PROPUESTA DE DISEÑO DE UN ÁREA INFORMÁTICA FORENSE PARA UN EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD INFORMÁTICOS (CSIRT)

Mónica Uyana[1], Milton Escobar[2]

[1] *Universidad de las Fuerzas Armadas, Sangolquí, Ecuador*
[2] *Universidad de las Fuerzas Armadas, Sangolquí, Ecuador*

Departamento de Seguridad y Defensa; Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador

monica.uyana@gmail.com

Resumen:

El presente artículo tiene por objeto dar a conocer sobre los ataques y estrategias de invasión que van siendo perfeccionados día tras día por las personas con conocimientos avanzados en el área informática y de sistemas, quienes en su mayoría atentan contra la integridad de la información, seguridad y privacidad de las personas, instituciones, gobiernos y sociedad, generando de este modo en varias instituciones públicas y privadas a nivel mundial, la necesidad inminente de desarrollar organismos especializados en la operación y gestión de incidentes de seguridad llamados CSIRT (Equipo de Respuestas Ante Incidentes de Seguridad Informáticos), como una respuesta eficaz ante los nuevos riesgos, ataques, amenazas y vulnerabilidades informáticas que afectan de manera global; los Equipos de Respuesta con el pasar del tiempo e innovación tecnológica, han desarrollado nuevas áreas especializadas en combatir una gran cantidad de incidentes informáticos mediante la aplicación de una nueva rama en la ciencia y tecnología conocida como Informática Forense, la cual un área especializada que integra conceptos de seguridad, procedimientos, estándares y metodologías para el procesamiento de evidencias físicas y digitales, obtenidas mediante el adecuado uso de la cadena de custodia, permitiendo a los investigadores el correcto análisis de los vestigios e indicios informáticos recopilados en la escena, empleando equipamiento forense especializado, metodologías, y procedimientos legalmente establecidos, que permitan al investigador efectuar la recopilación y protección de los indicios obtenidos que pueden llegar a ser evidencias sustentables o probatorias, para el descubrimiento de los infractores, quienes posteriormente serán procesados en juicios basados en la Ley.

Palabras clave:Equipo de Respuesta Ante Incidentes de Seguridad Informáticos (CSIRT), Informática Forense, activos informáticos, ataques informáticos, almacenamiento, amenazas, evidencias, cadena de custodia, indicios, infractores, registros, sistemas, vulnerabilidad de sistemas.

Abstract:

This article aims to raise awareness about the attacks and invasion strategies that are being improved every day by people with advanced knowledge in information technologies and systems, most of whom threaten the integrity of the information security and privacy of people, institutions, governments and society, thereby generating several public and private institutions in the world wide web, the imminent

need to develop specialized agencies in the operation and management of security incidents called CSIRT (Computer Security Incident Response Team), as an effective response to new risks, attacks, threats and vulnerabilities, affecting the systems and information in all world; Response Teams with the passage of time and technological innovation, developed new specialized areas to combat a lot of IT incidents, implementing a new branch of science and technology known as Computer Forensics, which integrates a specialized area with security concepts, procedures, standards and methodologies for processing physical and digital evidence, obtained by the proper use of chain of custody, allowing researchers to the correct analysis of the remains and computer evidence collected at the scene using forensic specialized equipment, methodologies, and legally established procedures that allow the researcher to make the collection and protection of evidence obtained that can become sustainable or probative evidence for the discovery of the offenders, who will later be processed in judgments based on the law.

Keywords:Computer Security Incident Response Team (CSIRT), Computer Forensics, IT assets, cyber-attacks, storage, threats, evidence, chain of custody, evidence, offenders, records, systems, systems vulnerability.

I. Introducción

El campo de la Tecnológica engloba grandes innovaciones y servicios tecnológicos que no solo facilitan la vida cotidiana de sus usuarios, sino que son el actual medio de trabajo, desarrollo y producción a nivel mundial; sin embargo hoy en día los robos y atentados informáticos utilizando la innovación tecnológica son cada vez mayores, puesto que a más de generar pérdidas económicas se enfocanen el daño contra las personas, empresas, gobiernos y sociedad en general.

Hoy en día el comprobar el origen de los ataques informáticos e incluso identificar a un atacante puede ser una tarea realmente difícil y aún más si se desean utilizar las pruebas obtenidas como elementos en un proceso judicial si no se tiene una formación o especialización en temas informáticos altamente especializados que sustenten el conocimiento y validez de los resultados; frente a ésta óptica, es necesario conocer que todo incidente informático, ya se trate de un delito, accidente, conflicto, o de cualquier otro tipo, siempre deja vestigios en el lugar de los hechos, por lo cual es importante que el personal informático a cargo de la investigación conozca sobre la aplicación de nuevas invenciones y tecnología informática, así como el manejo de Leyes y Legislación en materia de Derecho Informático en contra de actos ilícitos con el fin de identificar, preservar, analizar y presentar las evidencias obtenidas de una manera legalmente aceptable antes jueces y tribunales para su sanción.

II. Metodología.

La metodología de investigación empleada en el presente estudio, pertenece al investigador Gordon Dankhe (1.986), recopilada y sintetizada en el libro “Metodología de la Investigación”[1]; esta metodología, clasifica a la investigación en exploratoria la cual tiene como objeto efectuar la recopilación de la información obtenida de las fuentes primarias y secundarias en la investigación para dar paso al desarrollo de la investigación descriptiva, la cual a su vez permitirá realizar la operacionalización de las

[1] Metodologías de la Investigación, McGraw Hill, México, 1996, Capítulo 4.

variables, identificando la variable independiente (VI)[2] y variable dependiente (VD)[3], indispensables para el desarrollo de las entrevistas y cuestionarios que aplicadas a un universo seleccionado permitirán medir el grado de relación que puede existir entre dichas variables, generando de este modo las justificaciones que nos llevarán a realizar la Propuesta del Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos (CSIRT).

a) Definición de términos

CSIRT: Según CERT/CC, un Computer Security Incident Response Team (CSIRT), es una organización responsable de recibir reportes de incidentes de seguridad, analizarlos y responderlos.

Esteganografía: Proviene del griego steganos que significa oculto, es la parte de la criptología en la que se estudia y aplican técnicas que permiten el ocultamiento de mensajes u objetos dentro de ellos llamados portadores con el fin de que no se conozca la real existencia de lo que se está ocultado

HASH: Función o método utilizado para investigaciones en la Informática Forense para generar claves o llaves que representen de manera única a un documento, registros, archivos, entre otros.

Indicio o Evidencia: Son las huellas, vestigios y demás elementos materiales del hecho delictuoso que pueden ser recopiladas de la escena del crimen y/o lugar de los hallazgos y que por sus características existe la posibilidad que estén relacionados con la comisión del delito investigado.

Informática Forense: Según el FBI, la Informática Forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional, encargada de analizar los sistemas informáticos en busca de evidencias que colaboren a llevar adelante una causa judicial o una negociación extrajudicial ante los tribunales civiles y/o penales.

III. Evaluación de resultados y discusión

La información es un bien valioso e incalculable en todos sus aspectos, y con la popularización de la innovación tecnológica los problemas de seguridad en los sistemas informáticos incrementan, generando que el descubrimiento de las infracciones producidas sigan siendo una ardua tarea para los investigadores debido a la inexistencia de áreas especializadas en evitar y descubrir los ataques cibernéticos; en el Ecuador hasta el mes de septiembre del año 2.013, existían 10’360.278 usuarios que emplean el servicio de Internet para el desarrollo de su vida cotidiana y laboral, colocando desapercibidamente una gran cantidad de información y transacciones en repositorios informáticos y sitios web que podían ser violentados y/o vulnerados, por diseminación de código malicioso, explotación de vulnerabilidades, fraudes financieros en la web, infección con malware, ataques de denegación de servicio (DoS), phishing, indisponibilidad de los servicios y aplicaciones informáticas, explotación de vulnerabilidades, acceso indebido a la información, entre otros, los cuales generan una

[2] (VI): Propuesta de Diseño de un Área Informática Forense.
[3](VD): Identificación de los ataques informáticos.

gran cantidad de casos a ser investigados por las autoridades competentes los cuales en su gran mayoría no pueden ser atendidos puesto que para efectuar la identificación, análisis y seguimiento de dichos incidentes informáticos se requieren de mayores conocimientos abarcados dentro de una nueva especialidad llamada informática forense.

Por lo anteriormente expuesto se considera importante realizar la Propuesta de Diseño de un Área Informática Forense para un Equipo de Respuestas ante Incidentes de Seguridad Informáticos (CSIRT), en el Comando Conjunto de las Fuerzas Armadas (CC.FF.AA), cuya implementación permitirá el seguimiento y esclarecimiento de los reportes sobre la vulneración de seguridad a los sistemas informáticos, identificación del aprovechamiento sobre la explotación de vulnerabilidades, fallas procedimentales y tecnológicas en las infraestructuras informáticas, entre otras acciones; minimizando de éste modo el impacto resultante de los actos informáticos ilícitos mediante la aplicación de la Informática Forense, iniciando de este modo con la propuesta de estructura funcional del Equipo de Respuestas Ante Incidentes de Seguridad Informáticos CSIRT para el CC.FF.AA.

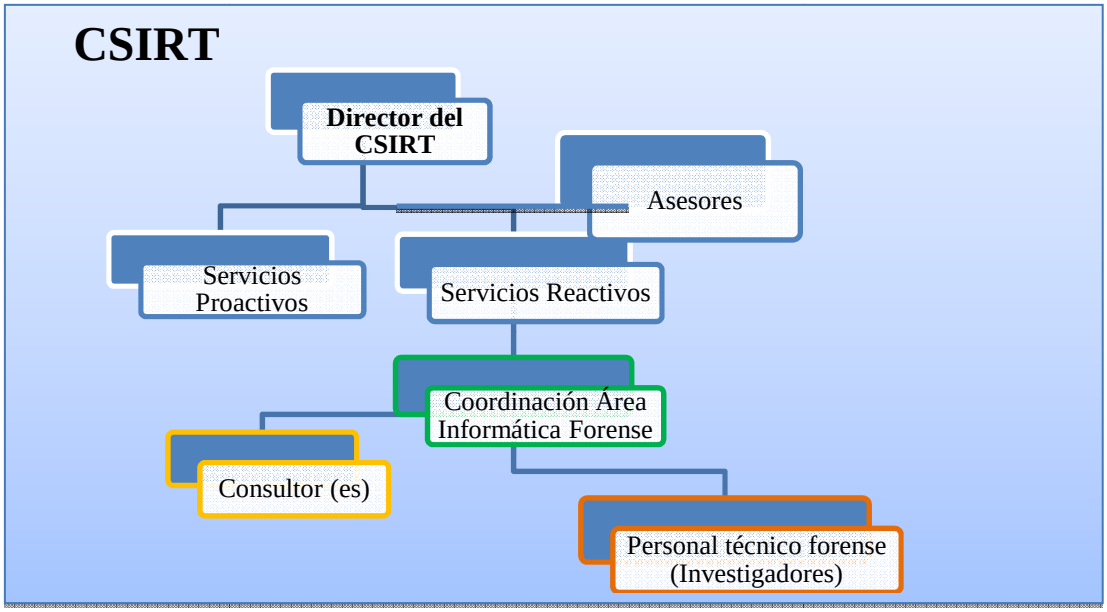

Figura 1: Propuesta de Diseño Interno del CSIRT para el Comando Conjunto de las Fuerzas Armadas (CC.FF.AA)

Servicios Proactivos: Los servicios proactivos dentro del CSIRT del CC.FF.AA deben ser servicios de alerta temprana, estadísticas sobre avances y cierres de incidentes informáticos, formación y comunicación a usuarios de la comunidad, publicación de alertas y avisos sobre seguridad informática.

Servicios Reactivos: Los servicios reactivos deben ser iniciados por la generación de un evento o requerimiento de atención a un incidente informático que describe un ataque de intrusión dentro del sistema o infraestructura tecnológica cuya seguridad ha sido comprometida y/o violentada, los servicios reactivos dentro del CSIRT del CC.FF.AA deben ser gestión de incidentes, gestión de vulnerabilidades, análisis forense y manejo de evidencias.

a) Diseño Interno del Área Informática Forense

El diseño interno del área Informática Forense del CSIRT para el CC.FF.AA, debe brindar y garantizar un ambiente seguro e integral para la operación diaria del personal forense, así como de las evidencias, el área deberá contar con suministro eléctrico permanente, acondicionamiento térmico, elementos de seguridad físicos, circuito cerrado de televisión, sistema de seguridad y detección de incendios, así como puerta de ingreso multilock accionada por un control biométrico que valide los accesos permitidos.

b) División del Área Informática Forense del CSIRT para el CC.FF.AA

El espacio físico disponible para el diseño del área corresponde a 180 m^2, los cuales estarán divididos en seis sub áreas de trabajo de libre acceso, con divisiones internas de vidrio o paneles móviles sin ventanas de altura no mayor al 1.20 mts., las cuales son un área de coordinación, un área de trabajo para consultor(es), un área de investigaciones, un laboratorio forense, un área para almacén de evidencias, una sala de reuniones.

El servicio de Internet en el área Informática Forense deberá ser permanentemente monitoreado y controlado, así como el análisis de información de documentos entrantes y/o salientes, y bloqueo de correos electrónicos pertenecientes a dominios que no consten en las listas permitidas; adicionalmente el uso de dispositivos de almacenamiento de información y equipos celulares de uso personal no deberán ser autorizados dentro del área, excepto aquellos autorizados por la autoridad competente.

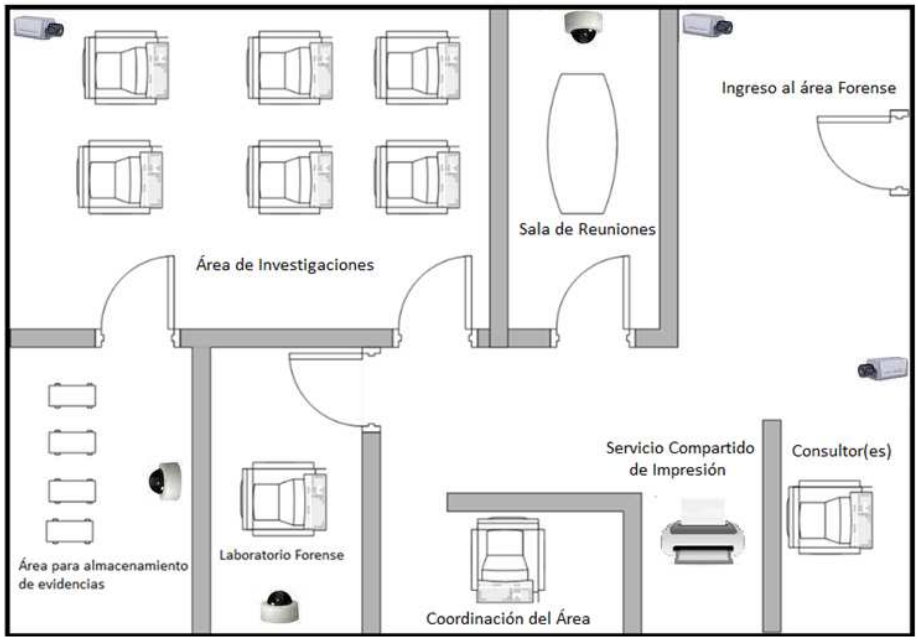

Figura 2: División del Área Informática Forense del CSIRT para el CC.FF.AA

En el presente diseño es importante considerar el aislamiento físico de dos sub áreas esenciales tales como son: el área de almacenamiento de evidencias y el laboratorio forense, puesto que dentro de éstas sub áreas se realizará el análisis de todo indicio y/o evidencia recopilada de los procesos de investigación, las mismas que deberán ser

preservadas de cualquier tipo de contaminación, interferencia, emisiones electromagnéticas, entre otros factores físicos y ambientales que alteren la naturaleza en la que fueron encontradas, motivo por el cual el acceso a las sub áreas mencionadas deberán ser estrictamente supervisadas por el Coordinador del área, adicionalmente se bloqueará cualquier conexión a Internet no autorizada, así como telefonía celular, con el fin de evitar cualquier fuga de información sobre el proceso de análisis de las evidencias, manipulación a los resultados, intervención, alteración o daño a las evidencias recopiladas por los investigadores forenses.

c) Seguridad Física para el Área Informática Forense

Al ser un área crítica y sensible que se encargará de la atención especial de las investigaciones sobre los incidentes informáticos reportados al CSIRT del CC.FF.AA, se requerirá de controles de acceso, credenciales, procedimientos, guardianía, alarmas, circuito cerrado de televisión, entre otras acciones de seguridad de alto nivel, puesto que la posibilidad de riesgos, amenazas y atentados nunca pueden ser descartados y podrían atentar contra la integridad de las personas, los datos, robo de información, integridad de los sistemas, entre otros y debe ser capaz de asegurar la capacidad de supervivencia del área ante eventos que pongan en peligro su existencia, protegiendo y conservando todos los activos, indicios y/o evidencias de riesgos, desastres naturales o actos mal intencionados.

La Seguridad Física del Área Informática Forense debe contar con los sistemas de detección de incendios, circuito cerrado de televisión, seguridad ambiental para el área, espacio y movilidad, tratamiento acústico, ambiente climatizado, instalaciones eléctricas seguras, seguridad en el cableado y equipamiento tecnológico, iluminación adecuada, y seguridad en la red para el área.

d) Herramientas Informáticas y Equipamiento para el Área Informática Forense

En la actualidad el incremento del uso de la tecnología ha facilitado el acontecimiento de delitos que involucra medios tecnológicos e información digital cambiando la manera tradicional de realizar las investigaciones, motivo por el cual hoy en día se deben emplear una variedad de equipos y herramientas forenses especializadas en la recopilación y tratamiento de los indicios y evidencias, dada la complejidad de los actuales sistemas y equipos tecnológicos a ser investigados, el investigador debe apoyarse en el uso de varias herramientas que permitan minimizar la cantidad de errores, pérdidas de información e incertidumbre de un proceso, lo cual puede ser logrado mediante el empleo de equipamiento informático forense especializado.

e) Selección de herramientas de software para Análisis Forense

Para la presente Propuesta de Diseño, se realizó la selección de dos herramientas de software especializadas las cuales son EnCase de Guidance Software y Forensic Tool Kit (FTK) de Access Data, puesto qu EnCase es una herramienta informática forense que permite asistir al investigador durante todo el proceso de investigación digital, este software permite el copiado comprimido de discos fuente empleando un estándar sin

pérdida conocido como "loss-less"[4], para crear copias comprimidas de los discos origen, los archivos comprimidos resultantes pueden ser analizados, buscados y verificados de manera semejante a los originales, esta característica ahorra cantidades importantes de espacio en disco del computador en el cual se realiza la investigación forense permitiendo de este modo trabajar al mismo tiempo con una gran diversidad de casos buscando la evidencia y realizando búsquedas en paralelo.

Access Data Forensic Tool Kit con su herramienta FTK ofrece un análisis forense completo proporcionando búsquedas y filtrados de ficheros que permiten encontrar de manera más ágil una evidencia, es una herramienta fácil de usar y contiene 270 formatos de ficheros diferentes los cuales pueden ser navegados a través de un explorador, genera logs e informes y es compatible con otras herramientas de software forense, permite efectuar búsquedas avanzadas para imágenes (jpg) y textos de Internet, recupera automáticamente ficheros y particiones borradas de un disco, y realiza el análisis de emails y ficheros (zip).

Servicios	EnCase	ForensicToolkit FTK
Clonación de discos	X	X
Validación de la integridad criptográfica de las evidencias	X	X
Información del sistema	X	X
Adquisición de imágenes en vivo	X	X
Recuperación de contraseñas	X	X
Recuperación de archivos borrados	X	X
Recuperación de correos borrados	X	X
Análisis Forense en Red	X	
Análisis Forense en Navegadores	X	X
Análisis de Dispositivos Móviles	X	
Análisis de documentos firmados electrónicamente	X	
Búsqueda de archivos	X	X
Reportes automáticos	X	X
Adquisición de evidencia de la RAM	X	
Herramientas de automatización	X	
Análisis de discos IDE y Serial ATA	X	X
Análisis de discos RAID y SCSI	X	
Reparación de sectores de disco defectuosos	X	X
Reparación de particiones dañadas	X	X
Recuperación de información eliminada por virus	X	X
Recuperación de imágenes ocultas (esteganografía)	X	X

Tabla 1: Beneficios de las herramientas de software seleccionadas

f) Selección de herramientas para la recolección de evidencias

Entre las herramientas para la recolección de evidencias para el análisis forense denotan Chat Examiner de Paraben, la cual es una herramienta diseñada para analizar los historiales de evidencias de conversaciones de chat que quedan en una máquina o estación de trabajo al ser investigados; E-Mail Examiner de Paraben, diseñada para analizar los formatos más comunes de clientes de correo electrónico como Outolook y Thunderbird; Network E-Mail Examiner, diseñado para analizar el correo electrónico en

[4] Loss-Less: Término informático empleado para indicar la menor pérdida de datos o información.

red tales como Microsoft Exchange, Lotus Notes y Group Wise; Password Recovery Kit Forensic que recupera contraseñas de archivos, discos duros y aplicaciones de red; y Elcomsoft Password Recovery Bundle Forensic, que permite eliminar protecciones y descifrar archivos y discos duros de aplicaciones populares.

g) Selección de herramientas de hardware para Análisis Forense

Entre las herramientas de Hardware para el análisis forense denotan el equipo de investigación Forensic Recovery of Evidence Device Diminutive Interrogation Equipment (F.R.E.D.D.I.E), el cual es un servidor portable para el almacenamiento de evidencias y procesamiento de casos y el servidor de alta capacidad y procesamiento para la recuperación forense de información FREDC, el bloqueador de escritura Tableau Ultrablock FireWire Kit, el equipo de descifrado y almacenamiento de contraseñas Rac-A-Tack, el equipo para la previsualización en sitio de una evidencia contenida en un disco duro Voom Shadow2, el equipo de investigaciones portable EnCase Portable Sing, y el equipo de herramientas para análisis forense a celulares Paraben Device Seizure Field Kit.

g) Diseño de la red para el CSIRT y Área Informática Forense del CC.FF.AA

La infraestructura de la red forense debe estar separada del resto de la infraestructura del CSIRT del CC.FF.AA, con el fin de que cuente con una estructura propia de subredes y dominios permitiendo implementar segmentos de red con funciones específicas para la operación y administración del equipamiento forense los cuales deberán tener entre sus opciones de configuración y autenticación el acceso remoto.

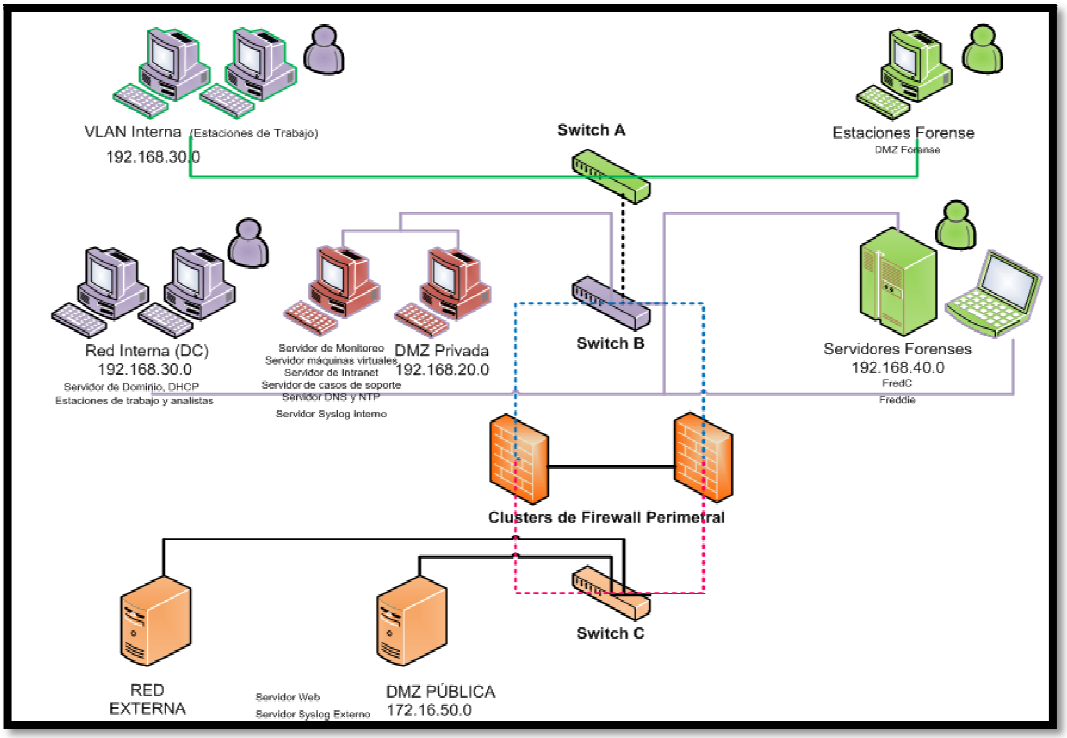

Figura 3: Diseño de la red para el CSIRT y Área Informática Forense del CC.FF.AA

h) Evaluación Económica al Proyecto

La evaluación económica del presente proyecto de investigación no contempla ningún cobro por la prestación de los servicios a ser provistos por el área Informática Forense del CSIRT del CC.FF.AA, por ser un proyecto de desarrollo social y por sus características, no generará ingresos o beneficios de tipo monetario durante su vida útil; sin embargo generará beneficios a la sociedad ecuatoriana mediante la exposición de los criterios que sustentan la ejecución del mismo.

El presupuesto económico necesario para efectuar la Propuesta de Diseño del Área Informática Forense para el CSIRT del Comando Conjunto de las Fuerzas Armadas (CC.FF.AA), es efectuado en base a la proyección del talento humano, adecuaciones internas para el área, adquisición del equipamiento tecnológico, infraestructura física, software, hardware, servicio de Internet, entre otros tipos de equipamientos y servicios necesarios para el buen funcionamiento del área forense.

Presupuesto Total Requerido para el Área Informática Forense		
Detalle	**Valor anual sin IVA ($) primer año**	**Valor anual sin IVA ($) años posteriores**
Adecuaciones para el área forense	43.170	0
Contratación del Talento Humano	186.072	186.072
Equipamiento Forense	88.040,6	0
Renovación y/o suscripción de licencias de software	0	4.900
Equipamiento Tecnológico	58274,33	0
Mantenimientos preventivos y/o correctivos	0	1.900
Servicio de Internet (3 - 5 Mbps)	1.661,88	1.361,88
Materiales de Oficina	4.001	4.001
TOTAL PRESUPUESTO REQUERIDO:	**381.219,81**	**198.234,88**

Tabla 2: Presupuesto total requerido para el Área Informática Forense

Es necesario destacar que en base al análisis del presupuesto económico requerido, el Comando Conjunto de las Fuerzas Armadas (CC.FF.AA), deberá prever en su presupuesto anual, los recursos necesarios para financiar la presente propuesta.

IV. Trabajos relacionados

El foro de Equipos de Seguridad para Respuesta a Incidentes (FIRST), fue la primera organización global reconocida en respuesta a incidentes, la cual fue formada en el año de 1.990 en respuesta al problema del gusano de Internet que atacó en el año de 1.998, el FIRST busca fomentar la cooperación y coordinación en la prevención de incidentes y promueve la cultura de compartir información entre sus miembros por medio de su sitio oficial, esta organización funciona bajo un marco operacional de reglas de alto nivel en la cual sus miembros desarrollan y comparten información técnica, herramientas, metodologías, procesos, así como mejores prácticas de seguridad con el fin de promover un ambiente electrónico global más seguro, el objetivo de esta organización es fomentar la cooperación y coordinación en la prevención de incidentes, promoviendo el intercambio de información entre sus miembros.

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), es otra organización que desde hace varios años apoya en la creación de diferentes grupos europeos dedicados a la seguridad de la información para la prestación de servicios de seguridad adecuados que garanticen el nivel elevado y efectivo de las redes y de la información en la Comunidad Europea, ENISA pone a disposición sus servicios en alertas y advertencias, análisis, tratamiento y apoyo a incidentes, respuesta de incidentes en sitio, análisis de vulnerabilidades, recopilación de pruebas forenses, seguimiento o rastreo, servicio de detección de intrusos, difusión de información relacionada con la seguridad, consultorías en seguridad, entre otros servicios publicados en su sitio oficial.

V. Conclusiones y trabajo futuro

Se puede concluir del presente proyecto de investigación que en la actualidad el valor de la información se encuentra en aumento y es vital la protección de la misma puesto que la delincuencia informática abarca todo tipo de comportamiento no ético, antijurídico y no autorizado empleando actos ilícitos, ataques e intrusiones a cualquier sistema, datos, equipos tecnológicos, entre otros, violentando sus accesos, alterando su funcionamiento y en su mayoría robando la información contenida en ellos, motivo por el cual la Propuesta de Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos (CSIRT), brindará la oportunidad a los expertos e investigadores informáticos forenses en identificar, analizar, y responder ante ellos de forma óptima, puesto que mientras más pronto se ejecuten las acciones de corrección de los ataques, se minimizarán los daños y los costos que involucren el restablecimiento de los servicios comprometidos así como la posible recuperación de la información afectada o robada.

La Propuesta de Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos (CSIRT), será una solución eficaz que brindará ayuda en el esclarecimiento de los actos ilícitos que permitirán la identificación de la información comprometida durante el ataque, empleando una cadena de custodia legalmente establecida que vele por la protección de los indicios y/o evidencias obtenidas que servirán de sustento legal ante los juicios contra los infractores descubiertos.

Por lo anteriormente expuesto se recomienda realizar la propuesta de diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos (CSIRT), puesto que ayudará en el planteamiento de recomendaciones sobre controles de seguridad frente a conductas anti sociales que han convertido a los activos, equipos y sistemas en medios perfectos para delinquir, por lo cual es necesario considerar nuevas formas de defensa e investigación que puedan ser utilizadas para el esclarecimiento de delitos informáticos, análisis de incidentes, reconstrucción de escenas de penetración a los sistemas, y ayuda en el planteamiento de recomendaciones sobre controles de seguridad futuros.

Referencias bibliográficas

Brezinski, D., & Killalea, T. (Febrero 2002). *Guidelines for Evidence Collection and Archiving.* IETF.

Brian Carrier, H. H. (2003). *Getting Physical with the Digital Investigation Process* (Vol. 2). International Journal of Evidence.

Carhuatocto, R. (2003). *Digital Forensics.* Barcelona: esCERET-UPC.

Ciardhuáin, S. (2004). *An Extended Model of Cybercrimen Investigations* (Vol. 3). International Journal of Digital Evidence.

José, C. M. (2006). *Buenas Prácticas en la Administración de la Evidencia Digital*. Recuperado el 21 de Octubre de 2013, de http://gecti. uniandes.edu.co/docs/doc_gecti_7_06.pdf

K, G. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs).*Pensilvania: Universidad Carnegie Mellon.

Ministerio de Comunicaciones República de Colombia. (2008). *Diseño de un CSIRT de Colombia.*Bogotá Colombia.

Noblett, M. G. (s.f.). *Recovering and Examining Computer Forensic Evidence*. Recuperado el 12 de Septiembre de 2013, de http://www.fbi.gov/hq/lab/fsc/backissu /oct2000 /computer.htm

R, C. (2012). *The Critical Sucess Factor Method: Establishing a Foundation for Enterprise Security Managment.* Hanscom, USA: Carniege Mellon.

Scientific Working Group on Digital Evidence: Standars and Principles. (s.f.). Recuperado el 22 de Octubre de 2013, de http://www.fbi.gov/hq/lab/fsc/backissu/ april2000/swgde.htm

Universidad Carnegie Mellon. (2004). *Steps for creating National CSIRT.*Pensilvania.

Eoghan Casey. (2004). *Digital Evidence and Computer Crime Forensic Science, Computer and the Internet* (2 ed.). Academi Press.

Mark Reith, C. C. (2002). *An Examination of Digital Forensic Models* (Vol. 1).

McKemmish, R. (1999). *What is forensic computing?* Austria: Canberra : Australian Institute of Criminology.

Neil Salkind. (1998). *Métodos de Investigación.* México: Prentice Hall.

Fernández Blenda, D. (2004). *Informática Forense, Teoría y Práctica.*Sevilla.

R, M. (1999). *What is forensic computing?* Austria: Australian Institute of Criminology.

Séamus Ciardhuáin, Ó. (s.f.). *Key Research Issues for Forensic Computing.*

Vacca, J. R. (2002). *Computer Forensic*. Charles River Media.

Justice, U. D. (s.f.). Electronic Crime Scene Investigation. EE.UU.

ACCESS DATA. (s.f.). Recuperado el 23 de Julio de 2013, de http://www.accessdata.com/products/ftk/

ArCERT, I. (s.f.). *Coordinación de Emergencias en Redes Teleinformáticas de la República de Argentina*. Recuperado el 12 de Junio de 2013, de http://www.icic.gob.ar/paginas.dhtml?pagina=100

CCN-CERT. (20 de Junio de 2007). *Centro Nacional de Inteligencia (CNI).* Recuperado el 30 de Mayo de 2013, de https://www.ccn-cert.cni.es

CNI. (20 de Junio de 2007). *CCN-CERT*. Recuperado el 11 de Junio de 2013, de https://www.ccn-cert.cni.es/index.php?option=com_docman&Itemid=237&lang=es

Comando Conjunto de las Fuerzas Armadas. (s.f.). Recuperado el 08 de Febrero de 2013, de http://www.ccffaa.mil.ec/index.php/institucion/organigrama

COMPUTER FORENSIC. (s.f.). Recuperado el 15 de Enero de 2013, de http://computer-forensics.sans.org/blog/2010/08/10/review-access-data-forensic-toolkit-ftk-version-3-part-2/

Diario el Universo. (26 de Agosto de 2012). Recuperado el 30 de Septiembre de 2012, de http://www.radioviva.com.ec/web/?p=6421