Universidad de las Ciencias Informáticas

“Facultad 2”

Título: Propuesta de un procedimiento para la gestión centralizada de logs, detección de ataques y análisis forense en Centros de Procesamiento de Datos.

Trabajo de Diploma para optar por el título de
Ingeniero Informático.

Autor: Juan Andrés Centelles Diez.

Tutor: Ing. Adrian Hernández Yeja.

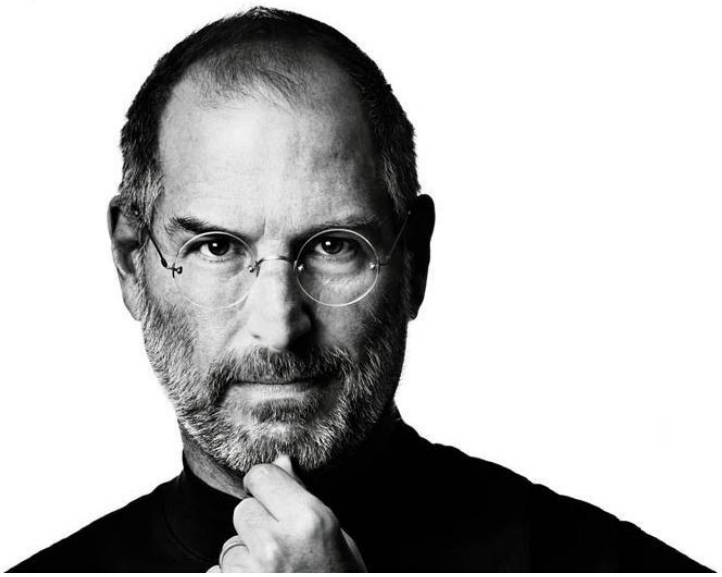
La Habana, junio del 2012.

”Año 54 de la Revolución”.

Pensamiento

La única manera de hacer un gran trabajo es amar lo que hace.

Steve Jobs



DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo al <nombre área> de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

_____

Juan Andrés Centelles Diez

_____

Ing. Adrian Hernández Yeja

DATOS DE CONTACTO

[insertar breve curriculum e información de contacto del tutor]
[insertar breve curriculum e información de contacto del asesor]
[insertar breve curriculum e información de contacto del consultante]

Agradecimientos

Agradezco a mis padres, hermanos y familia por hacerme quien soy.

A Lía por estar en todos los momentos difíciles y por el cariño.

A mi tío Omar por ser además de mi amigo, el productor de mis metas.

A mi prima Ilo por ser la voz de mi conciencia y mi confidente.

A Reider, por la confianza y el apoyo, Harlinson y Diana por ser mis segundos padres, Yusi, Mayi y Jesús por ser los mejores compañeros de cuarto en Venezuela.

A mi tutor por su consejo invaluable. A Ramón Alexander Anglada profesor y guía, por revelarme la magia del software libre en mis primeros años en la universidad.

A Yandy por compartir conmigo las líneas de código mas entretenidas por 3 largos años.

A Rainer por las carreras de último momento.

A Nuris, la mejor instructora de la UCI.

Al profe Joel y los muchachos del kenpo, de quienes aprendí muchísimo.

A los amigos con quienes inicié este viaje de tantos años que culmino hoy: José Raúl, Arniel, Rauber, Tellez, Yoan, Salmerón, Yazmín y Ricardo, Rainer, Ernesto, Víctor, Oscar, El Macho, Betty, Ailén, Neivis, Rafael.

A Serguei profesor, amigo y consultante voluntario. En fin a todas aquellas personas cuyo actuar hizo posible la realización de este trabajo y que por alguna razón olvidé mencionarlos.

Dedicatoria

Dedicado a Juan A. Centelles Riaño padre y abuelo querido.

A mis hermanos Milo y César esperando ser su fuente de inspiración…

Resumen

En un Centro de Procesamiento de Datos se genera gran cúmulo de información como resultado de las técnicas, mecanismos y herramientas utilizadas, lo que convierte en un verdadero reto el control y manejo de la misma. En la Universidad de las Ciencias Informáticas, el proyecto Centro de Datos del Centro de Telemática (TLM) presenta esta dificultad, que tributa a la aparición de vulnerabilidades y brechas de seguridad. En este marco se hace necesario garantizar la gestión centralizada de logs, análisis forense y la prevención de ataques. En el presente trabajo se desarrolla un procedimiento dirigido a la gestión centralizada de los logs generados, el análisis forense y la prevención de ataques. El mismo está orientado a la integración de las herramientas, mecanismos, técnicas empleadas en los Centros de Procesamiento de Datos, así como a la retroalimentación dinámica, tributando a la invulnerabilidad de los mismos. A lo largo de la investigación se proponen un conjunto de roles, etapas, artefactos, herramientas y actividades que sustentan el funcionamiento del procedimiento propuesto. Se describe la validación del procedimiento por el Método de Expertos, específicamente empleando el Método Delphi.

PALABRAS CLAVE: Logs, Análisis Forense, gestión, Centro de Procesamiento de Datos, retroalimentación.

ÍNDICE

Índice de Figuras

Índice de Tablas

Introducción

Con el desarrollo de las tecnologías informáticas los usuarios comenzaron a necesitar el acceso a mayor cantidad de recursos, los cuales no se encontraban en sus ordenadores; por lo que se hizo necesario interconectarlos entre sí. De esta forma la humanidad vio el nacimiento de Internet y por consiguiente el surgimiento de los ataques informáticos, métodos por los cuales un individuo empleando herramientas informáticas es capaz de desestabilizar, dañar o hacerse con el control de un sistema informático (red u ordenador). Los individuos capaces de realizar tales actos se denominaron ciberpiratas.

Por otra parte con el impulso de las nuevas Tecnologías de la Información y las Comunicaciones (TIC), y su impacto en el desarrollo de aplicaciones informáticas, la sociedad actual se ha digitalizado a grandes niveles. A partir de dicho desarrollo surgen nuevos servicios y tecnologías que tributan a un nivel de vida superior, así como a la optimización de los procesos en múltiples esferas. Por lo que estos servicios y sistemas informáticos se convirtieron en contenedores de información tan sensible como transacciones bancarias, registros penales, secretos industriales e incluso documentos gubernamentales clasificados. Basados en el concepto "***la información es poder***"[1] estos servicios individualmente han sido objeto de múltiples ataques por parte de hackers, los cuales para burlar los mecanismos de seguridad y controlar u obtener información sensible han empleado desde software novedoso hasta ingeniería social, siendo esta última su herramienta más efectiva.

En respuesta a las crecientes demandas de las nuevas tecnologías surgió la necesidad de aumentar la capacidad de procesamiento de los ordenadores además de proteger físicamente los servidores y concentrarlos en un mismo local con acceso restringido. Con este propósito se diseñaron centros especializados donde administrar y monitorizar los mismos en tiempo real, viendo así el surgimiento de los Centros de Procesamiento de Datos (CPD).Mas la centralización de la información los convirtió en blancos prioritarios de ataques informáticos siendo necesario a su vez la introducción y actualización de sistemas y técnicas de seguridad informática partiendo desde sistemas de detección de intrusos hasta complejos firewalls, analizadores de logs y zonas desmilitarizadas (DMZ), convirtiendo el proceso de análisis y detección en una tarea imprescindible.

[1] **Tomado de Sisterhood is Powerful, de Robin Morgan, poetisa norteamericana que modificó la frase original: Conocimiento es Poder, de sir Francis Bacon, filósofo y poeta inglés. Esta frase rápidamente se volvió popular convirtiéndose en un axioma.**

Esta novedosa realidad hace eco en la sociedad cubana, la cual ha ido insertándose en el conocimiento y utilización de modernas tecnologías, prácticamente inaccesibles para el país. En la Universidad de las Ciencias Informáticas, un proyecto de la Revolución Cubana devenido en parque tecnológico con el objetivo de llevar a cabo la informatización del país, existe un polo de desarrollo, el Centro de Telemática (TLM) el cual engloba un conjunto de proyectos productivos entre los cuales se encuentra el Proyecto Centro de Datos cuyo propósito fundamental es el diseño, despliegue y consultoría de Centros de Procesamiento de Datos (CPD).

En el Proyecto Centro de Datos no existe una solución que garantice la gestión centralizada de logs, análisis forense y prevención de ataques de manera integrada dado el amplio universo y la diversidad de mecanismos y herramientas que intervienen en los procesos antes mencionados, los cuales gozan de total independencia en cuanto a su arquitectura y diseño, razón que dificulta en extremo su integración. Es adecuado esclarecer que en el flujo regular del CPD se generan grandes cúmulos de datos como resultado final de las herramientas, mecanismos, eventos y su interacción Al no existir políticas o mecanismos que organicen, controlen, regulen y almacenen la información se dificulta la comprensión y análisis de los datos recolectados, hecho que podría indicar un manejo insuficiente de la información obtenida por las herramientas al estar funcionando de manera independiente y no como un todo, y que podría devenir en futuras vulnerabilidades o brechas de seguridad.

Teniendo en cuenta lo anteriormente planteado surge el **problema a resolver**: ¿Cómo garantizar la gestión centralizada de logs, detección de ataques y análisis forense en el proyecto Centro de Datos del centro TLM?

Así como emerge la **Idea a Defender:** Si se formula una propuesta de procedimiento capaz de garantizar la gestión centralizada de logs, prevención de ataques y análisis forense en el proyecto Centro de Datos del centro de Telemática (TLM), se facilitará el despliegue, diseño y consultoría de CPD que constituye una de las funciones principales de dicho proyecto.

Se define como **Objeto de estudio:** Los procesos relacionados con la gestión centralizada de logs, detección de ataques y análisis forense, y como **Campo de Acción:** La Organización de los procesos relacionados con la gestión centralizada de logs, detección de ataques y análisis forense en Centros de Procesamiento de Datos.

Se define como **Objetivo General:** Elaborar una propuesta de un procedimiento que garantice la gestión centralizada de logs, detección de ataques y análisis forense para Centros de Procesamiento de Datos.

Se identificaron como **Objetivos específicos:**

- ✓ Detallar los procesos que tienen lugar en los Centros de Procesamiento de Datos.
- ✓ Elaborar el marco teórico de la investigación de la propuesta de procedimiento.
- ✓ Diseñar un procedimiento capaz de garantizar la gestión centralizada de logs, detección de ataques y análisis forense en el proyecto Centro de Datos del centro TLM.
- ✓ Evaluar la propuesta de procedimiento tomando como muestra el proyecto Centro de Datos del centro TLM.
- ✓ Validar los resultados obtenidos en la aplicación de la propuesta de procedimiento.

Con el propósito de dar cumplimiento a los objetivos señalados se presentan como **Tareas de la investigación:**

- ✓ Realización de un estudio acerca de herramientas y procedimientos empleados a nivel mundial para la gestión centralizada de logs, detección de ataques y análisis forense.
- ✓ Realización de un estudio sobre las necesidades del proyecto Centro de Datos para la gestión centralizada de logs, detección de ataques y análisis forense.
- ✓ Realización de una propuesta de un procedimiento para la gestión centralizada de logs, detección de ataques y análisis forense, incluyendo su despliegue.
- ✓ Realización de un sistema de pruebas a las herramientas existentes para su inclusión en el procedimiento.
- ✓ Realización de un proceso de validación del procedimiento utilizando el Método de Expertos Delphi.

Al concluir la investigación se espera obtener como **posible resultado**: Un procedimiento capaz de garantizar la gestión centralizada de logs, detección de ataques y análisis forense en el proyecto Centro de Datos del Centro TLM.

Métodos de la Investigación:

Los **métodos Teóricos** de la investigación utilizados para dar cumplimiento a las tareas investigativas fueron:

El método **Analítico-Sintético** fue empleado para profundizar y desglosar toda la información encontrada sobre el análisis forense, la prevención de ataques y la gestión centralizada de logs.

El método **Histórico-Lógico** se empleó en el análisis del estado actual del proceso de gestión centralizada de logs, detección de ataques y análisis forense, siendo contempladas las herramientas existentes, así como las tendencias más novedosas, revolucionarias o conservadoras que pudieran contener soluciones a la problemática o pudieran tributar a la resolución de la misma.

Como también se emplearon algunos de los **métodos Empíricos:**

El método empírico de **Observación** fue utilizado en el entendimiento de la problemática, permitiendo identificar las características, procesos y comportamiento del campo, así como las necesidades del proyecto Centro de Procesamiento de Datos del Centro TLM.

El método empírico de **Experimentación** ha sido empleado en la prueba e identificación de las herramientas existentes, lo cual permite una mejor comprensión de los procesos que tienen lugar en el proyecto Centro de Datos del Centro TLM dada la interacción continua con los mismos, además de desempeñar un papel crucial en la selección de aquellas soluciones idóneas al ambiente y constituyendo el factor decisivo en la definición del procedimiento a desarrollar.

El método empírico de **Entrevista** fue utilizado para realizar consultas al personal capacitado identificado para la obtención de sugerencias y consejos basados en la experiencia de los mismos. Este método tributa directamente a la correcta construcción de la propuesta de procedimiento.

El documento consta de 3 capítulos:

Capítulo 1: “Fundamentación Teórica”, aborda las soluciones existentes al problema formulado, las tendencias más revolucionarias, herramientas, conceptos y metodología escogidos para proveer la solución más óptima a la problemática en cuestión.

Capítulo 2: “Presentación del procedimiento”, en el mismo se obtienen los roles, artefactos y herramientas seleccionadas para garantizar la gestión centralizada de logs, la prevención de ataques y el análisis forense.

Capítulo 3: “Validación del procedimiento”, es donde se aplica el procedimiento definido, así como el conjunto de técnicas definidas para la validación del mismo. En este caso de forma particular el mismo consta de dos etapas: La aplicación de métodos teóricos de validación basada en expertos y la aplicación práctica en un ambiente o escenario de prueba.

Capítulo 1: Fundamentación teórica.

1.1 Introducción

En el presente capítulo se presentan los temas fundamentales que sustentan la investigación, así como se mencionan diferentes conceptos o definiciones entre las que destacan Seguridad Informática, Logs y Centros de Procesamiento de Datos. Se abordan las herramientas utilizadas para garantizar la gestión centralizada de logs, la prevención de ataques y análisis forense.

1.2 Marco conceptual

En este epígrafe se procede a esclarecer los principales conceptos a abordar y a tener en cuenta a lo largo de la propuesta con el objetivo de facilitar la comprensión del procedimiento a consideración. Se definen brevemente las herramientas, técnicas, tecnologías y términos a emplear.

1.2.1 Procedimiento

Un procedimiento es la acción de proceder o el método de ejecutar alguna tarea específica. Se trata de una serie común de pasos definidos, que permiten realizar un trabajo de forma correcta. (1) El término procedimiento es usado para hacer referencia a todo aquel sistema de operaciones que implique contar con un número más o menos ordenado y clarificado de pasos cuyo resultado sea el mismo una y otra vez. (2)

1.2.2 Log

En cada sistema informático, ya sea sistema operativo, software, aplicación web, demonio (*daemon*) o servicio se encuentra la presencia de archivos de registro (archivos logs) los que pese a su simplicidad, desarrollan un papel importante en el funcionamiento del sistema en cuestión. Es posible definir log como aquel mensaje generado por el programador de un sistema operativo, una aplicación o un proceso en el cual se muestra un evento del sistema.

1.2.3 Servidor de logs

En un sistema informático la totalidad de las herramientas, sistemas operativos y servicios, además del propio sistema informático en sí generan logs. Por lo que existen demonios o servicios especializados en la gestión y control de este tipo de evidencia. Un servidor de logs está constituido por uno o más ficheros

de texto automáticamente creados y administrados por un servidor donde se almacena toda la actividad que se hace sobre éste. Cada servidor dependiendo de su implementación y/o configuración podrá o no crear determinados logs. (3)

1.2.4 Seguridad Informática

Se puede definir como seguridad informática al conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y/o conectados a una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. (4) El Glosario Nacional de Sistemas de Información de Seguridad de los EE.UU. define la Seguridad Informática, como la protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el almacenamiento, procesamiento o tránsito, y en contra de la denegación de servicio a los usuarios autorizados o de la prestación del servicio a usuarios no autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contabilizar esas amenazas. (5)

La misma es definida a su vez como una disciplina que se relaciona a diversas técnicas, procedimientos, mecanismos, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza la lógica y la física:

- ✓ **Seguridad lógica:** Hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático. (6)
- ✓ **Seguridad física:** Hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza. (7)

Técnicamente es imposible lograr un sistema informático ciento por ciento seguros, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos. Esto se debe a que la **Seguridad Informática es una idea subjetiva**[2], mientras que la inseguridad informática es una idea objetiva, por ello es prácticamente imposible tener control absoluto sobre la seguridad informática, porque lo subjetivo es incierto, cosa que no ocurre con la inseguridad informática, que se sabe a ciencia cierta, que ocurrirá de

[2] **Schneier Bruce, Beyond Fear. Thinking Sensibly about security in an uncertain world. CopernicusBooks. 2003**

continuar conviviendo irresponsablemente con las vulnerabilidades y los riesgos inherentes a los sistemas informáticos.

1.2.5 Amenaza

Se define una amenaza como una violación potencial de la seguridad, aunque no es necesario que ocurra la violación para que la amenaza exista. Las amenazas pueden ser clasificadas de manera general en naturales y humanas dentro de las cuales se encuentran otras subcategorías. Particularmente se hace énfasis en las humanas, que pueden ser malintencionadas o no y representan un factor importante en la protección y la seguridad informática en Centros de Procesamiento de Datos (CPD). (Ver Anexo 1 Figura 1)

1.2.6 Ataque Informático

Se conoce como el intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red. Los ataques en grupo suelen ser hechos por bandas de piratas informáticos por diversión, para causar daño, acceder a información sensible, espionaje y obtención de ganancias. Los blancos preferidos suelen ser los sistemas de grandes corporaciones o estados, pero ningún usuario de internet u otras redes está exento. (8)

Tipos de ataques informáticos

Los tipos de ataques se pueden clasificar de tres formas, según los efectos causados, según la forma de actuar y de ingeniería social.

Según los efectos causados se clasifican como: (9)

- ✓ **Interrupción:** cuando un recurso del sistema es destruido o se vuelve no disponible.
- ✓ **Intercepción:** una entidad no autorizada consigue acceso a un recurso.
- ✓ **Modificación:** alguien no autorizado consigue acceso a una información y es capaz de manipularla.
- ✓ **Fabricación:** cuando se insertan objetos falsificados en el sistema.

1.2.7 Evidencia digital

Tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. (10) La evidencia digital es considerada un desafío por aquellos que la analizan en busca de la verdad por su capacidad de ser anónima, volátil, duplicable, alterable o modificable y eliminable. (11)

1.2.8 Análisis forense

Ante la evolución vertiginosa de las técnicas de ataque informático, así como la digitalización de la información en la mayoría de las áreas, se hizo necesario conocer los objetivos, el origen y los mecanismos de los ataques de que son objeto los sistemas portadores de información sensible. Para ello se estableció la aplicación del proceso de análisis forense ante la ocurrencia de estas situaciones excepcionales.

Se denomina análisis forense al proceso de analizar una copia completa de un sistema que ha sufrido una intrusión o ataque. El mismo tiene como objetivo principal la obtención de evidencias que permitan el análisis completo y exhaustivo de para impedir la repetición de una incidencia similar futura, la puesta a disposición y procesado judicial de criminales y cibercriminales, la justificación para poder cuantificar los daños infligidos por los atacantes. Realizar un análisis forense permitirá, entre otras cosas, la recuperación del incidente de una manera más segura y evitará en la medida de lo posible que se repita la misma situación en cualquiera de las máquinas.

Si una vez realizado el análisis forense no se conoce con exactitud la respuesta a estas preguntas, no se tiene un análisis funcional. Esto puede derivar en futuros ataques bien por la misma persona o bien por diferentes medios de intrusión que se desconozcan.

1.2.9 Centro de Procesamiento de Datos

Un Centro de Procesamiento de Datos (CPD) puede ser definido como el conjunto de recursos físicos, lógicos, y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa. (12)

1.2.10 Cortafuegos (Firewalls)

En el mundo de las redes se hace imprescindible la existencia de un mecanismo regulador del tráfico de entrada a las mismas, lo que permite definir quienes, desde qué dirección o de qué manera pueden acceder a los recursos existentes en la red interna. Este mecanismo se denomina cortafuegos, en inglés firewall.

Un cortafuego es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Puede proteger a un ordenador en particular o a toda una red contra intrusiones provenientes de redes de terceros. Permite filtrar el tráfico entrante y saliente de un sistema conectado a una red. (Ver Anexo1 Figura 2) Su objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad Los sistemas *firewall* no brindan seguridad absoluta; todo lo contrario, solo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el *firewall* también son puntos débiles en la seguridad**.**

1.2.11 Sistemas de Detección de Intrusos (IDS)

Así mismo para toda red es de vital importancia conocer cuando se está desarrollando alguna actividad sospechosa o de índole maliciosa, por lo que es común y habitual el uso de Sistemas Detectores de Intrusos (IDS en inglés).

Un IDS, del inglés *Intrusion Detection System,* es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red en busca de intentos de accesos que comprometan la seguridad de los sistemas. Los IDS buscan patrones predefinidos característicos de actividades sospechosas en la red o host, analizan los paquetes de la red en busca de actividad sospechosa, por lo que esto aumenta la capacidad de prevención y alerta anticipada dado que el ataque es detectado al inicio del mismo.

1.3 Estado del Arte

En este epígrafe se realiza un estudio de las distintas herramientas que pudieran tributar a la propuesta de procedimiento diseñada, analizando las características principales con el fin de determinar las más idóneas en la concepción del procedimiento dado el escenario y la muestra definidos para el presente trabajo**.**

1.3.1 Herramientas para la gestión centralizada de logs estudiadas.

Para la elección de un servidor de logs adecuado a las características de la muestra definida para la propuesta de procedimiento se precisa, que este sea, libre y de código abierto, que tenga amplio soporte, no realice envío de paquetes en texto claro y preferentemente sea multiplataforma.

Rsyslog

Syslog es un protocolo muy sencillo cuyo funcionamiento se resume a un ordenador servidor ejecutando el servidor de *Syslog*, conocido como *syslogd* (demonio de Syslog) y un ordenador cliente que envía un pequeño mensaje de texto (de menos de 1024 bytes). Los mensajes de Syslog se suelen enviar mediante el protocolo de red UDP, por elpuerto514, en formato de texto plano. Algunas implementaciones del servidor, como *syslog-n y* rsyslog, permiten usar TCP en vez de UDP, y también ofrecen *Stunnel* para que los datos viajen cifrados mediante SSL/TLS. (13)

Ventajas:

- ✓ De código abierto.
- ✓ Puede ofrecer seguridad de los datos por canal cifrado TLS/SSL a través de Stunnel en otras implementaciones.
- ✓ Es de uso sencillo y ligero en cuanto a recursos de hardware.
- ✓ Posee versiones para Windows.

SmartLOG

SmartLOG es el sistema de gestión centralizada que permite monitorizarlas actividades que se realizan en la red. El sistema crea un entorno de gestión centralizado y eficiente de los ficheros de log. No es invasivo y está totalmente desacoplado de los sistemas hardware y software ya instalados. SmartLOG permite una adquisición y transferencia segura de todos los mensajes generados por cada sistema.

La transferencia de los mensajes de log se realiza a través de un canal seguro y cifrado SSL. Crea un sello de tiempo para cada mensaje de log, para garantizar una referencia temporal fiable y normalizar los formatos de tiempo, que pueden diferir entre los sistemas. Posteriormente los ficheros de log son cifrados

para garantizar la máxima privacidad. Al ser un sistema completamente autónomo no permite ningún acceso no autorizado a la información. (14)

Desventajas:

- ✓ Es una herramienta privativa.
- ✓ No es de código abierto.

1.3.2 Herramientas para la prevención de ataques estudiadas. Sistemas de Detección de Intrusos (IDS).

Para la selección de un IDS adecuado a la propuesta de procedimiento a realizar dada la muestra definida, se hace necesario que el mismo sea de código abierto o libre, tenga amplio soporte, permita la visualización efectiva de los datos recopilados, así como sea adaptable a ambientes específicos.

Dragón IDS

Dragón es un Sistema de Detección de Intrusos con una suite de múltiples funcionalidades capaz de funcionar como IDS de red y de *host*. Posee sensores (*Dragon Sensor*) que buscan anomalías, signos de delitos informáticos, ataques y uso indebido de la red. Permite enviar mensajes de correo electrónico, tomar medidas para detener el evento y registrarlo para su posterior análisis forense. Clasifican todos los eventos como sospechosos por lo que abundan en principio los falsos positivos, para contrarrestar esto trata de recopilar la mayor cantidad de información posible para determinar si el ataque tuvo éxito o no.

Ventajas:

- ✓ De red y host basado en versiones, gestionado por una única interfaz para facilitar su uso.
- ✓ Escalabilidad alta.
- ✓ Posee una interfaz gráfica de usuario fácil de usar y/o si se prefiere presenta la alternativa de las líneas de comando.

Desventajas:

- ✓ Es de código cerrado y no es libre.
- ✓ Exige muchos recursos de hardware al contener muchos módulos y funcionalidades.
- ✓ Decrece el rendimiento en redes de baja velocidad.

SNORT

Snort es una herramienta de detección de intrusiones de código abierto y multiplataforma que puede usarse para monitorizar redes TCP/IP y detectar una amplia variedad de tráfico sospechoso así como ataques externos. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida en el sistema. Provee al administrador de una gran cantidad de datos para tomar la decisión correcta al momento que se lleva acabo la actividad sospechosa.

Ventajas:

- ✓ Es de código abierto y multiplataforma.
- ✓ Dispone de gran cantidad de filtros predefinidos.
- ✓ Se actualiza constantemente ante casos de ataque, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.
- ✓ Permite personalizar las respuestas ante los ataques y amenazas registrados en su base de datos.

Desventajas:

- ✓ No soporta la notificación vía correo electrónico.
- ✓ Al funcionar con la interfaz de red en modo promiscuo no posee mecanismos de reducción de falsos positivos.

OSSEC HIDS (15)

En esta práctica se introduce la herramienta multiplataforma desarrollada en lenguaje C y de código abierto OSSEC, la cual constituye una consola con múltiples herramientas entre las cuales se encuentra

un detector de intrusos basado en nodo **(HIDS, *Host-based Intrusion Detection System*)** que lleva a cabo las siguientes funciones:

- ✓ Análisis de registros.
- ✓ Comprobación de integridad.

Ventajas:

- ✓ De código abierto.
- ✓ Es una herramienta multiplataforma.
- ✓ A pesar de ser un IDS de host define una estructura cliente servidor para monitorizar las estaciones de trabajo de una red.

Desventajas:

- ✓ Es una herramienta privativa.
- ✓ Solo funciona como IDS de Host.
- ✓ No tributa al posterior análisis forense.

1.3.3 Distribuciones para el análisis forense estudiadas.

Como criterio de selección escogido para las distribuciones orientadas al análisis forense a incluir en la propuesta se definió que fueran libres, de código abierto o al menos tuvieran herramientas libres de costo.

Hélix

Hélix es un Live CD (CD auto arrancable) basado en Ubuntu personalizado para análisis forense que ha sido diseñado cuidadosamente para no tocar el host en manera alguna. Hélix no monta de manera automática el espacio del área de intercambio (swap), ni los medios extraíbles con el fin de no alterar la evidencia digital. También posee un lado para auto iniciarse en Windows para la respuesta a Incidentes y Análisis forense, así como versiones comerciales y versiones libres de costo.

Ventajas:

- ✓ Posee versiones libres de costo.
- ✓ Es extremadamente cuidadoso en cuanto al manejo de evidencia digital.

Desventajas:

- ✓ Las versiones comerciales son muy superiores a las versiones libres de costo.
- ✓ Incluye herramientas privativas.

F.I.R.E. Linux

De las siglas en inglés (*Forensic and Incident Response Environment*) es un CD auto arrancable que incluye un conjunto de herramientas orientadas al campo de la auditoría forense electrónica, creadas por William Salusky y descargables gratuitamente. Entre estas se encuentran Nmap, whisker, hping2, hunt, fragrouter, Ethereal, Snort, tcpdump, chrootkit, airsnort, dsniff, Autopsy, VNC, SSH client, gpart, testdisk, todas muy utilizadas y recomendables. Las mismas le dan a F.I.R.E Linux sus características excepcionales:

- ✓ Capacidad para recolectar datos de un entorno informático sometido a intrusión o ataque.
- ✓ Posibilidad de realización de pruebas de penetración y vulnerabilidad.
- ✓ Recuperar datos de particiones dañadas o sometidas a incidencias.

Ventajas:

- ✓ Interfaz de usuario amigable.
- ✓ Descargable de forma gratuita.
- ✓ Permite la realización de pruebas de penetración.

Desventajas:

- ✓ Posee herramientas que posteriormente cerraron su código como Nessus.
- ✓ No consta de un buen soporte.

Backtrack

Backtrack es una distribución de Linux en un DVD autoarrancable desarrollado específicamente para realizar pruebas de penetración, el mismo es una combinación entre tres diferentes distribuciones de Linux para pruebas de penetración: IWHAX, WHOPPIX y Auditor, en su versión actual (5.0). Está basado en Ubuntu. Aunque está diseñado para pruebas de penetración también está equipado con múltiples herramientas para el análisis forense. (16)

1.3.4 Herramientas para el análisis forense estudiadas.

A continuación se detallan algunas de las herramientas contenidas o no en las distribuciones orientadas al análisis forense estudiadas que tributan al proceso de análisis forense.

Maltego

Maltego es una plataforma única desarrollada para entregar una imagen detallada de una amenaza existente en un entorno que una organización posee u opera. La única perspectiva ofrecida para las entidades basadas en recursos y red es la agregación de información publicada en Internet, la cual Maltego puede localizar, agregar y visualizar. Maltego es una aplicación para análisis forense y minería de datos (Data Mining) capaz de consultar varias fuentes de conocimiento públicas y de manera gráfica determinar las relaciones entre entidades como personas, compañías, sitios web y documentos. Maltego no es de código abierto aunque sí emplea el concepto de inteligencia de código abierto[3].

Ventajas:

- ✓ Emplea minería de datos.
- ✓ Utiliza el concepto de inteligencia de código abierto.
- ✓ Es regularmente utilizada por empresas de mediano a gran tamaño.

Desventajas:

- ✓ Demanda considerables recursos de hardware.
- ✓ No es una herramienta de código abierto.

Sleuth Kit

[3] **Hace referencia a una práctica de creación colaborativa del conocimiento inspirada en el movimiento Free and Open Source Software**

Sleuth Kit (en el pasado conocido como TSK) es una librería escrita en lenguaje C aunque a su vez es una colección de herramientas de líneas de comando, sistemas de archivos y ficheros de Unix para análisis forense. Posee un *framework* (*The Sleuth Kit Hadoop Framework*) que incorpora a TSK para análisis de larga escala en la tecnología de virtualización en la nube (*cloud computing*). Las herramientas del sistema de archivos permiten examinarlos archivos del sistema, de una computadora sometida a intrusión o ataque de forma no intrusiva, ya que estas herramientas no necesitan del sistema operativo para procesar los archivos del mismo, aquellos que han sido borrados o permanecen ocultos son mostrados. Para una forma de uso más amigable, puede ser utilizado en conjunto con un módulo de interfaz gráfico llamado Autopsy. (17)

Ventajas:

- ✓ Presenta una interfaz de usuario amigable.
- ✓ Es de código abierto.
- ✓ Es multiplataforma.

Desventajas:

- ✓ No posee mucho soporte.
- ✓ Requiere el pago de licencias para versiones corporativas.

Encase

Encase es una suite de software forense comúnmente usada para procesos judiciales. Es ampliamente usada ya que fue diseñada sobre los estándares forenses y está hecha para la recolección de datos de una computadora sometida a intrusión o ataque de manera no intrusiva y sin destruir o modificar la evidencia digital. Procesa y adquiere grandes colecciones de datos desde una gran variedad de dispositivos mediante procesos repetibles y seguros, identifica evidencia potencial análisis forense a nivel de disco, así como elabora reportes comprensibles de los resultados obtenidos, todo sin comprometer la integridad de la evidencia digital. (18)

Ventajas:

- ✓ Es muy cuidadosa en el manejo de la evidencia digital.

- ✓ Ampliamente empleada en el campo de proceso judiciales.

Desventajas:

- ✓ No es libre ni de código abierto.
- ✓ Se enfoca en los procesos judiciales.

1.3.5 Cortafuegos (Firewalls)

Para la selección del cortafuego a utilizar en la propuesta de procedimiento se necesita que el mismo sea de código abierto o libre, tenga amplio soporte y posea adecuada usabilidad.

Netfilter/Iptables

Netfilter es un poderoso filtro de paquetes implementado en el núcleo (*Kernel*) estándar de Linux. El espacio de usuarios de iptables es usado para almacenar las configuraciones. Actualmente soporta filtro de paquetes por estado, todo tipo de direcciones de red, traducción de puertos (NAT/NAPT) y múltiples capas de aplicación de interfaz (API) para extensiones 3d. Incluye además diferentes módulos para el manejo de protocolos tales como FTP. Al hablar de Netfilter se debe tratar como un todo respecto a iptables, ya que este último constituye parte indivisible de su sistema. (19)

Ventajas:

- ✓ Es una herramienta ligera.
- ✓ Soporta filtro de paquetes.
- ✓ Maneja protocolos como FTP y HTTP.
- ✓ Es libre y de código abierto.

Desventajas:

- ✓ No posee todas las herramientas necesarias para su implementación en un CPD.
- ✓ No es multiplataforma.

OpenBSD PF

Como Netfilter e ipfilter en otras plataformas, los usuarios de la distribución de Linux OpenBSD prefieren OpenBSD PF, su firewall predeterminado. Este maneja la traducción de red (NAT), normalice el tráfico TCP/IP, proveyendo un mayor control sobre el ancho de banda y la priorización de paquetes. También ofrece algunas funcionalidades excéntricas como la detección pasiva de Sistema Operativo. Posee excelente reputación en cuanto a agujeros de seguridad que han sido vistos en otros filtros de paquetes.

Ventajas:

- ✓ Es de código abierto.
- ✓ Es una herramienta ligera.
- ✓ Posee la posibilidad de definir filtros de seguridad personalizados.

Desventajas:

- ✓ No es multiplataforma.

PfSense

PfSense es una distribución personalizada de FreeBSD para su uso como firewall y router, es libre y de código abierto. Además de ser considerada una plataforma poderosa y flexible en cuanto a sus funcionalidades como *router* y *firewall* incluye una larga lista de utilidades y sistemas de paquetes que permiten el uso en otras áreas sin representar la base a brechas de seguridad o vulnerabilidades en el sistema base. PfSense es un proyecto popular iniciado en el año 2004 con más de un millón de descargas desde su introducción lo cual es atribuido a su confiabilidad altamente probada en un espectro de escenarios oscilantes desde computadoras personales en un hogar, grandes corporaciones, universidades y otras organizaciones protegiendo miles de dispositivos de red. (20)

Ventajas: (21)

- ✓ Open source y libre.
- ✓ Soporta NAT y OpenVPN.
- ✓ Requerimientos de hardware ligeros.
- ✓ Adaptable para pequeñas y grandes redes.
- ✓ Amigable interfaz gráfica para la visualización del tráfico de red. (22)

Desventajas:

Presenta algunas incompatibilidades con IPv6 y con el soporte VoIP.

1.3.6 Sistemas de control de acceso estudiados.

En conjunto a los cortafuegos, en las redes se necesita definir y controlar no solo quién tiene acceso a los recursos de la red interna, sino además qué recursos son accesibles y con qué privilegios. Para la selección de los sistemas de control de acceso a incluir en la propuesta se necesita que estos sean libres o de código abierto, tengan amplio soporte, así como sean adaptables a ambientes específicos.

SELinux

Del inglés Security-Enhanced Linux (Mejora de seguridad para Linux) SELinux es una funcionalidad que ofrece una variedad de políticas de seguridad para el *Kernel* de Linux. Posee un complejo y poderoso mecanismo de control de acceso, por lo que la curva de aprendizaje necesaria para sus usuarios base debe ser alta. Quedando definido el usuario corporativo como usuario base de SELinux. Aún así cuenta con una interfaz de usuario de Gnome (GUI) que facilita la escritura y edición de las reglas. Se encuentra en múltiples distribuciones como Suse, CentOs, Fedora, Ubuntu, Slackware, Debian, RHEL.

Ventajas:

- ✓ Soporta seguridad multinivel.
- ✓ Controla el inicio de procesos y la ejecución de procesos en el sistema.
- ✓ Política muy flexible.

Desventajas:

- ✓ No presenta buena usabilidad.
- ✓ Difícil de administrar las reglas
- ✓ Difícil de auditar.

AppArmor

AppArmor es un software de seguridad liberado y mantenido por Novell bajo la licencia GPL aunque a la vez puede ser visto como un *Framework*. El mismo fue creado como software alternativo a SELinux, presenta la sintaxis clásica de Unix, soporta *Wildcard*, expresiones regulares, características que lo hacen fácil de utilizar en cuanto a modificarlo y auditarlo. Aunque es nativo de OpenSuse y Suse es fácil de encontrar en Ubuntu.

Ventajas:

- ✓ Presta especial atención a la usabilidad.
- ✓ Protege proactivamente contra ataques cero-días.
- ✓ Sus perfiles determinan que recursos son accesibles y con que privilegios.

Desventajas:

- ✓ Bien documentado en las plataformas Opensuse/Suse.

1.3.7 Sistemas de monitorización estudiados.

Ante la evolución vertiginosa de las redes, equipos de cómputo y servicios, la administración de un CPD así como su protección, se torna más compleja. Por lo cual el análisis y monitorización de redes se ha convertido en una labor cada vez más importante y de carácter pro-activo. Para prevenir errores en un sistema existente es posible utilizar un equipo que se ocupe de estar controlando y observando el funcionamiento de la red. Para la selección del sistema de monitorización a incluir en la propuesta el mismo debe ser de código abierto o libre, debe ofrecer con claridad los reportes, así como debe contar preferentemente con una interfaz web.

Nagios

Nagios es un sistema de monitorización de equipos y de servicios de red, escrito en C y publicado bajo la GNU *General Public License* (GPL), el lenguaje con el cual está desarrollado asegura una rápida ejecución y su licencia avala la existencia de actualizaciones disponibles, así como cuenta con una comunidad de desarrolladores soportándolo. Este software fue creado con el objetivo de ayudar a los administradores a tener siempre el control de qué está pasando en la red que administran y conocer los problemas que ocurren en la infraestructura que administran antes que los usuarios de la misma los

perciban, para así no solo poder tomar la iniciativa, sino asumir la responsabilidad de hacer que las cosas sucedan; decidir en cada momento que y como se debe hacer, debido a que este software permite obtener datos, interpretarlos y tomar decisiones en base a ello.

Para facilitar tareas de explotación de datos, hay diferentes aditivos como un visor de reportes integrados, en el cual se puede ver el histórico de actividad y rendimiento de servicios, y además un visor de diagramas de red con el estado actual de cada equipo. (23)

Hobbit

Hobbit es un sistema de monitorización bajo licencia libre con el que es posible monitorizar desde pequeñas redes hasta enormes sistemas. La instalación requiere tener un sistema básico funcionando rápidamente en el cual realizar las configuraciones previas lo que permitirá controlar la configuración de Hobbit. Se pueden configurar las típicas alertas, siendo el correo electrónico la opción más obvia, pero también se puede asignar cualquier script para configurar respuestas más exóticas. La documentación online describe una técnica para reenviar alertas a teléfonos móviles. La interfaz basada en Web es limpia y fácil de comprender de un solo vistazo. (24)

Monit

Monit controla y monitoriza procesos, servicios, archivos, directorios y otras variables del sistema, tanto local como de forma remota. Puede instalar se desde su código fuente o bien desde un paquete previamente compilado proveniente del repositorio de una distribución de Linux. Monit es magnífico para monitorizar un único equipo, especialmente porque reiniciará los sistemas. Sin embargo, este sistema no es tan efectivo con redes grandes, aunque funcionaría bastante bien junto a Hobbit o Nagios, permitiendo una monitorización centralizada, así como el reinicio de los servicios locales. (25)

Ntop

Esta herramienta es un investigador de tráfico de red que muestra el uso de la misma, similar al popular comando de Unix top. Ntop está basada en libcap y ha sido escrita de manera portable de manera que el sea posible correr virtualmente en cualquier plataforma basada en Unix y en Windows. Los usuarios de esta herramienta pueden usar un navegador web para navegar a través de la información de tráfico de ntop (que actúa en este caso similar a un servidor web), además de obtener un indicio del estado de la red.

Ventajas:

- ✓ Posee una interfaz web.
- ✓ Es multiplataforma, corre en las plataformas basadas en Unix: Linux, BSD, Solaris, and MacOSX, así como en Windows incluidos en este último las versiones comprendidas entre Win95-Vista
- ✓ Muestra el tráfico de red de acuerdo a varios criterios.
- ✓ Emplea el protocolo de seguridad HTTPS.

Desventajas:

- ✓ La interfaz web ofrece una administración y configuración limitada.
- ✓ El lanzador gráfico de ntop solo está disponible para Windows. (26)

1.4 Modelación de funciones mediante IDEF0

Para el modelado de las actividades que componen la propuesta, así como para desglosar, diseñar y explicar de manera comprensible y detallada el funcionamiento del procedimiento fue definido el uso de IDEF0 (“Integration Definition for Function Modeling”), la cual es una técnica de modelación concebida para representar de manera estructurada y jerárquica las actividades que conforman un sistema o empresa, y los objetos o datos que soportan la interacción de esas actividades. (27) Sus modelos se componen de una serie jerárquica de diagramas que permiten mediante niveles de detalle, describir las funciones especificadas en el nivel superior. En las vistas superiores del modelo la interacción entre las actividades representadas permite visualizar los procesos fundamentales que sustentan la organización.

Características de IDEF0

Cada diagrama de la metodología IDEF0 representa una actividad necesaria para la tarea, en un grado de detalle específico. Las actividades se subdividen en diagramas que siguen en niveles inferiores hasta un grado de detalle necesario. Las flechas representan la relación entre las cajas. No dan informaciones del desarrollo temporal o la sucesión, pero describen los datos necesarios y las informaciones creadas por las actividades. (28) La metodología IDEF0 se caracteriza por ser una técnica comprensiva y expresiva, capaz de representar gráficamente una variedad de negocios y otros tipos de operaciones para cualquier nivel de detalle de una empresa. (29)

1.5 Conclusiones parciales

En este capítulo fueron definidos los principales conceptos y temas que sustentan la propuesta de solución, se realizó un estudio de las posibles herramientas a utilizar en la misma, así como se llevó a cabo un proceso de selección que basado en los resultados obtenidos de acuerdo a las especificaciones de la muestra definida, determinó las herramientas escogidas para garantizar la gestión centralizada de logs, la prevención de ataques y el análisis forense.

Capítulo 2: Presentación del Procedimiento.

2.1 Introducción

En el presente capítulo se presenta una propuesta de procedimiento capaz de garantizar la gestión centralizada de logs, prevención de ataques y análisis forense en Centros de Procesamiento de Datos. En el mismo se detallan las herramientas, fases, roles y actividades principales que tributan al cumplimiento de las necesidades que dieron fe al surgimiento de dicho procedimiento.

El procedimiento está definido para su aplicación en aquellos CPD que respondan a la siguiente arquitectura (Ver Figura 1).

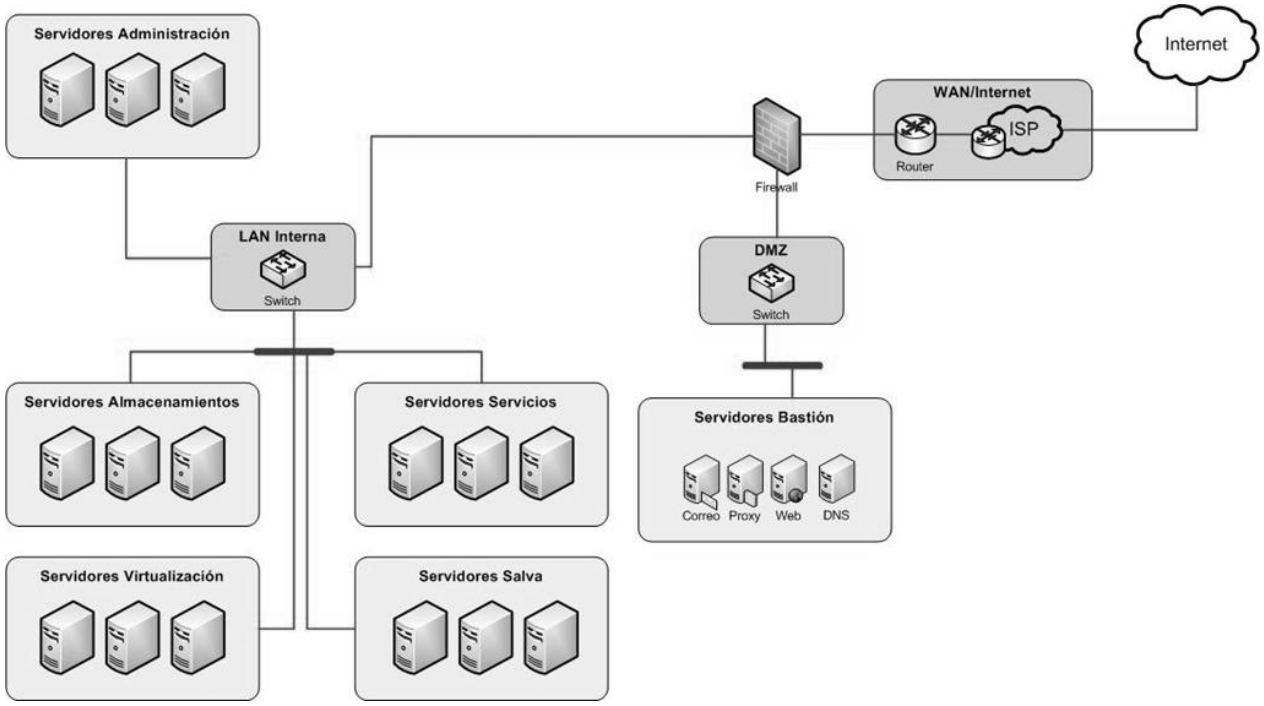


Figura 1: Topología de Red para un CPD Genérico.

La arquitectura para CPD definida por los especialistas del proyecto Centro de Datos del centro TLM comprende un *router* con salida a internet, dos switches de nivel 3: uno en la zona desmilitarizada (DMZ) y otro en la subred interna. Tras el *router* se posiciona un firewall, para regular la entrada de los paquetes a la red interna, así como en la zona desmilitarizada se ubican los servidores bastión: DNS, Correo, Proxy,

Web, así como un Servidor de Jabber de estimarse necesario. Para el establecimiento de la zona desmilitarizada ubica un *switch* encargado de re-direccionar los paquetes de entrada con destino a la DMZ, y de dar salida a aquellos cuyo origen es alguno de los servidores bastión. Ubica el restante *switch* para el re-direccionamiento de paquetes desde y hacia la red interna. Define además varias subredes como subred para Servidores de Almacenamiento, Servidores de Servicios, Servidores de Administración, Servidores de Salva y Servidores de Virtualización. Es importante esclarecer que el estándar de arquitectura definido para un CPD genérico no es estático, sino que puede adecuarse a las particularidades del escenario a desplegar.

2.2 Alcance y Objetivos

Este procedimiento garantiza la gestión centralizada de logs, prevención de ataques y análisis forense en Centros de Procesamiento de Datos (CPD) de manera efectiva, es aplicable además a otros CPD. Puntualiza y especifica la distribución del capital humano en función a los recursos disponibles, definiendo roles, fases, actividades y artefactos, así como valora un flujo básico predeterminado de respuesta diseñado para admitir múltiples flujos alternos que garantizan la capacidad de evolución del sistema. Logra una propuesta flexible que tributa a la seguridad informática en general en cualquier tipo de CPD capaz de adaptarse ante las cambiantes tendencias del campo.

Con este procedimiento se pretenden alcanzar los siguientes objetivos:

- ✓ Generar un proceso de mejora continua en los mecanismos de prevención de ataques.
- ✓ Establecer una distribución precisa del capital humano, así como las actividades, fases, roles y artefactos en un CPD.
- ✓ Lograr un vínculo estrecho entre el proceso de análisis forense y la detección de ataques de manera que se fortalezca sobre la marcha la seguridad informática del CPD.
- ✓ Contribuir al despliegue de otros CPD a través de una solución flexible.
- ✓ Optimizar el proceso de actualización a las nuevas tecnologías.

2.3 Herramientas escogidas para la propuesta.

Se definió utilizar rsyslog como implementación de syslog para la gestión centralizada de logs, Snort fue escogido como Sistema Detector de Intrusos, para la prevención de ataques se hizo necesario configurar la interfaz de red en modo promiscuo para lo cual se estableció un puerto espejo (*port mirrored*) que capta todo el tráfico del switch y lo envía a la ubicación física del IDS. Nagios por su parte fue seleccionado para la monitorización de los activos del CPD, así como para firewall se escogió PfSense que es fácil de configurar y efectivo en conjunto con SELinux como sistema de control de acceso en la DMZ y ofrece una alternativa más efectiva en cuanto a seguridad informática, para el análisis forense se eligió el toolkit BackTrack5 que provee un conjunto de herramientas en esta área como *Sleuth Kit*, *Authopsy*, *Maltego*, nmap y ntop. En la Figura 4 se observa la ubicación de algunas de las herramientas a emplear como parte de la propuesta a realizar.

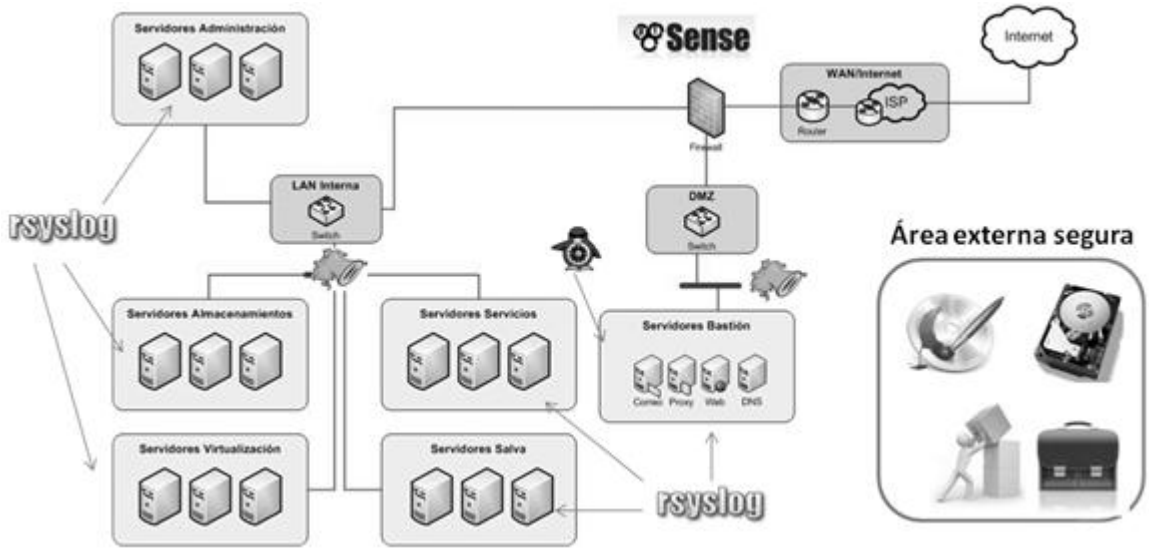


Figura 2: Solución empleando herramientas para la topología del CPD.

2.4 Roles Propuestos

El proceso de gestión centralizada de logs, prevención de ataques y análisis forense requiere la presencia de personal capacitado en el CPD, que desempeñarán un rol determinado y cubrirán las expectativas deseadas, desarrollarán una serie de actividades dentro de cada fase, interactuando con artefactos específicos; para ello deben tener entre sus competencias un buen dominio de las técnicas y herramientas

que utilizarán. Se ha de partir que en un CPD se han definido tres roles específicos: Técnico, Administrador de Servicios y Especialista. Los roles definidos para dicho procedimiento se engloban en el rol Especialista antes mencionado como especializaciones del mismo. A continuación se describen las responsabilidades asignadas.

- ✓ **Especialista en Jefe**: Es el encargado de definir las políticas de seguridad generales en el CPD, desempeña una labor esencial en la elaboración de las listas de acceso, así como juega un papel principal en las decisiones a tomar en cada una de las fases por las que transita el CPD.

- ✓ **Especialista de Acceso**: Es responsable de la configuración y supervisión de las herramientas de monitorización y acceso, además de los dispositivos de interconexión del sistema, en total sincronización con las políticas de seguridad definidas por el Especialista en Jefe.

- ✓ **Especialista de Copia de Seguridad**: Es el rol autorizado a almacenar en un área externa definida por el Especialista en Jefe los logs centralizados de los sistemas involucrados en el centro. Es el único cuya responsabilidad consiste esencialmente en la realización de copias de seguridad a todas las estaciones de trabajo, así como la restauración de las mismas en caso de fallos, todo según el diseño del Especialista en Jefe.

- ✓ **Especialista Forense**: Es el rol que se encarga de obtener después de un ataque toda la evidencia digital posible, utilizando sofisticadas técnicas y herramientas generalmente desde un *CD* autoarrancable para evitar la corrupción de los datos. Uno de sus objetivos prioritarios es identificar origen y mecanismo del ataque, además de patrones que tributen a la detección preventiva. Su actuar es crucial en la fase de retroalimentación.

2.5 Artefactos Generados

A lo largo del flujo de vida regular de un CPD, particularmente en el área de la seguridad informática, se genera mucha información como resultado de las herramientas, actividades, métodos y eventos involucrados. Por lo que al no estar definida una manera de procesar, almacenar y organizar dicha información, los datos recolectados no pueden ser claramente interpretados lo que tributa al surgimiento de brechas de seguridad y vulnerabilidades. Con este propósito se diseñaron un conjunto de artefactos

que organizarán la información generada, facilitando su análisis, estudio, almacenamiento y control. (Ver Anexo 2)

- ✓ **Políticas del CPD:** Documento que detalla, organiza, regula y controla el flujo de vida del CPD. Engloba la configuración de los recursos de hardware y software, además del establecimiento de las políticas definidas para cada área del CPD. Es el documento rector del funcionamiento del CPD.

- ✓ **Plan de Contingencia:** Artefacto que establece el proceder adecuado ante situaciones excepcionales vinculadas a amenazas, eventos maliciosos o de índole sospechosa en la totalidad del CPD. Determina la manera de actuar y las técnicas a emplear ante las situaciones anteriormente conocidas.

- ✓ **Lista de Control de Acceso:** Artefacto o documento que puede estar contenido dentro del documento Políticas del CPD, donde se registra la información relativa a las direcciones, puertos, MAC, usuarios y contraseñas que pueden acceder desde el exterior al CPD, además de determinar el grado de acceso a dichos recursos. Constituye un mecanismo de defensa contra los ataques de ingeniería social, *phishing* y suplantación de identidad.

- ✓ **Informe Forense:** Documento que abarca la totalidad de resultados del proceso de recolección y análisis de evidencias digitales llevado a cabo por un equipo especializado ante la ocurrencia de un ataque en el CPD. El mismo permite conocer las vulnerabilidades explotadas por el atacante lo que tributa a al erradicación de las mismas.

- ✓ **Bitácora del CPD:** Documento que registra la totalidad de eventos que tienen lugar en el flujo de vida del CPD. Permite llevar el seguimiento de eventos difíciles de conectar entre sí que guardan relación con un evento superior, tributa al proceso de retroalimentación entre el personal operativo, así como se torna una fuente de consulta para el proceso de toma de decisiones.

2.6 Presentación de Procedimiento

Se definen en el procedimiento en cuestión un total de cinco etapas: Monitorización, Análisis de Impacto y Preservación, Detección de Ataque, Análisis Forense y Retroalimentación. Donde a lo largo de las mismas

se realizan disímiles actividades por roles específicos definidos. En la Figura 5 se aprecia la totalidad de las etapas que integran el procedimiento que está siendo descrito.

Funcionamiento del Procedimiento

En la elaboración del procedimiento fueron definidos un total de cuatro roles con tareas y responsabilidades específicas a lo largo de las diferentes fases propuestas en la solución. A lo largo de cada fase se generan artefactos, así como se realizan tareas específicas asignadas a los roles definidos. A continuación se enuncian y detallan las funciones de los elementos antes expuestos.

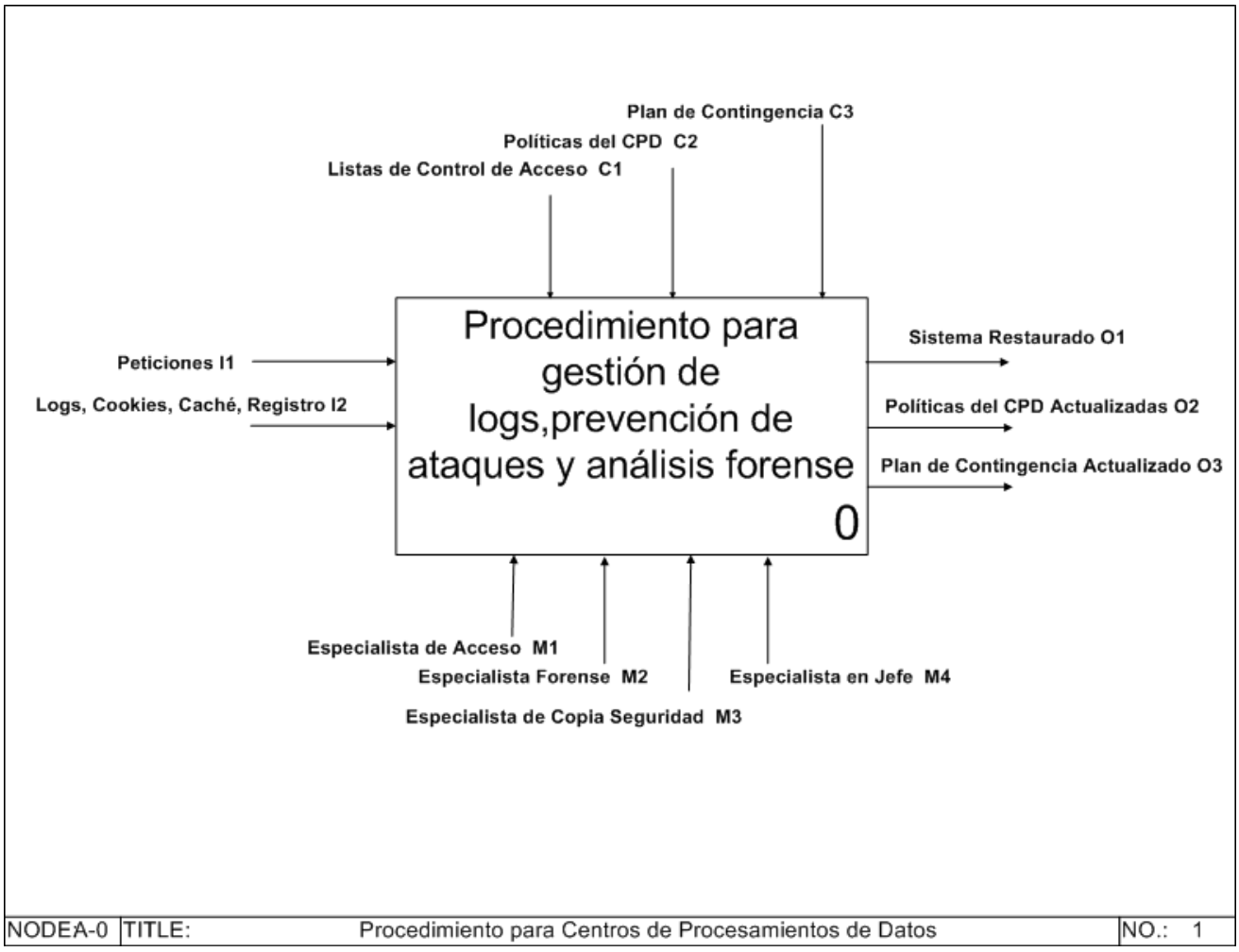


Figura 3: Procedimiento General

Como controles se definieron los documentos Lista de Control de Acceso, Políticas del CPD y Plan de Contingencias, los que definen y regulan todo el flujo de actividades o ciclo de vida del procedimiento propuesto. Como mecanismos fueron definidos los roles especialistas definidos, que son los responsables de aplicar las técnicas definidas en las Políticas del CPD. Las entradas son las peticiones y eventos que arriban al CPD desde el exterior o el interior. Las salidas son los artefactos Políticas del CPD actualizadas, Plan e Contingencia actualizado y el Sistema restaurado.

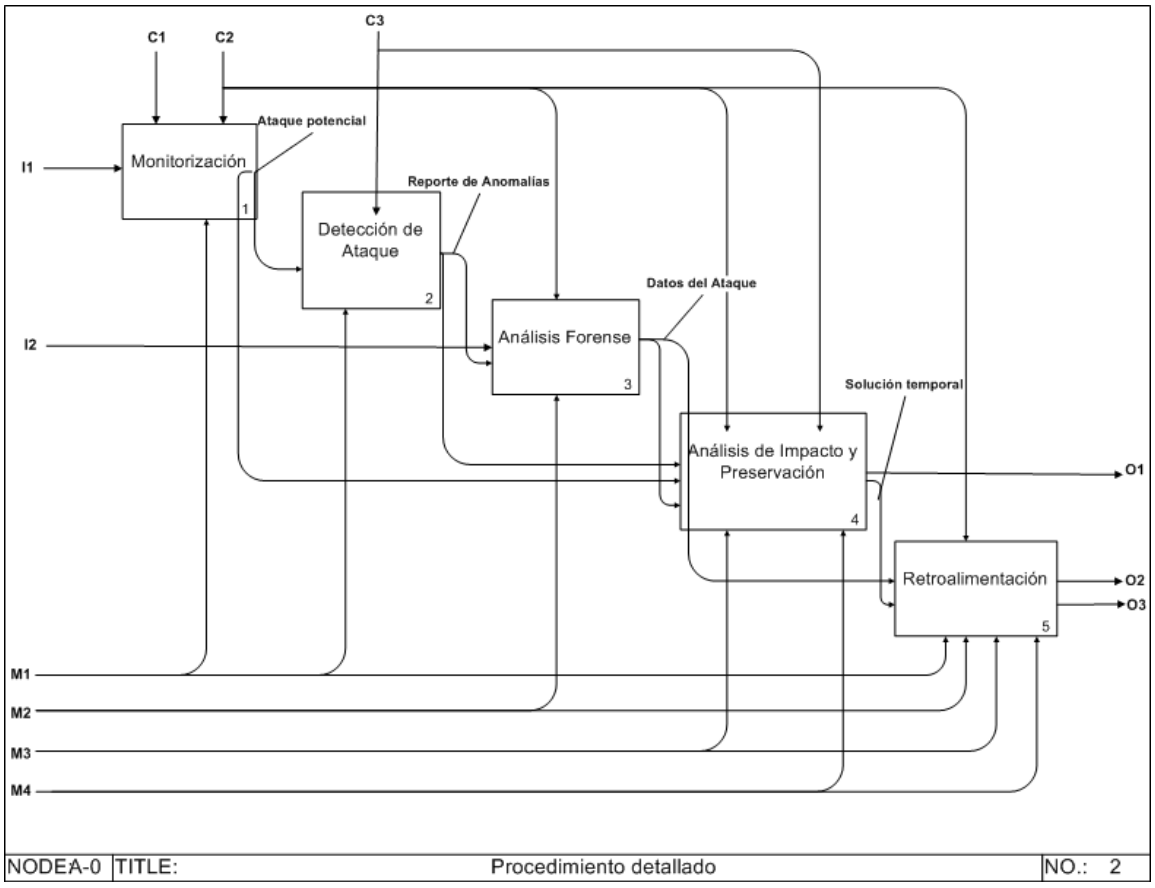


Figura 4: Etapas del Proceso Detallado

Etapa de Monitorización

La etapa de Monitorización se caracteriza por la detección de actividades sospechosas en la infraestructura de red, así como el registro y captura de todos los eventos que ocurren en tiempo real. En la misma se está a la espera de todos los eventos ocurridos en el CPD, los cuales son almacenados para

su posterior estudio. El Especialista de Acceso es el máximo responsable en esta etapa, es el encargado de aplicar las políticas definidas en el CPD comprendiendo desde la configuración de los dispositivos de hardware y software hasta la aplicación inmediata del Plan de Contingencia. A partir de esta etapa se puede proceder a la Detección de un Ataque o según el caso al Análisis de Impacto y Preservación.

Herramientas: *Snort*, *PfSense*, *ntop, SELinux*.

Artefactos: Lista de Control de Acceso, Políticas de Seguridad.

Roles que intervienen: Especialista de Acceso, Especialista en Jefe.

Especialista en Jefe: Es el encargado de diseñar a lo largo de esta etapa las políticas de seguridad generales que regirán la configuración de los sistemas de control de acceso y seguridad del CPD, así como los dispositivos o recursos de hardware (*switches* L2 y L3, *routers y hubs*). Define y elabora las listas de control de acceso, así como los privilegios de los usuarios autorizados según su rol y área de trabajo.

Especialista de Acceso: Es el encargado de configurar los recursos de hardware y software, revisar periódicamente la tabla de enrutamiento de los dispositivos de interconexión, así como de actualizar la configuración y las políticas de seguridad definidas por el Especialista en Jefe. Sirviéndose de la herramienta ntop analiza el comportamiento de la red en busca de patrones que pudieran indicar anomalías en la red o actividades maliciosas.

Actividades:

1. Supervisión de la monitorización de red y detección de Intrusos.

   Realizada por el Especialista de Acceso, en la misma ante un ataque desconocido el rol activo tiene la responsabilidad de cerrar la conexión del atacante, detectar el ataque según patrones manuales que escapen a la lógica del sistema y notificar al Especialista en Jefe para recibir instrucciones sobre el proceder y la decisión a tomar.

2. Chequeo de Tablas de enrutamiento de los dispositivos de interconexión.

Durante esta actividad el Especialista de Acceso analiza las tablas de enrutamiento de los dispositivos de interconexión tales como *switches* L3, *routers* y *gateways,* así como se sirve en algunos casos de los *logs* almacenados con origen en los IDS, firewalls para el análisis de paquetes de red todo en busca de indicios y patrones que indiquen un ataque al CPD sin detectar.

3. Chequeo de Configuración.

   En esta etapa el Especialista en Jefe verifica que las políticas de seguridad definidas por él estén siendo aplicadas por el Especialista de Acceso.

4. Control de acceso al sistema.

   El Especialista en Jefe tiene una participación en la elaboración de las listas de acceso, pero en esta actividad en particular es el Especialista de Acceso quien revisa los logs donde se registra cada intento de conexión. Por su parte el Especialista de Acceso es el responsable de la configuración de SELinux, donde determina el nivel de privilegios de procesos, demonios y usuarios en los recursos del CPD.

5. Actualización de las configuraciones en función a los cambios en las políticas de seguridad en el CPD.

   De existir algún cambio en las políticas de seguridad elaboradas por el Especialista en Jefe el Especialista de Acceso tiene la responsabilidad de configurar los recursos de hardware o software necesarios para dar total soporte a las mismas.

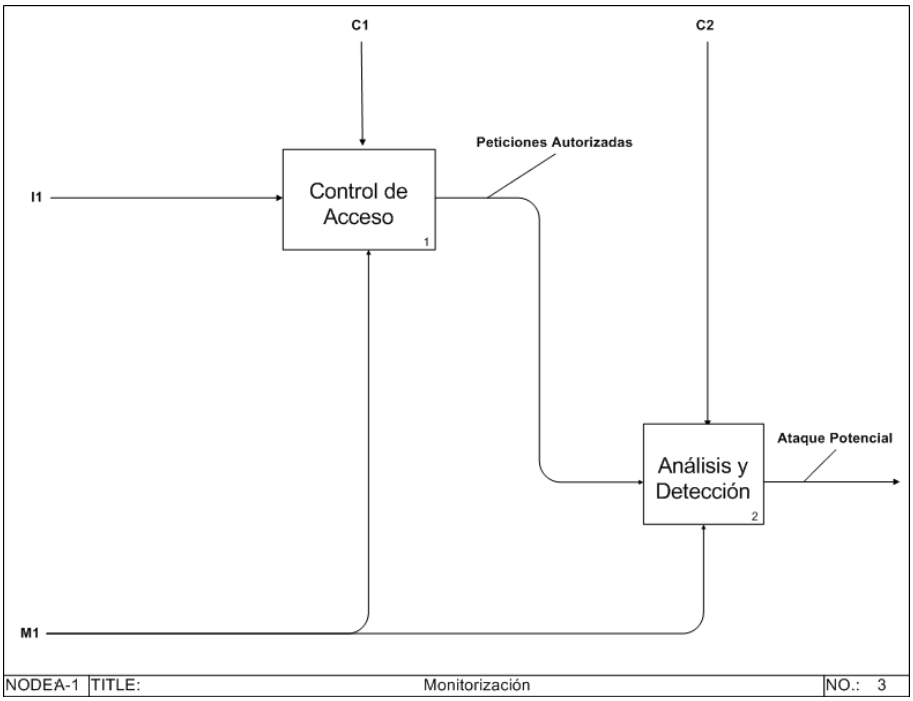


Figura 5: Etapa de Monitorización

Etapa Análisis de Impacto y Preservación.

La etapa de Análisis de Impacto y Preservación es donde se lleva a cabo el proceso de salva del CPD, tiene una importancia elevada ya que de la misma depende el proceso de restauración ante fallos y en caso de ocurrencia de los mismos tributa al análisis forense así como a la etapa de Retroalimentación. En la misma además se analiza o predice el impacto de un ataque en curso y se toman medidas para mitigar los riesgos desde la aplicación de la sección del plan de contingencia para el caso en particular, hasta medidas más desesperadas como el aislamiento total del CPD. También en esta fase se realiza la restauración de los recursos afectados (dígase configuraciones, salvas de datos y puntos de restauración) En esta etapa intervienen el Especialista de Acceso, Especialista de Copia de Seguridad y Especialista en Jefe.

Herramientas: Syslog.

Artefactos: Plan de Contingencia.

Entrada: Logs, Políticas de Seguridad.

Salida: Puntos de restauración, *Backup* files.

Roles que intervienen: Especialista de Copia de Seguridad, Especialista en Jefe.

Especialista de Copia de Seguridad: Es el encargado de realizar el proceso de salva de los logs centralizados en el servidor de logs además de supervisar el control y gestión de las copias realizadas, así como los logs obtenidos en las estaciones de trabajo.

Especialista en Jefe: Es el responsable de definir el área externa asegurada para almacenar las salvas de logs realizadas, así como el tiempo de almacenamiento, período de inicio e intervalo de dicho proceso de salva.

Actividades:

1. Obtención de los logs de los sistemas involucrados.

   El Especialista de Copia de Seguridad obtiene todos los *logs* de los sistemas involucrados en el CPD.

2. Análisis de los logs obtenidos e identificación de patrones que indiquen anomalías o ataques.

   En esta actividad el Especialista de Copia de Seguridad estudia y analiza los logs en busca de patrones que desenmascaren un ataque no detectado aún, ante lo cual está en el deber de identificar patrones clave e informar a todo el grupo de Administradores. Esta actividad puede dar paso directamente a la Etapa de Análisis Forense o a la Etapa de Retroalimentación.

3. Realización de copia de seguridad de los logs obtenidos hacia un área externa segura.

   El Administrador de Copia de Seguridad realiza copias de los logs almacenados en el Servidor de logs hacia un área externa segura definida por el Especialista en Jefe en las políticas de seguridad.

4. Supervisión y control de copias de seguridad entre estaciones de trabajo, sistemas involucrados y salvas en áreas externas.

   El Administrador de Copias de Seguridad es el encargado de realizar salvas o copias de seguridad a todos los recursos de *software* para su previa restauración en caso de fallos, así como hacer

copias de configuraciones o puntos de restauración a las configuraciones de los recursos de hardware. También tiene el deber de comprobar y controlar el almacenamiento de las mismas, así como el mantenimiento y actualización de las copias realizadas.

5. El aislamiento del sistema ante ataque inminente, es una medida drástica pero necesaria a tomar cuando durante el análisis de impacto se determina una pérdida total en el CPD o el comprometimiento de la información de manera inminente, peligrosa o de manera que el sistema es incapaz de mitigar los riesgos que implica.

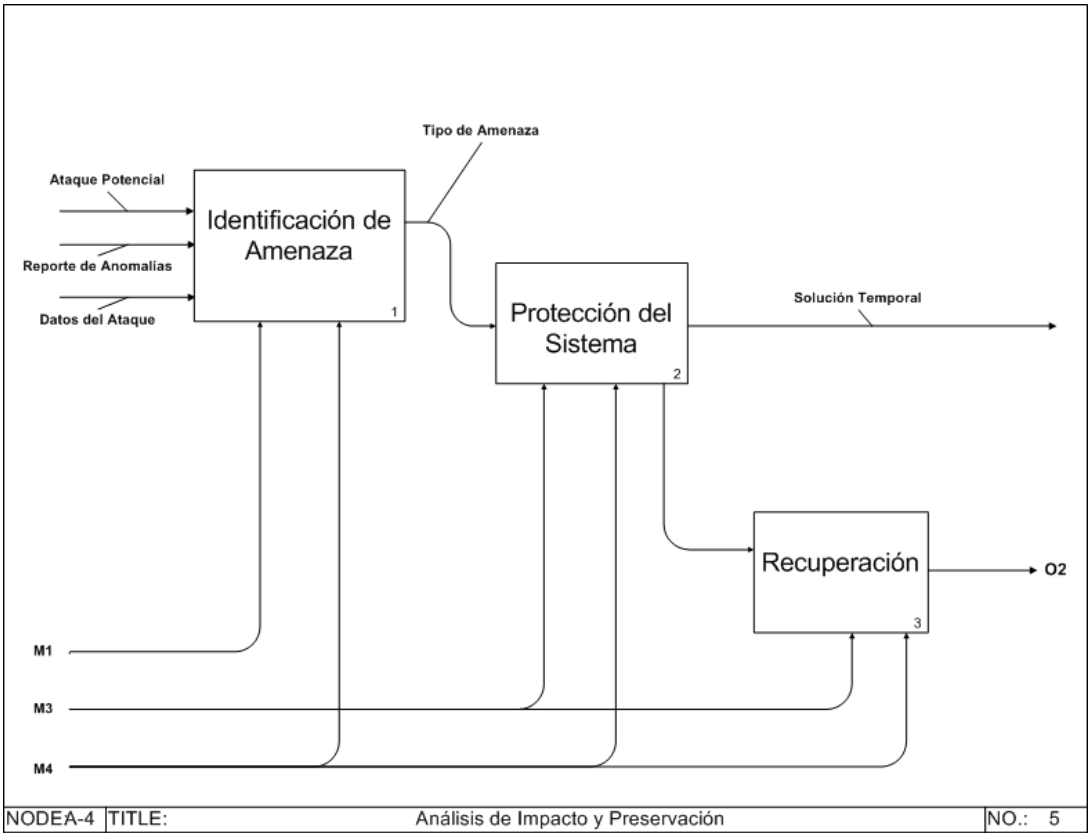


Figura 6: Etapa Análisis de Impacto y. Preservación

Etapa de Detección de Ataque

La siguiente es una etapa crítica ya que tiene lugar cuando alguno de los sistemas del CPD está bajo ataque, en la misma es donde se decide la respuesta para contrarrestar o neutralizar el ataque para así

minimizar los daños. Se caracteriza además por la reacción ante las intrusiones, la regulación de los paquetes que entran o no a la red del CPD y así como el acceso a los recursos del mismo por parte de procesos y servicios. El Especialista de Acceso desempeña un papel fundamental en esta etapa ya que tiene la responsabilidad de detectar aquellos ataques que consigan burlar la configuración establecida para los dispositivos de hardware y software, así como en este caso tiene el deber de notificar al Especialista en Jefe quien a partir de esta fase determina el flujo de eventos a seguir, ya sea dar paso al Análisis Forense o de ser posible al Análisis de Impacto y Preservación. A su vez los nodos (computadoras personales o servidores) presentes en el Centro de Cómputo se integran a esta etapa mediante la detección de actividades maliciosas por parte de los antivirus.

Herramientas: *Snort*, *PfSense.*

Artefactos:

Entrada: Plan de Contingencias, Políticas de Seguridad.

Salida: Reporte de Anomalías, Sistema Restaurado.

Roles que Intervienen: Especialista de Acceso, Especialista en Jefe.

Especialista de Acceso: Al ocurrir una intrusión u otro tipo de ataque tiene la responsabilidad de cerrar la conexión y los puertos en caso que Snort no lo haga de manera automática. Trata de identificar el origen del ataque y obtener la mayor cantidad de datos posibles del atacante. Tiene el deber de notificar al Especialista en Jefe ante una anomalía o ataque desconocido que requiera una medida de índole mayor para acatar su decisión.

Especialista en Jefe: Participa en la toma de decisiones para contrarrestar ataques desconocidos, y es el responsable de iniciar la etapa de análisis forense.

Actividades:

1. Supervisión de la detección de ataques.

   El Especialista de Acceso se encarga de verificar que las herramientas definidas han detectado un ataque. En caso de no suceder lo anterior, si se identifica un ataque que el sistema ha pasado por

alto, identifica el mecanismo de ataque, intenta cerrar la conexión y notifica al Administrador del CPD. Esta actividad da paso al activar el flujo alterno anterior a las etapas Análisis Forense y Retroalimentación.

2. Supervisión de las acciones para contrarrestar el ataque.

   El Especialista de Acceso supervisa la respuesta dada por el sistema ante un ataque, si durante el proceso de respuesta identifica una variación en el ataque no prevista, en conjunto al Especialista en Jefe toman el control del sistema y anulan el ataque de ser posible de forma manual.

3. Obtención de origen y datos de ataque y atacante de ser posible.

   El Especialista de Acceso trata de forma paralela a la ocurrencia del ataque de obtener la mayor cantidad de datos del atacante como el tipo de ataque, origen, objetivo y cualquier otra información capaz de tributar al esclarecimiento de las vulnerabilidades y a facilitar una investigación.

4. Notificación e informe.

   Ante cualquier variación o anomalía en los mecanismos prediseñados el Especialista de Acceso consulta directamente al Especialista en Jefe y juntos participan en el proceso de toma de decisiones para dar respuesta a la agresión.

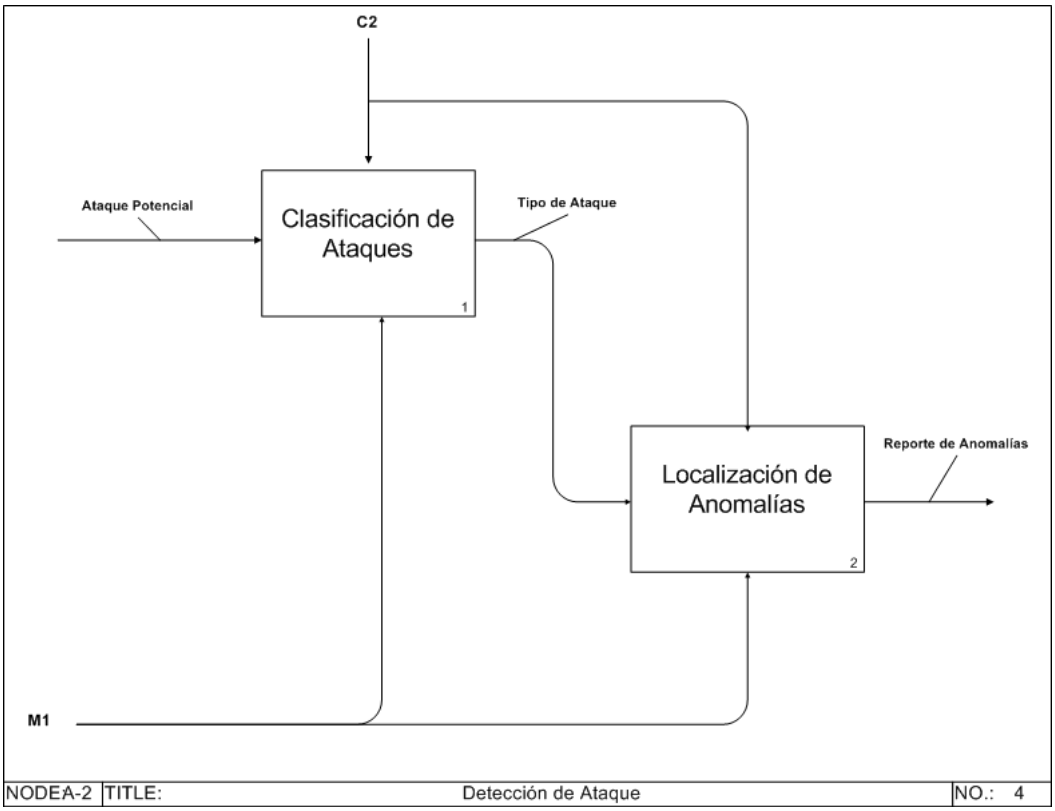


Figura 7: Etapa Detección de Ataque

Etapa de Análisis Forense

Esta etapa posee una gran importancia ya que los resultados de la misma tributan completamente a la etapa de Retroalimentación y por ende al proceso de actualización de los mecanismos de seguridad y las políticas definidas en función de amenazas hasta entonces desconocidas. También se analiza o predice el impacto de un ataque en curso y se toman medidas para mitigar los riesgos desde la aplicación de la sección del plan de contingencia para el caso en particular, hasta medidas más desesperadas como el aislamiento total del CPD. También en esta fase se realiza la restauración de los recursos afectados (dígase configuraciones, salvas de datos, entre otras) En esta etapa intervienen el Especialista de Acceso, Especialista de Copia de Seguridad y Especialista en Jefe.

Herramientas que intervienen: *Backtrack 5*.

Artefactos:

Entrada: Logs, Cache, Registro, Cookies, Tablas de enrutamiento.

Salida: Plan de Contingencia, Reporte de Daños.

Roles que intervienen: Especialista Forense, Especialista en Jefe, Especialista de Copia de Seguridad.

Especialista Forense: Es el responsable de realizar el análisis forense de las estaciones de trabajo atacadas, así como las tablas de enrutamiento de los dispositivos de interconexión en busca de obtener la mayor cantidad de datos posibles.

Especialista en Jefe: Es el responsable de decidir el tipo proceso de recuperación al que serán sometidas las estaciones de trabajo atacadas.

Especialista de Copia de Seguridad: Es el encargado de restaurar las estaciones de trabajo y recursos atacados a su estado inicial.

Actividades:

1. Identificar origen y datos del ataque.

   Si durante la etapa de ataque el Especialista de Acceso no pudo identificar el origen del ataque, el Especialista Forense en esta actividad utiliza sus herramientas con este propósito, a través del análisis de la tabla de rutas de los dispositivos de interconexión así como los *logs* de los *sniffers* y *firewalls* vinculados al ataque. Así como realiza análisis exhaustivo del registro, la caché, las *cookies* y los logs del sistema de la estación de trabajo atacada.

2. Identificar objetivo del ataque.

   En esta actividad el Especialista Forense y el Especialista en Jefe trabajan en conjunto para descifrar el objetivo del ataque, así como cuantifican los daños al sistema.

3. Supervisión del proceso de recuperación.

   El Especialista en Jefe determina el proceso de recuperación para las estaciones de trabajo atacadas, restaurándolas a su estado anterior o cambiando totalmente su configuración. Para lo

último se colegian los resultados de la Etapa de Retroalimentación que determinan las nuevas medidas de seguridad.

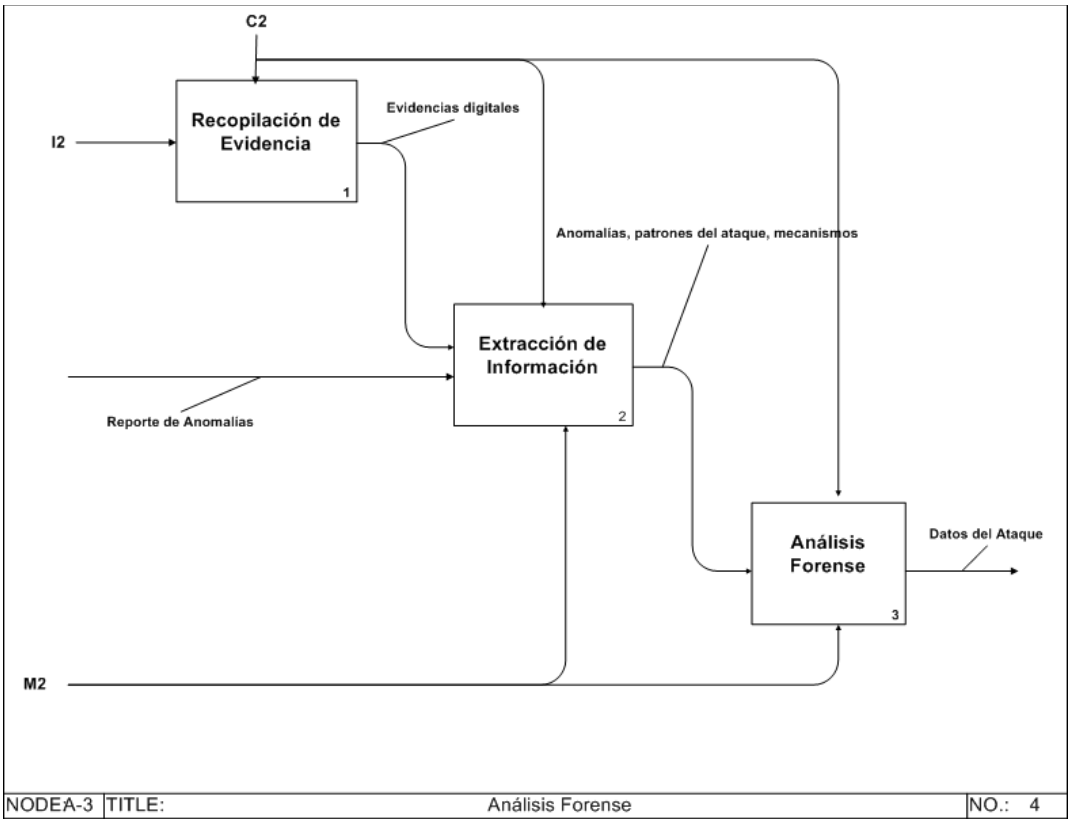


Figura 8: Etapa de Análisis Forense.

Etapa de Retroalimentación

Esta etapa es considerada la más importante ya que aglutina el resultado de las demás etapas del procedimiento convirtiendo al mismo en un proceso continuo capaz de evolucionar, mitigando las vulnerabilidades y potenciando respuestas acertadas ante las nuevas formas de ataque. Esta entra en vigencia cuando el CPD ya ha sido atacado sin posibilidad de mitigar los riesgos, en la misma se comienza con la recopilación de la evidencia digital con el objetivo de identificar el tipo de ataque, origen y mecanismo utilizado y se trata de crear conexiones con personas u entidades responsables del mismo. Los resultados de esta etapa son procesados en la etapa de retroalimentación.

Herramientas: -

Artefactos:

Entrada: Reporte de Anomalías, Reporte de Daños, Plan de Contingencia.

Salida: Políticas del CPD Actualizadas, Plan de Contingencia Actualizado.

Roles que intervienen: Especialista en Jefe, Especialista de Acceso, Especialista Forense, Especialista de Copia de Seguridad.

Especialista Forense: Es el encargado tras un análisis forense de identificar el tipo de ataque y el mecanismo empleado por el mismo, así como las señales dejadas en el sistema que constituyen indicadores del mismo que pudieran tributar a su futura detección.

Especialista en Jefe: Es el responsable de actualizar las políticas de seguridad existentes de acuerdo a las nuevas exigencias y necesidades del sistema actual de acuerdo a la evolución y surgimiento de nuevos ataques. Para ello se apoya en los resultados de un análisis forense, en el hallazgo de patrones que indiquen comportamientos maliciosos en los logs centralizados, y en fuentes fidedignas que indiquen nuevas formas de ataques, *bugs* en sistemas involucrados o mejores prácticas de seguridad informática.

Especialista de Acceso: Es el encargado de actualizar las configuraciones de los recursos de hardware y software del CPD en función a las políticas de seguridad definidas por el Especialista en Jefe.

Especialista de Copia de Seguridad: Es el responsable de aplicar las políticas de seguridad definidas por el Especialista en Jefe en cuanto al almacenamiento de las copias de seguridad y los procesos de restauración de configuraciones.

Actividades:

1. Investigación de nuevos ataques y prácticas de seguridad informática.

   El grupo de Administradores tiene el deber de valorar la actualización del sistema al detectar o hallar nuevos mecanismos de ataques o nuevas prácticas de seguridad.

2. Identificación de nuevos patrones de ataque y vulnerabilidades.

Fruto de la investigación realizada en la actividad anterior el grupo de Administradores debe identificar patrones que permitan la detección y prevención de nuevos ataques aún cuando no hayan sido blanco de los mismos.

3. Actualización de políticas de seguridad.

   El Especialista en Jefe ante los patrones y soluciones definidas en la actividad anterior es el encargado de llevar a cabo la actualización de las políticas de seguridad existentes.

4. Actualización de configuraciones.

   Según los cambios en las políticas de seguridad cada administrador debe realizar los cambios pertinentes en su área ya sea en las configuraciones o en su proceder.

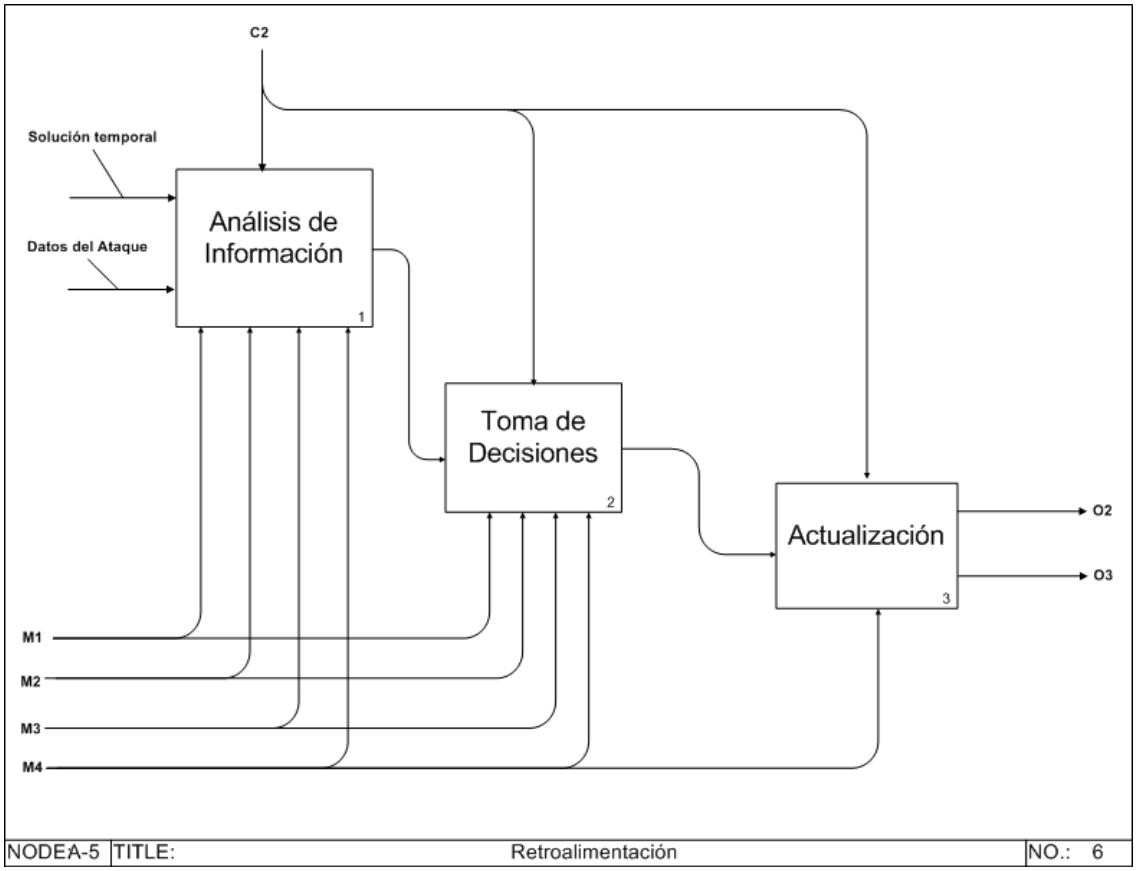


Figura 9: Etapa de Retroalimentación.

Flujos del Procedimiento

Flujo #1- Prevención: Cuando una actividad sospechosa, potencialmente maliciosa o una amenaza posible, es detectada por las herramientas de monitorización**,** se procede a la etapa de Análisis de Impacto y Preservación. En esta etapa como su nombre indica se persiguen dos grandes objetivos: Identificar los riesgos (en función del tipo de ataque que pudiera sobrevenir) y mitigarlos (de ser un posible ataque identificar una solución temporal o permanente). Luego se avanza a la etapa de Retroalimentación donde toda la información recopilada es procesada para la mejora de las técnicas y prácticas de Seguridad Informática del CPD.

Flujo Alterno #1: Si el Análisis de Impacto arroja la ocurrencia de un ataque inminente, y no se conoce manera alguna de evitarlo o controlarlo se procede a medidas extremas como aislar al CPD. Luego se registran al detalle los sucesos en el **Documento Bitácora del CPD**[4], lo que permite tener una referencia para estudiar todos los logs generados en esa fecha a fin de detectar cualquier otra actividad que haya podido pasar desapercibida. Esta actividad es diaria y continua.

Flujo Alterno #2: Si el Análisis de Impacto arroja la ocurrencia de un ataque con el que el CPD ha lidiado antes, se aplica la solución definida luego se procede a registrar detalladamente los sucesos ocurridos en el Documento Bitácora del CPD.

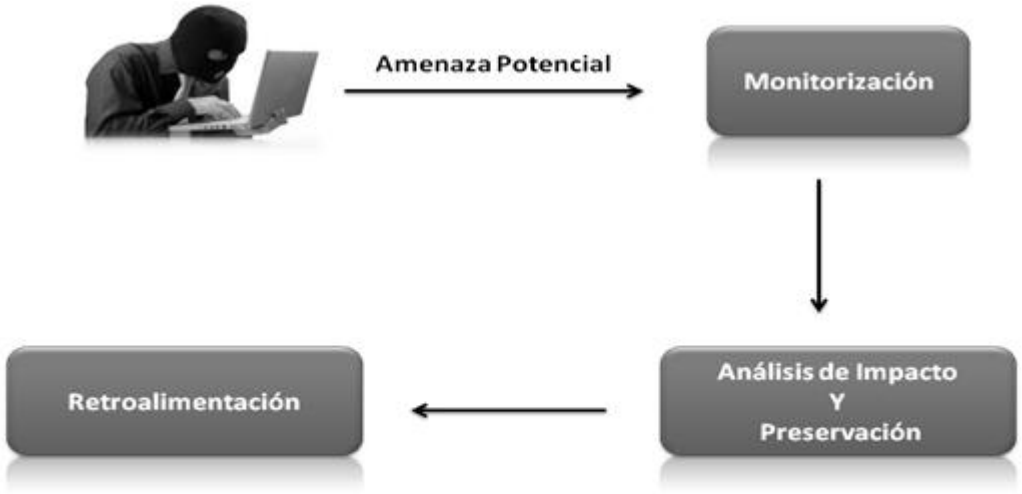


Figura 10: Flujo Prevención de Ataques

[4] **Documento donde se registran los hechos ocurridos a lo largo del funcionamiento del CPD.**

Flujo #2- Detección: Este flujo ocurre en el caso que un Ataque Informático logra burlar la etapa de monitorización, u ocurre en tiempo real. Los Ataques de este tipo llevan de por si un largo trabajo recopilando al información del sistema objetivo de manera sutil y esporádica por lo que es difícil rastrear sus antecedentes, a menudo están sustentados en técnicas de ingeniería social. En este caso en la Etapa de Detección del Ataque se procede a identificar en tiempo real el origen del atacante, mientras de forma simultánea se inicia la etapa de Análisis de Impacto y Preservación, donde se analizan los riesgos y se mitigan, de no ser posible lo último se aísla el CPD. Todos los eventos ocurridos son registrados en el Documento Bitácora del CPD. Se avanza a la etapa de Retroalimentación donde se analizan los datos recolectados por las herramientas con el fin de encontrar patrones que permitan la prevención futura de ataques similares.

Flujo Alterno #1: Cuando el Ataque es de índole interna u ocasionado por virus al avanzar a la etapa de Análisis de Impacto y Preservación se procede a aislar la subred de origen del ataque, así como se busca la solución del problema o en el caso de contar con la solución se aplican las medidas pertinentes. Todos los eventos son registrados en el Documento Bitácora del CPD.

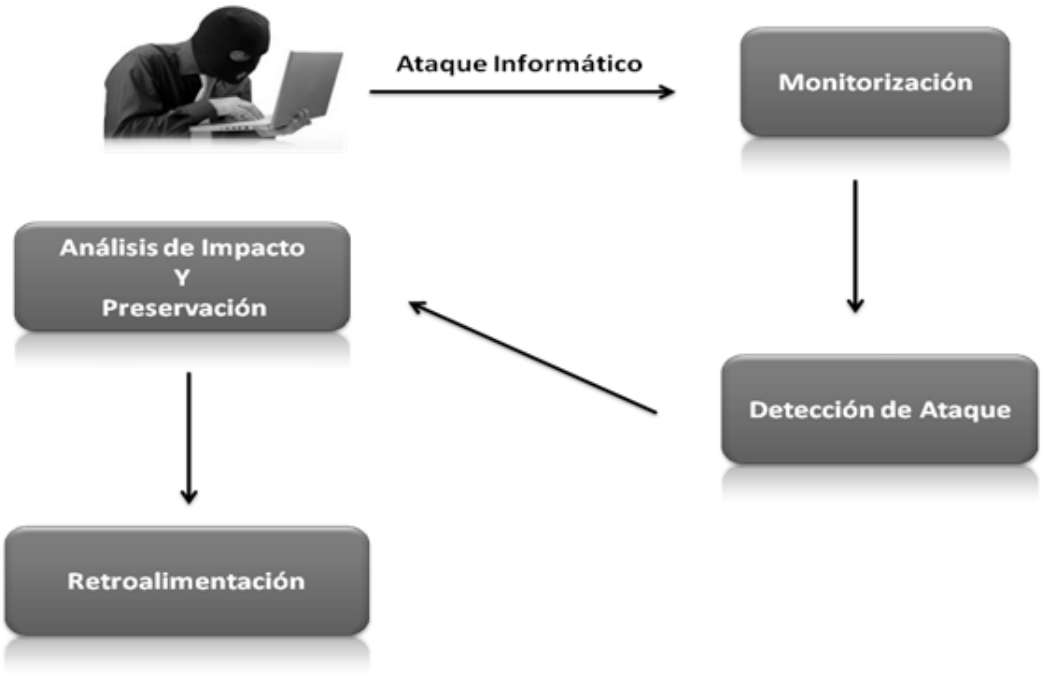


Figura 11: Flujo Detección de Ataques

Flujo #3- Análisis Forense: Este caso ocurre cuando un Ataque burla las etapas de Monitorización y Detección de Ataque, puede ser el caso que el Atacante se haga con el control del CPD evitando la activación de la etapa Análisis de Impacto y Preservación modificando los datos monitoreados o inhabilitando las herramientas de seguridad. Al conocerse la ocurrencia del Ataque se activa la etapa de Análisis Forense donde se obtienen tantos datos como sea posible del mismo: origen, mecanismo, entidades implicadas, vulnerabilidades explotadas, patrones, objetivos perseguidos por el Atacante. El Proceso de Análisis Forense implica el inicio de un Proceso Judicial. Los datos generados en la etapa de Análisis Forense son insertados en la etapa de Retroalimentación donde se actualizan las políticas del CPD y se eliminan las vulnerabilidades identificadas, así como se insertan los patrones manifestados con el fin de garantizar la prevención y detección de Ataques similares.

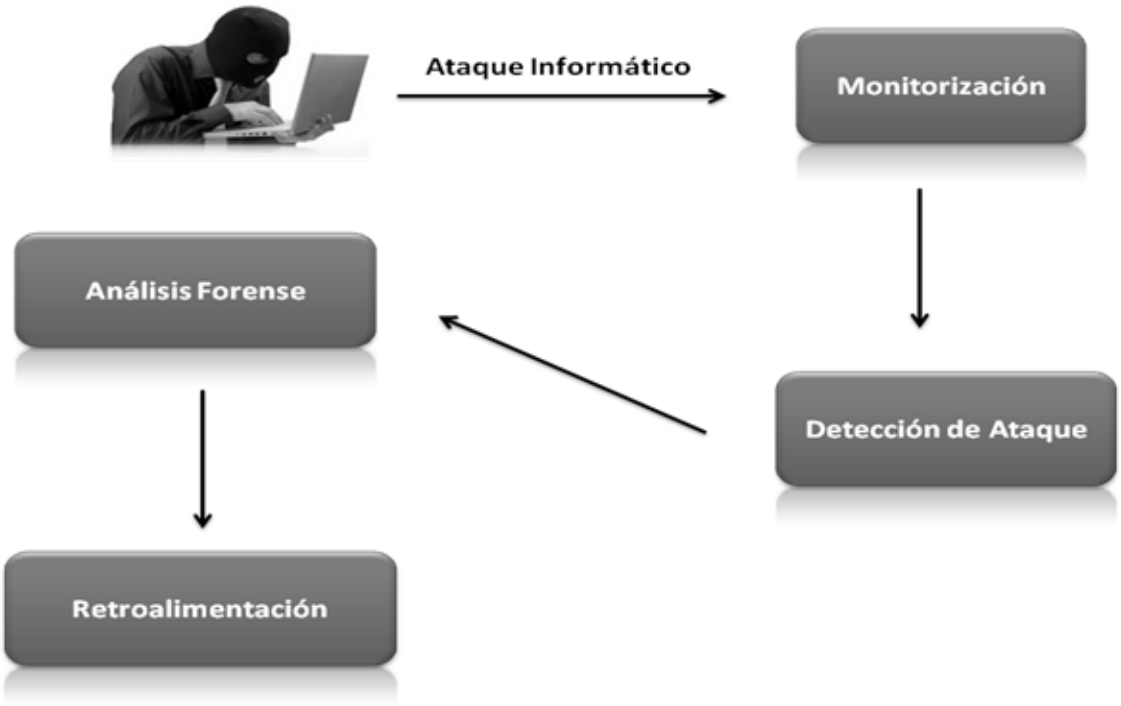


Figura 12: Flujo Análisis Forense

2.7 Conclusiones parciales

Al finalizar el capítulo se puede concluir que con el procedimiento desarrollado, será posible garantizar la gestión centralizada de logs, prevención de ataques y análisis forense en Centros de Procesamiento de Datos (CPD) con los recursos actuales. Para ello se describieron los objetivos a cumplir por las personas que utilizarán el procedimiento. Se realizó además, la descripción de cada proceso y subproceso perteneciente al procedimiento, así como los roles que los desarrollan; las actividades, herramientas, técnicas y artefactos que utiliza para su desarrollo con calidad.

Capítulo 3: Validación del Procedimiento

3.1 Introducción

En el presente capítulo se procede a validar la propuesta de procedimiento, con el objetivo de demostrar su validez, eficacia y capacidad de dar solución a la problemática planteada. Para ello se define un conjunto de técnicas y mecanismos que avalan y sustentan el correcto funcionamiento de la solución en cuestión.

3.2 El método Delphi

Para validar la propuesta se definió el empleo del método de expertos Delphi en conjunto al desarrollo práctico y la explotación de resultados. El método de expertos Delphi posee tres características principales: anonimato, retroalimentación controlada y respuesta estadística del grupo, trata además de obtener las ventajas de la interacción directa de los expertos de expertos y eliminar los inconvenientes. El mismo es un método de estructuración de la comunicación entre un conjunto de personas que pueden contribuir significativamente a la resolución de un problema complejo (30); es un método de pronosticación de los más confiables con la finalidad de confeccionar un cuadro para situaciones complejas, a través de la elaboración estadísticas de las opiniones de un grupo de expertos en el tema tratado (31). Rebasa el marco de las condiciones actuales más señaladas de un fenómeno y alcanzar una imagen integral y amplia de su evolución reflejando valoraciones individuales de los expertos basados ya en su experiencia intuitiva o en su análisis lógico.

El método esta basado en la organización de un diálogo anónimo entre los expertos consultados de manera individual, mediante al aplicación de un cuestionario y con el propósito de obtener un consenso general o los motivos de discrepancia entre los mismos. Los expertos seleccionados son sometidos a un conjunto de interrogantes sucesivas cuyas respuestas son procesadas de manera estadística para conocer el nivel de discrepancia o concordancia en cuanto al tópico consultado.

Por los elementos antes expuestos se decidió emplear una variante de dicho método propuesta por Silvia Colunga y Georgina Amayuela, con el fin de propiciar una mayor objetividad a los criterios de los especialistas a partir de la introducción de escalas valorativas y empleada además en múltiples trabajos de maestría y doctorado detallados a continuación.

Licenciado Carlos Álvarez Martínez de Santelices en su tesis de maestría: “Experimentos virtuales para la enseñanza del Electromagnetismo” (32), donde se aglutinan las conclusiones del estudio de numerosas tesis de maestría y doctorado para ese tipo de investigación, la tesis de maestría del Ingeniero Rolando Quintana Aput: “Propuesta de indicadores para medir competencias del personal según el rol en proyectos multimedia” (33) y también la de Violena Hernández Aguilar: Protofase a la ingeniería de requisitos para facilitar la comprensión del negocio a informatizar en el desarrollo de software de gestión (34),Tesis de maestría de la Ing. Marbys Marante Valdivia “Proceso para planear la cartera de servicios en la adopción de una iniciativa SOA” (35).

3.3 Aplicación del método Delphi

Para la aplicación del método Delphi fueron definidas las etapas Selección de expertos, Elaboración de un cuestionario en aras de validar la propuesta realizada y el análisis de la concordancia de los expertos.

3.3.1 Selección de expertos

Entiéndase por experto a la persona, grupo de personas u organización con conocimientos amplios o aptitudes en un área particular del conocimiento, capaces de, valorar, formular conclusiones objetivas y dar recomendaciones acerca del problema en cuestión (36).

Para determinar el número de expertos se puede emplear el criterio de la Ley de Probabilidad Binomial utilizando la expresión:

$$m = \frac{p * (1 - p) * k}{i^2}$$

Figura 13: Expresión de la Ley de Probabilidad Binomial

Así como el Gráfico de Dalkay, citado por Zatsiorski en (37) que describe los errores en la evaluación según la cantidad de expertos (Ver Anexo 3 Figura 1).

Las condiciones determinadas para la selección de los expertos fueron:

- ✓ Graduado de nivel superior.

- ✓ Dos años de nivel superior como mínimo.
- ✓ Conocimientos en el área de seguridad informática o análisis forense, preferentemente en el campo de los CPD.
- ✓ Conocimientos sobre el funcionamiento y administración de los CPD.

Dichas cualidades en conjunción a las propias del experto como la sinceridad, honestidad, profesionalidad y responsabilidad, permitirán arrojar resultados certeros que tributarán a alcanzar los objetivos trazados.

Expertos Consultados:

- ✓ DrC. Walter Baluja García: Profesor Universitario y Vicerrector del Instituto Superior Politécnico José Antonio Echavarría (ISPJAE). Con 15 años de experiencia en el campo de las Telecomunicaciones.
- ✓ DrC. Caridad Anías Calderón: Profesor Titular Universitario del ISPJAE. Con 31 años de experiencia en el campo de la Gestión de Redes.
- ✓ Ing. Manuel Cheong Gómez: Administrador de Red del Ministerio de Informática y las Comunicaciones (MIC). Con 2 años de experiencia en el campo de la Informática.
- ✓ Tec. Eduar Palomo Gené: Administrador de Redes del Nodo Central de la UCI. Con 6 años de Experiencia en el campo de la Gestión de Servicios.
- ✓ Tec. Adrián Cepero Corcho: Especialista Principal de Seguridad Informática del MIC. Con 3 años en el campo de las Telecomunicaciones y Electrónica.
- ✓ Tec. Dionis Navarro Rodríguez: Especialista General de Seguridad del MIC. Con 2 años de experiencia en el campo de la Informática y las Comunicaciones.
- ✓ Ing. Daniel Tasé Guerra: Especialista Principal Departamento de Informática en la Unión Eléctrica de Cuba (UNEC) con sede en Santiago de Cuba. Con 21 años de experiencia en el área de la Electrónica y las Telecomunicaciones.

Se procedió a calcular el coeficiente de competencia de los expertos basados en la fórmula:

$$K = \frac{(Kc + Ka)}{2}$$

Figura 14: Fórmula para coeficiente de expertos.

Donde (K) es el coeficiente de competencia, (Kc) es el coeficiente de conocimiento que posee el experto respecto al tópico a consideración y (Ka) es el coeficiente de argumentación del experto obtenido a partir de la suma de los puntos alcanzados en una tabla patrón donde se exponen los elementos a tener en cuenta para el cálculo a realizar (Ver Tabla 1).

Nro.	Fuentes de Argumentación	Grado de Influencia		
		Alto	Medio	Bajo
1	Análisis teórico realizado	0.3	0.2	0.1
2	Experiencia obtenida.	0.5	0.4	0.2
3	Trabajos de autores nacionales.	0.05	0.05	0.05
4	Trabajos de autores extranjeros	0.05	0.05	0.05
5	Conocimiento del tema	0.05	0.05	0.05
6	Intuición	0.05	0.05	0.05

Tabla 1: Elementos a tener en cuenta y su peso.

Cada experto se autoevalúa marcando su nivel de competencia en los aspectos a considerar y el resultado obtenido es empleado para hallar el coeficiente de argumentación calculado. Como es posible observar a continuación (Ver Tabla 2).

Experto	Coeficiente de Competencia (K)	Coeficiente Alto	Coeficiente Medio	Coeficiente Bajo
		Si 0,8 <= K < 1,0	Si 0,5 <= K < 0,8	Si K < 0,5
1	0.85	x		
2	0.7		x	
3	0.8	x		
4	0.9	x		
5	0.9	x		
6	0.9	x		
7	0.8	x		

Tabla 2: Coeficiente de competencia calculado por experto.

Durante el proceso de selección de los expertos se tuvo como requisito que los mismos presentaran un coeficiente por encima de 0,25, valor definido como rango mínimo necesario en el proceso. Se reparó además en los factores años de experiencia y categoría científica, identificándolos como decisivos en la emisión de criterios certeros por parte de los expertos sobre la propuesta a valorar. Del cúmulo de expertos seleccionados en cuanto a categoría científica, el 28.5% es Doctor en Ciencias particularmente en el tema de Gestión de Redes, Seguridad Informática o Análisis Forense, el 0% es Máster en Ciencias, un 28.5% es Ingeniero y el restante 43.5% es de Técnicos Especializados. En cuanto a los años de experiencia se cuenta con que de la muestra de expertos escogida el 100% de ellos tiene de 2 a 31 años de experiencia en el campo, de ellos el 28.5% tiene 2 años de experiencia y el restante 71.5% tiene más

de 5 años desempeñándose en el medio, lo que supera con creces el valor mínimo suficiente establecido para este aspecto de 2 años de experiencia. Para la clara visualización de los datos anteriormente expuesto. (Ver Figura 15)

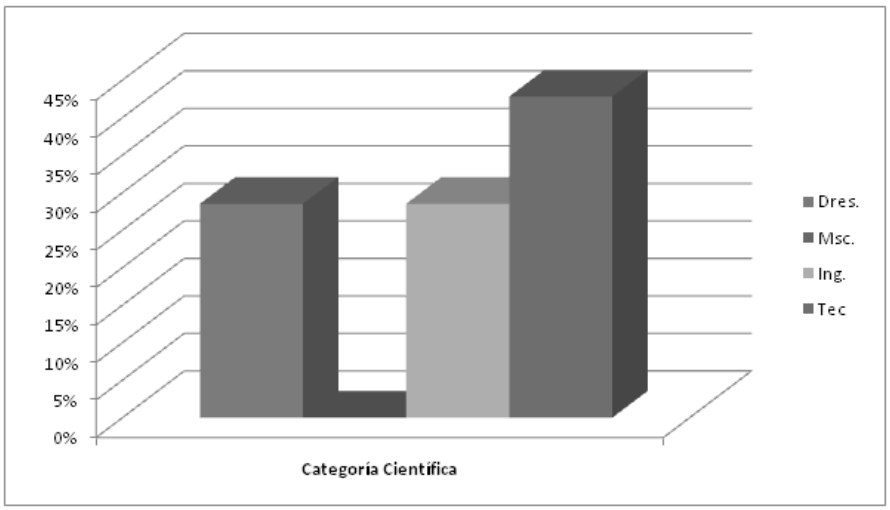


Figura 15: Balance de Expertos convocados en cuanto a criterios de selección.

3.3.2 Elaboración de un cuestionario en aras de validar la propuesta realizada.

Dada las particularidades del presente trabajo que engloba dos temas complejos y serios como el análisis forense y la gestión de redes, se hacía prácticamente imposible encontrar más de un experto capaz de dominar al nivel adecuado ambos tópicos. Por lo que se decidió crear no uno sino dos cuestionarios con un grupo de preguntas comunes y otras específicas de acuerdo al perfil dominado por el experto. Los cuestionarios elaborados constan de seis preguntas principales con varios incisos. Para el caso del cuestionario de gestión de redes la primera pregunta y sus incisos están encaminados a determinar la correcta ubicación de las herramientas tomadas a consideración en la propuesta realizada, así como en la segunda se centra en comprobar la correcta selección de las herramientas a emplear. Para el caso del cuestionario para informática forense se trata de esclarecer si la selección de herramientas fue correcta así como su nivel de impacto en el proceso de análisis forense. Las preguntas que ambos cuestionarios tienen en común se centran en determinar el correcto diseño del procedimiento propuesto, en cuanto a etapas y roles definidos en la propuesta. Las respuestas a estas preguntas se categorizan en Óptimas (C1), Funcionales (C2) y

No Funcionales (C3). El cuestionario fue enviado por correo electrónico o en formato duro a cada uno de los expertos explicando además la esencia de la propuesta a realizar con el fin de facilitar el proceso de comprensión de la misma. El cuestionario fue diseñado con el fin de permitir la retroalimentación presentando un espacio extra para recepcionar las recomendaciones y sugerencias que pudieran surgir por parte de los expertos y de las cuáles se nutrirá el proceso.

3.3.3 Análisis de los resultados obtenidos.

Para llevar a cabo el análisis de los resultados fueron puestos en práctica los métodos estadísticos indicados por el método Delphi. (Ver las frecuencias absolutas en la Tabla 3).

Nro.	Aspectos	C1	C2	C3	Total
1	Correcta ubicación de las herramientas propuestas.	7	0	0	7
2	Correcta selección de las herramientas a emplear.	6	1	0	7
3	.Correcta definición del flujo general del procedimiento.	6	1	0	7
4	Correcta definición de las etapas del procedimiento.	6	1	0	7
5	Nivel de Prioridad de las etapas.	5	2	0	7
6	Correcta definición de los roles.	6	0	1	7
Total de aspectos a validar		6			

Tabla 3: Frecuencias Absolutas

Partiendo de los resultados producto de la tabla anterior se obtiene la frecuencia acumulada, donde los datos de cada fila, con excepción de la primera, se obtienen mediante al suma del valor anterior como se muestra en la Tabla 4.

Nro.	Aspectos	C1	C2	C3
1	Correcta ubicación de las herramientas propuestas.	7	7	7
2	Correcta selección de las herramientas a emplear.	6	5	5
3	.Correcta definición del flujo general del procedimiento.	6	5	5
4	Correcta definición de las etapas del procedimiento.	6	7	7
5	Nivel de Prioridad de las etapas.	5	7	7
6	Correcta definición de los roles.	6	6	7

Tabla 4: Frecuencias Absolutas Acumuladas

Después de realizado este paso se procede a efectuar el cálculo de las frecuencias relativas acumuladas, para lo que se toman los valores de las frecuencias absolutas acumuladas y se dividen por la cantidad de expertos (Ver Figura 5).

Nro.	Aspectos	C1	C2	C3
1	Correcta ubicación de las herramientas propuestas.	0,9999	0,9999	0,9999
2	Correcta selección de las herramientas a emplear.	0,8571	0,7142	0,7142
3	.Correcta definición del flujo general del procedimiento.	0,8571	0,7142	0,7142
4	Correcta definición de las etapas del procedimiento.	0,8571	0,9999	0,9999
5	Nivel de Prioridad de las etapas.	0,7142	0,9999	0,9999
6	Correcta definición de los roles.	0,8571	0,8571	0,9999

Tabla 5: Frecuencias Relativas Acumuladas.

Usando la función (Distribución Normal. Estándar Invertida) se hallaron las imágenes de las frecuencias relativas acumuladas y se adicionan las salidas donde:

Suma: Es la sumatoria de cada fila y columna según el caso.

P: El promedio de la suma de cada fila.

N: La división de la sumatoria de las sumas de las filas por el resultado de la multiplicación del número de categorías por el número de pasos.

N-P: Es el número promedio que otorgan los expertos consultados a cada paso de la propuesta.

Punto de corte: Es el promedio de la suma de las columnas.
Estos resultados se encuentran recogidos en la Tabla 6.

						N=2,1066		
No.	**Aspectos**	**C1**	**C2**	**C3**	**Suma**	**P**	**N-P**	
1	Correcta ubicación de las herramientas propuestas.	3,7190	3,7190	3,7190	11,1570	3,719	-1,6123	Óptimas
2	Correcta selección de las herramientas a emplear.	1,0675	0,5659	0,5659	2,1994	0,733	1,3734	Óptimas
3	Correcta definición del flujo general del procedimiento.	1,0675	0,5659	0,5659	2,1994	0,733	1,3734	Óptimas
4	Correcta definición de las etapas del procedimiento.	1,0675	3,7190	3,7190	8,5056	2,835	-0,7285	Óptimas
5	Nivel de Prioridad de las etapas.	0,5659	3,7190	3,7190	8,0039	2,668	-0,5613	Óptimas
6	Correcta definición de los roles.	1,0675	1,0675	3,7190	5,8541	1,951	0,1552	Óptimas
Suma		8,5552	13,3565	16,0079	37,9197			
Puntos de Corte		1,4258	2,2260	2,6679				

Tabla 6: Puntos de Corte

Los puntos de corte tributan significativamente al hallazgo del grado de adecuación de cada paso del procedimiento según la opinión brindada por los expertos consultados. Por otra parte para realizar el cálculo del grado de adecuación de los aspectos a validar se realiza como plasma la Tabla 7.

Óptimas	Funcionales	No Funcionales
N-P =<1,4258	**< N-P =<**2,2260	**<N-P =<**2,6679

Tabla 7: Grado de Adecuación de los aspectos a validar.

Mediante este análisis es posible observar que los expertos consideraron óptimos todos los aspectos a validar en el procedimiento, lo que evidencia la utilidad del mismo dada la muestra y escenario definido en la problemática planteada. A partir del cúmulo de datos obtenido a lo largo de los cálculos realizados es posible calcular el coeficiente de Kendall (W) que decide el nivel de concordancia entre los expertos. Los valores que puede tomar oscilan entre 0 y 1 y se calcula por la fórmula mostrada en la siguiente figura:

$$W = \frac{12s}{k^2(N^3 - N)}$$

Figura 16 : Fórmula para el cálculo del coeficiente de Kendall.

Para facilitar el proceso se elabora una tabla de aspectos (ver Tabla) donde se introducen los siguientes elementos:

RJ: Valor numérico otorgado a través del criterio del experto a cada aspecto a evaluar.

Valor medio de RJ: Sumatoria de los RJ dividida por N.

N: Total de aspectos a evaluar (cantidad de preguntas realizadas: 6).

Desviación media: Diferencia entre RJ y la media.

S: Suma de los cuadrados de las desviaciones medias.

K: Número total de expertos.

	E1	E2	E3	E4	E5	E6	E7	RJ
Pregunta 1	5	4	5	4	4	5	4	22
Pregunta 2	4	4	4	4	3	4	4	19
Pregunta 3	4	4	4	3	4	4	4	19
Pregunta 4	4	4	4	4	3	5	4	19
Pregunta 5	5	5	4	3	3	4	4	20
Pregunta 6	5	4	4	4	2	4	4	19

Tabla 8: Aspectos a evaluar contra expertos.

Ya conociendo el coeficiente de Kendall (**W = 0,2993**), es posible calcular el Chi cuadrado real (X2) que muestra la existencia de concordancia o no entre los expertos, el mismo se obtiene a través de la fórmula: $X^2 = K\ (N-1)\ W$ Siendo el valor calculado de Chi cuadrado real X^2real=0,39047619. Este valor se compara con el valor de la tabla de Distribución Chi cuadrado Inversa (Anexo 2 Tabla 10) $X^2(\alpha;\ N-1)$. Si $X^2real<X^2(\alpha;\ N-1)$ existe concordancia entre los expertos. $X^2(0.05;\ 5)$. Siendo **α** el valor del coeficiente de error en la evaluación de los expertos (Ver Anexo 2 Tabla 9) y siendo **N** = 6, Datos que son empleados para obtener el valor $X^2(\alpha;\ N-1)$ en la tabla de Distribución Chi cuadrado Inversa. Teniendo $X^2(\alpha;\ N-1) = 2,167$ lo que evidencia la existencia de concordancia entre los expertos.

3.3.3 Aplicación práctica del procedimiento tomando como muestra el proyecto Centro de Datos del salón de exposiciones de la UCI.

3.4.1 Pruebas realizadas a Snort

Snort está configurado y corriendo sobre una PC Dual Core virtualizada con 1 GB de memoria RAM sobre la plataforma Ubuntu versión 11.10 con la interfaz de red en modo promiscuo, responde ante las peticiones ping, mensajes ICMP no autorizados enviando alertas, también funciona como registrador de paquetes (packet logger).

Caso de prueba #1
Descripción: Prueba la funcionalidad de Snort como IDS
Condiciones de ejecución: La llegada de uno o más paquetes al escenario definido. Snort debe tener configuradas un conjunto de reglas determinadas por las políticas del CPD. Snort debe tener correctamente definidas las configuraciones para el almacenamiento y generación de logs.
Entrada/Pasos de ejecución: Paquete entrante. Snort analiza el paquete entrante, extrae todos los datos del mismo, busca en el archivo de configuración (/etc/snort/snort.conf) donde se encuentran las reglas definidas, así como donde se definió el almacenamiento de los logs y el formato de los mismos. Compara la información obtenida del paquete con lo establecido por las reglas, de encontrar alguna anomalía envía una alarma. Construye un archivo log con los datos recopilados del paquete.
Resultado esperado: Snort envía una alerta y genera un log.
Explicación del Resultado: (Ver Anexo 4 Figura 1 y 2)
Evaluación de la prueba: Prueba Satisfactoria.

Tabla 9: Pruebas realizadas a Snort

3.4.2 Pruebas realizadas a Nagios

Nagios como herramienta fue sometida a varias pruebas de rutina con los activos del CPD, el mismo arroja variada información sobre el estado de los recursos existentes en el escenario definido. Por sus características se eligió ejecutarlo en modo de demonio, así como representa un factor de peso en el control de los activos del CPD.

Caso de prueba #2
Descripción: Prueba de monitorización de activos del CPD con Nagios
Condiciones de ejecución: Nagios debe estar instalado en al menos un nodo del escenario de red. Nagios debe tener configurado el escenario de red a monitorizar, el formato de notificación al usuario, y los parámetros para generación de logs.
Entrada/Pasos de ejecución: No posee entradas Nagios se comunica con los nodos presentes en el escenario de red y recopila información referente a si están caídos y demás.
Resultado esperado: Nagios elabora un reporte del escenario de red monitorizado y sus activos.
Explicación del Resultado:(Ver Anexo 4 Figuras 3 y 4)
Evaluación de la prueba: Prueba Satisfactoria

3.4.3 Pruebas realizadas a Ntop

Caso de prueba #3
Descripción: Prueba de análisis y detección de anomalías con el escenario de red.
Condiciones de ejecución: Ntop precisa estar correctamente configurado, bien definido por las políticas de seguridad los patrones correctos en el tráfico de red habitual del escenario.
Entrada/Pasos de ejecución: No posee entradas. Ntop recopila los datos del comportamiento de la red y elabora reportes gráficos que ofrecen mayor claridad en el proceso.
Resultado esperado: Ntop elabora un reporte gráfico sobre los patrones del uso de la red.
Explicación del Resultado: Ver Anexo 4 Figura 5
Evaluación de la prueba: Prueba Satisfactoria

3.5 Conclusiones parciales

En este capítulo se realizó un análisis minucioso con el fin de validar el procedimiento propuesto, para ello se emplearon métodos teóricos (método Delphi) y prácticos como la presentación de pruebas de distintos componentes del procedimiento desplegados en un escenario controlado.

Conclusiones

- ✓ Se realizó un estudio de las principales herramientas existentes que tributan a la propuesta de procedimiento, lo que permitió escoger las más idóneas para la muestra definida.
- ✓ Se definieron un conjunto de etapas, herramientas, actividades, artefactos y roles como parte de la propuesta de procedimiento realizada donde se da cumplimiento a los objetivos específicos.
- ✓ Se elaboró y aplicó un cuestionario a un conjunto de expertos para la validación de la propuesta que tributaron al correcto empleo de herramientas y técnicas, y por ende, al diseño acertado del procedimiento en cuestión.
- ✓ Fue realizado un conjunto de casos de pruebas a las herramientas seleccionadas dentro de la muestra seleccionada que demostraron el funcionamiento adecuado del procedimiento propuesto.

Referencias Bibliográficas

1. **Definicion De.** Definicion.de. *Procedimiento.* [En línea] 2008. [Citado el: 5 de noviembre de 2011.] http://definicion.de/procedimiento/.
2. **Definición ABC.** Procedimiento. *Definición ABC.* [En línea] 2008. [Citado el: 6 de noviembre de 2011.] http://www.definicionabc.com/general/procedimiento.php.
3. **Alegsa.** Servidor de log. *Alegsa.* [En línea] 2009. [Citado el: 10 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/log%20de%20servidor.php.
4. **Mastermagazine.** Mastermagazine. *Mastermagazine.* [En línea] 2004. [Citado el: 6 de noviembre de 2011.] http://www.mastermagazine.info/termino/6638.php.
5. **University of Nevada Las Vegas. OIT.** Office of Information Technology. *Definition of Information Security.* [En línea] 2012. [Citado el: 19 de junio de 2012.] http://oit.unlv.edu/network-and-security/definition-information-security.
6. **Alegsa.** Seguridad Lógica. *Alegsa.* [En línea] 2009. [Citado el: 11 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/seguridad%20logica.php.
7. —. Seguridad Física. *Alegsa.* [En línea] 2009. [Citado el: 11 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/seguridad%20fisica.php.
8. —. Ataque Informático. *Alegsa.* [En línea] 2009. [Citado el: 11 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/ataque%20informatico.php.
9. **DelitosInformaticos.com.** Delitos Informaticos. *Seguridad:Clasificación y tipos de ataques contra sistemas de información.* [En línea] DelitosInformaticos.com, 25 de marzo de 2001. [Citado el: 4 de noviembre de 2011.] http://delitosinformaticos.com/seguridad/clasificacion.shtml.
10. **Casey, Eogham.** *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* s.l. : Academic, 2000. pág. 279.
11. Informática Forense. *Informática Forense.* [En línea] Blogspot, 26 de junio de 2009. [Citado el: 16 de junio de 2012.] http://forense-infor.blogspot.com/2009/06/informatica-forense.html.
12. **Pérez Arevalo, Arturo.** *Administración de centros de cómputo.* FACULTAD DE CONTADURÍA Y CIENCIAS ADMINISTRATIVAS , UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO. Michoacán : UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO, 2010.
13. **RSyslog.** The enhanced syslog for Linux and Unix rsyslog. *The enhanced syslog for Linux and Unix rsyslog.* [En línea] http://www.rsyslog.com/.
14. **bit4id.** SMartLog: Recogida, Filtrado, Custodia y Firma de Logs. *bit4id.* [En línea] 2010. www.bit4id.com.
15. **Pérez Conde, Carlos.** *Seguridad en Sistemas. LAboratorio:OSSEC.* Seguridad en Sistemas Informáticos, Universidad de Valencia. Valencia : s.n., 2008.
16. **Ali, Shakeel y Tedi, Heriyanto.** *BackTrack 4: Assuring Security by Penetration Testing.* BIRMINGHAM - MUMBAI : Packt Publishing, 2011. pág. 392. ISBN 978-1-849513-94-4.
17. **Carrier, Brian.** Sleuth Kit. *Sleuth Kit.* [En línea] 2012. [Citado el: 4 de mayo de 2012.] http://www.sleuthkit.org/.
18. **Guidance Software, Inc.** Guidance Software | EnCase. *Guidance Software | EnCase.* [En línea] 2012. [Citado el: 25 de mayo de 2012.] http://www.guidancesoftware.com/encase-forensic.htm.

19. **Andreasson, Oskar.** Iptables. *Iptables.* [En línea] 2008. [Citado el: 5 de junio de 2012.] http://www.iptables.info/.
20. **BSD Perimeter LLC .** PfSense. *PfSense.* [En línea] BSD Perimeter LLC , 2011. [Citado el: 21 de febrero de 2012.] http://www.pfSense.org/.
21. **WindowsITPro.** WindowsITPro. *pfSense.* [En línea] Penton Media, Inc, 11 de septiembre de 2008. [Citado el: 20 de junio de 2012.] http://www.windowsitpro.com/article/firewall3/pfSense.
22. **Saletan, Paul.** Surveypoint. *pfSense: A Router That Stands Up To Traffic.* [En línea] Creative Commons Attribution 3.0 License, 2010. [Citado el: 20 de junio de 2012.] http://tech.surveypoint.com/pfSense-a-router-that-stands-up-to-traffic.html.
23. Nagios. [En línea] [Citado el: 3 de junio de 2012.] http://www.nagios.org/.
24. Hobit Sourceforge. [En línea] [Citado el: 3 de junio de 2012.] Hobbit: http://hobbitmon.sourceforge.net.
25. Monit. [En línea] [Citado el: 4 de junio de 2012.] http://www.tildeslash.com/monit/.
26. **Ntop.** Ntop. *Ntop.* [En línea] 2012. [Citado el: 5 de junio de 2012.] http://www.ntop.org/products/ntop/.
27. **PDCA.** IDEF. *PDCA.* [En línea] PDCA, junio de 2008. [Citado el: 6 de mayo de 2012.] http://www.pdca.es/pruebas/idef.html.
28. **IDEF.** IDEF Family of Methods a Structure Approach to Enterprise Modeling and Analysis. *IDEF.* [En línea] junio de 2008. [Citado el: 6 de mayo de 2012.] http://www.idef.com.
29. **AQA.** Resumen Metodología IDEF0. *AQA.* [En línea] 2008. [Citado el: 6 de mayo de 2012.] http://www.aqa.es/doc/MetodologiaIDEF/Resumen.pdf.
30. **Landeta, Jon.** *Aplicación del Método Delphi en la elaboración de la tabla simétrica de las tablas input-output.* Instituto de Economía Aplicada a la Empresa, Universidad del País Vasco. Catalunya : s.n., 2003.
31. **Fernández, A y Rubén, R.** *Modelo Informático para la autogestión del aprendizaje para la universalización de la enseñanza.* Granada : s.n., 2005.
32. **Álvarez Martínez de Santelices, Carlos.** *Experimentos virtuales para la enseñanza del Electromagnetismo.* Universidad de Camagüey. Camagüey : s.n., 2004.
33. **Quintana Aput, Rolando.** *Propuesta de indicadores para medir competencias del personal según el rol en proyectos multimedia. Universidad de las Ciencias Informáticas.* La Habana : s.n., 2007.
34. **Hernández Aguilar, Violena.** *Protofase a la ingeniería de requisitos para facilitar la comprensión del negocio a informatizar en el desarrollo de software de gestión.* Universidad de las Ciencias Informáticas. La Habana : s.n., 2009.
35. **Marante Valdivia, Marbys.** *Proceso para planear la cartera de servicios en la adopción de una iniciativa SOA.* Universidad de las Ciencias Informáticas. Ciudad de la Habana : s.n., 2010.
36. **Durand, R.** *El método delphi y la perspectiva del hidrógeno.* España : s.n., 1971.
37. **Zatsiorski, M.** *Metrología deportiva.* Moscú, URSS : Planeta, 1989.
38. *Sintonizar Hobit, Nagios y Monit.* **Kemp, Juliet.** 41, Linux-Magazine, págs. 20-23.
39. **Ambrosi, Alain, Peugeot, Valérie y Pimienta, Daniel.** *Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información.* s.l. : C & F Éditions., 2005.
40. **Neira Ayuso, Pablo.** Netfilter. *Netfilter.* [En línea] 2010. [Citado el: 7 de junio de 2012.] http://www.netfilter.org/.
41. **Paterva.** Maltego. *Maltego.* [En línea] [Citado el: 7 de junio de 2012.] http://www.paterva.com/web5/client/overview.php.

42. **Colunga, Silvia y Amayuela, Georgina.** *La Psicología Educativa, su objeto, métodos y problemas principales.* Camagüey : Universidad de Camagüey, 2003.
43. **Kaspersky Lab ZAO .** Kaspersky Lab. *Kaspersky Lab.* [En línea] Kaspersky Lab ZAO , 2012. [Citado el: 12 de marzo de 2012.] http://www.kaspersky.com/about.
44. *Dactiloscopia: Análisis Forense con BackTrack y Sleuth Kit.* **SEIFRIED, KURT.** 42, Linux-Magazine, págs. 20-25.
45. **Sourcefire.** ClamAv. [En línea] 2009. [Citado el: 7 de junio de 2012.] http://www.clamav.net/lang/en/.
46. Big Brother. [En línea] [Citado el: 5 de junio de 2012.] http://www.bb4.org/.
47. **Ercole, Santiago y Usseglio, Maximiliano.** Ataques y Vulnerabilidades. *Slideshare.* [En línea] 2012. [Citado el: 20 de noviembre de 2011.] http://www.slideshare.net/lamugre/ataques-y-vulnerabilidades.

Bibliografía

1. **Definicion De.** Definicion.de. *Procedimiento.* [En línea] 2008. [Citado el: 5 de noviembre de 2011.] http://definicion.de/procedimiento/.
2. **Definición ABC.** Procedimiento. *Definición ABC.* [En línea] 2008. [Citado el: 6 de noviembre de 2011.] http://www.definicionabc.com/general/procedimiento.php.
3. **Alegsa.** Servidor de log. *Alegsa.* [En línea] 2009. [Citado el: 10 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/log%20de%20servidor.php.
4. **Mastermagazine.** Mastermagazine. *Mastermagazine.* [En línea] 2004. [Citado el: 6 de noviembre de 2011.] http://www.mastermagazine.info/termino/6638.php.
5. **University of Nevada Las Vegas. OIT.** Office of Information Technology. *Definition of Information Security.* [En línea] 2012. [Citado el: 19 de junio de 2012.] http://oit.unlv.edu/network-and-security/definition-information-security.
6. **Alegsa.** Seguridad Lógica. *Alegsa.* [En línea] 2009. [Citado el: 11 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/seguridad%20logica.php.
7. —. Seguridad Física. *Alegsa.* [En línea] 2009. [Citado el: 11 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/seguridad%20fisica.php.
8. —. Ataque Informático. *Alegsa.* [En línea] 2009. [Citado el: 11 de noviembre de 2011.] http://www.alegsa.com.ar/Dic/ataque%20informatico.php.
9. **DelitosInformaticos.com.** Delitos Informaticos. *Seguridad:Clasificación y tipos de ataques contra sistemas de información.* [En línea] DelitosInformaticos.com, 25 de marzo de 2001. [Citado el: 4 de noviembre de 2011.] http://delitosinformaticos.com/seguridad/clasificacion.shtml.
10. **Casey, Eogham.** *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* s.l. : Academic, 2000. pág. 279.
11. Informática Forense. *Informática Forense.* [En línea] Blogspot, 26 de junio de 2009. [Citado el: 16 de junio de 2012.] http://forense-infor.blogspot.com/2009/06/informatica-forense.html.
12. **Pérez Arevalo, Arturo.** *Administración de centros de cómputo.* FACULTAD DE CONTADURÍA Y CIENCIAS ADMINISTRATIVAS , UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO. Michoacán : UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO, 2010.
13. **RSyslog.** The enhanced syslog for Linux and Unix rsyslog. *The enhanced syslog for Linux and Unix rsyslog.* [En línea] http://www.rsyslog.com/.
14. **bit4id.** SMartLog: Recogida, Filtrado, Custodia y Firma de Logs. *bit4id.* [En línea] 2010. www.bit4id.com.
15. **Pérez Conde, Carlos.** *Seguridad en Sistemas. LAboratorio:OSSEC.* Seguridad en Sistemas Informáticos, Universidad de Valencia. Valencia : s.n., 2008.
16. **Ali, Shakeel y Tedi, Heriyanto.** *BackTrack 4: Assuring Security by Penetration Testing.* BIRMINGHAM - MUMBAI : Packt Publishing, 2011. pág. 392. ISBN 978-1-849513-94-4.
17. **Carrier, Brian.** Sleuth Kit. *Sleuth Kit.* [En línea] 2012. [Citado el: 4 de mayo de 2012.] http://www.sleuthkit.org/.
18. **Guidance Software, Inc.** Guidance Software | EnCase. *Guidance Software | EnCase.* [En línea] 2012. [Citado el: 25 de mayo de 2012.] http://www.guidancesoftware.com/encase-forensic.htm.

19. **Andreasson, Oskar.** Iptables. *Iptables.* [En línea] 2008. [Citado el: 5 de junio de 2012.] http://www.iptables.info/.
20. **BSD Perimeter LLC .** PfSense. *PfSense.* [En línea] BSD Perimeter LLC , 2011. [Citado el: 21 de febrero de 2012.] http://www.pfSense.org/.
21. **WindowsITPro.** WindowsITPro. *pfSense.* [En línea] Penton Media, Inc, 11 de septiembre de 2008. [Citado el: 20 de junio de 2012.] http://www.windowsitpro.com/article/firewall3/pfSense.
22. **Saletan, Paul.** Surveypoint. *pfSense: A Router That Stands Up To Traffic.* [En línea] Creative Commons Attribution 3.0 License, 2010. [Citado el: 20 de junio de 2012.] http://tech.surveypoint.com/pfSense-a-router-that-stands-up-to-traffic.html.
23. Nagios. [En línea] [Citado el: 3 de junio de 2012.] http://www.nagios.org/.
24. Hobit Sourceforge. [En línea] [Citado el: 3 de junio de 2012.] Hobbit: http://hobbitmon.sourceforge.net.
25. Monit. [En línea] [Citado el: 4 de junio de 2012.] http://www.tildeslash.com/monit/.
26. **Ntop.** Ntop. *Ntop.* [En línea] 2012. [Citado el: 5 de junio de 2012.] http://www.ntop.org/products/ntop/.
27. **PDCA.** IDEF. *PDCA.* [En línea] PDCA, junio de 2008. [Citado el: 6 de mayo de 2012.] http://www.pdca.es/pruebas/idef.html.
28. **IDEF.** IDEF Family of Methods a Structure Approach to Enterprise Modeling and Analysis. *IDEF.* [En línea] junio de 2008. [Citado el: 6 de mayo de 2012.] http://www.idef.com.
29. **AQA.** Resumen Metodología IDEF0. *AQA.* [En línea] 2008. [Citado el: 6 de mayo de 2012.] http://www.aqa.es/doc/MetodologiaIDEF/Resumen.pdf.
30. **Landeta, Jon.** *Aplicación del Método Delphi en la elaboración de la tabla simétrica de las tablas input-output.* Instituto de Economía Aplicada a la Empresa, Universidad del País Vasco. Catalunya : s.n., 2003.
31. **Fernández, A y Rubén, R.** *Modelo Informático para la autogestión del aprendizaje para la universalización de la enseñanza.* Granada : s.n., 2005.
32. **Álvarez Martínez de Santelices, Carlos.** *Experimentos virtuales para la enseñanza del Electromagnetismo.* Universidad de Camagüey. Camagüey : s.n., 2004.
33. **Quintana Aput, Rolando.** *Propuesta de indicadores para medir competencias del personal según el rol en proyectos multimedia. Universidad de las Ciencias Informáticas.* La Habana : s.n., 2007.
34. **Hernández Aguilar, Violena.** *Protofase a la ingeniería de requisitos para facilitar la comprensión del negocio a informatizar en el desarrollo de software de gestión.* Universidad de las Ciencias Informáticas. La Habana : s.n., 2009.
35. **Marante Valdivia, Marbys.** *Proceso para planear la cartera de servicios en la adopción de una iniciativa SOA.* Universidad de las Ciencias Informáticas. Ciudad de la Habana : s.n., 2010.
36. **Durand, R.** *El método delphi y la perspectiva del hidrógeno.* España : s.n., 1971.
37. **Zatsiorski, M.** *Metrología deportiva.* Moscú, URSS : Planeta, 1989.
38. *Sintonizar Hobit, Nagios y Monit.* **Kemp, Juliet.** 41, Linux-Magazine, págs. 20-23.
39. **Ambrosi, Alain, Peugeot, Valérie y Pimienta, Daniel.** *Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información.* s.l. : C & F Éditions., 2005.
40. **Neira Ayuso, Pablo.** Netfilter. *Netfilter.* [En línea] 2010. [Citado el: 7 de junio de 2012.] http://www.netfilter.org/.
41. **Paterva.** Maltego. *Maltego.* [En línea] [Citado el: 7 de junio de 2012.] http://www.paterva.com/web5/client/overview.php.

42. **Colunga, Silvia y Amayuela, Georgina.** *La Psicología Educativa, su objeto, métodos y problemas principales.* Camagüey : Universidad de Camagüey, 2003.
43. **Kaspersky Lab ZAO .** Kaspersky Lab. *Kaspersky Lab.* [En línea] Kaspersky Lab ZAO , 2012. [Citado el: 12 de marzo de 2012.] http://www.kaspersky.com/about.
44. *Dactiloscopia: Análisis Forense con BackTrack y Sleuth Kit.* **SEIFRIED, KURT.** 42, Linux-Magazine, págs. 20-25.
45. **Sourcefire.** ClamAv. [En línea] 2009. [Citado el: 7 de junio de 2012.] http://www.clamav.net/lang/en/.
46. Big Brother. [En línea] [Citado el: 5 de junio de 2012.] http://www.bb4.org/.
47. **Ercole, Santiago y Usseglio, Maximiliano.** Ataques y Vulnerabilidades. *Slideshare.* [En línea] 2012. [Citado el: 20 de noviembre de 2011.] http://www.slideshare.net/lamugre/ataques-y-vulnerabilidades.

Recomendaciones

- ✓ La implementación de un autómata u otra técnica de Inteligencia Artificial (preferentemente un sistema experto basado en casos) que permita automatizar la etapa de Retroalimentación.
- ✓ La implantación y puesta en práctica del presente procedimiento en el CPD del proyecto Centro de Datos del centro TLM, así como en los CPD existentes en el país.