Propuesta de investigación: Modelo de análisis forense digital para el sistema de negociación electrónico de la Bolsa Boliviana de Valores, basado en la Norma ISO/IEC 27037:2012

Mary Anahy Pomar Montes de Oca
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
anahypomar.2020@gmail.com

Resumen—Este artículo se refiere a un modelo de análisis forense digital, que a partir de los incidentes críticos de información permita estar capacitados ante alguna posible amenaza, con el objetivo de poder recopilar evidencia suficiente y necesaria que sirva como evidencia y prueba ante un tribunal, teniendo en cuenta los lineamientos propuestos en la norma técnica IS0/IEC 27037:2012. Esta norma proporciona directrices para la identificación, recolección, adquisición y preservación de la evidencia digital en una organización.

Palabras clave—Análisis forense, digital, incidente; ISO/IEC 27032:2012.

I. INTRODUCCIÓN

A causa de la globalización y con el avance tecnológico en materia de análisis forense digital, en nuestro país, el tema ganó importancia a partir de la gestión de incidentes, ya que a partir de los incidentes de información críticos, si bien en algunas organizaciones existe un equipo de respuesta a incidentes (CSIRT), como es el caso de la Bolsa Boliviana de Valores (BBV), todavía no se tiene un modelo de análisis forense digital definido para poder abordar, analizar y responder a posibles amenazas. Las técnicas a ser utilizadas y realizadas en la recopilación y preservación de las mismas, son apoyadas por la norma ISO/IEC 27037:2012, que es una nueva norma para la Recopilación de Evidencias.

La BBV, implementó una nueva plataforma de negociación electrónica, para buscar un sistema que cumpla con estándares internacionales. Luego de un proceso de licitación internacional, contrató a bolsas y mercados españoles, Bolsas de Mercados Españoles (BME), para que adecúen sus sistemas SMART a la realidad del mercado de valores bolivianos.

Lo que se busca conseguir, es apoyar la respuesta a incidentes de seguridad de TI, en el sistema de Negociación electrónico SMART-BBV, fortaleciendo la Seguridad tecnológica de la BBV y estar preparados para los incidentes informáticos. Es preciso tener un modelo de análisis forense digital, para poder actuar, disminuyendo las posibles intrusiones y en caso de que éstas ocurran, se puedan controlar a tiempo, reduciendo el impacto que puedan causar en la entidad.

A. Planteamiento del problema

La BBV implementó una nueva plataforma de negociación electrónica, con el propósito de buscar un sistema que cumpla con estándares internacionales, a través de un proceso de licitación internacional. Se contrató bolsas y mercados españoles, Bolsas de Mercados Españoles (BME), para poder adecuar su sistema SMART a la realidad del mercado de valores bolivianos. El resultado es el sistema electrónico de negociación SMART-BBV, que adopta tecnología de punta y reglas de negociación estándares, que en esta primera etapa permite a las agencias de bolsas realizar operaciones de compra y venta de valores seriados entre ellas, de forma remota desde sus propias oficinas.

La implementación de ésta moderna plataforma tecnológica junto a otros proyectos que se vienen realizando, está configurando una nueva bolsa que busca siempre mayor eficiencia, equidad, competitividad y transparencia. En la actualidad la misma es importante, de acuerdo a la coyuntura del país y al crecimiento económico. Con esta tecnología las negociaciones en un recinto físico y a viva voz quedan atrás, generándose un modelo de mercado con un proceso de formación de precios más eficiente al tratarse de un mercado ciego. Además, el sistema permite registrar órdenes de forma masiva y los cierres se procesan de forma automática, pudiendo realizarse más operaciones y manejar mayores volúmenes de valores.

El sistema de negociación actual presenta varios problemas relacionados con: la transparencia de las operaciones realizadas, limitación del universo de participantes y la democratización de la información. Una de las soluciones a estos problemas es la implementación de un Sistema de Negociación Electrónica.

Para analizar este tema es necesario conocer las causas de la inexistencia de un modelo de análisis forense digital en la empresa, en este caso de la BBV. Teniendo en cuenta los lineamientos propuestos en la norma técnica ISO/IEC

Para referenciar este artículo (IEEE):

[N] M. Pomar, «Propuesta de investigación: Modelo de análisis forense digital para el sistema de negociación electrónico de la Bolsa Boliviana de Valores, basado en la Norma ISO/IEC 27037:2012», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 128-130, 2020.

27037:2012, esta norma proporciona directrices para la identificación, recolección, adquisición y preservación de la evidencia digital en una organización.

B. Objetivo

Diseñar el modelo de análisis forense digital para realizar el manejo de incidentes de seguridad de TI en el sistema de negociación electrónica de la BBV.

C. Hipótesis

La carencia de un modelo de análisis forense digital incide en el sistema de negociación electrónico de la BBV, sujeto a la norma ISO/IEC 27037:2012.

D. Preguntas de investigación

- ¿Cuáles son los fundamentos teóricos sobre el modelo de análisis forense digital para la BBV?.
- ¿Cuál es el estado actual de la implementación del análisis forense digital en la BBV?
- ¿Qué resultados se obtienen una vez puesta en la práctica la estrategia la implementación del análisis forense digital mediante un modelo, en la BBV?

E. Marco teórico

Análisis Forense Digital: Se define como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial [1].

Dentro del Análisis Forense Digital, podemos mencionar las siguientes fases;

- Identificación del incidente.
- Recopilación de evidencias.
- Preservación de la evidencia.
- Análisis de la evidencia.
- Documentación y presentación de los resultados.

Evidencia digital: se entiende como el conjunto de datos en formato binario, comprende los ficheros, su contenido o referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado [2].

Equipo de respuesta a incidentes: requiere establecer, entre otros aspectos, unos procedimientos y métodos de análisis que nos permitan identificar, recuperar, reconstruir y analizar evidencias de lo ocurrido y una de las ciencias que cubren estas necesidades es la Ciencia Forense, la cual nos aporta las técnicas y principios necesarios para realizar nuestra investigación, ya sea criminal o no [3].

Sistema de negociación electrónico: El sistema de negociación electrónico es un sistema concurrente que permite transar valores a distancia o de manera remota. Este sistema cumple con cualidades o atributos requeridos en un mercado financiero y que está basado en los siguientes principios:

- Accesibilidad: lograr que todos los participantes del mercado accedan a él en exactamente las mismas condiciones y sin privilegios.
- Equidad: todos los participantes de un mercado financiero deben recibir exactamente el mismo trato y oportunidad.
- Mercado "ciego": aquel mercado financiero en el que la negociación ocurre sin que los operadores conozcan a sus contrapartes.
- Oportunidad: lograr que todos los participantes del mercado accedan a él, a un mismo tiempo y que cuenten todos con la misma información en el mismo momento.
- Precio "justo": precio de un instrumento financiero pactado como resultado de la concurrencia de muchos oferentes y demandantes.
- Profundidad: atributo de un mercado de valores en el que se negocian una gran cantidad de instrumentos financieros y donde intervienen muchos oferentes y demandantes de esos instrumentos.
- Transparencia: todas las transacciones financieras son resultado de la misma información disponible para todos los participantes y donde ninguno de ellos tiene acceso o hace uso de información asimétrica o privilegiada.

Por lo tanto, gracias a este sistema las negociaciones en el mercado de valores se realizarán oportunamente, de manera equitativa, dentro de un mercado ciego, generando precios justos para los valores y promoviendo la profundidad del mercado, en un escenario transparente [4].

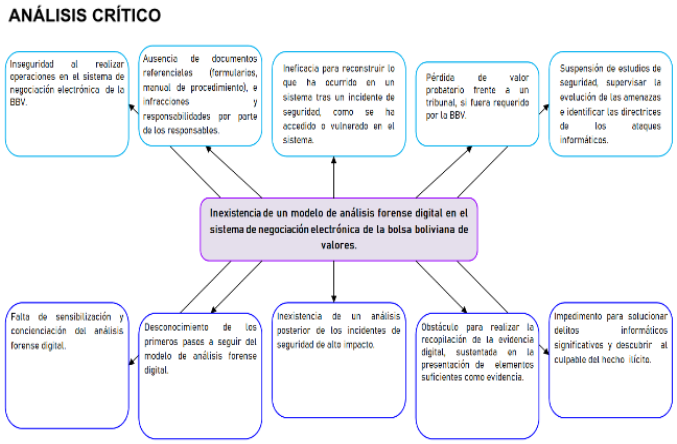

Fig. 1. Técnica del árbol de problemas

BBV: La bolsa cumple la función de facilitar la negociación de valores registrados en ella, brindando al mercado y a sus miembros los sistemas y mecanismos adecuados para que se ejecuten esas transacciones. Estas facilidades incluyen la provisión de un recinto físico, esquemas tecnológicos sofisticados, así como la definición de reglas claras de funcionamiento.

De esta manera, la bolsa proporciona condiciones y facilidades que brindan confianza, a la hora de comprar y vender valores [5].

Gestión de incidentes: La gestión de incidentes es un área de procesos perteneciente a la gestión de servicios de tecnologías de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento

del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan [6].

Norma ISO/IEC 27037:2012: En inglés: "*Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*". Esta norma viene a renovar las antiguas directrices RFC 3227 con recomendaciones de la ISO 27037 más dirigidas a dispositivos actuales y más acorde con el estado de la técnica actual. Esta norma ISO 27037 está claramente orientada al procedimiento de la actuación pericial en el escenario del recojo, identificación y secuestro de la evidencia digital; no entra en la fase de Análisis de la evidencia [7].

II. Conclusiones

Se puede concluir que, con la implementación del Modelo de análisis forense digital para el sistema de negociación electrónica de la BBV, basado en la norma ISO/IEC 27037:2012, es indispensable la utilización de herramientas jurídicas para el proceso de investigación y posterior condena de un delito informático.

Esta propuesta de modelo de análisis forense debe estar lista para aplicarse acorde a los requerimientos necesarios, de tal forma que, si hay un ataque, se tenga el modelo listo para detectar al atacante y actuar conforme a las leyes.

Referencias

[1] Análisis Forense Digital – Miguel López Delgado. https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[2] SMART-BBV https://www.bbv.com.bo/Media/Default/ConozcaBBV /SistemaSMART.PDF.

[3] Bolsa Boliviana de Valores (BBV) /https://www.bbv.com.bo/ConozcaBBV

[4] Perito Informático y Tecnológico – PeritoIT/https://peritoit.com/2012/10 /23/isoiec-270372012-nueva-norma-para-la-recopilación-de-evidencias/