to know if it improves the level of admissibility of the evidence applying PREDECI, applying a globally validated survey to a criminal investigation institution of Riobamba, by means of an application based on PREDECI. After a statistical analysis it is determined that there is a high percentage of improvement in the necessary aspects of admissibility of the evidence that would guarantee a greater admissibility of the digital evidence in the court.

Keywords: Predeci, digital preservation, digital evidence, admissibility

Resumen.
Actualmente, toda institución genera información digital que, por mandato legal, por responsabilidad social, por valor cultural e histórico debe ser preservada en el largo

[1] Universidad Nacional de Chimborazo, Ecuador. Correo-e: fmolina@unach.edu.ec
[2] Universidad Estatal de Bolivar, Ecuador. Correo-e : juankasl@outlook.com
[3] Escuela Superior Politécnica de Chimborazo. Ecuador. Correo-e: wluna@espoch.edu.ec
[4] Escuela Superior Politécnica de Chimborazo. Ecuador. Correo-e: rlozada@espoch.edu.ec
[5] Escuela Superior Politécnica de Chimborazo. Ecuador. Correo-e: jguaina@espoch.edu.ec

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

plazo mediante técnicas, métodos o modelos adecuados, que permitan de una manera técnica disponer de la información digital accesible e informacionalmente útil en un futro cercano y lejano. En el mundo y en Ecuador existe la base legal que motiva y exige se cumpla esta responsabilidad, así también existen varios modelos de preservación digital. Esta investigación pretende conocer si mejora el nivel de admisibilidad de la evidencia aplicando PREDECI, aplicando una encuesta validada mundialmente a una institución de investigación criminal de Riobamba, por medio de un aplicativo basado en PREDECI. Luego de un análisis estadístico se determina que existe un alto porcentaje de mejora en los aspectos necesarios de admisibilidad de la evidencia que garantizarían una mayor admisibilidad de la evidencia digital en la corte.

Palabras claves: Predeci, preservación digital, evidencia digital, admisibilidad

Introducción.

Actualmente todo dispositivo digital es capaz de generar información que personal o institucional que puede convertirse en evidencia en caso de presentarse un incidente de seguridad. Esta evidencia es útil para investigar casos relacionados con actividades cibercriminales o de ataques informáticos, el problema es que muchas veces la recolección, el manejo y análisis, la preservación y la presentación de esta información no se realizan de manera adecuada **(Martínez, 2012).** Para que esta información se convierta en evidencia se debe aplicar adecuadamente los procesos de informática forense. Esta actividad permite recuperar, analizar, preservar y presentar datos que han sido procesados electrónicamente y almacenados en un sistema informático que podrán ser utilizados como evidencia en un proceso judicial.

Uno de los beneficios de la preservación digital es lograr que el material digital sea accesible informacionalmente en el tiempo. Las entidades y/o personas que requieran preservar material digital pueden ser hospitales, bibliotecas, museos, fiscalías, instituciones de investigación criminal o cualquier otra entidad que tenga la responsabilidad u obligación legal de custodiar datos digitales. El tipo de organización, de dispositivo y la tecnología hardware y software también juega un papel clave en la capacidad de preservar y recuperar la evidencia digital, y en su admisibilidad en la corte

En el ámbito forense, la preservación de la evidencia digital es un aspecto de especial importancia al momento de decidir la admisibilidad en un proceso judicial vigente, o en un futuro proceso, reabierto por apelaciones, o como fuente de información histórica. En el caso particular de las instituciones de investigación criminal, existe un vacío que el Modelo PREDECI pretende cubrir, y que puede ser aplicado en otros entornos.

Es necesario investigar sobre la adecuada preservación de la evidencia digital de las instituciones que tiene la obligación de preservar la información y que pueden convertirse en

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

evidencia para un caso judicial, así, este articulo pretende responder a la pregunta de investigación siguiente: ¿Mejora nivel de admisibilidad de la evidencia aplicando PREDECI?, para ello, se presenta un fundamento teórico, se aplica una metodología adecuada, se obtienen los resultados y luego de un análisis se presentan las conclusiones.

Fundamento Teórico

Repositorios Institucionales

Un repositorio institucional (RI) es un conjunto de servicios para almacenar y hacer accesibles materiales de investigación en formato digital creados por una institución y su comunidad, una colección digital del producto de la investigación llevada a cabo por esa comunidad.

La Preservación Digital

La preservación digital o en inglés Digital Preservation (DP), se define como los procesos y acciones que contribuyen a garantizar el acceso continuo e indefinido a la información y los registros que existen en un formato digital. (Van der Merwe, 2009). Ferreira la define como "la capacidad de asegurar que la información digital se mantiene con las cualidades accesibles y suficientes de autenticidad, que se pueden interpretar en el futuro con uso de una plataforma tecnológica diferente utilizado al momento de su creación" (Ferreira, 2006), La preservación Digital tiene como objetivo superar la debilidad del soporte físico, la obsolescencia tecnológica y la vulnerabilidad del medio digital para garantizar la autenticidad, integridad, fiabilidad, así como el acceso seguido a la información, siendo esta la única manera de garantizar y promover la memoria colectiva e institucional.

En las Directrices para la preservación digital se define la preservación como las acciones destinadas a mantener la accesibilidad de los objetos digitales a largo plazo (UNESCO, 2004). En Digital Preservation Coalition - DPC Handbook (2008) se define como las actividades necesarias para asegurar el acceso continuado a materiales digitales hasta cuando sea necesario, a pesar de los obstáculos que representan los fallos en los soportes o los cambios tecnológicos. (Digital Preservation Coalition, 2008).

En Trusted digital repositories (Research Libraries Group, 2002), indica que la preservación digital son las gestiones de actividades necesarias para asegurar el mantenimiento a largo plazo de la cadena de bits y la accesibilidad continuada del contenido.

Aspectos relativos a la Evidencia

Evidencia se conocen como cualquier cosa que tienden a probar lógicamente o refutar un hecho de un problema en un caso judicial (Swanson, 2006). Evidencia digital se define como información de valor probatorio legal que es almacenado o transmitido en forma digital (Casey, 2011). Otra definición de evidencia digital es cualquier dato almacenado o

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

transmitido por medio de un equipo que apoya o refuta una teoría de cómo un delito ocurrió, o puede abordar un elemento crítico como intención o una coartada (Casey, 2011). La evidencia digital plantea desafíos particulares a la Corte Penal Internacional - International Criminal Court ("ICC"). Es definida como información transmitida o almacenada in formatos digitales que puede utilizarse para procedimiento en un caso judicial.

Biros y Weiser, definen forense digital como "conocimiento científico y métodos aplicados a la identificación, colección, preservación, examen y análisis de información almacenada o transmitida en forma binaria de una manera aceptable para su aplicación en asuntos legales". (Biros, Weiser, & Mosier, 2006). La evidencia en casos legales es admitida o no admitida basada en el peso relativo de su valor probatorio y perjudicial. Dado que el sistema jurídico se basa en antecedentes, investigadores forenses deben introducir la cohesión y la coherencia en el creciente campo de extraer y examinar las evidencias. (Ami-Narh, 2008).

Normativa legal de admisibilidad de la Evidencia

Los Tribunales penales internacionales incorporan elementos del derecho consuetudinario y las tradiciones de derecho civil en diversos grados. En general, el sistema de derecho común contiene más prohibiciones y normas sobre exclusión de evidencia de que es irrelevante o poco fiable, mientras que en el sistema de derecho civil la mayor parte de la evidencia es admitido y los jueces posteriormente evalúan su valor probatorio (Decision on the admission into evidence of materials contained in the prosecution's list of evidence., 2010).

La Regla 69 de las Reglas de la ICC- International Criminal Court, de Procedimiento y Evidencias dirige a los jueces a admitir Evidencias, "teniendo en cuenta, entre otras cosas, el valor probatorio de las Evidencias y cualquier perjuicio que pueda suponer para un juicio justo o para la justa evaluación del testimonio de un testigo." (Decision on Confirmation Charges, 2007). De conformidad con la Regla 63, jueces de la ICC determinan el valor probatorio y el "peso adecuado" de los medios de Evidencia admitidos en el final de un caso, cuando consideran la evidencia como un todo.

La evidencia debe satisfacer "normas mínimas de relevancia y fiabilidad" para ser admitido. La admisión de evidencias no en sí mismo una señal de que la evidencia es exacta; los jueces evalúan su peso por separado.

Las Evidencias y el material digital deben ajustarse a un "Protocolo de e-corte", incluso antes de que se presente en la Audiencia de Confirmación. El Protocolo está diseñado para "asegurar la autenticidad, exactitud, confidencialidad y conservación de las actas. (Molina & Rodriguez, 2015a)

Legislación Internacional

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada sobre delitos informáticos y preservación de la evidencia. Según las Naciones Unidas, cuando se trata de procesar evidencias digitales, los parámetros están determinados

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

básicamente por aquellos lineamientos establecidos en 1966 por el artículo 9 de la Ley Modelo sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional –"UNCITRAL" por sus siglas en inglés-: "Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en 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".

En México, son especificados en el artículo 210-A del Código Federal de Procedimientos Civiles de esa nación, que es dónde se establece, primero, que "Para valorar la fuerza probatoria de la información digital, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas".

En República Dominicana, La promulgación de la nueva Ley No.126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, de fecha 29 de septiembre de 2002. El plazo de 40 años está establecido en la Ley No.126-02 en su artículo 52, el cual dispone lo siguiente: "Art. 52.- Término de conservación de los registros. Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término de cuarenta (40) años, contados a partir de la fecha de la revocación o expiración del correspondiente certificado."

En Colombia, Ley 527. ART. 11. "….. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente".

En Perú. - El Proyecto de ley Nro. 3003/2013-CR, crea el sistema de defensa y preservación digital en el archivo de la nación, en su artículo 6 indica "Las entidades oficiales del archivo general de la nación, serán responsables de la gestión de documentos y todo el proceso de escaneado técnico y de la administración de sus archivos y ejercerán el control de la documentación durante todo el proceso de defensa y preservación digital."

En Ecuador, la Ley del Sistema Nacional de Archivos, indica que "es obligación del Estado velar por la conservación 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 privado, así como la de personas particulares"

En otros países como Estados Unidos, Alemania, Austria, y Gran Bretaña, España, Holanda, Francia, existen leyes muy duras para los delitos informáticos, y para los procesos de preservación digital, pues esto ocasionen resultados adversos ante una corte.

Análisis de Proyectos y modelos de Preservación Digital

En la historia de la preservación digital han sido muchos los proyectos puestos en marcha, tanto a nivel internacional como particular de universidades y centros científicos. Estos

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

proyectos han abarcado diversas áreas, desde la concienciación de los organismos productores y conservadores de información a herramientas desarrolladas, incluso por comités expertos.

Existen diversas iniciativas de modelos de conservación digital. Todos los modelos tienen en su horizonte la preservación digital a largo plazo.

- El modelo de ciclo de vida de conservación. - propuesto por el Digital Curation Center (DCC), propone una conceptualización de todas las actividades necesarias en una unidad de custodia.
- INTERPares.- Se pretende desarrollar el conocimiento esencial para la preservación a largo plazo de los documentos digitales. (The International Research on Permanent Authentic Records in Electronic Systems, 2013).
- PLANETS.- Preservation and Long-term Access through Networked Services, es un proyecto con la misión de tratar los retos que tiene planteados la preservación digital. (Open Planets Foundation , 2007).
- DAMM.- Su objetivo es extraer características de estos objetos para la validación futuro. Capacidad para identificar los formatos de archivo en riesgo y en necesidad de atención. (Tessella, 2013).
- PREMIS.- Se basa en un Metadata basado en OAIS, bajo la forma de un esquema de metadatos. (PREMIS Data Dictionary, 2012). Se enfoca en estrategias de implementación de metadatos preservación en Archivos Digitales. Los metadatos PREMIS se concentran sólo sobre los elementos que afectan directamente a la preservación. (Caplan, 2009).
- NDSA Un conjunto escalonado de directrices y prácticas destinadas a ofrecer, instrucciones de referencia claros en la preservación de los contenidos digitales en cuatro niveles progresivos de sofisticación a través de cinco áreas funcionales diferentes. (National Digital Stewardship Alliance, 2015)
- OAIS .- El modelo OAIS, ISO 14721:2003, es un modelo de referencia utilizado para la conservación y preservación de archivos digitales. (CCSD, 2012). Es un modelo de referencia que se utiliza para la conservación de archivos digitales.
- PREDECI .- PREDECI proporciona un marco para la comprensión y mayor conciencia de los conceptos necesarios para la preservación de la evidencia digital al largo plazo, incluyendo la terminología y conceptos, para describir y comparar las arquitecturas y operaciones de evidencias digitales actuales y futuras, considerando las diferentes estrategias de preservación a largo plazo. (Molina & Rodriguez, Preservation of Digital Evidence: Application in Criminal Investigation., 2015b). El modelo aborda las funciones de preservación del modelo OAIS incluyendo los aspectos fundamentales en el entorno de instituciones de investigación criminal, manteniendo la estructura global como la ingesta, administración de preservación, almacenamiento, administración de datos, plan de

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

preservación, acceso. También se aborda la preservación del entorno de creación de evidencia, y la capacidad de incrementar evidencia, así como administrar evidencia digital en repositorios de confianza externos, muy diferente a tener un solo archivo, una sola técnica o una sola estrategia como lo plantea OAIS. (Molina & Rodriguez, The preservation of digital evidence and its admissibility in the court., 2017)

Determinación de requerimientos insatisfechos

Los jueces y los abogados deben tener un entendimiento común de los elementos que garantizan la admisibilidad de evidencia digital en la corte. El marco legal es la misma en la mayoría de los tribunales. (Thomson, 2011).

En general, existen tres preguntas o desafíos principales que se analizan generalmente para la autenticidad de los registros digitales. 1.- Gestión de identidad – ¿Quién es el autor de los expedientes? – Tribunales buscan maneras de atar al autor a la información digital ofrecida como Evidencia. 2.- ¿Es el programa de computadora que generan los registros confiables? – y 3.- El que interviene en la preservación específicamente, ¿Fueron los registros alterados, manipulados o dañados después de que se crearon? – Existen numerosos ejemplos de lo fácil que es modificar registros digitales, a menudo sin ninguna Evidencia de detección.

Para abordar estas cuestiones, los tribunales han creado enfoques para determinar la admisibilidad de evidencia digital. Aunque se determina una “barra baja" a la admisibilidad de las Evidencias, las organizaciones no gubernamentales (ONG) deben desarrollar estrategias para recolectar y preservar evidencia digital que puede cumplir el estricto examen de admisibilidad. Independientemente del custodio y del tipo de evidencia digital, esta debe ser preservada cumpliendo con los requisitos, normas y principios analizados en este documento.

Algunos aspectos relevantes que expresamente no poseen los modelos mencionados, y que para el ámbito de las instituciones de investigación criminal son determinantes y fundamentales, son Museo de Herramientas (Acurio, 2008), Terminología la (National Digital Stewardship Alliance, 2014), Control de calidad ingesta (Alvarez, 2004), Ingesta parcial, Metadatos del entorno de la evidencia a preservar (Dappart, 2013). (Gómez, 2013), Garantizar la integridad del original (Rao, 2014), Evaluación de riesgos (Acurio, 2008), Almacenamiento distribuido (Castillo, 2008), Tiempo de preservación (UNESCO, 2004), Certificaciones de la estrategia (ISO, 2012).

Se definen como requisitos mínimos de admisibilidad, adicionalmente a los mencionados antes, los siguientes: La legalidad de la evidencia, respeto por los derechos fundamentales, La fiabilidad de las evidencias, junto con su pertinencia, la efectividad de los mismos, el respeto a las normas de protección de datos, el respeto del secreto de las comunicaciones y el respeto por el derecho a la libertad de expresión, Confidencialidad, Autenticidad,

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

integridad, Roles de responsabilidad de ingesta y de administración, creación de evidencia Digital, Evidencia física – recogida y almacenamiento, "Transmisión" de evidencia Digital, Almacenamiento de información, archivo y preservación de evidencia Digital; documentación que debe ser creada y mantenida para registrar de ser posible cada paso del ciclo de vida preservación de la evidencia.

El valor de evidencia incluso cuidadosamente preservado y recuperado puede perderse si no se mantiene la "Cadena de custodia" se refiere a la "documentación cronológica y cuidadosa de evidencia para establecer su relación con un presunto crimen o incidente". Según (Molina & Rodriguez, 2017), indica que no existe un modelo de preservación digital completo, específico, para aplicarlo en el ámbito de la investigación criminal, escenario en el cual es necesario un modelo de preservación de evidencia digital especifico y que considere los requerimientos mínimos exigidos por la legislación mundial.

Metodologia.

La ejecución de esta investigación se ha basado en cuatro bloques metodológicos diferenciados:

- Revisión de la bibliografía y establecimiento de los marcos jurídicos, normativos y teóricos.
- Análisis de las metodologías modelo y técnicas de preservación existentes y su aplicabilidad en entorno de instituciones de investigación criminal.
- Obtención de datos sobre la gestión de los datos digitales mediante herramientas cualitativas.
- Aplicación del modelo de preservación de evidencia digital.

Tipo y Diseño de la Investigación

La presente investigación es de tipo experimental, prospectivo, transversal, descriptivo, los datos son recogidos a propósito de la investigación, y son medidos en una sola ocasión, el análisis estadístico es univariado. La investigación se apoya en el contexto teórico para determinar la relación entre los modelos existentes de gestión de documentos digitales y que pueden adaptarse para dar respuesta a la preservación de evidencias digitales. La población son todos los actores que intervienen en el proceso judicial de la Fiscalía de Chimborazo, esto es 74 actores, distribuido en 5 Custodios de Evidencia, 24 Fiscales, 35 Jueces, 5 Peritos Informáticos, y 5 Técnicos Administradores del modelo, que en adelante se denominarán "Actores". La muestra es el total de la población de la unidad de análisis. Se emplea la técnica de encuesta, de manera sincrónica. Para la aplicación de los instrumentos se utiliza el catálogo de criterios para repositorios digitales NESTOR (Nestor working Group, 2009), el mismo que, incluido los ajustes requeridos por el entorno especifico es validado por juicio de expertos. Con objeto de determinar qué aspectos y qué variables influyen en la gestión de la preservación de la evidencia y su admisibilidad en la corte, se realiza el tratamiento

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

estadístico de los datos en una hoja electrónica de cálculo, se realiza un análisis de varianza ADEVA, y se aplica la prueba de Fisher en el análisis de varianza y la separación de medias de Tukey, se analiza el error estándar y obteniendo el porcentaje de buena clasificación del modelo hallado y los coeficientes con sus correspondientes exponenciales e intervalos de confianza para las mismas al 95%. Para la validación del instrumento, se ejecuta el análisis de fiabilidad de la encuesta, se aplica el Alfa de Cronbach cuyo coeficiente es de 0,831, lo que proporciona una fiabilidad aceptable del instrumento de consulta.

Resultados.

De la aplicación del modelo PREDECI y su valoración se obtiene que para los Peritos, Custodios, Fiscales, Jueces y técnicos del área judicial, al modelo PREDECI asignan calificaciones promedio de 4,03; 4,54; 4,38; 4,45 y 4,68 / 5,00 puntos, equivalentes a una calificación entre intermedia y alta, valores entre los cuales difieren muy significativamente ($P < 0,05$), tanto en un análisis estadístico de los aspectos (preguntas: p=0.0033) como de los actores (p=0,002).

En la figura se puede observar la importancia intermedia que los custodios y técnicos califican al modelo PREDECI en este aspecto; los peritos, fiscales y jueces le dan una importancia intermedia.

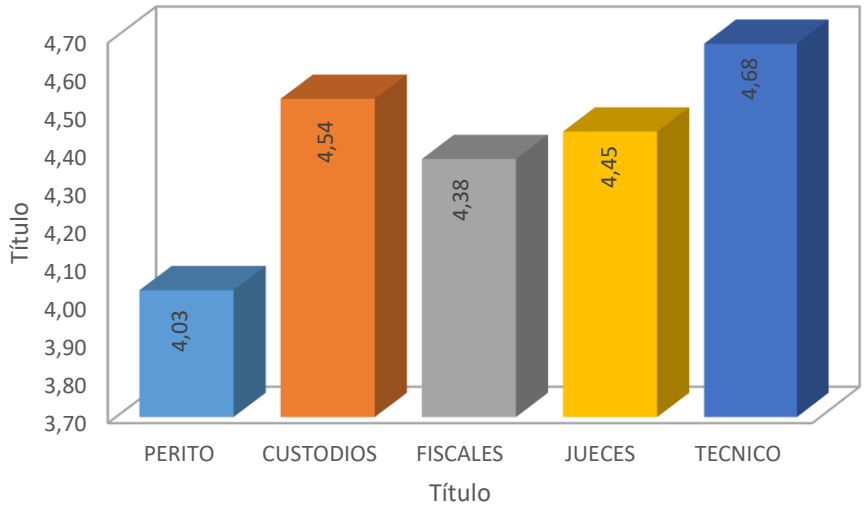

Figura 1 : Tabulación Análisis de aplicación de PREDECI
Elaborado por: (Molina & Rodriguez, 2017)

Los Custodios y técnicos, y especialmente los jueces y fiscales, le otorgan una importancia alta al hecho de que PREDECI permita con sus procesos garantizar una adecuada preservación de la evidencia, y por tanto garantiza una mayor admisibilidad de la evidencia digital si se preserva en un repositorio que cumpla con los aspectos del modelo PREDECI.

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

Conclusiones

- Existen modelos para entornos específicos, muchos se centran en aspectos específicos, pero no consideran que la evidencia digital requiera de la tecnología digital para preservar el entorno, así como contenidos adicionales relacionados para asegurar su admisibilidad, evitando así la manipulación, y que la evidencia deba ser considerada como una sola unidad de información o "paquete de datos".
- El modelo PREDECI es capaz de alinear los objetivos de preservación de la evidencia digital de la institución en términos de los aspectos de admisibilidad e integridad de la evidencia y por lo tanto mejora la admisibilidad de la evidencia en la corte.
- El modelo PREDECI incluye algunos de los aspectos no considerados, a)legalidad de la evidencia, b)confidencialidad, c)control de calidad ingesta, d)ingesta parcial, e)metadatos de entorno, f)transmisión, g)museo de herramientas, h)garantía de integridad de evidencia originales, i) almacenamiento distribuido j) terminología, k) certificación de la estrategia, y l) aspectos de trazabilidad y continuidad de la preservación; Todas estos aspectos se organizaron en cuatro dimensiones, y juntos, permiten mejorar la admisibilidad de la evidencia digital en la corte largo plazo.
- Para los actores del sistema judicial, al modelo PREDECI le asignan calificaciones promedio de 4,03 a 4,68 / 5,00 puntos, equivalentes a una “alta importancia”. A todos los actores influyen altamente en la determinación del nivel de admisibilidad de la evidencia digital en la corte, por lo que la aplicación de un modelo de preservación digital, en este caso PREDECI, garantiza una mayor admisibilidad de la evidencia digital en la corte, se concluye que el 100% de encuestados, asegura que el uso del aplicativa basado en el modelo PREDECI, para preservación de evidencia digital, en un nivel alto, elevaría la admisibilidad de la evidencia digital en la corte.

Referencias bibliográficas.

Acurio, S. (2008). Manual de Manejo de Evidencias Digitales y entornoes Informáticos. Recuperado el 17 de 12 de 2015, de https://www.oas.org/juridico/spanish/cyber/cyb47_manual_sp.pdf

Alvarez, B. R. (2004). Avances en criptología y seguridad de la información. Ediciones Díaz de Santos.

Ami-Narh, J. T. (2008). Digital forensics and the legal system: A dilemma of our times. Australian Digital Forensics Conference. Edith Cowan University. Obtenido de http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

Biros, D., Weiser, M., & Mosier, G. (2006). Development of a national repository of digital forensic intelligence. Journal of Digital Forensics, Security and Law,, 1(2), 5-17.

Caplan, P. (2009). Understanding Premis. D-Lib Magazine, Vol. 15, No. 3/4.

Casey, E. (2011). Digital Evidence and Computer Crime, 3d ed. London: Academic Press.

Castillo, J. M. (2008). Emmagatzematge distribuït i preservació digital: una panoràmica d'alternatives. Textos universitarios de biblioteconomia.

CCSD. (2012). Reference Model for an Open Archival Information System (OAIS) 650.0-M-2. Washington, DC, USA.

Dappart, A. (2013). DePICT - a conceptual model for digital preservation. UNITED KINGDOM. Obtenido de http://eprints.port.ac.uk

Decision on Confirmation Charges, Case No. ICC-01/04-01/06 (International Criminal Court 29 de Enero de 2007). Obtenido de https://www.icc-cpi.int/drc/lubanga/Documents/LubangaEng.pdf

Decision on the admission into evidence of materials contained in the prosecution's list of evidence., Case No. ICC-01/05-01/08 (19 de Noviembre de 2010). Obtenido de https://www.icc-cpi.int/CourtRecords/CR2010_10652.PDF

Digital Preservation Coalition. (2008). Preservation Management of Digital Materials: The Handbook. Glasgow: Digital Preservation Coalition. Recuperado el 13 de 12 de 2015, de http://www.dpconline.org/pages/handbook/docs/DPCHandbookIntro.pdf

Ferreira, M. (2006). Introdução à Preservação Digital: Conceitos, estratégias e actuais consensos. doi:ISBN 9728692307

Gómez, L. (2013). Delitos, prueba y evidencia digital. Obtenido de http://listas.hackcoop.com.ar/archivos/bla/attachments/20131026/b708d60b/attachment.pdf

ISO. (2012). Space data and information transfer systems -- Audit and certification of trustworthy digital repositories. ISO 16363:2012.

Martínez, R. (04 de 1 de 2012). La importancia de la evidencia y el análisis forense digital. Obtenido de http://www.bsecure.com.mx/opinion

Molina, F., & Rodriguez, G. (2015a). Digital Preservation and Criminal Investigation: A Pending Subject. En F. Molina Granja, & G. Rodriguez, New Contributions in Information Systems and Technologies (págs. pp 299-309). United State: Springer International Publishing. doi:978-3-319-16485-

Molina, F., & Rodriguez, G. (2015b). Preservation of Digital Evidence: Application in Criminal Investigation. Science and Information Conference. (págs. 1284 - 1292). London, United Kingdom.: Springer. doi:DOI: 10.1109/SAI.2015.7237309

Molina, F., & Rodriguez, G. (2017). MODEL FOR DIGITAL EVIDENCE PRESERVATION IN CRIMINAL RESEARCH INSTITUTIONS – PREDECI. Int. J. of Electronic Security and Digital Forensics., 9(2), 150-166

Molina, F., & Rodriguez, G. (2017). The preservation of digital evidence and its admissibility in the court. nt. J. of Electronic Security and Digital Forensics., 9(1), 1-18.

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

National Digital Stewardship Alliance. (2014). NDSA National Agenda for Digital Stewardship. Recuperado el 28 de 10 de 2014, de http://www.digitalpreservation.gov/ndsa/documents/2014NationalAgenda.pdf

National Digital Stewardship Alliance. (2015). National Digital Stewardship Alliance.

Nestor working Group. (2009). Catalogue of Criteria for Trusted Digital Repositories. Version 2. Frankfurt: Nestor working Group Trusted Repositories - Certification.

Open Planets Foundation. (2007). PLANETS. Obtenido de http://www.planets-project.eu

PREMIS Data Dictionary. (2012). Obtenido de http://www.loc.gov/standards/premis/v2/premis-2-2.pdf

Rao, V. (2014). Immerging Digital Preservation Technology: It's Design, Initiatives and Challenges. International Journal of Innovate Research & Development.

Research Libraries Group. (2002). Trusted Digital Repositories:Attributes and Responsibilities. California: RLG, Inc. Recuperado el 15 de 12 de 2016, de http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf

Swanson, C. R. (2006). Criminal Investigation, 9th ed. New York: McGraw-Hill. .

Tessella. (2013). Digital Preservation Maturity Model - White Paper. }

The International Research on Permanent Authentic Records in Electronic Systems. (2013). The InterPARES Project. (A. &. School of Library, Editor, & T. U. Columbia, Productor) Recuperado el 5 de 10 de 2014, de http://www.interpares.org/

Thomson, L. (2011). Admissibility of Electronic Documentation as Evidence in U.S. courts.

UNESCO. (2004). Carta sobre la preservación del patrimonio digital. Actas de la Conferencia General. Paris.

Van der Merwe, A. a. (2009). Planning an effective digital preservation from a research organization. Obtenido de http://www.ais.up.ac.za/digi/docs/avdmerwe-paper.pdf

ISSN: 2602-8085
Vol. 3, N°1.1. p. 118-130, enero - marzo, 2019

Para citar el artículo indexado.

Molina F., Santillán J., Luna W., Lozada R. & Guaiña J. (2019) Preservación digital y la admisibilidad de las evidencias. *Revista electrónica Ciencia Digital* 3(1.1), 118-130. Recuperado desde:
http://cienciadigital.org/revistacienciadigital2/index.php/CienciaDigital/article/view/364/782