Modelo de Cadena Custodia basada en ISO 27037 y Legislación Boliviana dirigida a evidencias digitales

Rubén David Quispe Amaru
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
rubendqa@gmail.com

***Resumen*—Una parte de la sociedad de La Paz enfrenta delitos informáticos por los que quieren acceder a información confidencial para llevar a cabo daño económico, demandas legales y pérdida de reputación. Las entidades afectadas denuncian estos delitos para su investigación ante la Policía, la Fiscalía, el Ministerio Público para que los investigadores gestionen de manera adecuada las evidencias digitales para garantizar su integridad. Este trabajo fue realizado con la intención de mostrar la necesidad de contar con un modelo de cadena de custodia basada en la ISO 27037 y la legislación boliviana para garantizar la integridad de la evidencia digital relacionado con el delito informático. Los temas encontrados son muy extensos y no se pueden cubrir a detalle en este artículo, sin embargo, se puede tomar como una introducción para quienes quieran elaborar el modelo de cadena de custodia dirigida a evidencias digitales.**

Palabras clave—cadena de custodia, evidencia digital, ISO 27037, legislación boliviana.

I. INTRODUCCIÓN

Actualmente, la Policía, la Fiscalía, el Ministerio Público y otros de Bolivia reciben denuncias por delitos informáticos, en donde los delincuentes están utilizando las Tecnologías de Información y la Comunicación (TIC) para cometer este tipo de delito, esto exige que los investigadores deben estar capacitados y actualizados en la gestión de las evidencias digitales para garantizar la integridad de estas evidencias.

Desde este punto de vista, las evidencias digitales (documentos, e-mail, base de datos, aplicaciones, dispositivos digitales y otros) permanecen en el lugar del delito. La recuperación y preservación de la evidencia es fundamental, en el proceso de la investigación, para encontrar al autor del delito.

En este sentido, la cadena de custodia en evidencias digitales tiene una gran importancia en la investigación por delito informático, en donde los investigadores aplicarán en la identificación, recolección, adquisición y preservación de las evidencias para evitar que no sea: dañada, contaminada, destruida, alterada y sustituida, y para garantizar la integridad desde la identificación hasta su disposición final.

Ciertamente, la cadena de custodia asegura que los investigadores, en el delito informático, han realizado los procesos correctos para gestionar las evidencias digitales, que son aceptados en todo el país y describe a las personas que están involucrados con la evidencia.

En este sentido, una de las definiciones más aceptadas de la cadena de custodia, es el sistema de control y registro, que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su identificación, recolección, adquisición y preservación, que tiene el propósito de garantizar la autenticidad de dichas evidencias, hasta su disposición final.

En los últimos años se ha visto la incursión de normas, leyes sobre el manejo de la evidencia digital, delito informático y cadena de custodia como: la ISO 27037:2012 *"Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recolección, adquisición y preservación de evidencias digitales"* que proporciona actividades específicas en el manejo de evidencia digital, La legislación boliviana como el código penal [1], la Ley Orgánica del Ministerio Público de Bolivia, que en su Artículo 40.- (Atribuciones) Las y Los Fiscales de Materia. Inciso 10 indica, asegurarse que todos los indicios y elementos de prueba recolectados sean debidamente resguardados dentro de la cadena de custodia, en particular los recolectados de la víctima [2].

II. MARCO TEÓRICO

A. Delito informático

Los delitos informáticos son todos los actos, conductas, ilícitas, ejecutados por la capacidad mental del hombre, los mismos que tienden a involucrarse con la tecnología en especial con los dispositivos de comunicación para cometer delitos cuyo objeto es causar daños o impedir el uso de las redes informáticas, vulnerando derechos y garantías universales protegidos, los cuales son susceptibles de sanción por el derecho penal [3].

B. La Cadena de Custodia

La cadena de custodia implica la identificación, recolección, adquisición y preservación; donde la recolección está ligada al indicio del hecho u objeto, la adquisición es acorde al lugar donde se encontraba (en términos generales una fotografía de donde se encontró lo que se recolectó) y la preservación es acorde al procedimiento de resguardo [4].

C. Principios de la Cadena de Custodia

La cadena de custodia de la evidencia se caracteriza por una serie de principios, que aseguran su funcionalidad y confiabilidad en instancias de juicio fundamentándose en los siguientes principios legales [5].

Para referenciar este artículo (IEEE):

[N] R. Quispe, «Modelo de cadena custodia basada en ISO 27037 y legislación boliviana dirigida a evidencias digitales» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 92-93, 2020.

- Aseguramiento de la prueba: surge de la necesidad de protección de los medios probatorios, del tiempo y del interés de las partes afectadas.
- Licitud de la prueba: se refiere a que los canales y medios de obtención de pruebas sean legales y estén debidamente establecidos.
- Veracidad de la prueba: se basa en la obtención y preservación de una prueba libre de vicio y artimaña.
- Necesidad de la prueba: la prueba acredita el hecho, es decir que la prueba sea útil a la investigación probando un hecho.
- Obtención coactiva de la prueba: el estado emplea la coerción para garantizar la recaudación de la prueba.

D. Evidencia digital

Es una denominación usada de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional, que puede ser utilizado como prueba en un proceso legal y se refiere a la información contenida dentro de un elemento físico electrónico.

E. Norma ISO 27037

Contenida en siete capítulos la Norma de la Organización Internacional para la Normalización es una importante guía para el tratamiento de la evidencia digital, aunque dicha norma no es vinculante para los Estados y las instituciones que tienen la competencia de desarrollar la investigación criminal, sin embargo, supone un importante instrumento para los investigadores particulares y cualquier profesional en formación que se interese por la evidencia digital y su manejo.

F. Legislación Boliviana

A continuación, se mencionan algunas leyes bolivianas que se pueden aplicar al Modelo de Cadena de Custodia dirigida a evidencias digitales.

Constitución Política del Estado Plurinacional de Bolivia: Es la norma fundamental de organización del estado para la convivencia de la sociedad.
Código Penal: Es el código que establece los delitos y las penas que son aplicables en los delitos.
Código del Procedimiento Penal: Son las que determinan los trámites por seguir en las actuaciones judiciales.
Código Civil: Son normas relativas al régimen de las personas, de las obligaciones, de los hechos y actos jurídicos de los contratos.

III. Discusión

En la División de Cibercrimen de la Fuerza Especial de Lucha Contra el Crimen (FELCC) de la ciudad de La Paz, se atiende aproximadamente de tres a cuatro casos por delitos informáticos en el día, en la cual las víctimas solicitan de que se realice una investigación [6].

La División enfrenta diversas problemáticas como el desconocimiento de las personas del trato especial que deben tener las evidencias relacionados con el delito informático. Las evidencias digitales, están siendo tratadas de alguna forma con las cadenas de custodia de evidencias físicas y biológicas, sin embargo, es necesario crear una cadena de custodia con características específicas para gestionar estas evidencias. Los investigadores, la fiscalía y otros que realizan este trabajo no son altamente capacitados en la gestión de estas evidencias, son pocos los que están capacitados, que se encuentran en las distribuciones policial como en el Instituto de Investigaciones Técnico Científicas (IITCUP), División de Cibercrimen, Instituto de Investigaciones Forenses (IDIF), el Ministerio Público y en otras instituciones así lo confirma el Tte. Carlos Ricardo Vargas Lima Director de la División de Cibercrimen, por consiguiente el conocimiento de un adecuado tratamiento en evidencias digitales debe ser homogéneo a nivel inter institucional entre el Ministerio de Gobierno, la Policía Boliviana y la Administradora de la justicia [7].

Ante esta realidad, el Tte. Vargas indica que poco o nada se está haciendo con respecto a la cadena de custodia que permita garantizar la integridad de la evidencia digital, relacionado con el delito informático, desde su identificación hasta su disposición final; esto es debido a que aún no se cuenta con experiencias documentadas con respecto a este tratamiento, por consiguiente los investigadores, fiscales, peritos informáticos, jueces y funcionario de la división, no cuentan con la suficiente información o un modelo para la eficiente y eficaz, identificación, recolección, adquisición, y preservación de la evidencia digital.

IV. Conclusiones

Las entidades públicas y privadas que sufren delitos informáticos presentan denuncias a la Policía, la Fiscalía y al Ministerio Público para su investigación. Los investigadores en delito informático entran en contacto con la evidencia digital desde la identificación, recolección, adquisición y preservación de la evidencia, es por esta razón que se debe contar un modelo de cadena de custodia basada en la ISO 27037 y Legislación Boliviana (Ley Orgánica del Ministerio Público, 11 de julio de 2012, Código penal y Código de civil de Bolivia) dirigida a evidencias digitales, para garantizar la integridad de la evidencia digital relacionado con el delito informático.

Referencias

[1] C. B. Centellas Tarquino, Código Penal y Código de Procedimiento Penal concordado, La Paz: Diseño, diagramación e impresión propia, 2014.

[2] Ley Orgánica del Ministerio Público, La Paz: Gaceta Oficial del Estado Plurinacional de Bolivia, 2012.

[3] J. Riofrío, Los delitos informáticos y su tipificación en la Legislación Ecuatoriana, Ecuador: Loja, 2012.

[4] C. García, Cadena de Custodia Digital de las Evidencias para la Realización de un Peritaje, Guatemala, 2014.

[5] T. Marqués y J. Serra, «Cadena de Custodia en el Análisis Forense Implementación de un Marco de Gestión de la Evidencia Digital,» RECSI, pp. 2-5, 2014.

[6] La Razón, «En La Paz, los juicios por delitos informáticos crecieron 890%,» 7 mayo 2012. [En línea]. Available: http://www.la-razon.com/suplementos/informe/Paz-juicios-delitos-informaticos-crecieron_0_1609639058.html. [Último acceso: 2019].

[7] La Razón Digital, «Quintana dice que corresponde elaborar una ley sobre delitos informáticos,» 12 octubre 2014. [En línea]. Available: https://www.la-razon.com/nacional/animal_electoral/Quintana-corresponde-elaborar-delitos-informaticos_0_2142385787.html. [Último acceso: 2019].