MARCO DE REFERENCIA PARA LA IMPLEMENTACION DE UN LABORATORIO DE INFORMATICA FORENSE.

Luz Mery Díaz Patiño
Universidad Piloto de Colombia
Bogotá, Colombia
luzmdiazpat@hotmail.com

Resumen—El presente documento brinda una visión general de los aspectos a tener en cuenta en la implementación de un laboratorio de informática forense.

Dada la importancia que tiene la presentación de evidencia digital en un proceso judicial y al gran aumento de los delitos informáticos que se presentan día a día, es vital que las empresas que manejan información crítica de su negocio a través de dispositivos y elementos de computación cuenten con una área dentro de su estructura organizacional que tenga la función de llevar a cabo las investigaciones a los incidentes o eventos que a causa de una violación a ocasionado un impacto negativo a la organización.

Esta unidad debe contar con la estructura física adecuada, con recursos tecnológicos apropiados y con profesionales altamente especializados para realizar eficientemente cada una de las actividades a ejecutar.

Abstract—This paper provides an overview of the aspects to consider in implementing a computer forensics.

Given the importance of presenting digital evidence in a judicial proceeding and the large increase of computer crimes that occur every day, is vital that companies manage information critical business across devices and computing elements have an area within its organizational structure that has the function of carrying out investigations of incidents or events because of a violation caused a negative impact to the organization.

This unit must have adequate physical structure with appropriate technological resources and highly skilled professionals to efficiently perform each of the activities to be executed.

Índice de Términos—Evidencia digital, hardware, informática forense, investigación, software forense.

I. INTRODUCCION

Cuando se comete un delito y en este involucra medios tecnológicos de información digital se deben aplicar procedimientos, técnicas y herramientas especializadas para llevar a cabo cada una de las actividades en la recolección, tratamiento y disposición de evidencia digital.

A raíz del aumento de los delitos informáticos mediante el uso de equipos electrónicos, se han diseñado técnicas, herramientas y buenas prácticas en informática forense, orientadas a la colección, preservación, análisis y presentación de evidencia digital. En ese sentido, los cuerpos y órganos que llevan a cabo las investigaciones en materia judicial, así como las organizaciones, empresas e instituciones encargadas que tiene la función de gestión de riesgo, seguridad, administración del fraude han comenzado a implantar laboratorios de informática forense con el objeto de investigar las incidencias que se presenten.

Para realizar un trabajo integro y eficiente es importante contar con un laboratorio especializado en ciencias forense que cuente con personal idóneo, infraestructura física y tecnológica apropiada , con hardware y software recomendado para el análisis de datos con el fin de obtener evidencia que cumpla con los principios de admisibilidad y tenga validez en un proceso judicial.

II. JUSTIFICACION

Las organizaciones, las personas, los sistemas de información y dispositivos tecnológicos están expuestos a un número cada vez más elevado de amenazas que son aprovechadas para cometer actos ilícitos para causar daños convirtiéndose estas conductas en lo que se conoce como delito informático.

Existe una amplia variedad de herramientas y técnicas que tienen como finalidad la recolección de evidencia digital a fin de identificar pruebas concretas que determine las causas del incidente.

Actualmente en Colombia existe un porcentaje mínimo de empresas que tengan dentro de su estructura organizacional una área para desarrollar la función de investigación delitos informáticos por el contrario pagan altas sumas de dinero a profesionales que tienen el conocimiento en esta rama que cobran hasta $600.000 por hora.

III. CONCEPTOS

Incidente de seguridad: Es un evento o conjuntos de ellos, inesperados y no deseados que tienen una probabilidad significativa de poner en riesgo las operaciones del negocio y amenazar la seguridad de la información [2].

ERESI: Equipo de Respuesta a Incidentes de Seguridad de la Información. Es un equipo de miembros de la organización que son de confianza y tienen las habilidades adecuadas para manejar los incidentes durante su ciclo de vida [2].

Delito Informático: Son todas las conductas ilícitas realizadas por un ser humano, susceptibles de ser sancionadas por el derecho penal en donde hacen un uso indebido de cualquier medio informático, con la finalidad de lograr un beneficio [2].

Cadena de custodia: Es un proceso documentado en donde se recolecta la evidencia la recaudada, no se puede tomar como un documento, sino por el contrario, es la forma de adicionar características relevante frente al elemento material probatorio recaudado como los son: Mismidad, autenticidad e Integridad [4].

Almacén de evidencias: Lugar donde se almacenan los elementos físicos de prueba, en condiciones ambientales y de seguridad que permitan garantizar la preservación de las mismas [4].

Almacenamiento: Bodegaje de los elementos materia de prueba y evidencia física en los almacenes de evidencias generales y transitorios teniendo en cuenta las condiciones mínimas necesarias para su conservación [4].

Análisis: Estudio técnico – científico al lugar de los hechos y a los elementos materia de prueba y evidencia física [4].

IV. ESTANDARES

A continuación se mencionan algunos estándares que son un marco de referencia y mejores prácticas como apoyo en seguridad de la información, gestión de incidentes e informática forense.

ISO 18044: Gestión de los Incidentes de la Seguridad de la Información [2].

GTC 169: Gestión de los Incidentes de la Seguridad de la Información [2].

IOCE: The International Organization on Computer Evidence.

HB 171: Guía para la administración de evidencia computacional [2].

V. EVALUACION Y VIABILIDAD DEL PROYECTO.

Para llevar a cabo con éxito el proyecto de implementación de una sección, área o departamento de informática forense, es importante que la alta gerencia este en conocimiento del objetivo, alcance, costo y beneficio que representa en el corto o largo plazo esta inversión.

Es importante que exista una clasificación y evaluación de riesgos de los activos de la organización que permita identificar impacto y probalidad de las amenazas y el apetito de riesgo que esta dispuesta la gerencia a tolerar.

VI. REQUERIMIENTOS MINIMOS A TENER EN CUENTA PARA LA IMPLEMENTACIÓN DEL AREA DE INFORMATICA FORENSE.

Las instalaciones de un área de investigación de informática forense, deben garantizar la seguridad la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, humanos y demás elementos que se encuentren en estas dependencias; por consiguiente debe contar con las suficientes seguridades de control de acceso, requerimientos de ambientales para un desempeño eficiente de su función. A continuación se mencionan algunos aspectos a considerar en diseñar la implementación de esta unidad.

A. Seguridad física.

Control de acceso mediante sistemas biométricos o tarjetas de proximidad y cerraduras de seguridad.

El personal que labore dentro de las instalaciones deberá portar permanentemente

la credencial otorgada para acceder a este sitio en todo momento en un lugar visible.

Sistema de video 7 X 24 de circuito cerrado en todas las áreas para grabar todos los acontecimientos que sucedan dentro del laboratorio.

Sistema de alarma con sensor de movimiento en lo posible que se encuentre intercomunicado con la estación de policía más cercana y con el equipo de seguridad de la empresa.

B. Condiciones ambientales.

El laboratorio debe poseer las condiciones ambientales ideales para proteger los recursos que reposan en este sitio y no invalidar el resultado de los análisis ni la calidad requerida de los dispositivos elementos que contienen la evidencia digital original.

Para mantener la esterilidad biológica se recomienda desinfectar la superficie de trabajo con lejía al 2% y Jaulas de Faraday para proteger los dispositivos electrónicos de la interferencia electromagnética, UPS y un generador eléctrico. Uso de materiales aislantes para minimizar el ruido y la vibración [3].

Sistemas de climatización e instalación de filtros de filtros para evitar el paso del polvo, humedad el sobrecalentamiento y deterioro de los equipos y demás elementos electrónicos [3].

Se recomienda instalar un sistema de refrigeración con una temperatura estable de 22°C y mantener un límite de humedad del 65% dentro de las instalaciones [3].

Sistema de extinción de incendio acorde con el material eléctrico y magnético que almacenara en las instalaciones [3].

C. Infraestructura y diseño físico de las áreas.

Deberá contar con elementos esenciales; como cableado de red con punto de red en todas las áreas del laboratorio, cableado telefónico [3].

UPS o generador eléctrico en caso de falta de energía eléctrica [3].

Se recomienda que la parte externa del laboratorio en lo posible no cuente con ventanas al exterior se sugiere divisiones con paneles móviles para las distintas áreas [3].

Se sugiere que las instalaciones estén divididas en tres áreas: Almacenamiento, mecánica y análisis [3].

El área de almacenamiento debe contar con un cubículo previo con una puerta de acceso con seguridad multilock a la ubicación de los armarios de evidencia [3], ningún personal sin autorización podrá acceder a esta zona. Las persona que estén autorizadas deberán tener un registro de control de acceso con la hora y nombre de quién accedió a ella.

Para el correcto almacenamiento de la evidencia dependiendo de la naturaleza de la misma se recomienda usar contenedores antiestáticos y/o esponja antiestática para ayudar a aislar de fuentes eléctricas y de campos magnéticos [3].

En el área denominada mecánica se realizará el desmontaje, ensamblaje y manipulación física de los computadores, para llevar a cabo esta tarea se debe disponer de herramientas y equipos especializados [3].

El área de análisis tendrá los puestos de trabajo que se requieren para cada uno de los especialistas, cada uno con sus correspondientes armarios y elementos necesarios para desarrollar su función.

Para llevar a cabo cada una de las actividades que incluye el análisis de las evidencias estas áreas debe contar con el software y el hardware que la alta gerencia en conjunto con el departamento de seguridad de la información aprobó para esta área.

Se recomienda que los equipos de cómputo forense estén aislados de la red de la empresa y no deben tener acceso a internet, deben estar totalmente restringidos.

D. Herramientas de Informática Forense

Se debe proveer de software especializado en análisis forense para preservar la información de tal forma que se mantenga su valor probatorio ante los entes judiciales.

Existen varios tipos de herramientas que contemplan funcionalidad para realizar los procedimientos de investigación de informática forense software tanto libre como comercial.

A continuación menciono algunas herramientas que desde mi punto de vista son soluciones robustas, que contienen funciones importantes para realizar procedimientos forenses confiables.

1) **HELIX:** Esta Herramienta cuenta con una versión gratuita que brinda varias funcionalidades para realizar los procesos de investigación forense [1].
2) **EN CASE**: Es un software comercial que permite realizar procedimientos de extracción de imágenes forenses y análisis [1].
3) **ACCESDATA_FTK**: Es un software comercial y tiene una versión gratuita que permite ejecutar procedimientos de extracción de imágenes forense y análisis [1]
4) **DEFT**: Este software cuenta con un kit de herramientas para realizar los procedimientos de investigación de informática forense [1].
5) **BACKTRACK 5**: Es una distribución GNU/ LINUX tiene un kit de herramientas que permite realizar los procedimientos de informática forense [1].

Adicionalmente, se debe contar con el hardware apropiado para soportar los datos de la investigación, servidores de última tecnología, con procesador y memoria RAM para un óptimo desempeño, discos duros con la suficiente capacidad de almacenamiento, equipos periféricos de laboratorio, impresora, cámara digital, protectores para escritura, entre otros**.**

D. Asignación de recurso humano especializado.

La unidad de investigación de informática Forense debe contar con profesionales altamente capacitados, éticos, idóneos para realizar las funciones asignadas al cargo, como la ejecución de los procedimientos establecidos para la solución, la identificación, adquisición, análisis y presentación de las evidencias digitales, informes e indagatorias antes las entidades judiciales, entre otros.

Es importante definir y oficializar la política, normas, procedimientos y estándares para el desempeño de cada una de las funciones y actividades que desarrollarán los funcionarios a cargo de esta área.

VII. CONCLUSION

Una vez se ha recolectado la evidencia, aplicando los procedimientos apropiados para garantizar integridad y la mismidad de los datos, se debe iniciar el ensamble, análisis y articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis, ó identificar si falta evidencias para completar o aclarar la escena del delito.

Para realizar este proceso de análisis es necesario contar con los recursos apropiados tanto técnicos como humanos y áreas físicas, que permita a los especialistas en informática forense desarrollar sus funciones, reflejadas en procedimientos de investigación para encontrar, interpretar y analizar adecuadamente evidencia digital. Adicionalmente, la organización debe contar con políticas, normas y procedimientos debidamente documentados que soporten las funciones a cargo de esta área.

REFERENCIAS

[1].Vallejo, Wilmar. Material de estudio diplomado de Informática Forense
[2].Echeverry, Jhon Jairo. Material de estudio diplomado de Informática Forense.
[3].Gómez, Leopoldo Sebastian. Computer forensics – Hardware and software guildelines
[4] Manual de Cadena de custodia

Autor:

Luz M. Díaz P.
Ingeniero de Sistema Universidad Manuela Beltrán
Especialista en Seguridad de la Información de la Universidad Piloto de Colombia.
Diplomado en Informática Forense de la Universidad Piloto de Colombia.